Turnitin Student

SKRIPSI FINAL_Muhammad Fadhil Putra_After Sidang

Vision #4

Document Details

Submission ID
trn:oid:::7690:126842042

Submission Date
Jan 25, 2026, 12:41 PM GMT+7

Download Date
Jan 25, 2026, 12:47 PM GMT+7

File Name
SKRIPSI FINAL_Muhammad Fadhil Putra_After Sidang.pdf

File Size
2.1 MB

67 Pages

11,128 Words

77,665 Characters

22% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Top Sources

19% Internet sources
7% Publications
16% Submitted works (Student Papers)

Top Sources

19% Internet sources
7% Publications
16% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
eprints.untirta.ac.id		3%
2	Internet	
repository.ar-raniry.ac.id		2%
3	Internet	
journal.aptii.or.id		<1%
4	Internet	
sads.instiki.ac.id		<1%
5	Student papers	
Binus University International on 2025-11-22		<1%
6	Publication	
Nurasmawati Nurasmawati, Mansur Mansur, Nurmi Hidayasari. "Analisis Kerenta...		<1%
7	Internet	
id.scribd.com		<1%
8	Internet	
garuda.kemdikbud.go.id		<1%
9	Internet	
eprints.iainu-kebumen.ac.id		<1%
10	Student papers	
Universitas Sultan Ageng Tirtayasa on 2025-07-16		<1%
11	Internet	
amartakarya.co.id		<1%

12 Internet
repository.upi.edu <1%

13 Student papers
Universitas Pancasila on 2025-08-22 <1%

14 Internet
docplayer.info <1%

15 Internet
jurnal.polibatam.ac.id <1%

16 Internet
repository.upnvj.ac.id <1%

17 Internet
dspace.uii.ac.id <1%

18 Student papers
Universitas PGRI Madiun on 2025-10-21 <1%

19 Student papers
Universitas Malikussaleh on 2026-01-20 <1%

20 Internet
ejurnal.swadharma.ac.id <1%

21 Internet
ojs.unikom.ac.id <1%

22 Internet
repository.uin-suska.ac.id <1%

23 Internet
fr.wikipedia.org <1%

24 Internet
repository.teknokrat.ac.id <1%

25 Publication
Syahrul Dwi Hilda, Nono Heryana, Azhari Ali Ridha. "WEBSITE SECURITY ANALYSIS... <1%

26 Internet
j-innovative.org <1%

27 Internet
repository.bakrie.ac.id <1%

28 Internet
www.researchgate.net <1%

29 Internet
journal.smartpublisher.id <1%

30 Internet
jurnal.itg.ac.id <1%

31 Student papers
polteksn on 2025-08-19 <1%

32 Publication
Dawam Agung Pribadi, Wiwin Winarti. "EVALUASI KEAMANAN SISTEM INFORMASI... <1%

33 Student papers
Universitas Pancasila on 2025-08-07 <1%

34 Internet
mafiadoc.com <1%

35 Internet
repo.undiksha.ac.id <1%

36 Internet
repositori.usu.ac.id <1%

37 Internet
repository.nurulfikri.ac.id <1%

38 Publication
Bagus Setya Putra, Dwi Budi Santoso. "Analisis Keamanan Website Berbasis Word... <1%

39 Publication
Muhammad Sani, Muhammad Asep Subandri. "Analisis Kerentanan Website Desa... <1%

40 Student papers
Universitas Maritim Raja Ali Haji on 2025-01-12 <1%

41 Internet
www.scribd.com <1%

42 Student papers
UNIVERSITAS BUDI LUHUR on 2025-07-24 <1%

43 Internet
id.123dok.com <1%

44 Student papers
Universitas Pancasila on 2025-08-04 <1%

45 Student papers
Universitas Putera Batam on 2020-11-30 <1%

46 Internet
bekascatatan.blogspot.com <1%

47 Internet
ojs.ninetyjournal.com <1%

48 Publication
Suci Rahayu. ""Mas-mas Jawa Supremacy": Identitas Pria Jawa sebagai Kriteria Pa... <1%

49 Student papers
Universitas Brawijaya on 2023-07-24 <1%

50 Internet
ejurnal.seminar-id.com <1%

51 Internet
repository.iainpare.ac.id <1%

52 Internet
123dok.com <1%

53 Student papers
Telkom University on 2025-06-30 <1%

54 Internet
repository.uksw.edu <1%

55 Internet
repository.unpar.ac.id <1%

56 Internet
smart.stmikplk.ac.id <1%

57 Student papers
Syiah Kuala University on 2019-09-18 <1%

58 Student papers
Universitas Muhammadiyah Surakarta on 2015-03-19 <1%

59 Student papers
Universitas Pendidikan Indonesia on 2025-01-19 <1%

60 Internet
geograf.id <1%

61 Internet
journal.unilak.ac.id <1%

62 Internet
repository.undhirabali.ac.id <1%

63 Internet
www.coursehero.com <1%

64 Internet
www.slideshare.net <1%

65 Student papers
Academic Library Consortium on 2025-01-09 <1%

66 Student papers
American Intercontinental University Online on 2013-05-25 <1%

67 Student papers
Universitas Muhammadiyah Surakarta on 2015-04-07 <1%

68	Internet	
ejournal.unma.ac.id		<1%
69	Internet	
es.scribd.com		<1%
70	Internet	
jalantikus.com		<1%
71	Internet	
pdfs.semanticscholar.org		<1%
72	Internet	
repo.iain-tulungagung.ac.id		<1%
73	Internet	
repository.atmaluhur.ac.id		<1%
74	Internet	
support.google.com		<1%
75	Student papers	
Perpustakaan on 2025-08-06		<1%
76	Student papers	
UIN Syarif Hidayatullah Jakarta on 2025-08-01		<1%
77	Student papers	
Universitas Islam Riau on 2025-07-17		<1%
78	Student papers	
Universitas Islam Riau on 2025-11-24		<1%
79	Student papers	
Universitas Respati Indonesia on 2020-09-28		<1%
80	Student papers	
Universitas Respati Indonesia on 2025-08-27		<1%
81	Internet	
adoc.pub		<1%

82 Student papers
iGroup on 2019-01-28 <1%

83 Internet
journal.polbitrada.ac.id <1%

84 Internet
kumparan.com <1%

85 Student papers
polteksSn on 2025-08-19 <1%

86 Internet
repository.unhas.ac.id <1%

87 Internet
repository.upnjatim.ac.id <1%

88 Internet
www.logique.co.id <1%

89 Publication
Sabariman Sabariman, Haeruddin Haeruddin, Deven Lee. "ANALISIS KERENTANA... <1%

90 Publication
Susetyo Susetyo, Noermanzah Noermanzah. "Kemampuan dan Kesulitan Mahasi... <1%

91 Student papers
UPN Veteran Yogyakarta on 2026-01-13 <1%

92 Student papers
Universitas Muria Kudus on 2017-09-20 <1%

93 Student papers
Universitas Pendidikan Ganesha on 2025-08-04 <1%

94 Internet
eemisas.aknpacitan.ac.id <1%

95 Internet
ejournal.warunayama.org <1%

96 Internet
etheses.uin-malang.ac.id <1%

97 Internet
file.upi.edu <1%

98 Internet
journal.universitasmulia.ac.id <1%

99 Internet
laptopi.net <1%

100 Internet
meet-hello.btp.ac.id <1%

101 Internet
ojs.ipem.ecampus.id <1%

102 Internet
repository.isi-ska.ac.id <1%

103 Internet
repository.uma.ac.id <1%

104 Internet
www.jpti.journals.id <1%

105 Student papers
Universitas Andalas on 2024-03-15 <1%

106 Student papers
Universitas Tarumanagara on 2025-12-23 <1%

107 Student papers
Galatasaray University on 2025-06-24 <1%

108 Student papers
IAIN Pekalongan on 2023-12-17 <1%

109 Student papers
Universitas Muhammadiyah Purwokerto on 2025-12-11 <1%

110 Student papers

Universitas Respati Indonesia on 2020-09-16 <1%

111 Student papers

Universitas Respati Indonesia on 2025-08-25 <1%

112 Student papers

Universitas Tarumanagara on 2025-12-17 <1%

113 Student papers

iGroup on 2012-11-26 <1%

ANALISIS KERENTANAN DAN MITIGASI KEAMANAN WEB MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* (STUDI KASUS: SPADA Universitas Sultan Ageng Tirtayasa)

SKRIPSI

Sebagai salah satu syarat memperoleh gelar Sarjana Komputer (S.Kom)

Muhammad Fadhil Putra

NIM : 3337210065

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS SULTAN AGENG TIRTAYASA

2026

LEMBAR PERNYATAAN MENGENAI SKRIPSI

Dengan ini saya menyatakan bahwa skripsi saya berjudul Analisis Kerentanan dan Mitigasi Keamanan Web Menggunakan Metode *Vulnerability Assessment* (Studi kasus: SPADA Universitas Sultan Ageng Tirtayasa) adalah benar karya saya dengan arahan para pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip yang diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Dengan ini saya melimpahkan karya tulis saya kepada Universitas Sultan Ageng Tirtayasa

Cilegon, Januari 2026

Muhammad Fadhil Putra

3337210065

LEMBAR PENGESAHAN

Judul Skripsi : Analisis Kerentanan dan Mitigasi Keamanan Web Menggunakan Metode *Vulnerability Assessment* (Studi Kasus: SPADA Universitas Sultan Ageng Tirtayasa)

Nama : Muhammad Fadhil Putra

NIM : 3337210065

Disetujui oleh

Pembimbing,

Dr.-Ing. Muhammad Iman Santoso, S.T.,M.Sc.	Fitri Damyati S.Kom., M.M
NIP. 19770130200312100 7	NIP. 197310312005011001

Mengetahui,

Dekan Fakultas Teknik	Ketua Program Studi Informatika
Prof. Dr. Jayanudin, S.T., M.Eng.	Nanang Krisdianto, S.T., M.Kom.
NIP. 197808112005011003	NIP. 197504092006041004

PRAKATA

Puji dan syukur penulis panjatkan kepada Allah SWT Yang Maha Esa, karena atas penyertaan-Nya penulis dapat menyelesaikan skripsi ini yang berjudul "Analisis Kerentanan dan Mitigasi Keamanan Web Menggunakan Metode *Vulnerability Assessment* (Studi Kasus: SPADA Universitas Sultan Ageng Tirtayasa)". Penulisan skripsi ini dibuat dalam rangka memenuhi syarat untuk mencapai gelar Sarjana Komputer (S.Kom) pada Universitas Sultan Ageng Tirtayasa.

Setelah menyelesaikan studi dan juga skripsi ini, penulis menyadari bahwa semua yang telah penulis lakukan ini tidak dapat tercapai jika bukan karena bantuan dari banyak pihak, oleh karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya atas berbagai bantuan dan dukungan kepada pihak yang telah membantu penulis dalam menyelesaikan skripsi ini, terkhusus kepada:

1. Bapak Prof. Dr. Ir. Fatah Sulaiman, ST., MT., selaku Rektor Universitas Sultan Ageng Tirtayasa.
2. Bapak Prof. Dr. Jayanudin, S.T., M.Eng., selaku Dekan Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
3. Nanang Krisdianto, S.T., M.Kom., selaku Ketua Program Studi Informatika, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
4. Bapak Royan Habibie Sukarna, S.Kom., M.Kom., selaku Sekretaris Program Studi Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
5. Bapak Dr.-Ing. Muhammad Iman Santoso, S.T., M.Sc. dan Fitri Damyati S.Kom., M.M. selaku pembimbing I dan II yang telah meluangkan waktu dan memberikan bimbingan berharga kepada penulis selama proses penyusunan Tugas Akhir ini.
6. Seluruh dosen dan staf administrasi program studi Informatika, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa, yang telah memberi penulis ilmu, bantuan, dan pelayanan akademik selama penulis menempuh proses perkuliahan
7. Kedua orang tua penulis, Bapak H. Andi Pratama Putra, S.H. & Alm. Hj. Meriza Yudiana S.Sos, yang selalu menjadi sumber kekuatan serta doa yang

tiada henti, penulis menyampaikan rasa terima kasih yang sebesar-besarnya atas setiap pengorbanan, dukungan moral maupun materiil, serta semangat yang tidak pernah surut di saat penulis merasa lelah, ragu, maupun ingin menyerah. Kasih sayang, nasihat, dan dukungan yang diberikan menjadi penopang terbesar yang menguatkan langkah penulis hingga sampai pada titik ini. Penulis juga menyampaikan terima kasih yang setulusnya kepada Ibu sambung penulis Ibu Diana Eliatni, atas perhatian, kesabaran, dukungan, serta doa yang senantiasa menyertai dan menguatkan penulis selama proses penyusunan karya ini.

8. Kepada Winda Wahyu Ningsih, yang telah banyak membantu, menyemangati penulis dengan segala caranya dan menjadi *support system* selama proses penyusunan skripsi ini. Terima kasih atas kesabaran serta doa yang senantiasa diberikan.
9. Teman-teman Rumah Ahnaf yang tidak bisa saya sebutkan satu per satu yang selalu mendukung dan membantu penulis selama penyusunan skripsi ini.
10. Teman-teman Informatika Angkatan 2021, terima kasih atas kebersamaan, canda tawa, semangat saling mendukung, dan kenangan selama perkuliahan yang tidak akan terlupakan.
11. Kepada semua pihak yang telah berkontribusi dan memberikan dukungan maupun bantuan dalam penyusunan skripsi ini.

Akhir kata, penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, dengan segala kerendahan hati, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat baik secara akademis maupun praktis

Cilegon, 19 Januari 2026

Penulis

ANALISIS KERENTANAN DAN MITIGASI KEAMANAN WEB MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* (STUDI KASUS: SPADA Universitas Sultan Ageng Tirtayasa)

Muhammad Fadhil Putra

RINGKASAN

Latar Belakang: Penelitian ini dilatarbelakangi oleh pentingnya keamanan aplikasi web dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi pada sistem pembelajaran daring, khususnya SPADA Universitas Sultan Ageng Tirtayasa. Masalah ini muncul karena aplikasi web berpotensi memiliki kerentanan yang dapat dimanfaatkan pihak tidak bertanggung jawab, sehingga diperlukan analisis terstruktur berbasis standar yang diakui. Berdasarkan tinjauan teori, penelitian ini memiliki alasan teoritis yang kuat melalui acuan OWASP *Top* 10 Tahun 2021 serta alasan praktis untuk membantu pengelola sistem meningkatkan keamanan web. Penelitian ini bertujuan memberikan manfaat praktis berupa analisis kerentanan dan arahan mitigasi yang sesuai kondisi sistem.

Perumusan Masalah: Berdasarkan latar belakang yang telah diuraikan, masalah yang diteliti dirumuskan secara jelas dan terfokus: (1) jenis kerentanan apa yang teridentifikasi pada SPADA UNTIRTA berdasarkan OWASP *Top* 10 2021, (2) bagaimana tingkat risiko serta dampaknya pada CIA Triad, dan (3) rekomendasi mitigasi apa yang dapat diterapkan.

Tujuan Penelitian: Tujuan utama dari penelitian ini adalah untuk mengidentifikasi kerentanan keamanan, menganalisis tingkat risiko dan dampaknya terhadap CIA Triad, serta menyusun rekomendasi mitigasi untuk meningkatkan keamanan web SPADA UNTIRTA berdasarkan OWASP Top 10 2021.

Metode Penelitian: Metode yang digunakan adalah *Vulnerability Assessment* pada aplikasi web SPADA UNTIRTA dengan tahapan information gathering, manual explore menggunakan OWASP ZAP, serta pemindaian lanjutan menggunakan Acunetix sebagai verifikasi. Ruang lingkup dibatasi pada layanan publik dan tidak mencakup pengujian jaringan internal/server/basis data (*black-box testing*).

Hasil Penelitian: Hasil penelitian menunjukkan adanya beberapa kerentanan dengan tingkat risiko medium dan low, terutama pada kategori *Security Misconfiguration.* Kerentanan yang ditemukan meliputi *CSP Header* tidak diterapkan, keberadaan file sensitif yang dapat diakses publik (mis. *composer.lock* dan *phpinfo.php*), penggunaan TLS 1.0/1.1, serta *timestamp disclosure*. Dampak kerentanan menunjukkan pengaruh dominan terhadap aspek *Confidentiality* dan *Integrity*.

80

Kesimpulan: Berdasarkan hasil yang telah diperoleh, penelitian ini menyimpulkan bahwa SPADA UNTIRTA memiliki kerentanan dominan pada aspek konfigurasi keamanan, dengan risiko utama pada *Confidentiality* dan *Integrity*, sehingga diperlukan mitigasi berupa penerapan CSP, pembatasan/penonaktifan akses file sensitif, penonaktifan TLS versi lama, serta penguatan konfigurasi server untuk meminimalkan pengungkapan informasi sistem.

