Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang

Aldo Fajarino[1], Yesi Novaria Kunang[2], Hendra Marta Yudha[3], Edi Surya Negara[4], Nita Rosa Damayanti[5]

[1,2,4,5]Prodi Magister Teknik Informatika, Universitas Bina Darma Palembang, Indonesia
[3]Prodi Teknik Elektro, Universitas Tridinanti Palembang, Indonesia
e-mail: alfajarino@gmail.com[1], yesinovariakunang@binadarma.ac.id[2], hendramy@univ-tridinanti.ac.id[3], e.s.negara@binadarma.ac.id[4], nita_rosa@binadarma.ac.id[5]

Abstract

As one of the universities in Palembang City, XYZ University has its own web server that functions as an information system in the academic and financial activities of its users. Testing of security systems on information systems needs to be done, web server security is very important to avoid destruction, data theft, data manipulation, and so on. In this study, the OWASP framework and the ISSAF framework were used and then the two methods were compared. The results of this study found several security holes that have been recommended to developers and successfully repaired. There needs to be a comprehensive improvement starting from server configuration, sanitization improvement of character input filters from users, installation of Intrusion Detection System and Intrusion Prevention System.

Keywords*: framework, OWASP, ISSAF, web security, vulnerability*

Abstrak

Sebagai salah satu perguruan tinggi di Kota Palembang, Universitas XYZ telah memiliki server web sendiri yang berfungsi sebagai sistem informasi dalam kegiatan akademik dan keuangan penggunanya. Pengujian terhadap sistem keamanan pada sistem informasi perlu dilakukan, keamanan server web adalah hal yang sangat penting untuk mencegah terjadinya perusakan, pencurian data, manipulasi data, dan lain sebagainya. Dalam penelitian ini digunakan framework OWASP dan framework ISSAF yang kemudian kedua metode tersebut dikomparasi. Hasil dari penelitian ini ditemukan beberapa celah keamanan yang telah direkomendasikan ke pengembang dan berhasil diperbaiki. Perlu ada perbaikan secara menyeluruh mulai dari konfigurasi server, perbaikan sanitasi filter input karakter dari user, pemasangan Intrusion Detection System dan Intrusion Prevention System.

Kata kunci*: framework, OWASP, ISSAF, web security, vulnerability*

1. PENDAHULUAN

Universitas XYZ Palembang adalah lembaga pendidikan di Kota Palembang yang telah menerapkan beberapa sistem informasi, baik berbasis website maupun desktop, masalah yang terjadi saat ini yaitu sistem keamanan web server belum pernah diuji. Pengujian sangat penting untuk mengetahui apakah suatu web server aman dari kejahatan yang dilakukan oleh penyerang. Menyikapi permasalahan yang terjadi sekarang ini mengharuskan untuk mampu menutupi celah keamanan tersebut serta melindungi seluruh data yang dimilikinya agar dapat mengindari hal-hal yang tidak diinginkan seperti perusakan *web server*, pencurian data, manipulasi data, ataupun menghapus data yang dilakukan oleh penyerang yang tidak bertanggung jawab. Adapun tujuan penelitian adalah untuk mengevaluasi dan meningkatkan keamanan sistem *web server* Universitas XYZ Palembang, dapat

membantu *programmer* dalam identifikasi celah keamanan yang ada agar dapat segera ditutup dan ditanggulangi celah keamanan tersebut.

Framework merupakan *platform* yang menyediakan kerangka kerja mengklasifikasi suatu masalah juga menyediakan standar yang dapat dibangun, menyediakan fungsionalitas spesifik sebagai bagian dari platform *software* yang lebih besar untuk memberikan fasilitas *develop* aplikasi, produk, dan solusi perangkat lunak [1]. Pada penelitian ini, penulis menggunakan kombinasi dari *framework Open Web Application Security Project (OWASP)* yang berfokus dalam memperbaiki keamanan *software* aplikasi dan *framework Information System Security Assessment Framework (ISSAF)* yang melakukan evaluasi keamanan pada sebuah jaringan komputer, sistem, maupun suatu aplikasi. Penelitian sebelumnya terkait dengan keamanan *server* dilakukan oleh Rezshal Hidayah, Penelitian bertajuk "*Hardening* Web Aplikasi Dengan Menggunakan *OWASP Security Testing Guide (WSTG)* Pada *Website* ABC" dilakukan tahun 2021, menjelaskan bahwa penelitian ini menggunakan metodologi *OWASP* untuk mendeteksi kerentanan pada *website* ABC dengan menggunakan tiga teknik yaitu *crawling,* validasi data dan pengujian sisi client dan pengujian penetrasi tidak dilakukan secara keseluruhan karena hanya menggunakan metode *OWASP TOP 10* [2].

2. METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan menerapkan langkah studi literatur, pengumpulan data objek, uji penetrasi *web server* menggunakan *framework ISSAF*, *framework OWASP*, analisa dan pelaporan, kemudian komparasi *framework*. Langkah penelitian yang dilakukan adalah sebagai berikut.