Kata Kunci: *Acunetix*, *OWASP Top 10*, *OWASP ZAP*, *SPADA UNTIRTA, Vulnerability Assessment*

ANALISIS KERENTANAN DAN MITIGASI KEAMANAN WEB MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* (STUDI KASUS: SPADA Universitas Sultan Ageng Tirtayasa)

Muhammad Fadhil Putra

ABSTRAK

Keamanan aplikasi web merupakan aspek krusial dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, khususnya pada sistem pembelajaran daring seperti SPADA Universitas Sultan Ageng Tirtayasa. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada SPADA UNTIRTA menggunakan metode *Vulnerability Assessment*.

Proses pengujian dilakukan melalui beberapa tahap, meliputi information gathering, manual explore menggunakan OWASP ZAP, serta pemindaian lanjutan dengan Acunetix Web Vulnerability Scanner sebagai alat verifikasi. Pengujian difokuskan pada aplikasi web yang dapat diakses publik dengan batasan ruang lingkup black-box testing.

Hasil penelitian menunjukkan adanya beberapa kerentanan dengan tingkat risiko *medium* dan *low*, terutama pada kategori *Security Misconfiguration*. Kerentanan utama yang ditemukan meliputi tidak diterapkannya *Content Security Policy (CSP)*, keberadaan file sensitif yang dapat diakses publik seperti *composer.lock* dan *phpinfo.php*, penggunaan protokol TLS versi lama (TLS 1.0 dan 1.1), serta pengungkapan informasi waktu sistem (*timestamp disclosure*). Analisis dampak menunjukkan pengaruh dominan terhadap aspek *Confidentiality* dan *Integrity*. Penelitian ini merekomendasikan penerapan CSP yang ketat, pembatasan akses file sensitif, penonaktifan TLS lama, serta penguatan konfigurasi server untuk meminimalkan pengungkapan informasi sistem.

Kata kunci: *Vulnerability Assessment*, OWASP Top 10, OWASP ZAP, Acunetix, SPADA UNTIRTA

VULNERABILITY ANALYSIS AND WEB SECURITY MITIGATION USING THE VULNERABILITY ASSESSMENT METHOD (CASE STUDY: SPADA, UNIVERSITAS SULTAN AGENG TIRTAYASA)

Muhammad Fadhil Putra

ABSTRACT

Web application security is crucial to preserve the confidentiality, integrity, and availability of information, particularly in online learning systems such as SPADA at Universitas Sultan Ageng Tirtayasa. This study aims to analyze security vulnerabilities in SPADA UNTIRTA *using the Vulnerability Assessment.*

The testing process consists of several stages, including information gathering, manual exploration using OWASP ZAP, and further scanning with Acunetix Web Vulnerability Scanner as a verification tool. The assessment is limited to the publicly accessible web application with a black box testing scope.

The results reveal several vulnerabilities with medium and low risk levels, predominantly under Security Misconfiguration. The main findings include the absence of Content Security Policy (CSP), publicly accessible sensitive files such as composer.lock and phpinfo.php, the use of legacy TLS versions (TLS 1.0 and 1.1), and timestamp disclosure. Impact analysis indicates dominant effects on confidentiality and integrity. This study recommends enforcing a strict CSP header, restricting access to sensitive files, disabling legacy TLS protocols, and strengthening server configuration to reduce system information disclosure.

Keywords: *Vulnerability Assessment*, *OWASP Top 10*, OWASP ZAP, Acunetix, SPADA UNTIRTA

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

turnitin Page 25 of 78 - Integrity Submission Submission ID trn:oid:::7690:126842042

BAB I
PENDAHULUAN

1.1 Latar Belakang

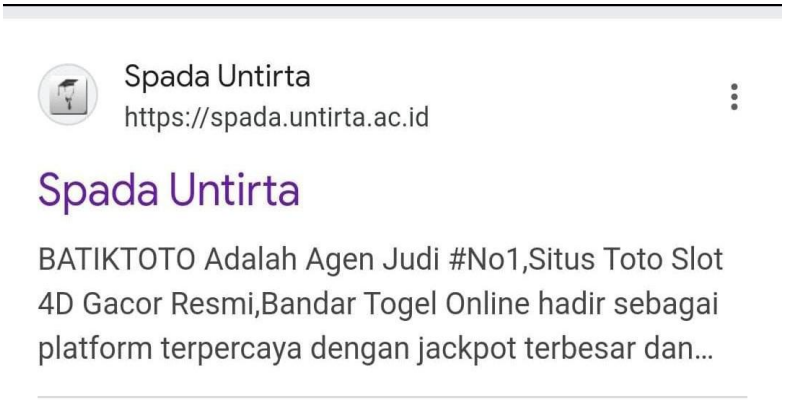
Kemajuan teknologi terus berkembang dengan sangat cepat, menciptakan perubahan signifikan dalam berbagai aspek kehidupan. Salah satu dampaknya adalah peningkatan penggunaan situs web yang kini menjadi kebutuhan utama di berbagai sektor, seperti institusi pemerintahan, pendidikan, organisasi, hingga kebutuhan individu. Seiring dengan pertumbuhan tersebut, aspek keamanan informasi menjadi semakin krusial. Meningkatnya jumlah pengguna yang terhubung ke internet membuka peluang bagi pelaku kejahatan *cyber* untuk memanfaatkan celah keamanan dan melakukan aktivitas yang merugikan. Oleh karena itu, pengembangan sistem keamanan komputer yang tangguh menjadi kebutuhan mendesak untuk melindungi data dan mencegah ancaman dari pihak yang tidak bertanggung jawab.

Berdasarkan data Hootsuite (*We Are Social*) [2], penggunaan internet di Indonesia telah mencapai 212,9 juta pengguna atau 77% dari total populasi sebesar 276,4 juta jiwa. Peningkatan jumlah pengguna internet yang terjadi setiap tahun berbanding lurus dengan pertumbuhan volume informasi yang tersedia di internet. Seiring dengan kemajuan sistem informasi, risiko keamanan dan berbagai bentuk ancaman siber juga semakin meningkat. Data dari AwanPintar.id mencatat bahwa Indonesia menghadapi rata-rata 13.733.440 serangan siber per hari pada semester pertama 2024, atau setara dengan 158 serangan per detik [3]. Kondisi ini menunjukkan bahwa seiring meningkatnya adopsi teknologi digital, ancaman keamanan siber juga mengalami peningkatan yang signifikan, sehingga pengujian keamanan sistem aplikasi berbasis web menjadi semakin penting untuk mengantisipasi berbagai risiko keamanan yang mungkin timbul.

Dalam bidang pendidikan, keberadaan Sistem Pembelajaran Daring (SPADA) telah menjadi standar penting untuk mendukung proses belajar mengajar secara digital. SPADA diimplementasikan di hampir seluruh perguruan tinggi dan universitas di Indonesia untuk memudahkan pengelolaan kegiatan pembelajaran, meningkatkan aksesibilitas, serta memfasilitasi interaksi antara mahasiswa dan

pengajar. Universitas Sultan Ageng Tirtayasa (UNTIRTA) sebagai salah satu lembaga pendidikan tinggi di Indonesia juga memanfaatkan jaringan internet untuk menjalankan aplikasi berbasis web SPADA. Namun, hingga saat ini, belum semua sistem SPADA di institusi pendidikan telah melalui pengujian keamanan secara menyeluruh.

Pentingnya pengujian keamanan SPADA terletak pada fungsinya yang vital dalam mengelola data penting terkait proses pembelajaran, termasuk materi kuliah, catatan aktivitas, serta informasi pribadi mahasiswa dan pengajar. SPADA menghubungkan seluruh elemen pendidikan untuk mendukung distribusi materi pembelajaran, pengumpulan tugas, dan komunikasi daring. Di dalamnya tersimpan data sensitif seperti informasi identitas pengguna, catatan akademik, dan data akses yang berpotensi dieksploitasi jika terdapat celah keamanan. Penelitian terdahulu menunjukkan bahwa banyak platform daring di institusi pendidikan masih memiliki celah keamanan yang rentan terhadap serangan seperti *Cross-Site Scripting (XSS)* dan *SQL Injection* [4]. Oleh karena itu, pengujian keamanan yang komprehensif sangat penting untuk mengidentifikasi dan menutup potensi kerentanan guna mencegah risiko kebocoran data yang dapat membahayakan privasi pengguna serta merusak reputasi institusi pendidikan. Analisis mendalam terhadap potensi kerentanan ini menjadi langkah penting dalam meningkatkan keamanan web secara keseluruhan.



Gambar 1 Contoh insiden keamanan pada situs SPADA UNTIRTA yang terdeteksi melalui hasil pencarian Google.

Sebagai bukti empiris dalam Gambar 1 hasil pencarian Google menunjukkan situs resmi SPADA Universitas Sultan Ageng Tirtayasa mengalami *defacement SEO* berupa cuplikan iklan judi online. Fenomena ini membuktikan bahwa serangan *web defacement* tidak hanya mengganggu operasional teknis, tetapi juga merusak reputasi institusi pendidikan serta menurunkan tingkat kepercayaan pengguna. Data Pusopskamsinas [5] mencatat sebanyak 9.749 kasus web defacement terjadi di Indonesia, dengan sekitar 32% di antaranya menargetkan sektor perguruan tinggi. Selain itu, penelitian [6] menunjukkan bahwa defacement bertema promosi judi online semakin meluas dengan memanfaatkan teknik *dorking* dan *crawling* sistematis untuk menyisipkan konten berbahaya pada situs pendidikan. Temuan ini menegaskan bahwa situs akademik, termasuk SPADA UNTIRTA, berpotensi besar menjadi sasaran serangan yang berdampak langsung pada aspek *Confidentiality, Integrity, dan Availability (CIA Triad)*.

Berdasarkan kondisi tersebut, diperlukan suatu pengujian keamanan yang sistematis untuk mengetahui tingkat kerentanan aplikasi web SPADA UNTIRTA. Pengujian keamanan pada penelitian ini dilakukan dengan metode *Vulnerability Assessment*, yaitu metode yang digunakan untuk mengidentifikasi dan mengevaluasi potensi kerentanan keamanan pada sistem aplikasi web. Metode ini banyak digunakan dalam penelitian keamanan aplikasi web karena mampu memberikan gambaran kondisi keamanan sistem dari sisi pengguna publik serta menjadi dasar dalam penyusunan langkah mitigasi. Penerapan *Vulnerability Assessment* dalam penelitian keamanan web telah banyak dilakukan pada sistem informasi berbasis web, khususnya di lingkungan pendidikan dan pemerintahan [7].

Dalam proses analisis hasil pengujian, penelitian ini menggunakan OWASP Top 10 tahun 2021 sebagai acuan untuk mengelompokkan dan membahas jenis kerentanan yang ditemukan. OWASP Top 10 dipilih karena merupakan standar internasional yang banyak digunakan dalam penelitian dan praktik keamanan aplikasi web, serta relevan dengan jenis ancaman yang umum terjadi pada aplikasi web modern [8].

Pengujian dilakukan dengan alat bantu yaitu *OWASP Zed Attack Proxy (ZAP)* sebagai alat utama untuk mendeteksi kerentanan keamanan aplikasi web, serta

Acunetix Web Vulnerability Scanner sebagai alat verifikasi tambahan. OWASP ZAP dipilih karena bersifat open source, mudah digunakan, dan memiliki kemampuan dalam mendeteksi berbagai jenis kerentanan seperti *SQL Injection, Cross-Site Scripting (XSS),* dan kesalahan konfigurasi keamanan. Sementara itu, Acunetix digunakan untuk memverifikasi hasil pengujian serta mendeteksi kelemahan lain pada sisi konfigurasi server dan protokol komunikasi, sehingga hasil analisis yang diperoleh menjadi lebih akurat dan objektif.

Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan pada sistem SPADA Universitas Sultan Ageng Tirtayasa serta memberikan rekomendasi mitigasi guna meningkatkan keamanan sistem. Secara teoretis, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan kajian keamanan aplikasi web, khususnya pada sistem pembelajaran daring. Secara praktis, hasil penelitian ini diharapkan dapat dimanfaatkan oleh pengelola sistem informasi UNTIRTA sebagai bahan evaluasi dan perbaikan keamanan aplikasi web.

Dengan alasan yang telah dijelaskan maka peneliti memutuskan mengambil judul skripsi ” Analisis Kerentanan dan Mitigasi Keamanan Web Menggunakan Metode *Vulnerability Assessment* (Studi Kasus: SPADA Universitas Sultan Ageng Tirtayasa)”.

1.2 Rumusan Penelitian

Adapun rumusan masalah yang dapat diambil dari latar belakang tersebut adalah sebagai berikut:

1. Apa saja jenis kerentanan keamanan yang teridentifikasi pada sistem SPADA Universitas Sultan Ageng Tirtayasa berdasarkan kategori OWASP Top 10 tahun 2021?
2. Bagaimana tingkat risiko dari setiap kerentanan tersebut serta dampaknya terhadap aspek *CIA Triad (Confidentiality, Integrity, Availability)*?
3. Apa rekomendasi mitigasi keamanan yang dapat diterapkan berdasarkan hasil analisis kerentanan untuk meningkatkan keamanan web SPADA Universitas Sultan Ageng Tirtayasa?

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai penulis dalam penelitian ini yaitu:

1. Mengidentifikasi kerentanan keamanan yang terdapat pada sistem SPADA Universitas Sultan Ageng Tirtayasa berdasarkan kategori OWASP *Top* 10 tahun 2021.
2. Menganalisis tingkat risiko dan dampak setiap kerentanan terhadap aspek *Confidentiality, Integrity, dan Availability (CIA Triad).*
3. Menyusun rekomendasi mitigasi keamanan berdasarkan hasil analisis kerentanan untuk meningkatkan keamanan web SPADA Universitas Sultan Ageng Tirtayasa.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Penelitian ini diharapkan berkontribusi pada pengembangan pengetahuan di bidang keamanan informasi, khususnya dalam konteks keamanan aplikasi web, dengan memberikan pemahaman lebih mendalam tentang penerapan metode *Vulnerability Assessment*, termasuk OWASP Top 10, penggunaan OWASP ZAP dan *Acunetix Web Vulnerability Scanner*, untuk mengidentifikasi dan menganalisis risiko pada sistem pembelajaran daring. Penelitian ini juga akan menjadi validasi empiris mengenai efektivitas OWASP dalam konteks sistem informasi pendidikan di Indonesia, mengisi celah dalam literatur keamanan siber karena belum ada studi spesifik tentang SPADA UNTIRTA dengan metodologi ini, sehingga dapat menjadi referensi bagi peneliti lain untuk mengembangkan metodologi analisis kerentanan di masa mendatang.

1.4.2 Manfaat Praktis

1. Bagi Penulis, Mendapatkan pengetahuan dan pemahaman yang lebih mendalam tentang keamanan sistem informasi, khususnya dalam menganalisis kerentanan dan menerapkan mitigasi keamanan pada website menggunakan metode *Vulnerability Assessment*.

2. Bagi Universitas, Memberikan kontribusi akademik dalam bidang keamanan web serta memberikan gambaran nyata mengenai kondisi keamanan web SPADA.
3. Bagi Peneliti Selanjutnya, Penelitian ini dapat menjadi referensi dan landasan bagi peneliti selanjutnya dalam melakukan analisis keamanan web menggunakan metode *Vulnerability Assessment* dan tools pengujian yang relevan.

1.5 Batasan Penelitian

Dalam pembuatan skripsi penelitian ini, penulis membatasi penelitian yang akan dianalisis yaitu:

1. Penelitian ini hanya difokuskan pada analisis keamanan aplikasi web SPADA Universitas Sultan Ageng Tirtayasa yang dapat diakses publik, tanpa melakukan pengujian pada jaringan internal, server, atau basis data (*black-box testing)*.
2. Metode yang digunakan ialah *Vulnerability Assessment*, dengan acuan OWASP Top 10 Tahun 2021 sebagai analisis dari hasil identifikasi kerentanan.
3. Pengujian hanya dilakukan menggunakan tools yang telah ditentukan dalam instrumen penelitian, yaitu OWASP ZAP, Acunetix, serta alat footprinting seperti Ping, Whois, dan DNSRecon, tanpa menggunakan metode pentesting lanjutan yang bersifat destruktif.
4. Rekomendasi mitigasi yang diberikan hanya berupa analisis teknis berdasarkan temuan kerentanan, dan tidak mencakup implementasi langsung pada sistem SPADA UNTIRTA.

1.6 Sistematika Penulisan

Sistematika penulisan dari skripsi ini diuraikan dalam 5 bab, dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Menjelaskan latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan dari penelitian.

BAB II TINJAUAN PUSTAKA

Membahas tentang penelitian terdahulu yang menjadi referensi penulis dalam penelitian, serta membahas teori dan konsep yang relevan dengan topik yang dikaji.

BAB III METODOLOGI PENELITIAN

Menjelaskan mengenai metode yang digunakan untuk memecahkan masalah yang telah dijelaskan pada perumusan masalah

BAB IV HASIL DAN PEMBAHASAN

Berisi penjelasan dan analisa dari metode yang digunakan dan hasil yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Menjelaskan kesimpulan dan saran yang diperoleh setelah dilakukan penelitian. Kesimpulan diambil dari intisari bab-bab sebelumnya.

BAB II
TINJAUAN PUSTAKA

2.1 State of The Art

Dalam penyusunan skripsi ini, peneliti mengumpulkan informasi dari berbagai penelitian terdahulu sebagai bahan pembanding, baik terkait kekurangan maupun kelebihan yang telah ditemukan. Selain itu, peneliti juga mencari referensi dari buku dan skripsi untuk mendapatkan informasi mengenai teori yang berkaitan dengan judul penelitian, sehingga dapat dijadikan sebagai dasar teori ilmiah. Berikut ini merupakan tinjauan literatur yang digunakan sebagai rujukan dalam penelitian ini:

Penelitian pertama [9] menganalisis kerentanan pada domain uinjkt.ac.id dengan menggunakan OWASP *Top* 10 tahun 2021 sebagai pedoman utama dan OWASP ZAP sebagai alat pemindai kerentanan. Penelitian ini berhasil mengidentifikasi celah keamanan seperti *SQL Injection, Directory Listing*, dan *Sensitive Data Exposure*. Dengan pendekatan metodologi *NIST SP 800-115* yang meliputi tahap perencanaan, penemuan, penyerangan, dan pelaporan, penelitian ini memberikan rekomendasi mitigasi berbasis hasil uji kerentanan. Fokus penelitian ini adalah mencegah serangan yang dapat membahayakan data dan sistem institusi pendidikan. Persamaan mengacu pada OWASP *TOP* 10 sebagai pedoman utama dan OWASP ZAP sebagai alat. Perbedaannya penelitian ini menggunakan metodologi *NIST SP 800-115* .

Penelitian kedua [10] berfokus pada evaluasi risiko keamanan aplikasi Sistem Informasi Akademik (SIAKAD) UIN Ar-Raniry menggunakan metode *Vulnerability Assessment*. Dengan alat OWASP ZAP, penelitian ini mengidentifikasi kerentanan tingkat risiko sedang hingga lemah, seperti pengungkapan informasi sensitif dan kegagalan dalam pengaturan keamanan *header HTTP*. Tindakan mitigasi yang disarankan meliputi penggunaan pesan kesalahan kustom, konfigurasi ulang header, penyaringan input, dan pemantauan aktivitas pengguna. Selain itu, penelitian ini menyoroti pentingnya edukasi pengguna dan penerapan kebijakan keamanan untuk melindungi data sensitif. Persamaan dalam penelitian sama-sama menggunakan alat OWASP ZAP dan

OWASP Top 10 sebagai dasar pedoman. Perbedaannya adalah dalam ruang lingkup yang berbeda

Penelitian ketiga [11] melakukan analisis kerentanan dan audit keamanan pada website Kampus UNIPDU Jombang menggunakan pendekatan *Vulnerability Assessment (VA)* berbasis Acunetix. Tujuan utama penelitian ini yaitu mengidentifikasi dan menilai kelemahan keamanan sistem website melalui pemindaian otomatis yang berpedoman pada OWASP *Top* 10 tahun 2021. Proses pemindaian berhasil menemukan beberapa kerentanan penting, seperti penggunaan *reverse proxy, konfigurasi cloud service, serta sertifikat TLS/SSL* yang hampir kadaluarsa. Solusi yang diajukan mencakup pembaruan dan penguatan konfigurasi SSL, serta rekomendasi audit rutin pada aplikasi internal tanpa menggunakan WAF aktif. Penelitian ini menekankan pentingnya validasi keamanan berkala demi mempertahankan kepercayaan pengguna dan meningkatkan keamanan sistem informasi web di lembaga pendidikan. Persamaannya, kedua penelitian menggunakan Acunetix sebagai alat utama dan mengacu pada OWASP *Top* 10. Perbedaannya, penelitian ini fokus pada analisis kelemahan komponen web dan keamanan sertifikat SSL.

Penelitian keempat [12] Menggunakan *OWASP ZAP* bertujuan untuk mengevaluasi keamanan aplikasi web menggunakan metode Vulnerability Assessment dengan memanfaatkan OWASP ZAP sebagai alat pemindaian utama serta klasifikasi hasil berdasarkan OWASP Top 10 Tahun 2021. Penelitian ini melalui tahapan pengumpulan data, pemindaian kerentanan, serta analisis dan pengelompokan temuan berdasarkan tingkat risiko, sehingga diperoleh 23 temuan kerentanan yang terdiri dari kategori *high, medium, low,* dan *informational*, dengan sebagian besar temuan termasuk dalam kategori OWASP Top 10. Persamaan penelitian ini dengan penelitian yang dilakukan adalah sama-sama menggunakan OWASP ZAP untuk mengidentifikasi kerentanan keamanan aplikasi web serta mengacu pada OWASP Top 10 sebagai standar analisis. Perbedaannya terletak pada objek penelitian dan ruang lingkup sistem

Penelitian kelima [13] ini bertujuan untuk mengidentifikasi kerentanan keamanan pada aplikasi web cobaupgradediri.com menggunakan metode

Penetration Testing Execution Standard (PTES) dengan dukungan lingkungan Kali Linux dan tools seperti Nikto, OWASP ZAP, serta Burp Suite. Hasil pengujian menunjukkan adanya kerentanan *Missing Anti-clickjacking Header* dengan tingkat risiko *Medium* yang menyebabkan website rentan terhadap serangan *clickjacking*, sehingga diperlukan penerapan mekanisme *Anti-clickjacking Header seperti X-Frame-Options* atau *Content-Security-Policy (CSP*). Persamaan penelitian ini dengan penelitian yang dilakukan adalah sama-sama menganalisis keamanan aplikasi web untuk mengidentifikasi kerentanan, sedangkan perbedaannya terletak pada metode yang digunakan, di mana penelitian ini menggunakan PTES dengan fokus pada kerentanan spesifik *clickjacking*, sementara penelitian yang dilakukan menggunakan OWASP dengan acuan OWASP *Top* 10 Tahun 2021.

Penelitian keenam [14] menguji keamanan website riset (XYZ) menggunakan panduan *OWASP Web Security Testing Guide (WSTG)* melalui tujuh teknik pengujian, yaitu i*nformation gathering, configuration and deployment management testing, identity management testing, input validation testing, testing for error handling, business logic testing, dan client side testing*. Dalam proses pengujian, penelitian tersebut memanfaatkan Burp Suite dan Dirb sebagai tools utama, serta CVSS untuk mengukur tingkat kerentanan. Hasil penelitian menunjukkan terdapat delapan kerentanan pada website XYZ dengan kategori medium. Persamaan dengan penelitian ini adalah sama-sama berfokus pada pengujian keamanan aplikasi web untuk mengidentifikasi kerentanan dari sisi pengguna. Perbedaannya, penelitian tersebut menggunakan pendekatan OWASP WSTG dengan Burp Suite/Dirb dan pengukuran CVSS, sedangkan penelitian ini menggunakan OWASP dengan OWASP Top 10 Tahun 2021 sebagai acuan analisis serta memanfaatkan OWASP ZAP dan Acunetix untuk pemindaian dan verifikasi temuan.

Penelitian ketujuh [15] Menggunakan Framework ISSAF. Penelitian ini bertujuan untuk mengetahui celah keamanan pada website Lembaga X yang menyimpan data sensitif dengan menggunakan metode penetration testing berdasarkan Framework ISSAF. Framework ISSAF pada penelitian tersebut mencakup sembilan tahap asesmen pengujian, yaitu *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites,*

Maintaining Access, dan Covering Tracks. Pada pelaksanaannya, penelitian menggunakan beberapa tools, salah satunya *Vega Vulnerability Scanner* untuk proses pemindaian kerentanan pada tahap *vulnerability identification*. Hasil penelitian menunjukkan bahwa ditemukan 18 celah keamanan pada website Lembaga X, kemudian diberikan saran perbaikan untuk meningkatkan keamanan website. Persamaan dengan penelitian ini adalah sama-sama melakukan pengujian keamanan website untuk mengidentifikasi kerentanan dan menyusun masukan pengamanan. Perbedaannya, penelitian tersebut menggunakan metode penetration testing berstandar ISSAF (dengan tahapan pengujian yang luas sampai *maintaining access* dan *covering tracks*), sedangkan penelitian ini mengacu OWASP Top 10 Tahun 2021 serta memanfaatkan OWASP ZAP dan Acunetix untuk pemindaian dan verifikasi temuan.

Dengan demikian, tinjauan literatur yang telah diuraikan memberikan dasar yang kuat dalam memahami berbagai pendekatan, standar, dan alat yang digunakan dalam analisis keamanan aplikasi web. Penelitian-penelitian sebelumnya umumnya menerapkan metode *Vulnerability Assessment* dengan acuan OWASP *Top* 10 untuk mengidentifikasi kerentanan keamanan pada sistem berbasis web. Namun, hingga saat ini belum ditemukan penelitian yang secara khusus menganalisis keamanan situs SPADA Universitas Sultan Ageng Tirtayasa sebagai objek penelitian. Oleh karena itu, penelitian ini memberikan kontribusi dengan melakukan analisis kerentanan keamanan pada platform SPADA UNTIRTA menggunakan metode *Vulnerability Assessment* dan mengacu pada OWASP *Top* 10 tahun 2021 sebagai dasar analisis. Selain mengidentifikasi potensi celah keamanan, penelitian ini juga menyajikan rekomendasi mitigasi yang disesuaikan dengan hasil pengujian, sehingga diharapkan dapat memberikan wawasan dan referensi dalam penerapan keamanan aplikasi web di lingkungan akademik, khususnya pada sistem pembelajaran daring.

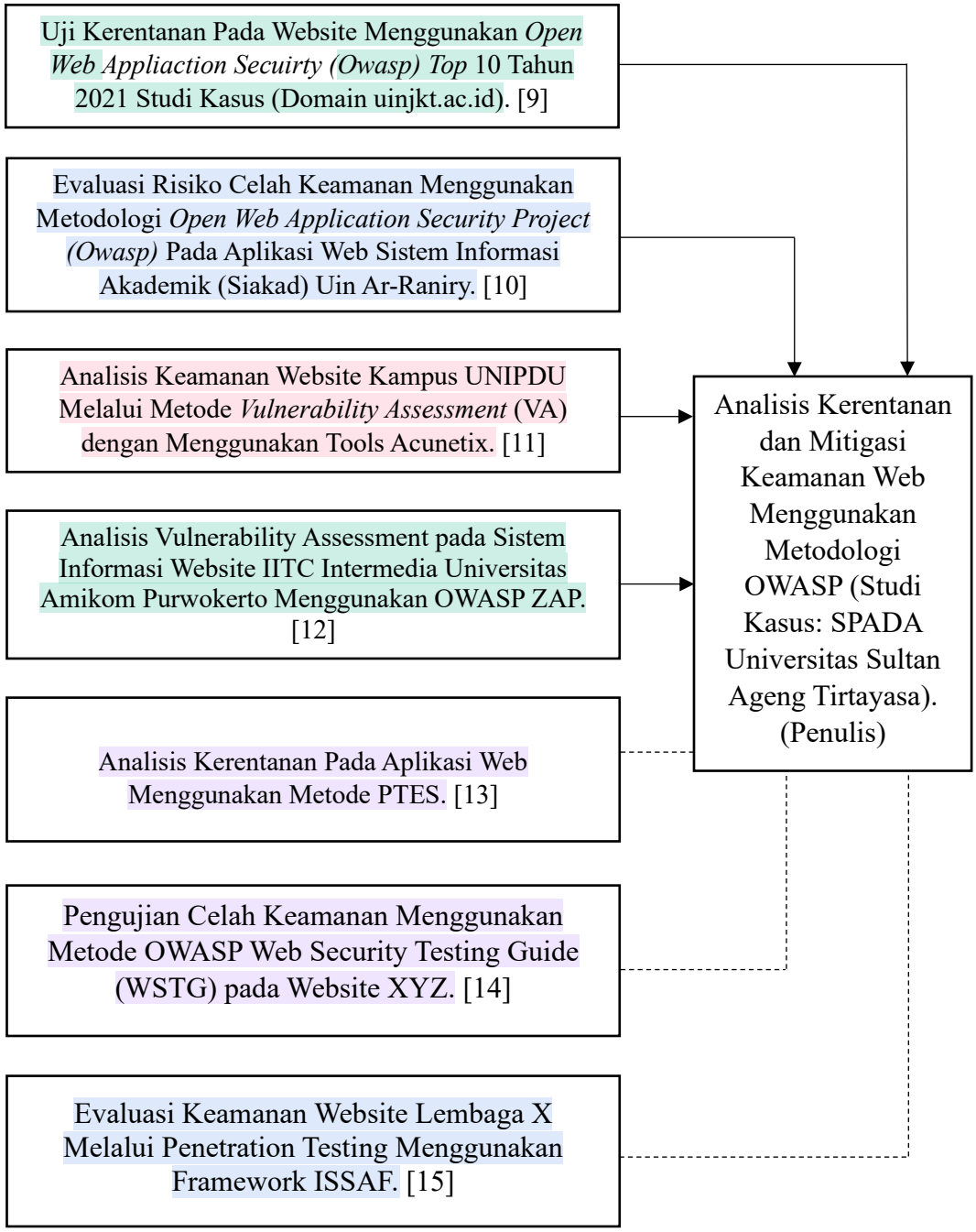
Tabel 1 *State of the art*

No	Nama Peneliti	Judul	Metode Penelitian	Hasil Penelitian
1	[9]	Uji Kerentanan Pada Website Menggunakan *Open Web Appliaction Secuirty (Owasp) Top* 10 Tahun 2021 Studi Kasus (Domain uinjkt.ac.id)	*NIST SP 800-115*	Mengidentifikasi *SQL Injection, Directory Listing, dan Sensitive Data Exposure*.
2	[10]	Evaluasi Risiko Celah Keamanan Menggunakan Metodologi *Open Web Application Security Project (Owasp)* Pada Aplikasi Web Sistem Informasi Akademik (Siakad) Uin Ar-Raniry	*Vulnerability Assessment*	Kerentanan tingkat risiko sedang hingga rendah, seperti pengungkapan informasi sensitif.
3	[11]	Analisis Keamanan Website Kampus UNIPDU Melalui Metode *Vulnerability Assessment* (VA) dengan Menggunakan Tools Acunetix	*Vulnerability Assessment*	Ditemukan kerentanan pada *reverse proxy, cloud service*, dan SSL kadaluarsa. Solusi berupa pembaruan SSL dan audit internal tanpa WAF aktif.
4	[12]	Analisis Vulnerability Assessment pada	*Vulnerability Assessment*	Ditemukan 23 kerentanan (1 *high*, 4 *medium*, 9 *low*, 9 *informational*) di

No	Nama Peneliti	Judul	Metode Penelitian	Hasil Penelitian
		Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP		website yang diuji, dimana 15 temuan termasuk kategori OWASP *Top* 10 seperti masalah konfigurasi header keamanan, manajemen sesi, dan komponen usang, serta rekomendasi mitigasi teknis disampaikan.
5	[13]	Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES	PTES	Ditemukan kerentanan *Missing Anti-clickjacking Header* dengan tingkat risiko Medium yang menyebabkan website rentan terhadap serangan *clickjacking* serta diperlukan penerapan *Anti-clickjacking Header*
6	[14]	Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ	OWASP WSTG	Menggunakan tujuh teknik pengujian WSTG dan menemukan delapan kerentanan dengan kategori medium pada website XYZ.
7	[15]	Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF	ISSAF	Ditemukan 18 celah keamanan pada website Lembaga X dan diberikan saran peningkatan keamanan website.