2.1. Studi Literatur

Langkah awal penelitian adalah mencari berbagai sumber data pustaka, mulai dari *framework ISSAF* beserta tahapannya yaitu Pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, penetrasi, peningkatan akses dan hak istimewa, enumerasi lebih lanjut, kompromi pengguna jarak jauh, mempertahankan akses, dan menutupi jejak. [3] Selanjutnya kerangka *OWASP* mencakup *Reconaissannce* atau pengintaian, analisis, eksploitasi, mempertahankan akses, dan pelaporan atau *reporting.* [4]

2.2. Pengumpulan Data

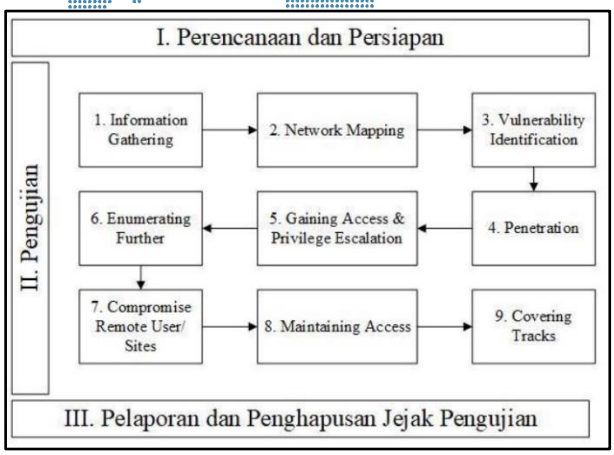
Langkah pengumpulan data dalam penelitian ini adalah dengan mengumpulkan data observasi *web server* dan wawancara *web developer*. Data yang didapat kemudian menjadi acuan untuk melakukan penetrasi menggunakan beberapa tools. Beberapa jenis serangan yang biasa ditemukan pada *server website* seperti *Cross Site Scripting (XSS)* dan Injeksi SQL juga diterapkan ke halaman inputan user sebagai percobaan awal secara manual.

2.3. Kerangka *Information System Security Assessment Framework (ISSAF)*

Metode *ISSAF* memiliki beberapa langkah penilaian yang terdiri dari 3 fase pengujian yang meliputi perencanaan dan persiapan, pengujian, pelaporan serta

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

menghapus jejak pengujian [5]. Adapun tahapan-tahapan dalam *framework ISSAF* terlihat pada gambar berikut.

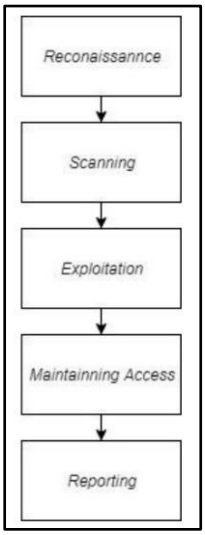


Gambar 1. Tahapan Kerangka *ISSAF*

Langkah pertama yaitu pengumpulan informasi tentang server menggunakan tools *Whois Domain* dan *SSL Scan,* kemudian dilakukan *network mapping* dengan ZenMap, Identifikasi kerentanan dan *penetrasi network* dengan LOIC dan acunetix, kemudian tahapan *gaining access & privilege escalation* sampai dengan *covering tracks,* percobaan penanaman *webshell* menggunakan tools SQLMap dan BurpSuite*.*

2.4. Kerangka *Open Web Application Security Project (OWASP)*

Metode *OWASP* adalah kerangka kerja yang bersifat *open source* dan berfokus pada perbaikan kemanan *software* atau program aplikasi. Dibangun oleh sebuah organisasi bertujuan untuk menemukan celah keamanan dalam sebuah aplikasi web. [6] Adapun tahapan-tahapan dalam framework *OWASP* dapat dilihat dalam gambar berikut.

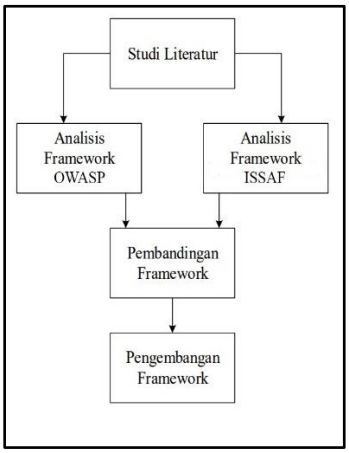


Gambar 2. Tahapan Kerangka *OWASP*

Menurut standar yang dari terapkan pada *OWASP,* terdapat beberapa langkah yang dapat dilakukan untuk memberikan penilaian serta menguji keamanan pada sebuah *server web*, yaitu *Reconaissannce*, *Scanning, Exploitation, Maintaining Access,* dan *Reporting*. [7] Tools yang dipakai dalam metode *OWASP* yaitu *OWASP ZAP*, *web browser*, dan Dirb.

2.5. Pembandingan *Framework*

Dalam melakukan pembandingan *framework*, peneliti menggunakan pendekatan yang ditulis oleh Nadya yang berjudul Pengembangan Kerangka Kerja Arsitektur Enterprise [8]. Adapun langkah pembandingan yang dilakukan dapat terlihat pada gambar berikut ini.



Gambar 3. Pembandingan *Framework*

Komparasi *framework* atau membandingkan hasil adalah langkah yang dilakukan dalam pengembangan *framework*, kekurangan dari *framework OWASP* akan ditutupi dengan kelebihan dari *framework ISSAF* begitupun sebaliknya, semua tahapan masing-masing kerangka kerja dilakukan agar jenis serangannya lengkap.

3. HASIL DAN PEMBAHASAN

Pada bagian ini disampaikan hasil pengujian terhadap data yang telah didiagnosa sebelumnya kemudian dilakukan penetrasi menggunakan masing-masing *framework.*

3.1. Uji Penetrasi dengan *Framework ISSAF*

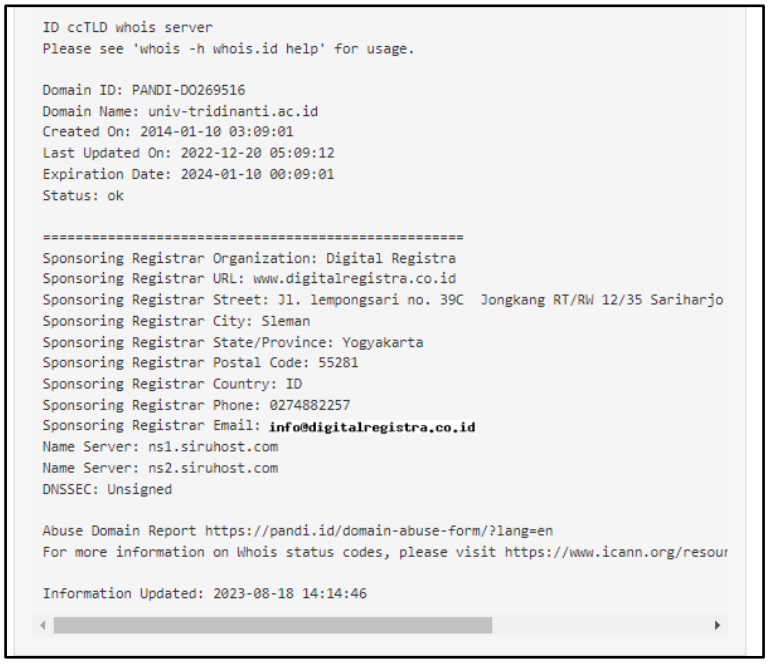
Adapun tahapan pengujian dan tools yang digunakan menggunakan metode *ISSAF* dapat terlihat pada tabel berikut :

Tabel 1. Penerapan *Framework ISSAF*

No	Tahapan dan langkah	*Source*	Tools yang digunakan
1	Pengumpulan Informasi	*Domain Info* *SSL (Secure Socket Layer)*	Whois Domain, SSL Scan SSL Scan
2	Pemetaan *Network*	*Network Information*	Zen Map

No	Tahapan dan langkah	*Source*	Tools yang digunakan
3	Identifikasi *Vulnerability*	*Web Scanner Vulnerability (WSV)*	Acunetix
4	*Penetration*	DoS Attack XSS (Cross Site Scripting)	Low Orbit Ion Canon (LOIC), Acunetix
5	*Gaining Access & Privilege Escalation*	*SQL Injection*	SQL Map
6	*Enumerating Further*	*Database Fetching*	SQL Map
7	*Compromise Remote User*	*Web Shell Injection*	Burp Suite, SQL Map
8	*Maintaining Access*	*Elevated Rights, Permission*	SQL Map
9	*Covering Tracks*	*Access Log Control*	Burp Suite, Shell

A. Pengumpulan Informasi *(Information Gathering)*

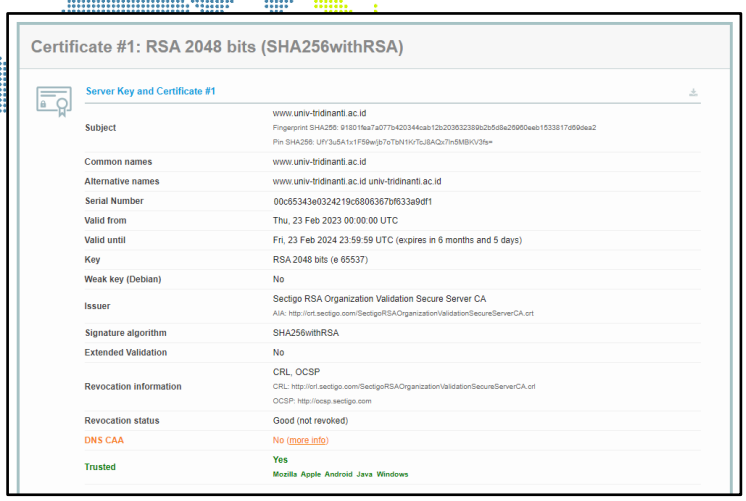


Gambar 4. *Whois Domain*

Tabel 2. *Whois Domain* Universitas Tridinanti

Domain univ-tridinanti.ac.id	
Domain ID	PANDI-DO269615
Nama Domain	univ-tridinanti.ac.id
Dibuat	10 Januari 2014
Expiration Date	10 Januari 2024
Status	OK

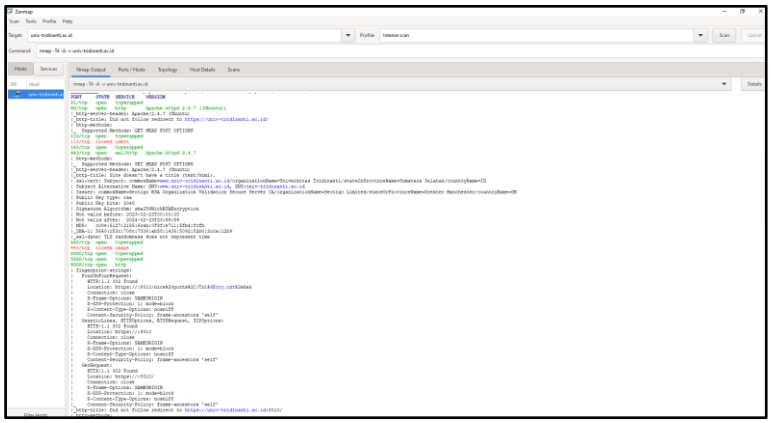
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 5. Hasil *SSL Scan*