2.2 Keterkaitan Penelitian

Dari penelitian terdahulu yang sudah didapatkan, sehingga keterkaitan penelitian terdahulu dengan penelitian ini adalah:



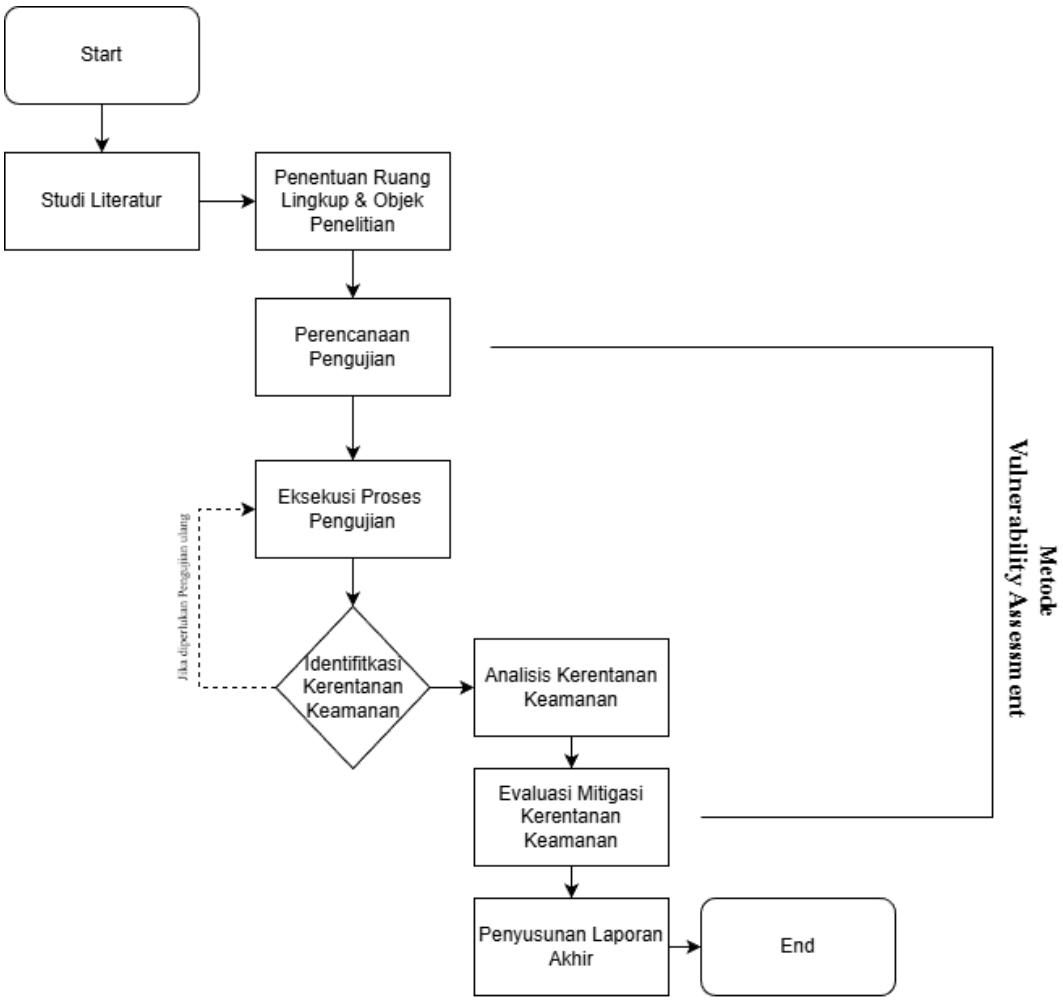
Gambar 2 Diagram Keterkaitan Penelitian

14

BAB III
METODOLOGI PENELITIAN

3.1 Alur Penelitian

Alur dalam penelitian ini mencakup tahapan identifikasi kerentanan, analisis risiko, serta penyusunan rekomendasi mitigasi berdasarkan metode *Vulnerability Assessment*. Tahapan tersebut divisualisasikan dalam bentuk flowchart Gambar 3.



Gambar 3 Alur penelitian

Melalui flowchart yang terdapat pada Gambar 3 dapat dijelaskan alur penelitian ini adalah:

1. Studi Literatur

   Mengumpulkan literatur, dan melakukan studi pada literatur yang didapat dengan tujuan untuk mendapatkan berbagai tinjauan pustaka yang relevan dengan permasalahan yang diteliti sebagai bahan rujukan dalam pembahasan hasil penelitian.

2. Penentuan Ruang Lingkup & Objek Penelitian

   Menentukan ruang lingkup penelitian dan target sistem aplikasi yang akan diuji. Dalam penelitian ini, ruang lingkupnya adalah situs SPADA Universitas Sultan Ageng Tirtayasa.

3. Perencanaan Pengujian

   Perencanaan ini mencakup pemilihan tools yang akan digunakan serta tahap pengujian yang akan dilaksanakan. Pada penelitian ini digunakan OWASP ZAP sebagai alat utama untuk melakukan pengujian keamanan web dan Acunetix Web Vulnerability Scanner sebagai alat pendukung untuk verifikasi hasil.

4. Eksekusi Proses Pengujian

   Tahap ini diawali dengan proses *information gathering* untuk mengumpulkan informasi awal terkait domain dan teknologi yang digunakan pada sistem SPADA UNTIRTA. Selanjutnya dilakukan *manual explore* melalui OWASP ZAP untuk memetakan struktur halaman web dan endpoint yang akan diuji. Setelah itu, pengujian dilanjutkan dengan menggunakan *Acunetix Web Vulnerability Scanner* untuk melakukan pemindaian. Semua hasil pemindaian dicatat, termasuk jenis dan tingkat risiko kerentanan yang ditemukan, untuk kemudian dianalisis lebih lanjut pada tahap berikutnya.

5. Identifikasi Kerentanan Keamanan

   Mengidentifikasi setiap kerentanan berdasarkan deskripsi masalah, potensi risiko, dan dampaknya pada situs SPADA. Kerentanan yang ditemukan akan dirinci untuk menjadi bahan analisis risiko lebih lanjut.

6. Analisis Kerentanan Keamanan

   Menganalisis setiap kerentanan yang ditemukan dengan mengacu pada OWASP Top 10 2021 dan menilai dampaknya terhadap aspek *CIA Triad (Confidentiality, Integrity, Availability).*

7. Evaluasi Mitigasi Kerentanan Keamanan

   Menentukan langkah-langkah mitigasi yang direkomendasikan untuk setiap kerentanan yang ditemukan. Rekomendasi ini disusun berdasarkan tingkat keparahan kerentanan dan prioritas perbaikan untuk mengurangi risiko keamanan.

8. Penyusunan Laporan Akhir

   Menyusun laporan akhir yang mencakup seluruh proses penelitian, hasil identifikasi, analisis kerentanan, dan rekomendasi mitigasi. Laporan ini dirancang sebagai dokumentasi lengkap hasil penelitian yang dapat menjadi acuan untuk meningkatkan keamanan situs SPADA Universitas Sultan Ageng Tirtayasa.

3.2 Lokasi dan Objek Penelitian

Lokasi penelitian dilakukan di luar jaringan internet Universitas Sultan Ageng Tirtayasa. Penelitian ini dilakukan di luar universitas, misalnya di lingkungan peneliti atau tempat lain yang tidak terhubung dengan jaringan universitas tersebut. Objek dari penelitian ini adalah Sistem Pembelajaran Daring (SPADA) Universitas Sultan Ageng Tirtayasa.

3.3 Instrumen Penelitian

Dalam melakukan penelitian ini memerlukan beberapa alat yang digunakan untuk mempermudah pengerjaannya. Instrumen yang digunakan di antaranya berupa *software* dan *hardware*.

3.3.1 *Software*

Software yang digunakan dalam penelitian ini adalah:

1. Sistem Operasi Windows 11

   Windows 11 digunakan sebagai sistem operasi utama yang menjalankan perangkat lunak virtualisasi. Dengan antarmuka yang stabil dan dukungan teknologi virtualisasi, Windows 11 memungkinkan penelitian berjalan dengan lancar menggunakan *Oracle VM VirtualBox*.

2. *Oracle VM VirtualBox* 6.1

Oracle VM VirtualBox 6.1 digunakan sebagai perangkat lunak virtualisasi yang memungkinkan instalasi dan eksekusi Kali Linux dalam lingkungan yang aman dan terisolasi. Dengan menggunakan VirtualBox, pengujian keamanan dapat dilakukan tanpa mempengaruhi sistem utama.

3. Sistem Operasi Kali Linux 2020.4

Kali Linux 2020.4 adalah sistem operasi berbasis Linux yang dirancang khusus untuk pengujian keamanan. Sistem ini menyediakan berbagai alat, termasuk OWASP ZAP , yang digunakan untuk mengidentifikasi kerentanan keamanan pada situs web target.

4. OWASP ZAP 2.16.1

OWASP ZAP adalah alat pengujian keamanan web yang digunakan untuk mengidentifikasi berbagai kerentanan, seperti SQL Injection, Cross-Site Scripting (XSS), dan konfigurasi yang tidak aman. Alat ini bekerja dengan melakukan pemindaian otomatis serta pengujian manual terhadap aplikasi web.

5. Acunetix *Web Vulnerability Scanner*

Acunetix *Web Vulnerability Scanner* digunakan untuk memverifikasi hasil uji dari OWASP ZAP serta mendeteksi kelemahan tambahan pada konfigurasi server, enkripsi, dan header keamanan. Alat ini juga memberikan penilaian risiko kerentanan menggunakan standar CVSS, sehingga hasil analisis menjadi lebih akurat dan terukur.

3.3.2 *Hardware*

Hardware yang digunakan dalam penelitian ini adalah:

1. Laptop

   Menggunakan laptop dengan spesifikasi:

   a. Processor: AMD Ryzen 7 5800H with Radeon Graphics @ 3.20 GHz
   b. RAM: 8 GB
   c. Storage: SSD 456 GB
   d. Graphics: AMD Radeon™ RX 5500M with 4GB GDDR6

BAB IV
HASIL DAN PEMBAHASAN

4.1 Waktu dan Ruang Lingkup

Penelitian ini dilaksanakan dalam kurun waktu tanggal 29 September hingga 10 Oktober. Lalu peneliti melakukan penelitian ulang pada 29 Oktober. Ruang lingkup penelitian difokuskan pada sistem web SPADA Universitas Sultan Ageng Tirtayasa (UNTIRTA) sebagai objek utama. Lingkup pengujian dibatasi hanya pada analisis keamanan aplikasi web yang dapat diakses publik, tanpa melakukan perubahan langsung terhadap konfigurasi internal server maupun basis data yang bersifat sensitif.

4.2 Perencanaan Pengujian

Tahap perencanaan pengujian dilakukan untuk merancang langkah-langkah yang akan ditempuh dalam melakukan uji kerentanan terhadap aplikasi web SPADA Universitas Sultan Ageng Tirtayasa. Perencanaan ini meliputi pemilihan tools yang sesuai serta tahapan pengujian yang akan dilaksanakan.

4.2.1 Tools yang Digunakan

Beberapa tools yang digunakan dalam penelitian ini adalah sebagai berikut:

1. *Ping* = memastikan domain aktif serta mendapatkan alamat IP dan *Latency*
2. *Whois* = memperoleh informasi pendaftaran domain
3. *Dnsrecon* = mengidentifikasi record DNS
4. *Whatweb* = mendeteksi teknologi web yang digunakan

4.2.2 Tahapan Pengujian

Tahapan pengujian yang direncanakan adalah sebagai berikut:

1. *Information Gathering* = pengumpulan informasi awal menggunakan *Ping, Whois, Dnsrecon,* dan *Whatweb*
2. *Scanning* Kerentanan = uji dengan OWASP ZAP melalui *manual explore* dan Acunetix Web Vulnerability Scanner.
3. Identifikasi dan Analisis kerentanan = klasifikasi hasil berdasarkan tingkat keparahan serta pemetaan ke *OWASP Top 10*

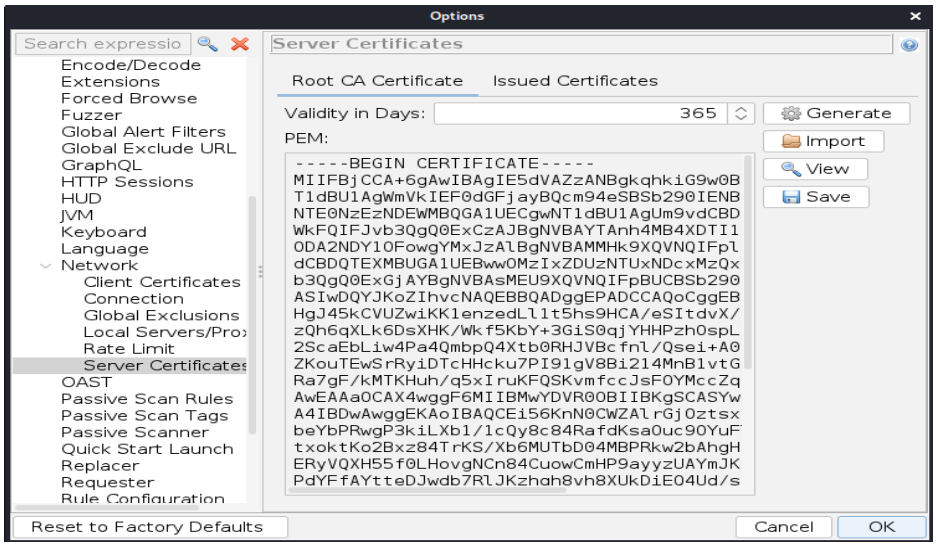
4. Evaluasi Mitigasi = menyusun solusi yang mengatasi kerentanan yang ditemukan

4.2.3 Konfigurasi Aplikasi OWASP ZAP

Sebelum melakukan tahap eksekusi pengujian, OWASP ZAP terlebih dahulu dikonfigurasi agar dapat digunakan secara optimal dalam penelitian ini. Konfigurasi ini dilakukan untuk menjaga konsistensi, keamanan, dan kemudahan dalam proses analisis.

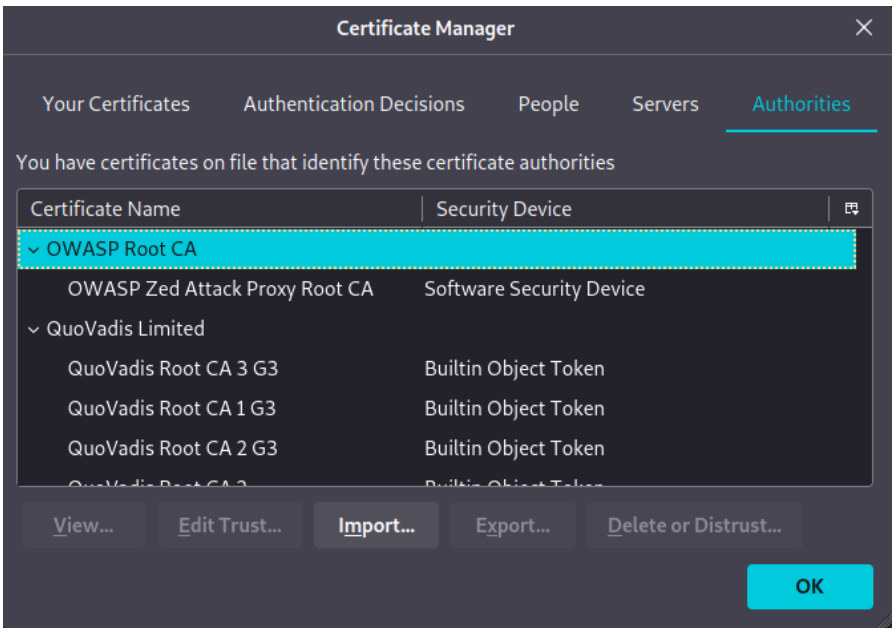
Pengaturan awal OWASP ZAP dijalankan dengan konfigurasi *default*, yaitu *Attack Strength = Medium dan Alert Threshold = Medium*. Pemilihan pengaturan ini bertujuan agar proses pemindaian tetap moderat, mampu mendeteksi kerentanan umum, namun tidak terlalu agresif sehingga tidak menimbulkan risiko gangguan terhadap sistem target.

Selain itu, agar OWASP ZAP dapat menganalisis lalu lintas HTTPS secara penuh, dilakukan pembuatan dan pemasangan OWASP ZAP Root CA. Root CA ini merupakan sertifikat otoritas internal yang dihasilkan oleh OWASP ZAP untuk memungkinkan inspeksi komunikasi terenkripsi antara browser dan server. Dengan adanya Root CA, ZAP dapat membuat sertifikat sementara pada domain yang diuji sehingga seluruh request dan response HTTPS dapat dibaca tanpa menimbulkan peringatan keamanan di browser terlihat pada Gambar 4 dibawah.



Gambar 4 Sertifikat Root CA

Setelah sertifikat Root CA berhasil dibuat, sertifikat tersebut kemudian disimpan dan diimpor ke dalam browser Firefox pada mesin pengujian. Dengan langkah ini, setiap lalu lintas HTTPS dari aplikasi target yang melewati proxy ZAP dapat diinspeksi sepenuhnya, sehingga analisis keamanan dapat dilakukan secara komprehensif.



Gambar 5 Sertifikat Root CA berhasil diimpor

Gambar 5 menunjukkan bahwa sertifikat Root CA telah berhasil diimpor ke browser, sehingga OWASP ZAP dapat digunakan sepenuhnya.

4.3 Eksekusi Proses Pengujian

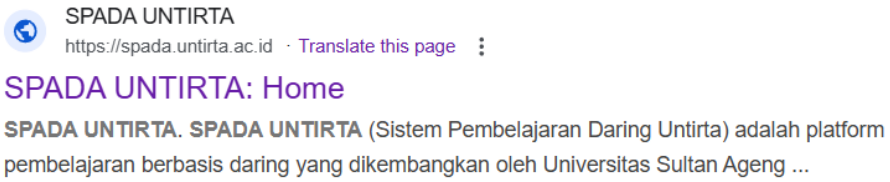
Setelah tahap perencanaan ditentukan, langkah selanjutnya adalah melakukan eksekusi proses pengujian. Pada tahap ini, seluruh metode dan tools yang telah direncanakan sebelumnya diimplementasikan secara langsung untuk memperoleh hasil nyata terkait kondisi keamanan aplikasi web SPADA UNTIRTA.