Hasil pencarian ditemukan bahwa *domain* univ-tridinanti.ac.id terdaftar oleh PANDI dengan ID PANDI-DO269615 *domain* univ-tridinanti.ac.id, didaftarkan di tahun 2014, berakhir pada tahun 2024 dan statusnya OK serta *SSL Scan* menunjukkan bahwa domain univ-tridinanti.ac.id telah menggunakan *SSL*.

B. Pemetaan *(Network Mapping)*



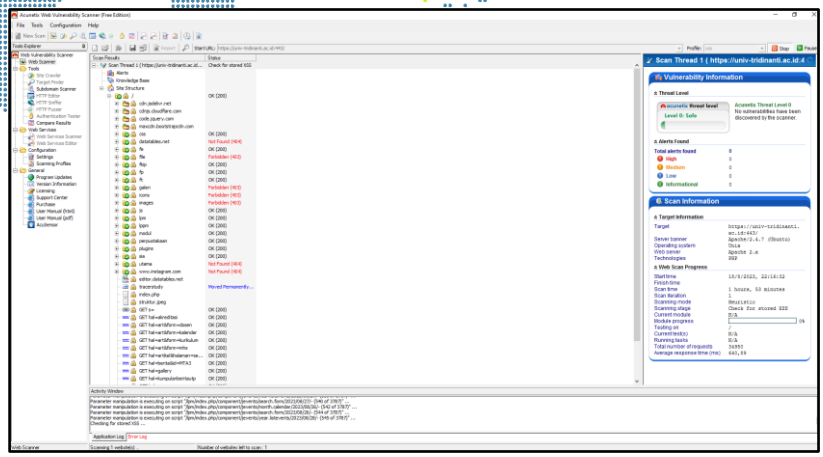
Gambar 5. *Network Mapping*

Tabel 3. *Status Port Domain* Universitas Tridinanti

Domain univ-tridinanti.ac.id		
Port	*Status*	*Services*
21	*Open*	*tcpwrapped*
80	*Open*	*http*
443	*Open*	*ssl/http*
110	*Open*	*tcpwrapped*
113	*Closed*	*ident*
445	*Open*	*tcpwrapped*
993	*Closed*	*imaps*
8008	*Open*	*http*

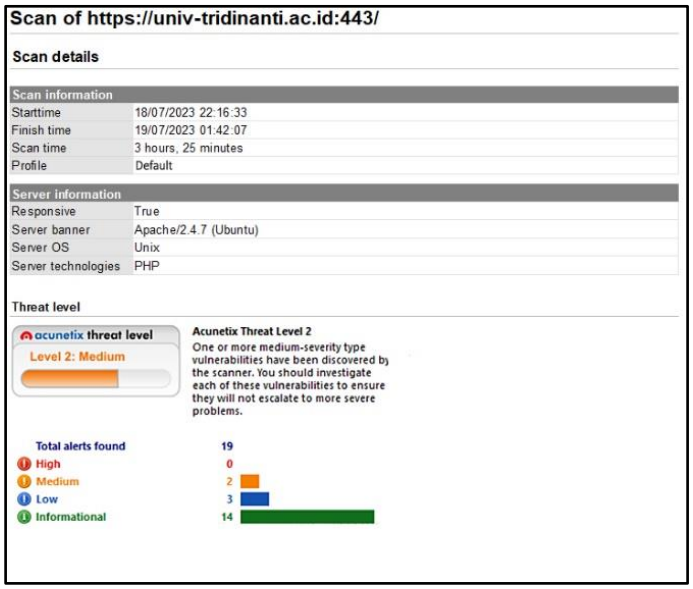
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

C. Identifikasi *(Vulnerability Identification)*



Gambar 6. Acunetix *Scan*

Jenis serangan yang dipilih dalam Acunetix yaitu *Crawling, Weak Passwords guessing, High Risk, XSS vulnerabilities* dan *SQL Injection Vulnerabilites*. Berdasarkan hasil uji yang telah dijalankan, domain univ-tridinanti.ac.id berada pada level 2 /Medium seperti terlihat pada gambar berikut:



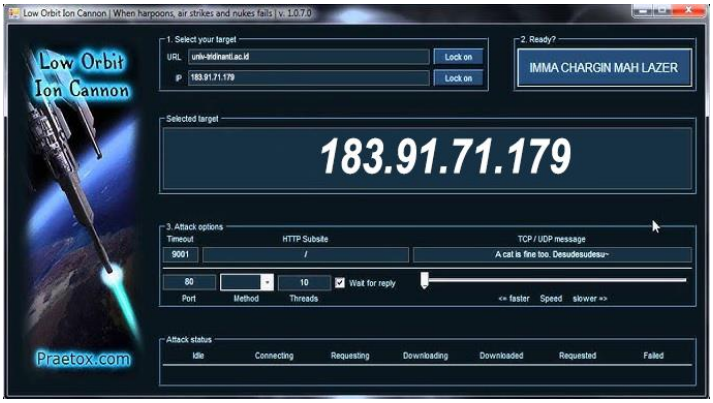
Gambar 7. Acunetix *Threat Level*

Tabel 4. Acunetix *Result*

Know Vulnerability	**Jumlah**	***Level Alert***
Development Configuration File	1	*Low*
Cross site scripting	1	*Medium*
HTML Form Without CSRF Protection	1	*Medium*
Blind SQL Injection	1	*Medium*
Slow HTTP Denial of Service Attack	1	*Medium*

Know Vulnerability	**Jumlah**	***Level Alert***
Documentation File	1	*Low*
Login page password-guessing attack	1	*Low*
Possible sensitive directory	1	*Low*
Content type not specified	5	*Informational*
Password type input with auto-complete enabled	9	*Informational*
TLS 1.1 Enabled	1	*Informational*

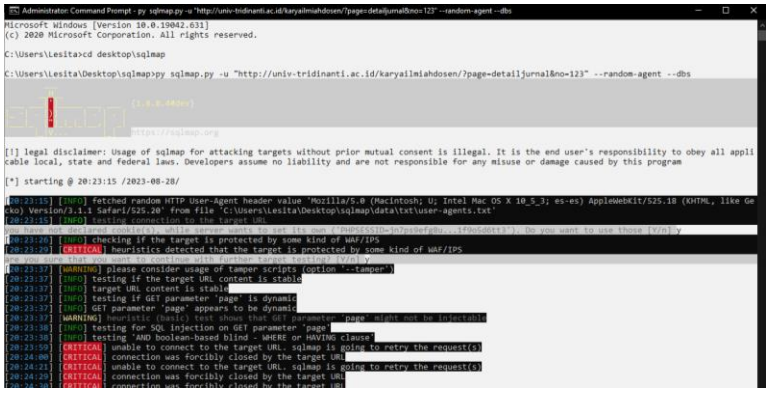
D. *Penetration*



Gambar 8. *Low Orbit Ion Cannon (LOIC)*

Penetrasi pada jaringan *network* dijalankan dengan uji stres menggunakan aplikasi loic dan menghasilkan gangguan yang sifatnya sementara dan terdeteksi sebagai serangan *denial service* oleh mikrotik.

E. *Gaining Access & Privilege Escalation*

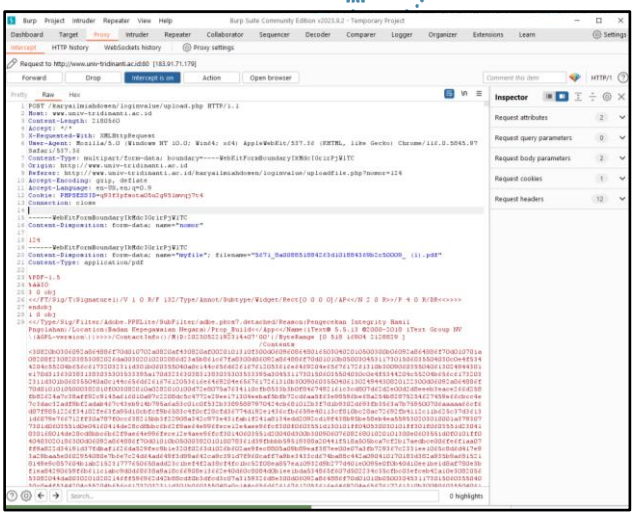


Gambar 9. *SQLMap*

Dari hasil percobaan injeksi SQL menggunakan SQLMap ditemukan bahwa sistem terproteksi oleh semacam *Web Application Firewall* (WAF) atau *Intrusion Protection System* (IPS) dengan hasil *connection was forcibly closed by the target url* atau koneksi diputus sehingga percobaan pengiriman webshell pun gagal.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Ketika penyerang berhasil login ke dalam website baik menggunakan metode injeksi SQL ataupun injeksi *(bypass)* halaman login, biasanya penyerang akan mencoba memasukkan file backdoor atau shell kedalam sistem menggunakan fitur upload file.



Gambar 10. *BurpSuite Intercept*

Eksploitasi jenis ini dapat dilakukan dengan memodifikasi file yang akan diupload menggunakan tools Burpsuite, caranya yaitu dengan *intercept request upload file* berekstensi yang diperbolehkan, kemudian menggantinya dengan file berisi *webshell* atau *backdoor* tadi atau *tampering*.

F. *Reporting*

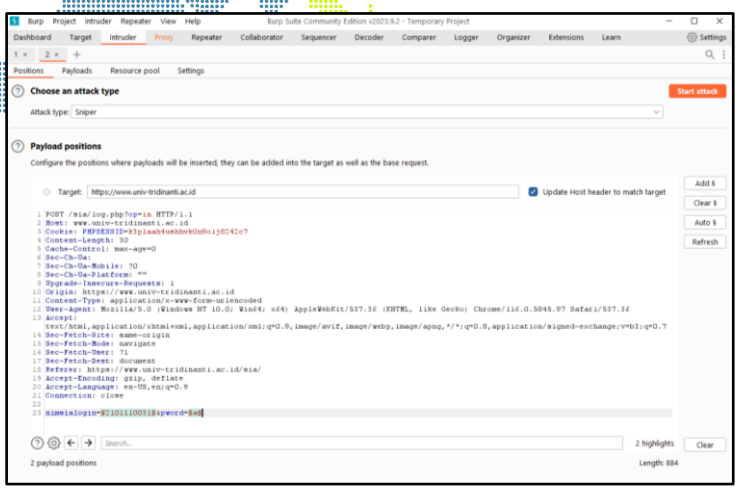
Tabel 5. Hasil Perbaikan terhadap kerentanan *website*