4.3.1 *Information Gathering*

Sebelum tahap eksekusi pengujian dilakukan, peneliti perlu terlebih dahulu mengumpulkan informasi dasar mengenai Aplikasi web SPADA UNTIRTA. Informasi tersebut berfungsi sebagai langkah awal untuk memahami struktur

aplikasi melalui metode *footprinting*. Setiap data yang diperoleh kemudian didokumentasikan dalam bagian pengumpulan informasi.

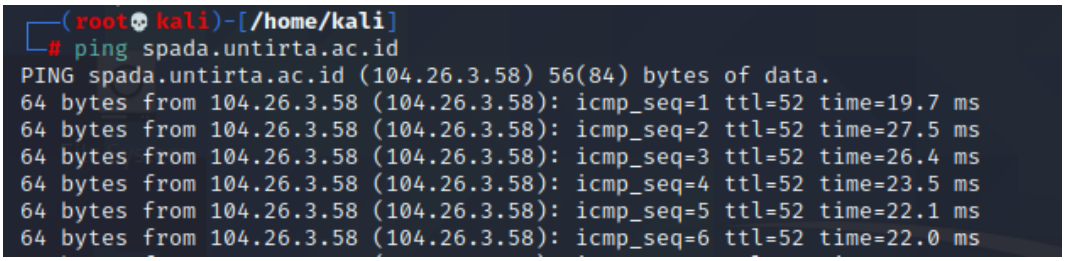
Sebagai langkah awal, peneliti melakukan verifikasi ketersediaan domain SPADA UNTIRTA melalui mesin pencari Google. Tujuan dari tahap ini adalah memastikan bahwa domain target dapat diakses publik dan terindeks oleh mesin pencari.



Gambar 6 Pencarian web SPADA UNTIRTA di Google

Dari hasil pencarian terlihat bahwa situs spada.untirta.ac.id aktif dan terindeks, dengan deskripsi singkat mengenai fungsinya sebagai platform pembelajaran daring Universitas Sultan Ageng Tirtayasa. Informasi ini menjadi titik awal untuk tahap pengujian berikutnya. Setelah memastikan domain dapat diakses publik, langkah selanjutnya adalah melakukan pengujian konektivitas menggunakan ping.

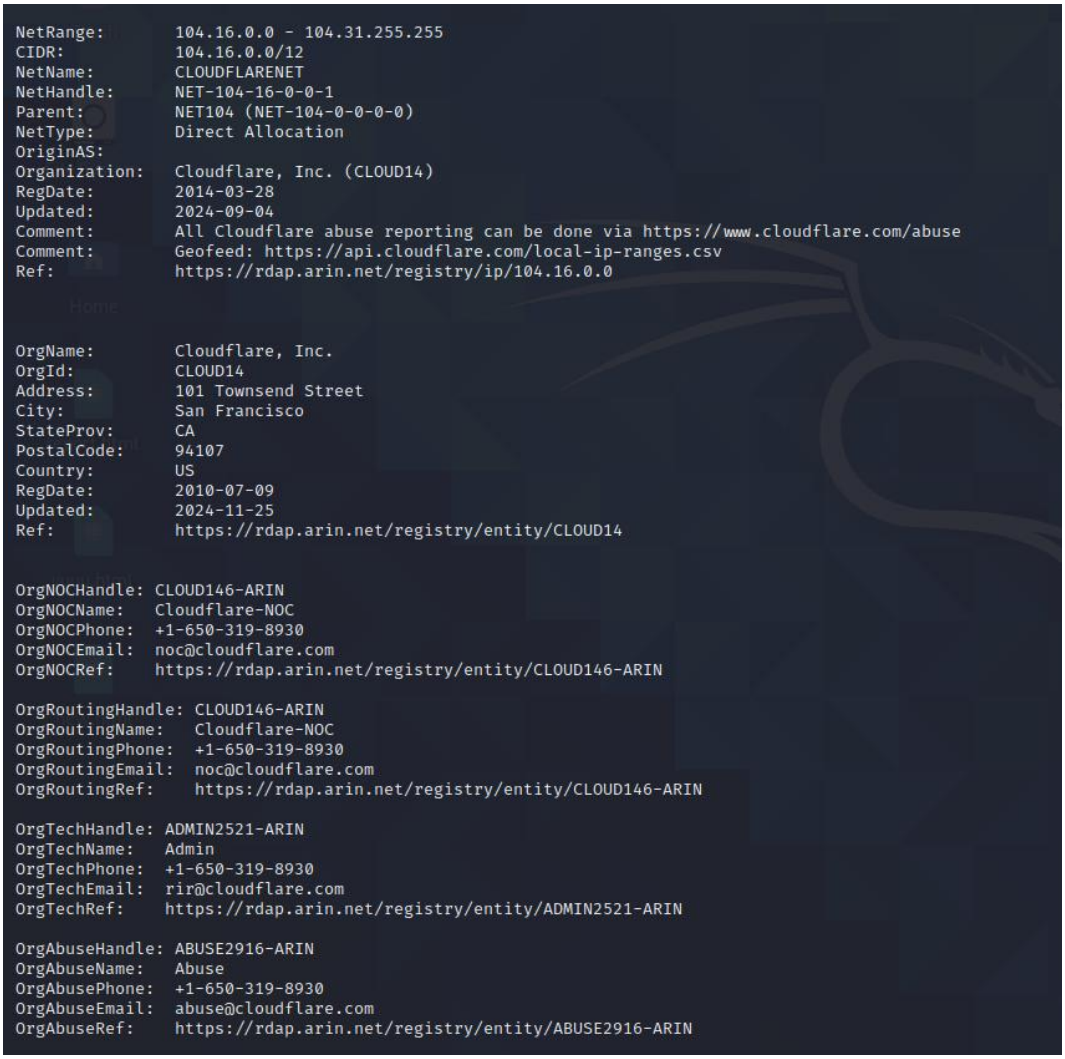
Setelah memastikan bahwa domain SPADA UNTIRTA dapat diakses publik melalui hasil pencarian Google, tahap berikutnya adalah melakukan pengujian konektivitas menggunakan perintah ping. Tujuan dari langkah ini adalah untuk memperoleh alamat IP dari server target sekaligus memastikan server dapat memberikan respon.



Gambar 7 Hasil PING pada domain SPADA UNTIRTA

Hasil PING ditunjukkan pada Gambar 7, di mana domain spada.untirta.ac.id merespons dengan alamat IP 104.26.3.58 dan waktu rata-rata berkisar antara 19-22

ms. Informasi alamat IP yang diperoleh ini selanjutnya digunakan untuk melakukan analisis WHOIS guna mengetahui detail kepemilikan dan pengelolaan domain.

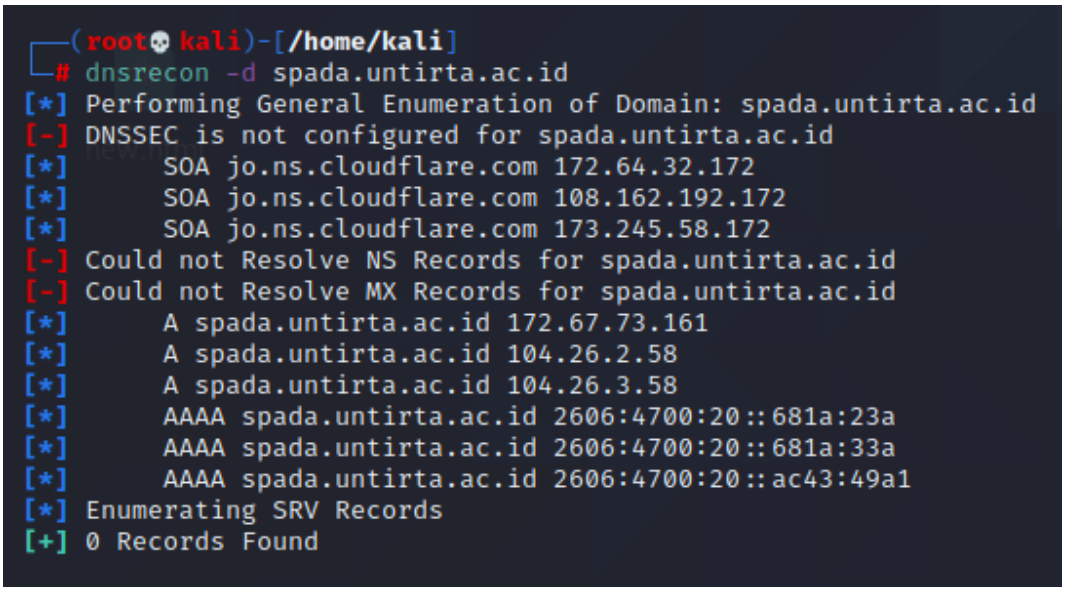


Gambar 8 Hasil WHOIS pada domain SPADA UNTIRTA

Hasil WHOIS pada domain spada.untirta.ac.id ditunjukkan pada Gambar 8. Dari hasil tersebut diketahui bahwa domain ini berada di bawah layanan Cloudflare, Inc., sebuah penyedia Content Delivery Network (CDN) dan keamanan web yang berbasis di San Francisco, Amerika Serikat.

Penggunaan Cloudflare menandakan bahwa server asli SPADA UNTIRTA dilindungi oleh lapisan keamanan tambahan berupa reverse proxy. Dengan demikian, alamat IP asli dari server aplikasi tidak ditampilkan secara publik, melainkan digantikan oleh alamat IP milik Cloudflare. Hal ini bertujuan untuk meningkatkan kinerja akses situs serta melindungi server utama dari serangan

langsung, seperti Distributed Denial of Service (DDoS) atau eksploitasi langsung ke alamat IP asli. Selanjutnya gunakan dnsrecon untuk mengumpulkan informasi server DNS yang digunakan dalam jaringan SPADA UNTIRTA



Gambar 9 DNS *Reconnaissance* pada domain SPADA UNTIRTA

Berdasarkan hasil pemeriksaan DNS pada domain spada.untirta.ac.id menggunakan dnsrecon, diketahui bahwa pengelolaan DNS untuk layanan SPADA UNTIRTA menggunakan nameserver milik *Cloudflare*. Selain itu, terlihat bahwa DNSSEC belum diaktifkan pada domain ini. Konfigurasi tersebut umum digunakan pada layanan yang memanfaatkan Cloudflare sebagai reverse proxy, karena seluruh permintaan akan dilewatkan melalui jaringan Cloudflare untuk memberikan perlindungan tambahan. Setelah mendapatkan informasi dasar mengenai konfigurasi DNS yang digunakan, langkah berikutnya adalah mengumpulkan informasi mengenai teknologi web dan komponen yang berjalan pada situs tersebut menggunakan WhatWeb.

Gambar 10 Hasil WhatWeb pada domain SPADA UNTIRTA

Hasil menggunakan WhatWeb pada domain spada.untirta.ac.id pada Gambar 10 menunjukkan bahwa situs ini menggunakan standar HTML5 dalam penyajian konten serta berada di bawah layanan Cloudflare sebagai *reverse proxy* sekaligus *Content Delivery Network (CDN)* untuk meningkatkan performa dan keamanan. Dari sisi konfigurasi, terdeteksi pula penggunaan beberapa header keamanan seperti *Strict-Transport-Security* (HSTS) untuk memastikan akses hanya melalui HTTPS, *X-Frame-Options* untuk mencegah serangan *clickjacking*, serta X-XSS-Protection untuk memberikan perlindungan dasar terhadap *cross-site scripting (XSS)*.

Berdasarkan proses *information gathering* yang telah dilakukan terhadap domain SPADA UNTIRTA, diperoleh beberapa temuan penting terkait infrastruktur dan konfigurasi awal sistem. Temuan-temuan ini menjadi dasar dalam memahami kondisi target sebelum dilanjutkan ke tahap pengujian kerentanan lebih lanjut, yaitu sebagai berikut:

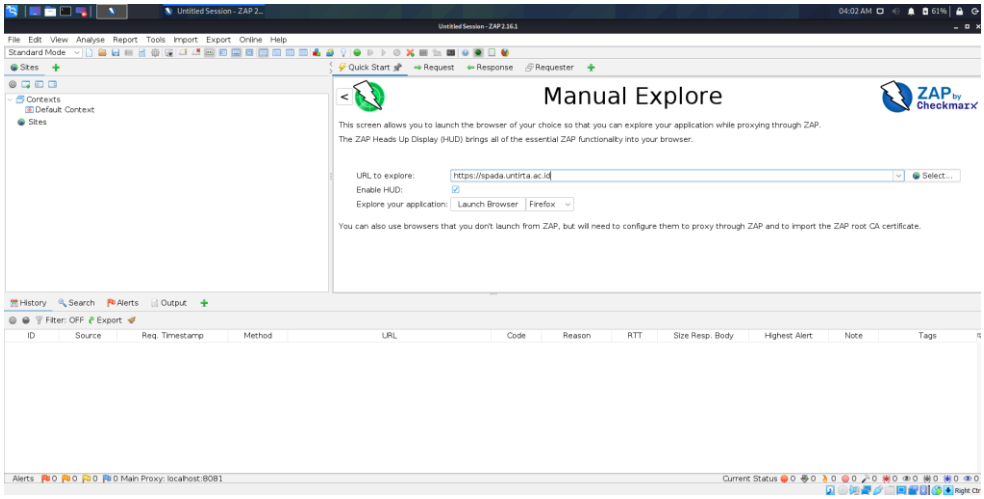
1. *Ping*: Diperoleh alamat IP utama web spada.untirta.ac.id yaitu 104.26.3.58 dengan rata-rata waktu respons sekitar 19-22 ms.
2. *Whois*: Domain berada di bawah layanan *Cloudflare, Inc*., sehingga server origin terlindungi oleh CDN dan detail infrastruktur asli tidak ditampilkan.
3. DNSRecon: Ditemukan beberapa alamat IP. DNSSEC tidak dikonfigurasi untuk domain ini, dan tidak ditemukan *MX record* maupun *SRV record*, yang berarti domain tidak menggunakan layanan email atau service khusus pada subdomain tersebut.
4. *WhatWeb*: terdapat beberapa header keamanan yang sudah diaktifkan, seperti *HSTS dan X-Frame-Options*.

4.3.2 Manual Explore

Pada tahap ini digunakan metode manual explore untuk melakukan pengujian aplikasi target. Pendekatan manual explore memungkinkan peneliti untuk menelusuri aplikasi web secara langsung menggunakan browser yang terhubung melalui proxy OWASP ZAP. Dengan cara ini, seluruh aktivitas permintaan (*request*) dan tanggapan (*response*) dari server akan direkam dan dianalisis oleh ZAP.

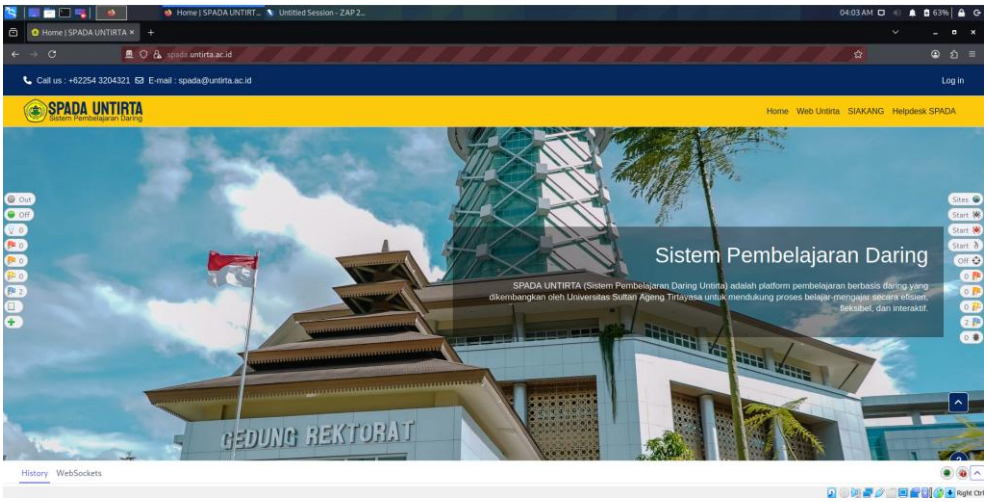
Berikut adalah langkah-langkah dalam melakukan manual explore:

1. Pada tampilan utama aplikasi OWASP ZAP, pilih opsi *manual explore*, lalu masukkan URL target beserta browser yang akan digunakan. Setelah itu, klik *launch browser* untuk memulai proses eksplorasi manual seperti yang ditunjukkan pada gambar.



Gambar 11 Eksekusi proses pengujian dengan Manual Explore

2. Tunggu beberapa saat hingga browser akan muncul dan proses manual explore siap dilakukan seperti digambar.



Gambar 12 Tampilan setelah Manual Explore dilakukan

3. Setelah browser berhasil diluncurkan, pilih domain target spada.untirta.ac.id pada panel *Sites*, kemudian jalankan Spider untuk menelusuri seluruh tautan

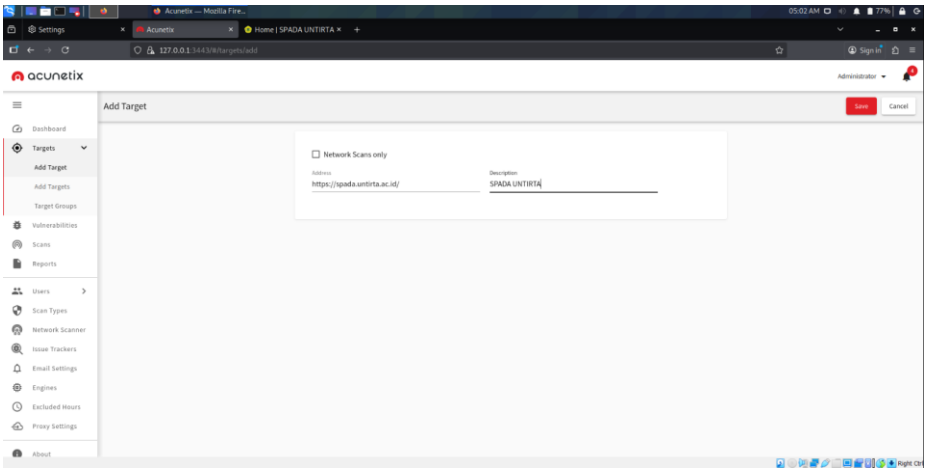
dan endpoint yang tersedia. Setelah proses Spider selesai, lanjutkan dengan *active scan* pada domain yang sama agar OWASP ZAP dapat mendeteksi potensi kerentanan secara otomatis.

4.3.3 Eksekusi Menggunakan Acunetix *Web Vulnerability Scanner*

Setelah tahap *manual explore* selesai dilakukan menggunakan OWASP ZAP, proses pengujian dilanjutkan dengan menggunakan Acunetix Web Vulnerability Scanner sebagai alat bantu verifikasi untuk memastikan keakuratan hasil pemindaian dan mendeteksi potensi kelemahan tambahan pada sistem. Penggunaan Acunetix dilakukan karena alat ini memiliki kemampuan dalam melakukan analisis mendalam terhadap konfigurasi server, enkripsi komunikasi, serta implementasi kebijakan keamanan pada aplikasi web.

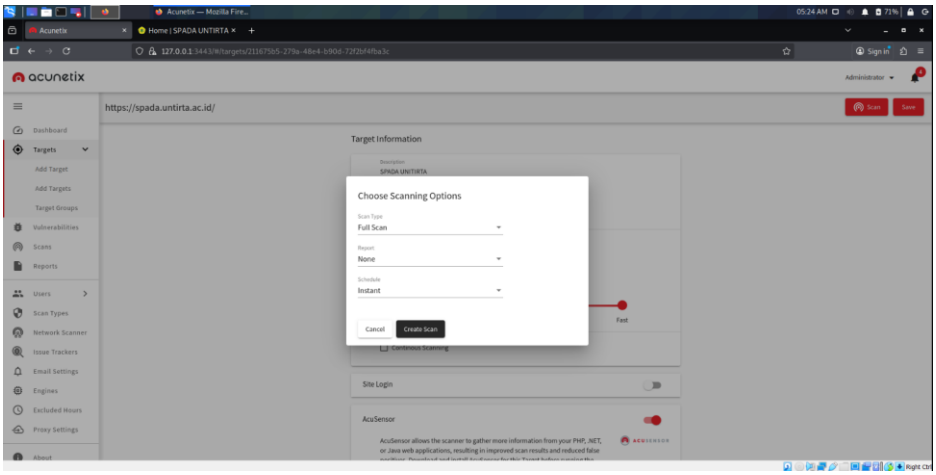
Berikut langkah-langkah menggunakan *acunetix vulnerability scanner*

1. Tahap awal dalam penggunaan Acunetix Web Vulnerability Scanner adalah menambahkan target atau alamat situs web yang akan diuji. Pada tahap ini, peneliti memasukkan alamat target yaitu https://spada.untirta.ac.id/ pada kolom Address dan memberikan keterangan SPADA UNTIRTA pada kolom Description. Setelah data target dimasukkan, langkah berikutnya adalah menyimpan konfigurasi dengan menekan tombol Save, kemudian sistem menambahkan target ke daftar untuk proses pemindaian berikutnya.



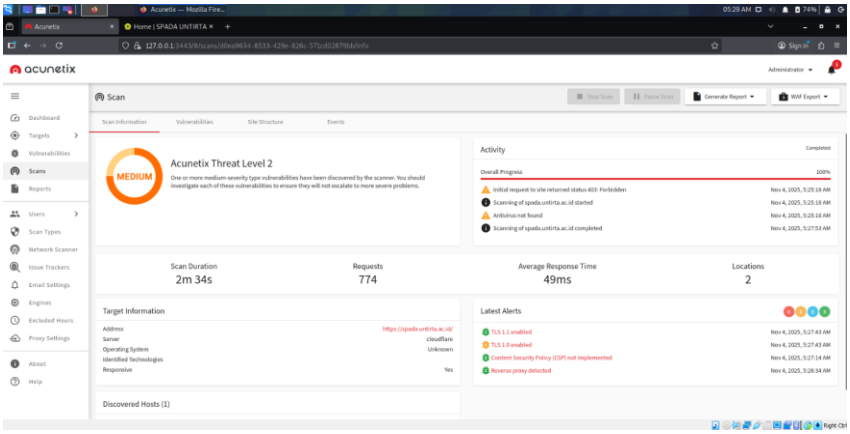
Gambar 13 Menambahkan Target Pengujian di Acunetix

2. Setelah target ditambahkan, tahap selanjutnya adalah melakukan pengaturan opsi pemindaian pada *Acunetix Web Vulnerability Scanner*. Pada tahap ini, peneliti memilih jenis pemindaian (*Scan Type*) yaitu *Full Scan*, agar seluruh halaman dan komponen aplikasi web dapat diperiksa secara menyeluruh. Pemilihan *Full Scan* dilakukan untuk memastikan proses pemindaian tidak hanya mendeteksi kerentanan umum, tetapi juga kelemahan konfigurasi dan kesalahan pada lapisan keamanan lainnya.



Gambar 14 Pengaturan Opsi Pemindaian pada Acunetix

3. Setelah semua pengaturan selesai, proses pemindaian dijalankan dan sistem *Acunetix Web Vulnerability Scanner* mulai melakukan analisis terhadap setiap halaman yang ditemukan. Pengguna hanya perlu menunggu hingga proses pemindaian mencapai status *completed* (100%). Hasil pemindaian ini kemudian disimpan dan digunakan untuk proses analisis pada tahap selanjutnya.



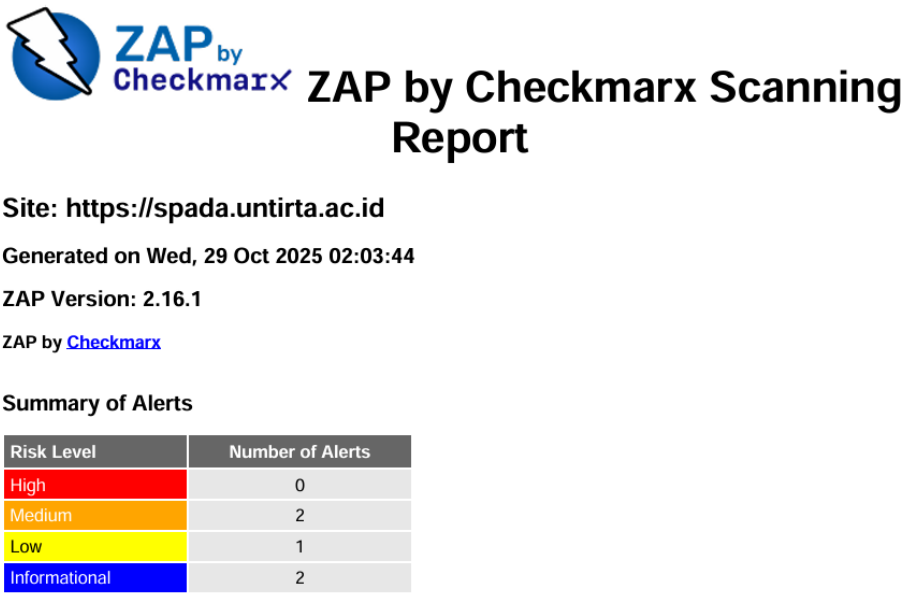
Gambar 15 Hasil Akhir Pemindaian Menggunakan Acunetix

4.4 Identifikasi Kerentanan Keamanan

Kerentanan keamanan yang ditemukan pada sistem diidentifikasi dan dianalisis untuk memahami risiko serta dampak yang mungkin ditimbulkan terhadap aplikasi. Proses identifikasi ini bertujuan untuk memberikan gambaran yang jelas mengenai jenis kelemahan yang ada, tingkat risikonya, serta konsekuensi yang dapat terjadi apabila celah tersebut dieksploitasi. Dengan demikian, setiap temuan akan menjadi bahan pertimbangan dalam proses evaluasi dan penyusunan langkah pengamanan lebih lanjut.

Berdasarkan hasil pengujian menggunakan OWASP ZAP dengan pendekatan manual explore, sistem menghasilkan sejumlah temuan yang dikategorikan ke dalam beberapa tingkat risiko. Laporan ini tidak hanya menampilkan daftar kerentanan yang terdeteksi, namun juga mengklasifikasikan tingkat keparahan masing-masing kelemahan, mulai dari High, Medium, Low, hingga Informational.

Hasil ringkasan dari eksekusi tersebut dapat dilihat pada Gambar 16 yang menampilkan jumlah keseluruhan kerentanan yang teridentifikasi beserta tingkat risikonya.



ZAP by Checkmarx Scanning Report

Site: https://spada.untirta.ac.id

Generated on Wed, 29 Oct 2025 02:03:44

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	1
Informational	2

Gambar 16 Hasil scanning dengan OWASP ZAP

Selanjutnya, rincian lebih lengkap mengenai jenis kerentanan yang berhasil dideteksi dapat dilihat pada Gambar 17 Bagian ini menampilkan daftar kerentanan dengan menyebutkan nama celah, kategori risiko, serta jumlah instansinya yang ditemukan selama proses pengujian.

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Hidden File Found	Medium	2
Timestamp Disclosure - Unix	Low	1
Modern Web Application	Informational	1
User Agent Fuzzer	Informational	108

Gambar 17 Hasil alert yang ditampilkan OWASP ZAP

Berdasarkan detail tersebut, terlihat bahwa aplikasi memiliki berbagai kelemahan keamanan dengan tingkat risiko yang bervariasi. Informasi ini tidak hanya memberikan gambaran mengenai jumlah dan kategori kerentanan, tetapi juga

menunjukkan potensi ancaman yang dapat muncul apabila celah-celah tersebut dimanfaatkan. Untuk memperjelas, hasil temuan tersebut kemudian dirangkum dalam tabel yang memuat nama celah, deskripsi singkat, tingkat risiko, serta potensi dampak yang mungkin ditimbulkan.

Tabel 2 Hasil pemindai OWASP ZAP

No	Nama Celah	Deskripsi	Risiko	Dampak
1	*Content Security Policy (CSP) Header Not Set*	Situs tidak memiliki pengaturan *Content Security Policy (CSP)*. Akibatnya, browser tidak memiliki pedoman untuk membatasi pemuatan konten dari sumber eksternal.	*Medium*	Membuka peluang serangan *Cross-Site Scripting (XSS)* dan injeksi skrip berbahaya.
2	*Hidden File Found (composer.lock, phpinfo.php)*	Ditemukan file sensitif yang masih dapat diakses publik seperti composer.lock dan phpinfo.php, yang berpotensi menampilkan konfigurasi sistem dan versi PHP.	*Medium*	Mengungkap informasi konfigurasi server yang dapat dimanfaatkan untuk serangan lanjutan.
3	*Timestamp Disclosure - Unix*	Server mengungkapkan informasi waktu sistem melalui header HTTP yang dikirim ke browser.	*Low*	Memberikan informasi waktu sistem yang dapat digunakan untuk memetakan aktivitas server.
4	*Modern Web Application Detected*	Sistem terdeteksi menggunakan teknologi web modern; temuan bersifat informatif dan tidak menimbulkan risiko langsung.	*Informational*	Menunjukkan kebutuhan pembaruan berkala agar komponen tetap aman dari kerentanan baru.
5	*User Agent Fuzzer Results - Informational*	Server merespons berbagai variasi *User Agent* yang dikirim selama pengujian. Hasil ini tidak menimbulkan risiko langsung namun memberikan informasi tentang perilaku server.	*Informational*	Dapat dimanfaatkan untuk pemetaan aplikasi oleh pihak tidak berwenang.

Berdasarkan hasil identifikasi menggunakan OWASP ZAP, dapat disimpulkan bahwa kelemahan utama pada sistem SPADA UNTIRTA berada pada sisi konfigurasi keamanan aplikasi. Celah seperti tidak diterapkannya *Content Security Policy (CSP)* dan masih dapat diaksesnya file sensitif menunjukkan bahwa sistem belum sepenuhnya menerapkan standar keamanan web yang direkomendasikan

OWASP. Walaupun tidak ditemukan kerentanan dengan tingkat risiko tinggi, hasil ini tetap penting sebagai dasar untuk peningkatan keamanan pada lapisan aplikasi dan konfigurasi server.

Setelah proses pemindaian utama menggunakan OWASP ZAP dilakukan, langkah selanjutnya adalah melakukan verifikasi hasil menggunakan Acunetix *Web Vulnerability Scanner*. Pengujian tambahan ini bertujuan untuk memastikan keakuratan temuan dari OWASP ZAP serta mengidentifikasi potensi kelemahan lain yang mungkin tidak terdeteksi sebelumnya. Acunetix memiliki kemampuan menganalisis sisi konfigurasi server, protokol komunikasi, dan penerapan enkripsi, sehingga hasil yang diperoleh dapat memberikan gambaran keamanan yang lebih menyeluruh. Hasil pemindaian Acunetix ditampilkan pada tabel berikut.

Tabel 3 Hasil Pemindai Acunetix Web Vulnerability Scanner

No	Nama Celah	Deskripsi	Risiko	Dampak
1	*Content Security Policy (CSP) Not Implemented*	Situs belum menerapkan header CSP sehingga tidak ada aturan untuk membatasi pemuatan skrip dan sumber eksternal.	*Medium*	Membuka peluang serangan *Cross-Site Scripting (XSS)* dan injeksi konten
2	*TLS 1.0 dan TLS 1.1 Masih Aktif*	Server masih mendukung protokol TLS versi lama yang rentan terhadap serangan downgrade dan kelemahan kriptografi.	*Medium*	Berisiko penyadapan data dan serangan *downgrade*
3	*Reverse Proxy Detected (Cloudflare)*	Terdeteksi penggunaan layanan reverse proxy (Cloudflare) yang dapat memengaruhi akurasi pemindaian terhadap konfigurasi asli server.	*Informational*	Menyembunyikan konfigurasi server asli sehingga menyulitkan audit konfigurasi langsung

No	Nama Celah	Deskripsi	Risiko	Dampak
4	*Modern Web Application Detected*	Aplikasi menggunakan komponen/kerangka kerja web modern; temuan bersifat informatif mengenai teknologi yang dipakai.	*Informational*	Menunjukkan kebutuhan pembaruan rutin untuk mencegah kerentanan pada komponen

Berdasarkan hasil pemindaian menggunakan Acunetix, ditemukan bahwa kelemahan pada *Content Security Policy (CSP)* juga muncul sebagaimana hasil dari OWASP ZAP, sehingga dapat disimpulkan bahwa temuan ini bersifat konsisten dan perlu menjadi prioritas utama dalam mitigasi. Selain itu, identifikasi terhadap protokol TLS 1.0 dan 1.1 yang masih aktif menunjukkan bahwa sisi enkripsi komunikasi antara server dan pengguna masih dapat diperkuat untuk mencegah penyadapan data. Dengan demikian, penggunaan dua alat ini memberikan hasil yang saling melengkapi OWASP ZAP fokus pada lapisan aplikasi, sedangkan Acunetix memperkuat analisis pada lapisan transport dan konfigurasi server. Hasil gabungan dari kedua pengujian ini menjadi dasar dalam tahap analisis kerentanan serta penyusunan langkah mitigasi keamanan pada sistem SPADA UNTIRTA.