No	Jenis Kerentanan	Rekomendasi Perbaikan	Hasil
1	*Cross Site Scripting*	*Script* harus memberikan filter karakter dari input pengguna	Berhasil
2	*SQL Injection*	Sanitasi karakter Input, Method POST maupun Method GET yang terenkripsi	Berhasil
3	*Application Error Message*	Perbaiki Source Code	Berhasil
4	*Cookie Without HttpOnly Flagset*	Konfigurasi session cookies dengan HttpOnly	Berhasil
5	*Possible Sensitive Directories*	Hapus / batasi akses ke directory tersebut	Berhasil
6	*Possible Sensitive File*	Hapus / batasi akses ke file tersebut	Berhasil

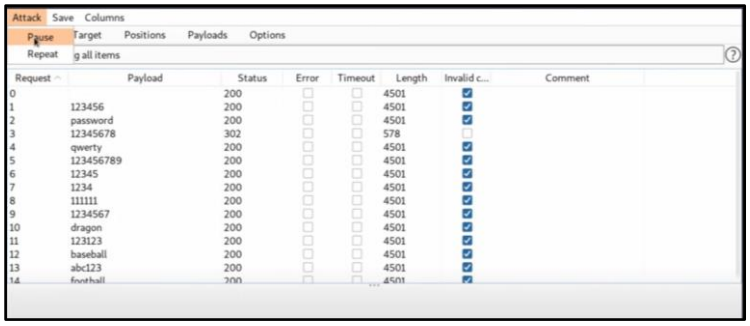
3.2. Uji Penetrasi dengan *Framework OWASP*

Testing for default credential menggunakan tools BurpSuite. Parameter *request* yang dikirim kemudian di-*intercept* oleh proxy dari BurpSuite dimodifikasi menjadi titik pemberian *payload* berupa *common password.*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

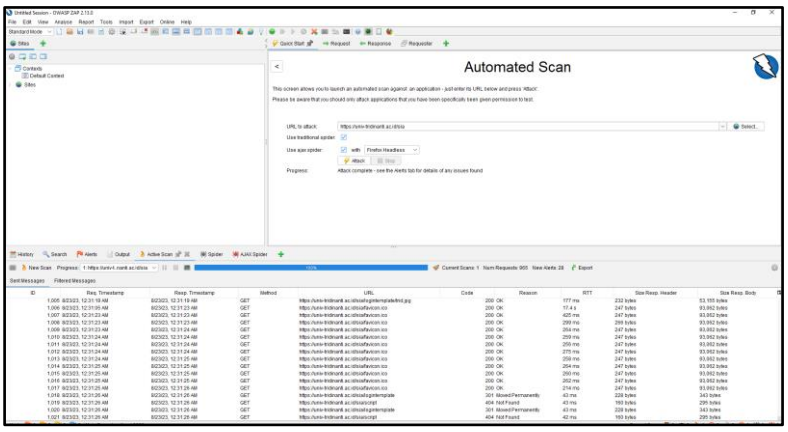


Gambar 11. *Paramater Intruder*



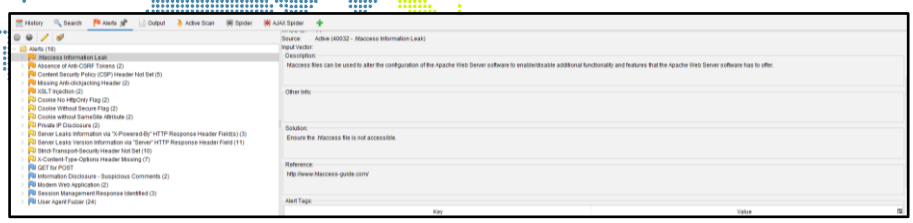
Gambar 12. *Common Password Payload*

Dalam percobaan testing, terdapat beberapa kelemahan yaitu sistem tidak melakukan pemblokiran ketika *user* melakukan kesalahan berulang dalam proses *login*, dalam hal ini perlu dilakukan pembatasan request login yang dilakukan serta pemblokiran terhadap request yang dianggap mencurigakan ke dalam sistem. *Authentication, authorization,* dan *session management* menggunakan *OWASP Zed Attack Proxy.*



Gambar 13. *Automated Scan OWASP ZAP*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 991-1005
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 14. *Risk Alert OWASP ZAP*

Dari hasil *automated scan OWASP ZAP* ditemukan beberapa *alert, risk level,* dan solusi yang dianjurkan seperti yang terlihat pada tabel berikut :

Tabel 6. *Alerts and solutions*

No	*Alert*	*Risk Level*	Solusi
1.	*.htaccess information leak*	*Medium*	Memastikan file .htaccess tidak bisa diakses.
2.	*Absence of Anti-CSRF Tokens*	*Medium*	Membuat Anti CSRF Token pada semua form.
3.	*Content Security Policy (CSP) Header Not Set*	*Medium*	Memastikan Webserver, Application Server, Load Balancer dikonfigurasi ke Content-Security-Policy header.
4.	*Anti-clickjacking Header*	*Medium*	Memastikan semua halaman web pada website menerapkan Content-Security-Policy and X-Frame-Options HTTP headers
5.	*XSLT Injection*	*Medium*	Mensanitasi dan menganalisa semua input user dari seluruh client side
6.	*Cookie No HttpOnly Flag*	*Low*	Memastikan HttpOnly Flag di set pada seluruh cookie
7.	*Cookie Without Secure Flag*	*Low*	Cookie yang berisi informasi sensitif atau berisi token harus selalu melewati channel terenkripsi.
8.	*Cookie without SameSite Attribute*	*Low*	Memastikan attribute SameSite menjadi Strict untuk semua cookie.
9.	*Private IP Disclosure*	*Low*	Hapus semua private IP Address dari Response Body / Tag Comment HTML
10.	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*	*Low*	Konfigurasi agar informasi "X-Powered-By" headers dihilangkan
11.	*HTTP Server Response Header*	*Low*	Konfigurasi agar informasi Server headers hanya mengandung informasi biasa (generic details)
12.	*Strict-Transport-Security Header*	*Low*	Memastikan bahwa konfigurasi diset ke Strict-Transport-Security.
13.	*X-Content-Type-Options Header Missing*	*Low*	Memastikan konfigurasi Content-Type header secara benar dan hanya mendukung web browser modern
14.	*GET for POST*	*Low*	Memastikan bahwa request method POST hanya diterima bila dilakukan POST, bukan method GET.
15.	*Information Disclosure - Suspicious Comments*	*Low*	Menghapus Comment yang memberikan return information.

Hasil Pengujian metode *OWASP* adalah dengan menguji menggunakan standar kontrol *OWASP* V 4.0 pada domain univ-tridinanti.ac.id berupa Otentikasi *(Authentication Testing),* Otorisasi *(Authorization Testing),* dan Manajemen Sesi *Testing* dinyatakan Lolos. Berdasarkan hasil pengujian menggunakan *OWASP Zap*, sistem informasi akademik Universitas Tridinanti tergolong aman ke dalam level medium, dan perlu diadakan perbaikan konfigurasi pada sistem. Beberapa rekomendasi *framework ISSAF* dan *framework OWASP* Versi 4 adalah sebagai berikut:

a) Menerapkan sistem deteksi / *Intrusion Detection System (IDS)*, sehingga dapat memonitoring serangan, baik dari dalam dan luar sistem.
b) Menjalankan sistem *backup* secara berkala. Agar apabila sistem rusak atau diambil alih oleh penyerang, maka masih dapat mengambalikan data yang hilang.

c) Rutin meng-*update* sistem operasi dan versi *software* penunjang seperti versi PHP terbaru, *Firewall*, dan *anti webshell*.
d) Menerapkan pemblokiran pada permintaan login yang tidak valid dan mencurigakan, serta *request* yang dilakukan secara berulang-ulang.

3.3. Pembandingan *Framework*

Pembandingan *Framework* dilakukan dengan menganalisa kedua *framework* yaitu *framework* ISSAF dan *framework* OWASP, kemudian seluruh tahapan dari masing-masing *framework* dilakukan agar saling melengkapi. Komparasi ini dilakukan dengan memanfaatkan hasil pembandingan masing-masing *framework* berdasarkan tahapan yang dilalui. Adapun hasil pembandingan tahapan masing-masing *framework* dan tools pendukungnya sebagai berikut :

Tabel 7. Pembandingan Framework

No.	Tahapan ISSAF	Tools ISSAF	Kelebihan & Kelemahan ISSAF	Tahapan OWASP	Tools OWASP	Kelebihan & Kelemahan OWASP
1	*Information Gathering*	Whois Domain, SSL Scan	Tahapan pengumpulan informasi yang cukup karena mencakup penelusuran network port yang terbuka.	Reconnaisance	Whois Domain, SSL Scan	Tahapan pengumpulan informasi belum mencakup *network mapping*
2	*Network Mapping*	ZenMap			-	
3	*Vulnerability Identification*	Acunetix	Tools Acunetix memerlukan inputan untuk masing-masing jenis serangan	Scanning	OWASP ZAP	Tools OWASP ZAP sudah dilengkapi dengan automated scan sehingga mempermudah dalam mencari identifikasi kerentanan.
4	*Penetration*	LOIC, Acunetix	Tahapan penetrasi juga mencakup jenis serangan ke jaringan network	Exploitation		Hasil Report dari tools OWASP ZAP sudah memberikan rekomendasi perbaikan
5	*Gaining Access & Privilege Escalation*	SQLMap	Dengan melakukan tahapan ini, percobaan pengambil alihan server bisa	Authentication Testing	BurpSuite, Browser	Authentication ataupun Authorization Testing perlu dilakukan karena form inputan user
6	*Enumerating Further*			Authorization Testing	BurpSuite	