4.5 Hasil Analisis Kerentanan Keamanan

Pada Penelitian ini menganalisis postur keamanan aplikasi web SPADA UNTIRTA melalui tahap *vulnerability identification* dengan dua alat pemindai otomatis, yaitu OWASP ZAP dan Acunetix. Penggunaan dua alat pemindaian ini lazim dilakukan pada studi evaluasi keamanan web karena masing-masing alat memiliki mekanisme deteksi dan bentuk keluaran laporan yang berbeda, sehingga peneliti memperoleh gambaran temuan yang lebih komprehensif [16].

Perbedaan keluaran alat terlihat pada pola pelaporan dan jumlah temuan. Penelitian [16] menunjukkan OWASP ZAP dapat menghasilkan sejumlah alert (misalnya 24 alert), termasuk temuan terkait kekurangan *security header* seperti tidak adanya CSP, sedangkan Acunetix memberikan ringkasan level risiko sistem (misalnya domain berada pada level medium). Temuan tersebut mengindikasikan bahwa penggunaan dua alat pemindai dapat membantu mengamati kelemahan konfigurasi dari sudut pandang pelaporan yang berbeda.

Karena pemindaian otomatis berpotensi menghasilkan false positive, analisis temuan dalam penelitian ini memprioritaskan temuan yang konsisten atau beririsan antar alat dan memiliki bukti artefak yang jelas pada keluaran pemindaian seperti header yang tidak ada, URL file sensitif yang dapat diakses, atau versi TLS yang terdeteksi. Pendekatan kehati-hatian ini sejalan dengan anjuran untuk meninjau ulang alert berkeyakinan lemah guna menekan *false positive* [16].

Berdasarkan komparasi hasil OWASP ZAP dan Acunetix pada SPADA UNTIRTA, penelitian ini merangkum empat temuan utama: (1) *CSP Header Not Set, (2) Hidden File Found (composer.lock dan phpinfo.php), (3) TLS 1.0/1.1 masih aktif, dan (4) Timestamp Disclosure (Unix).* Selanjutnya, setiap temuan dianalisis dari sisi makna keamanan, potensi dampak, dan implikasi perbaikannya.

1. *CSP Header Not Set*

   CSP merupakan mekanisme header yang membatasi sumber konten (misalnya script) yang boleh dieksekusi oleh browser. Ketika CSP tidak diterapkan, risiko serangan XSS meningkat karena browser tidak memiliki kebijakan pembatasan eksekusi script yang eksplisit. [17] menyatakan temuan *"Content Security Policy Header Not Set"* memungkinkan serangan XSS terjadi, sehingga dipandang sebagai celah konfigurasi yang perlu diperbaiki melalui penambahan kebijakan CSP yang sesuai.

2. *Hidden File Found (composer.lock dan phpinfo.php)*

   Temuan *hidden file* menunjukkan adanya file yang seharusnya tidak diekspos ke publik, namun dapat diakses langsung melalui URL. [18] menjelaskan bahwa ketika URL *composer.lock* dapat diakses, file tersebut dapat terunduh dan isinya memuat komponen manajemen dependensi proyek PHP yang menjaga konsistensi versi paket. Informasi dependensi ini berpotensi dimanfaatkan untuk memperkirakan komponen yang digunakan dan mengarahkan pencarian celah pada komponen tersebut, sehingga termasuk isu *information disclosure* akibat publikasi file yang kurang tepat.

   File phpinfo (sering dinamai info.php/phpinfo.php) menampilkan informasi konfigurasi PHP dan lingkungan server. Peneliti [19] mengategorikan kondisi ini sebagai *"PHP Information Disclosure*" dan menekankan bahwa halaman tersebut dapat mengungkap informasi sensitif seperti path, variabel

lingkungan, serta konfigurasi PHP; karena itu direkomendasikan untuk menghapus/menonaktifkan file tersebut dari direktori publik.

3. TLS 1.0/1.1 masih aktif

   Dukungan server terhadap versi TLS lama dipandang sebagai kelemahan kriptografi karena protokol lama memiliki kelemahan/kompatibilitas yang tidak lagi direkomendasikan. [19] menunjukkan kasus server yang masih mendukung TLS 1.0 dan TLS 1.1 dan disebut sebagai masalah yang perlu diperbaiki. Selaras dengan itu, [19] merekomendasikan mitigasi dengan menonaktifkan TLS 1.0 dan TLS 1.1 serta mengaktifkan TLS 1.2 dan TLS 1.3 agar komunikasi terenkripsi menggunakan versi yang lebih aman

4. *Timestamp Disclosure (Unix)*

   Timestamp disclosure merupakan temuan yang menunjukkan keberadaan informasi waktu/timestamp yang dapat terbaca pada response/halaman. [17] menyebut adanya kasus "puluhan ribu *timestamp disclosure*" pada studi website lain, yang mengindikasikan temuan ini dapat muncul masif jika tidak dikendalikan. Pada konteks SPADA UNTIRTA, temuan *timestamp disclosure* dianalisis sebagai informasi teknis tambahan yang sebaiknya diminimalkan karena berpotensi menambah informasi bagi pihak yang melakukan pengumpulan data teknis sistem.

Berdasarkan hasil analisis tiap temuan di atas, tahap selanjutnya adalah memetakan setiap kerentanan ke kategori OWASP Top 10 2021 untuk mengklasifikasikan jenis risiko secara terstruktur serta menjadi dasar penyusunan prioritas mitigasi

Tabel 4 Analisis kerentanan berdasarkan OWASP *Top* 10 Tahun 2021 dan CIA Triad

No	Jenis Kerentanan	Kategori OWASP *Top* 10 (2021)	Tingkat Risiko	Dampak (CIA Triad)	CWE ID
1	*Content Security Policy (CSP) Header Not Set / Not Implemented*	*A05: Security Misconfiguration*	*Medium*	*Integrity*	CWE-693
2	*Hidden File Found (composer.lock, phpinfo.php)*	*A05: Security Misconfiguration*	*Medium*	*Confidentiality*	CWE-200
3	*TLS 1.0 dan TLS 1.1* Masih Aktif	*A02: Cryptographic Failures*	*Medium*	*Confidentiality*	CWE-327

No	Jenis Kerentanan	Kategori OWASP *Top* 10 (2021)	Tingkat Risiko	Dampak (CIA Triad)	CWE ID
4	*Timestamp Disclosure - Unix*	*A05: Security Misconfiguration*	*Low*	*Confidentiality*	CWE-200

Hasil pemindaian menggunakan OWASP ZAP dan *Acunetix Web Vulnerability Scanner* menunjukkan bahwa sistem SPADA UNTIRTA masih memiliki kelemahan yang dominan pada konfigurasi keamanan (*security hardening*) serta mekanisme enkripsi komunikasi. Temuan-temuan ini mengindikasikan bahwa sebagian kontrol keamanan di lapisan *header*, akses file, dan *transport security* belum diterapkan secara optimal.

Kerentanan dengan perhatian utama adalah *Content Security Policy (CSP) Header Not Set* yang dipetakan ke *OWASP Top 10 2021* kategori *A05: Security Misconfiguration*. Ketiadaan *header Content-Security-Policy* membuat browser tidak memiliki aturan pembatasan pemuatan skrip maupun konten dari sumber tertentu. Dalam kondisi ini, apabila terjadi injeksi konten pada sisi aplikasi (misalnya melalui celah input atau integrasi pihak ketiga), peluang terjadinya *Cross-Site Scripting (XSS)* dapat meningkat karena eksekusi skrip menjadi lebih longgar. Dampak utamanya berkaitan dengan Integrity, karena halaman dapat dimanipulasi, serta berpotensi meluas ke *Confidentiality* apabila skrip berbahaya digunakan untuk mengakses informasi pengguna (misalnya token sesi).

Selain itu, teridentifikasi akses publik terhadap file sensitif seperti *composer.lock* dan *phpinfo.php*. Temuan ini juga dipetakan ke *A05: Security Misconfiguration*, karena menunjukkan kontrol akses pada server belum membatasi resource internal yang seharusnya tidak diekspos. File-file tersebut berpotensi mengungkap informasi teknis seperti versi PHP, modul aktif, dependensi aplikasi, hingga petunjuk struktur sistem. Dampak kelemahan ini terutama pada *Confidentiality*, karena informasi internal dapat digunakan untuk mempercepat tahap pengintaian (reconnaissance) dan menyusun serangan lanjutan yang lebih tepat sasaran.

Pada aspek enkripsi komunikasi, hasil pemindaian Acunetix menunjukkan bahwa TLS 1.0 dan TLS 1.1 masih aktif. Temuan ini lebih tepat dipetakan ke *A02: Cryptographic Failures*, karena berkaitan langsung dengan kelemahan kriptografi

pada lapisan transport (versi TLS yang sudah usang dan tidak direkomendasikan). Keberadaan TLS versi lama dapat meningkatkan risiko serangan seperti *downgrade* atau intersepsi komunikasi dalam kondisi tertentu. Dampaknya paling kuat pada *Confidentiality*, karena data yang ditransmisikan berisiko lebih mudah disadap, dan pada skenario tertentu dapat memengaruhi Integrity apabila lalu lintas dapat dimodifikasi.

Sementara itu, *Timestamp Disclosure (Unix*) dipetakan ke *A05: Security Misconfiguration* karena termasuk bentuk *information disclosure* yang muncul dari konfigurasi *header/response* server yang terlalu terbuka. Walaupun tingkat risikonya rendah, informasi waktu sistem yang terekspos dapat membantu penyerang menganalisis pola aktivitas layanan, memperkirakan waktu pembaruan sistem, atau menyelaraskan rangkaian pengujian pada tahap *reconnaissance*. Dampaknya terutama terhadap *Confidentiality* karena memberikan petunjuk teknis yang seharusnya tidak perlu tersedia bagi publik.

Secara keseluruhan, hasil analisis menunjukkan bahwa kelemahan paling dominan pada SPADA UNTIRTA berada pada *A05: Security Misconfiguration,* diikuti oleh *A02: Cryptographic Failures* pada lapisan komunikasi. Mayoritas temuan berkorelasi dengan dampak pada *Confidentiality* dan *Integrity*, sehingga risiko utama yang perlu diantisipasi adalah kebocoran informasi teknis/konfigurasi serta potensi manipulasi konten dan data akibat kontrol keamanan yang belum cukup ketat.

4.6 Evaluasi Mitigasi Kerentanan Keamanan

Berdasarkan hasil analisis sebelumnya, setiap kerentanan yang ditemukan pada sistem SPADA UNTIRTA memiliki langkah perbaikan yang dapat dilakukan agar sistem menjadi lebih aman. Langkah-langkah mitigasi berikut disusun berdasarkan hasil pengujian serta praktik keamanan web yang umum digunakan untuk menjaga aspek Confidentiality, Integrity, dan Availability (CIA Triad).

Tabel 5 Rekomendasi mitigasi kerentanan keamanan untuk meningkatkan keamanan Web SPADA UNTIRTA

No	Jenis Kerentanan	Dampak CIA Triad	Mitigasi
1	*Content Security Policy (CSP) Header Not Set / Not Implemented*	*Integrity*	- Pastikan bahwa server web, server aplikasi, load balancer, dan sebagainya dikonfigurasi untuk menetapkan *Content-Security-Policy.* - Terapkan header *Content-Security-Policy (CSP)* dengan aturan ketat seperti *default-src 'self'; script-src 'self'.* - Lakukan validasi input di sisi server untuk mencegah injeksi skrip berbahaya. - Tambahkan header keamanan tambahan seperti *X-XSS-Protection dan X-Frame-Options* untuk memperkuat keamanan browser [12].
2	*Hidden File Found (composer.lock, phpinfo.php)*	*Confidentiality*	- Pertimbangkan apakah komponen tersebut benar-benar diperlukan dalam lingkungan produksi. Jika tidak diperlukan, nonaktifkan komponen tersebut. Namun, jika diperlukan, pastikan akses terhadapnya memerlukan autentikasi dan otorisasi yang sesuai, atau batasi aksesnya hanya untuk sistem internal atau alamat IP tertentu, dan sebagainya. - Hapus file sensitif dari direktori publik atau pindahkan ke lokasi non-web accessible. - Gunakan file .htaccess atau konfigurasi server untuk menolak akses ke direktori internal. - Lakukan pemeriksaan keamanan rutin untuk mendeteksi file publik yang tidak seharusnya tersedia [20].
3	*TLS 1.0 dan TLS 1.1* Masih Aktif	*Confidentiality*	- Nonaktifkan dukungan TLS 1.0 dan 1.1, gunakan minimal TLS 1.2 atau TLS 1.3. - Gunakan sertifikat SSL/TLS valid yang diperbarui secara berkala dan mendukung enkripsi kuat. - Terapkan HTTP Strict Transport Security (HSTS) untuk memaksa koneksi terenkripsi [21].
4	*Timestamp Disclosure - Unix*	*Confidentiality*	- Nonaktifkan atau hapus informasi waktu sistem dari HTTP header melalui konfigurasi server.

No	Jenis Kerentanan	Dampak CIA Triad	Mitigasi
			- Gunakan pesan error generik agar detail sistem tidak ditampilkan ke pengguna. - Lakukan server hardening dengan menonaktifkan versi dan waktu sistem dari halaman publik [7].

Berdasarkan hasil evaluasi yang telah dilakukan, dapat disimpulkan bahwa setiap kerentanan yang ditemukan pada sistem SPADA UNTIRTA memiliki tingkat risiko yang berbeda-beda, namun semuanya tetap perlu ditangani dengan serius. Langkah-langkah mitigasi yang diterapkan tidak hanya sebatas pada perbaikan teknis, tetapi juga mencakup pembenahan kebijakan keamanan dan peningkatan kesadaran pengelola sistem terhadap pentingnya perlindungan data.

Penerapan *Content-Security-Policy (CSP)* menjadi hal yang sangat penting karena berfungsi sebagai lapisan pelindung utama terhadap potensi serangan *Cross-Site Scripting (XSS)*. Penghapusan file-file sensitif seperti phpinfo.php dan composer.lock juga harus dilakukan agar informasi konfigurasi internal tidak dapat diakses oleh pihak luar. Selain itu, pembaruan protokol enkripsi dengan menonaktifkan TLS 1.0 dan TLS 1.1 wajib dilakukan agar komunikasi antara pengguna dan server tetap aman dari risiko penyadapan data.

Mitigasi terhadap celah seperti Timestamp Disclosure memang terlihat sederhana, namun tetap penting untuk mencegah pengungkapan pola aktivitas server yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab. Semua tindakan ini tidak bisa dilakukan sekali saja, melainkan harus menjadi bagian dari proses pemeliharaan keamanan yang berkelanjutan, seperti audit rutin, pemantauan sistem secara periodik, serta pelatihan bagi administrator dalam menerapkan praktik keamanan yang benar.

Dengan diterapkannya berbagai langkah tersebut secara konsisten, sistem SPADA diharapkan dapat lebih terlindungi dari ancaman yang berpotensi merusak data dan mengganggu integritas informasi. Evaluasi mitigasi ini juga memberikan gambaran menyeluruh tentang area mana yang paling rentan dan perlu menjadi prioritas utama dalam penguatan keamanan ke depan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap sistem SPADA UNTIRTA maka dapat disimpulkan beberapa hal sebagai berikut:

1. Berdasarkan hasil pemindaian dan analisis, ditemukan empat jenis kerentanan keamanan pada sistem SPADA UNTIRTA, terdiri atas tiga kerentanan dengan tingkat risiko Medium dan satu kerentanan dengan tingkat risiko Low. Kerentanan yang teridentifikasi meliputi *Content Security Policy (CSP) Header Not Set, Hidden File Found (composer.lock dan phpinfo.php),* TLS 1.0 dan TLS 1.1 masih aktif, serta *Timestamp Disclosure (Unix).* Temuan ini menunjukkan bahwa kelemahan sistem lebih banyak disebabkan oleh pengaturan konfigurasi keamanan web dan hardening server yang belum optimal, terutama pada pengelolaan header keamanan dan pembatasan akses file internal. Berdasarkan pemetaan ke OWASP *Top* 10 tahun 2021, temuan *CSP Header Not Set, Hidden File Found, dan Timestamp Disclosure (Unix)* termasuk dalam kategori *A05: Security Misconfiguration*, karena berkaitan dengan konfigurasi keamanan yang kurang ketat dan adanya informasi/komponen yang terekspos ke publik. Sementara itu, temuan TLS 1.0 dan TLS 1.1 masih aktif dipetakan ke *A02: Cryptographic Failures* karena terkait langsung dengan penggunaan protokol enkripsi yang sudah usang dan berpotensi melemahkan keamanan komunikasi. Dengan demikian, hasil penelitian menegaskan bahwa area prioritas perbaikan berada pada pengetatan konfigurasi keamanan (A05) dan penguatan enkripsi komunikasi (A02) untuk menurunkan risiko kebocoran informasi serta potensi penyalahgunaan celah pada layanan.

2. Berdasarkan tingkat risikonya, tidak ditemukan kerentanan dengan kategori *High Severity*. Dari total empat temuan, tiga kerentanan (75%) tergolong *Medium* dan satu kerentanan (25%) tergolong *Low*. Kerentanan dengan tingkat risiko *Medium* memiliki potensi berdampak langsung terhadap aspek

Confidentiality dan Integrity, karena dapat menyebabkan kebocoran informasi sensitif, penyadapan data, atau manipulasi konten web. Sementara itu, kerentanan dengan tingkat risiko *Low*, yaitu *Timestamp Disclosure*, memiliki dampak terbatas namun tetap berpotensi dimanfaatkan untuk mengumpulkan informasi teknis mengenai sistem. Tidak ditemukan celah yang secara langsung memengaruhi aspek *Availability*, sehingga layanan SPADA masih dapat berjalan, meskipun terdapat risiko terhadap keamanan data dan integritas informasi.

3. Langkah mitigasi yang direkomendasikan untuk mengatasi temuan tersebut meliputi penerapan *Content-Security-Policy (CSP)* dengan konfigurasi yang tepat untuk mencegah serangan *Cross-Site Scripting (XSS)*, penghapusan file sensitif dari direktori publik untuk mencegah kebocoran informasi server, serta penonaktifan protokol TLS 1.0 dan 1.1 guna memastikan komunikasi data terenkripsi dengan aman. Selain itu, disarankan untuk menghapus informasi *timestamp dari header HTTP*, melakukan audit keamanan secara berkala dan memperbarui sertifikat enkripsi secara rutin

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, penulis memberikan beberapa saran sebagai berikut:

1. Untuk pengelola sistem SPADA UNTIRTA:

   Pengelola web SPADA disarankan untuk segera memperbaiki pengaturan keamanan sistem. Langkah yang bisa dilakukan antara lain dengan menambahkan *Content-Security-Policy (CSP)* untuk mencegah penyisipan skrip berbahaya, menghapus file sensitif seperti *phpinfo.php* dan *composer.lock* dari folder publik agar tidak bisa diakses orang luar, serta menonaktifkan protokol lama TLS 1.0 dan 1.1 dan menggantinya dengan versi terbaru seperti TLS 1.2 atau 1.3 agar data pengguna lebih aman. Selain itu, perlu dilakukan pemeriksaan keamanan secara rutin menggunakan alat seperti OWASP ZAP dan Acunetix, serta memberikan pelatihan dasar keamanan web bagi pengelola dan pengembang sistem supaya kesadaran terhadap pentingnya keamanan data bisa meningkat.

2. Untuk penelitian selanjutnya:

Dapat dilakukan pengujian lanjutan dengan metode berbeda, seperti NIST SP 800-115 dan Penelitian ini masih terbatas pada penggunaan dua alat pengujian, yaitu OWASP ZAP dan Acunetix. Peneliti selanjutnya disarankan untuk menggunakan lebih banyak alat uji, seperti Burp Suite atau Nessus, agar hasil pengujian lebih lengkap dan akurat. Selain itu, penelitian berikutnya dapat menambahkan uji coba serangan secara langsung (penetration testing) untuk melihat sejauh mana sistem mampu menahan serangan. Peneliti juga bisa meneliti aspek ketersediaan sistem (Availability) agar tidak hanya fokus pada kerahasiaan dan integritas data, tetapi juga pada kemampuan sistem dalam tetap berfungsi meskipun terjadi gangguan.

DAFTAR PUSTAKA

[1] W. A. S. & Hootsuite, “Digital 2024 Indonesia.” [Online]. Available: https://wearesocial.com/id/blog/2024/01/digital-2024/

[2] AwanPintar.id, “Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2024,” AwanPintar.id. [Online]. Available: https://www.awanpintar.id/wp-content/uploads/2024/08/2024_AwanPntar.id_Laporan_Ancaman_Digital_sem1_2024_Green.pdf

[3] T. Anugrah, “Penetration Testing Keamanan Website Stie Samarinda Menggunakan Teknik SQL Injection Dan XSS,” *Jurnal Informatika Dan Teknik Elektro Terapan*, vol. 12, no. 1, 2024, doi: 10.23960/jitet.v12i1.3882.

[4] R. Medical. et. RSIS, “Laporan Tahunan Laporan Tahunan,” pp. 1–91, 2024.

[5] L. M. Zagi, G. P. Digdo, and W. Shalannanda, “Just Dork and Crawl: Measuring Illegal Online Gambling Defacement in Indonesian Websites,” 2025, [Online]. Available: http://arxiv.org/abs/2508.19368

[6] Haeruddin, Gautama Wijaya, H. Winata, Sukma Aji, and Muhammad Nur Faiz, “Website Security Analysis Using Vulnerability Assessment Method (Case Study: Universitas Internasional Batam),” *Journal of Innovation Information Technology and Application (JINITA)*, vol. 6, no. 2, pp. 173–180, 2024, doi: 10.35970/jinita.v6i2.2476.

[7] D. Rohmaniah, W. M. Ashari, L. Lukman, and A. D. Putra, “Enhancing Website Security Using Vulnerability Assessment and Penetration Testing (VAPT) Based on OWASP Top Ten,” *Journal of Applied Informatics and Computing*, vol. 9, no. 2, pp. 404–411, 2025, doi: 10.30871/jaic.v9i2.9069.

[8] W. A. Tya, “Uji Kerentanan Pada Website Menggunakan Open Web Application Security Project (OWASP) Top 10 Tahun 2021 Studi Kasus (Domain uinjkt.ac.id),” 2023. [Online]. Available: https://repository.uinjkt.ac.id/dspace/bitstream/123456789/75009/1/WAHYU ADI TYA-FST.pdf

[9] D. Fata, “Evaluasi risiko celah keamanan menggunakan metodologi open web application security project (OWASP) pada aplikasi web sistem informasi akademik (SIAKAD) UIN Ar-Raniry,” 2023. [Online]. Available: https://repository.ar-raniry.ac.id/id/eprint/31189/%0Ahttps://repository.ar-raniry.ac.id/id/eprint/31189/1/Tugas Akhir - Darul Fata %28180705016%29.pdf

[10] M. R. Syaifudin, M. A. Murtadho, M. S. Wafa, and M. Masrur, “Analisis Keamanan Website Kampus UNIPDU Melalui Metode Vulnerability Assessment (VA) dengan Menggunakan Tools Acunetix UNIPDU Campus

Website Security Analysis Through Vulnerability Assessment (VA) Metho," *KOMPUTA : Jurnal Ilmiah Komputer dan Informatika*, vol. 14, no. 1, pp. 7–12, 2025, doi: 10.34010/komputa.v14i1.

[11] A. A. Zahrani, D. S. Alifah, Y. Cahyani, and I. Albana, "Analisis Vulnerability Assessment pada Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP," 2025.

[12] F. Widianto, E. S. Wijaya, H. Harjono, and A. P. Wicaksono, "Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 1, pp. 155–166, 2025, doi: 10.52436/1.jpti.609.

[13] A. I. Rafeli, H. B. Seta, and I. W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ," *Informatik : Jurnal Ilmu Komputer*, vol. 18, no. 2, p. 97, 2022, doi: 10.52958/iftk.v18i2.4632.

[14] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[15] M. A. Saputra, Dio Wahyu, Risqy Siwi Pradini, "Analisis dan Rekomendasi Keamanan Website Kampus X," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi (JIMIK)*, vol. 6, no. 1, pp. 830–843, 2025.

[16] M. Z. Febriansyah and A. Teddyyana, "ANALISA DAN PERBAIKAN KEAMANAN PADA WEBSITE SDN 9," vol. 7, no. 2, pp. 65–78, 2025.

[17] A. A. R. Syahrul Dwi Hilda, Nono Heryana, "Analisis Keamanan Website Pemerintah Desa Curug Menggunakan Open Web Application Security Project (Owasp)," *The Indonesian Journal of Computer Science*, vol. 13, no. 2, 2024.

[18] S. S. Anelia, J. Jayanta, and B. Hananto, "Uji Penetrasi Server Universitas PQR Menggunakan Metode National Institute Of Standards And Technology (NIST SP 800-115)," *Jurnal Ilmu Teknik dan Komputer*, vol. 7, no. 1, p. 34, 2023, doi: 10.22441/jitkom.2023.v7i1.005.

[19] Muh. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *Jurnal Media Informatika Budidarma*, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.

[20] V. Issue, "JUTIN : Jurnal Teknik Industri Terintegrasi Analisis Kerentanan Keamanan pada Website Kelurahan Rimba Sekampung dengan

Menggunakan Framework OWASP ZAP," vol. 8, no. 4, 2025, doi: 10.31004/jutin.v8i4.48523.

[21] S. Hebrok *et al.*, "We Really Need to Talk About Session Tickets: A Large-Scale Analysis of Cryptographic Dangers with TLS Session Tickets," *32nd USENIX Security Symposium, USENIX Security 2023*, vol. 7, pp. 4877–4894, 2023.

LAMPIRAN

Lampiran 1 Detail hasil scanning menggunakan OWASP ZAP

ZAP by Checkmarx Scanning Report

Site: https://spada.untirta.ac.id

Generated on Wed, 29 Oct 2025 02:03:44

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	1
Informational	2

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Hidden File Found	Medium	2
Timestamp Disclosure - Unix	Low	1
Modern Web Application	Informational	1
User Agent Fuzzer	Informational	108

Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://spada.untirta.ac.id/
Method	GET
Attack	
Evidence	
Other Info	

URL	https://spada.untirta.ac.id/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://spada.untirta.ac.id/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Hidden File Found
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://spada.untirta.ac.id/composer.lock
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	composer
URL	https://spada.untirta.ac.id/phpinfo.php
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	phpinfo
Instances	2
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

CWE Id	538
WASC Id	13
Plugin Id	40035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://spada.untirta.ac.id/
Method	GET
Attack	
Evidence	1761717489
Other Info	1761717489, which evaluates to: 2025-10-29 01:58:09.
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically
URL	https://spada.untirta.ac.id/
Method	GET
Attack	
Evidence	<script>(function(){window._cf_chl_opt = {cvId: '3',cZone: 'spada.untirta.ac.id',cType: 'managed' aNvAsKq3Q9MDZmNcRV4uuYFj43EUWG9AKe_sXeiFTt',cUPMDTk:"/?__cf_chl_tk=eZakXC2 __cf_chl_f_tk=eZakXC2aBRd7rKpzaWbVr38hnVehat1eeoldKi7Ak0c-1761717489-1.0.1.1-DdyE TtLfldxvhq6lo_bnszleLcwEmqA8ellFrXZxu6lKMsmq3f4QLMnxN0SZeU200Yg8KpheaKee0MBV mFE7Rwl3eDtVtdaev_eQhEdskIzL0SX81wRON74FmOkpVAo8ujymQFEe1oo2ubewiq1JgU0V fzH1z5Y4SOCl5b_NQy_eb1ILmUF10ip1ryDTVQBvX4I6oYfBwposraYx8FN142SrbQe1xECFB2 EDBuxBYvVwtsoAv8z3Ng8ZsyUxBbhCVfEzgheZMIYCMmgDRsfegjPHUZgzXzJSEsH_WPrzQ GWxPEa8ViCvpG5rtVFVTyiZfFcNWMZqMvkRVoodX8bJR5XYDR.bz_ycHcJwaijkYQvcRBfcCV HUTwZTmZTaEpJdca04Gthz5hFAM0qGNd30p2PpctStFH0DW74eR0JIGnQAROsE8XCman71 uJcduBUjDBVDG4el9KqU94b6Ln2n8cog2U9MPsopGA5a4kMjJPmrwZdgmBEXpDFz5JihT.nY3 Eu9jl8p7yunr_Rc1kodxG0SUol10nsdrJ8edsnFFcaMeSKFCp6nqMLTG_kPEPmX7LX3nQiLvUp 8IhwBDkP7wXd4imC3WBEKzyMwhwpdaDR7LqTDxg9xWmMEYj42o6UaipiXHbK482R7LuQFa G6VGeo9VNDmvPSJOlHXYS0llIZ32q9dgQet6bCZYVEBHlqY49DSgcPMh5D92jUM0TS6EhHl aQriRkwZ0tnzmXNMemM9iLy3uCPnfdRgDgTZ_N3Oxa5X0u0R2gbh1oPEZd2qWFpvRNWpoL nke1ND2NVARktVavQ6bihriga32QJ3KHEBWO1NTRNq4RIgROf4cj7Hy924EcDqW_NxWLt3Hj frMPF8u0fONWoowvbUs92Fi4imlfTwBhbXe6QRLVg5J7Eo6I.3IGeBeK3kNAQOxm91Z3vwT22 OTPqV6cPjZYDXot6uak6fOZEAQMYBcvDb8QwAq0RLsC0_K8Ct85GRBug0CPjxZwd68osOXE 1FBBqXfl5Xo86pwJSx_MXM3VP6FZVN.d1MqF17iQ_jPleGcZ4Gd4kAp4LHgFUY4awPg. h7MBE9HMdz3ueDtZWaIG_g3FHGH_E7lHmUjyaW_Omb3cmegdFaLjbagqtbURYM3H8WadZ naREx_2EYrETpRiRpy5uc5zCbATCwtlMhmMzSwSeNInm14cQRYVrJ0LbVF05OLNWvcwkEZ 0UsCtyPDsiLZLOqQTKMym1B02pmV6CY_qXrFK_UHwVxUguJloVY73jrhkFhppmLBo1mqVOr platform/h/b/orchestrate/chl_page/v1?ray=996070853a08cecf';window._cf_chl_opt.cOgUHash = _cf_chl_opt.cOgUHash.length).indexOf('?') !== -1 ? '?' : location.search;if (window.history && wi __cf_chl_rt_tk=eZakXC2aBRd7rKpzaWbVr38hnVehat1eeoldKi7Ak0c-1761717489-1.0.1.1-Ddy appendChild(a);}());</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
Instances	1
Solution	This is an informational alert and so no changes are required.

Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://spada.untirta.ac.id
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Lampiran 2 Detail hasil scanning menggunakan Acunetix web vulnerability scanner

Scan of spada.untirta.ac.id

Scan details

Scan information	
Start time	29/10/2025, 04:25:36
Start url	https://spada.untirta.ac.id/
Host	spada.untirta.ac.id
Scan time	3 minutes, 9 seconds
Profile	Full Scan
Server information	cloudflare
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	4
High	0
Medium	1
Low	0
Informational	3

Affected items

Web Server	
Alert group	**TLS 1.0 enabled**
Severity	Medium
Description	The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.
Alert variants	
Details	The SSL server (port: 443) encrypts traffic using TLSv1.0.

Web Server	
Alert group	**Content Security Policy (CSP) not implemented**
Severity	Informational

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
	
	Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:
	
	`Content-Security-Policy:`
	`  default-src 'self';`
	`  script-src 'self' https://code.jquery.com;`
	
	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	

```
GET / HTTP/1.1
Referer: https://spada.untirta.ac.id/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: spada.untirta.ac.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Reverse proxy detected**
Severity	Informational
Description	This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.
Recommendations	None
Alert variants	
Details	Detected reverse proxy: CloudFlare

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: spada.untirta.ac.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**TLS 1.1 enabled**
Severity	Informational
Description	The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time or writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.
Alert variants	
Details	The SSL server (port: 443) encrypts traffic using TLSv1.1.

Lampiran 3 Surat Izin Penelitian

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS SULTAN AGENG TIRTAYASA
FAKULTAS TEKNIK
Jalan Jendral Sudirman Km. 03 Kota Cilegon Provinsi Banten
Laman : www.ft.untirta.ac.id, email: ft@untirta.ac.id

Nomor : 1823/UN.43.3.7/KT/ 2025 05 November 2025
Lampiran :
Hal : Permohonan Penelitian Tugas Akhir / Skripsi

Kepada Yth,
UPATIK Universitas Sultan Ageng Tirtayasa

Di
Serang

Sehubungan dengan rencana Penyusunan Tugas Akhir/Skripsi/Tesis/Disertasi bagi mahasiswa kami, dengan ini mengajukan permohonan tempat penelitian di Perusahaan/Lembaga yang Bapak/Ibu pimpin.

Adapun data mahasiswa yang bersangkutan adalah sebagai berikut.

Nama	:	MUHAMMAD FADHIL PUTRA
NIM	:	3337210065
Fakultas	:	TEKNIK
Jurusan/Program Studi	:	Informatika
Semester	:	Ganjil
Telepon / HP	:	089631801308
Durasi (Lama Penelitian)	:	1 Minggu
Rencana Topik	:	"Analisis Kerentanan Web SPADA UNTIRTA"

Demikian permohonan kami sampaikan atas kerjasamanya dan perhatian Bapak/Ibu kami ucapkan terima kasih.

Wakil Dekan I

Dr. Ir. Bobby Kurniawan, ST., MT.
NIP. 197612132008121001

Tembusan :

- Ketua Program Studi Informatika