No.	Tahapan ISSAF	Tools ISSAF	Kelebihan & Kelemahan ISSAF	Tahapan OWASP	Tools OWASP	Kelebihan & Kelemahan OWASP
			dilakukan dengan menggunakan sedikit tools yaitu SQLMap sekaligus dengan menggunakan command injeksi shell.			merupakan celah yang biasa dieksploitasi penyerang
7	*Compromise Remote User*	SQLMap, BurpSuite		Session Management Testing	Dirb, OWASP ZAP	OWASP ZAP menyimpan setiap sesi serangan ke dalam databasenya sendiri.
8	*Maintaining Access*	SQLMap		Maintaining Access	OWASP ZAP, Browser	
9	*Covering Tracks*	Webshell				Tidak ada tahapan menutup jejak serangan
10	*Reporting*	-		Reporting	-	

Dengan menggabungkan kedua tahapan dari masing-masing *framework*, penulis dapat memberikan rekomendasi perbaikan pada *server* Universitas Tridinanti dalam konteks penguatan sistem dan peningkatan keamanan dimana pada *framework ISSAF* terdapat pola perlindungan dari sisi *network*, sedangkan *framework OWASP* melengkapinya dengan melindungi dari sisi aplikasi atau program. Ada tahapan pada *framework ISSAF* yang tidak dilakukan di tahapan *framework OWASP* dan begitu juga sebaliknya, sehingga dengan mengimplementasi kedua *framework* akan memperbanyak jenis serangan yang dilakukan sehingga membuat *programmer* atau *database administrator* bisa memperbaiki celah yang ditemukan.

3.4. Evaluasi Kemanan

Evaluasi kemanan dilakukan dengan perbaikan dari sisi code program, untuk jenis serangan *XSS* dan *SQL injection* dilakukan sanitasi karakter yang dimasukkan kedalam form input user, request method yang dikirimkan dienkripsi menggunakan metode *two-way encryption*, konfigurasi *session cookies*, serta menghapus file atau direktori sensitive di server, untuk jenis serangan *Bruteforce* dilakukan pemblokiran terhadap permintaan login yang tidak valid dan *request* mencurigakan yang berulang-ulang, serta menerapkan *IDS* pada server web.

4. SIMPULAN

Setelah dilakukan percobaan penetrasi ke server menggunakan *framework ISSAF* dan *OWASP*, ditemukan beberapa celah keamanan yang harus segera diperbaiki, dari segi infrastruktur jaringan perlu adanya penambahan *security device hardware* yang memadai, memperbarui versi program dan *services*, hingga pengembangan *software* yang lebih aman. Implementasi *framework* dalam konteks

penguatan sistem dan peningkatan keamanan perlu dilakukan guna memperkecil kemungkinan terjadinya serangan ke *server* Universitas Tridinanti.

Perlu adanya perbaikan secara menyeluruh dan berkelanjutan, adanya peninjauan kembali coding aplikasi dan konfigurasi sistem, Implementasi sanitasi filter meta karakter pada coding program yang dikembangkan, *update software* pendukung *server*, penggunaan *request method* yang tepat, *software* dan *services* yang tidak berlisensi dan yang bersifat *open source* agar tidak lagi digunakan. Menerapkan *Web Application Firewall (WAF)*, *Intrusion Detection System (IDS)*, serta *Intrusion Prevention System (IPS)* pada arsitektur jaringan, dan perlunya *firewall hardware* yang memfilter informasi dan lalu lintas data *endpoint*.

DAFTAR PUSTAKA

[1] Riehle, D. "Framework design: A role modeling approach" (Doctoral dissertation, ETH Zurich). 2000.
[2] Rezshal Hidayah. "Hardening Web Aplikasi Dengan Menggunakan OWASP Security Testing Guide (WSTG) Pada Website ABC." 2021.
[3] Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF". Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), 113-124, 2020.
[4] Rafeli, A. I., Seta, H. B., & Widi, I. W. "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ." Informatik: Jurnal Ilmu Komputer, 18(2), 97-103. 2022.
[5] Matteo Meucci "OWASP TESTING GUIDE". OWASP Foundation, 2008.
[6] Anthi, E., Williams, L., Javed, A., & Burnap, P. "Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks", computers & security, 108, 102352. 2021.
[7] Burp Suite. "How to use Burp Suite for penetration testing. Burp Suite". 2021.
[8] Safitri, N., & Pramudita, R. "Pengembangan Kerangka Kerja Arsitektur Enterprise". Bina Insani ICT Journal, 4(1), 73-82. 2017.
[9] A Ismail, "Audit Sistem Keamanan Server Web Sesuai Standar Permenkominfo tentang Keamanan Server Web (Studi Kasus Situs Resmi Pemerintah Daerah Kabupaten Kotawaringin Timur http://beta.kotimkab.go.id)", Fakultas Ilmu Komputer, Universitas Darwan Ali, Sampit 2011.
[10] D. Metasari, "Analisis Keamanan Website Di Universitas Muhammadiyah Surakarta." Universitas Muhammadiyah Surakarta, Surakarta, 2014
[11] H. P. Siagian, "Vulnerability Assessment pada Web Server Universitas Bina Darma." Universitas Bina Darma, Palembang, 2014.
[12] Yum Thurfah Afifa Rosallah. "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing Dan Metode OWASP(Open Web Application Security Project) Top 10 Pada Website Sistem Informasi Manajemen (SIM) Universitas Pembangunan Nasional Veteran Jakarta". Jakarta 2021.

[13] Jalal, A., & Zeb, M. A. "Security enhancement for e-learning portal". IJCSNS International Journal of Computer Science and Network Security. 2015.
[14] Rogers, L., & Allen, J. "Securing information assets: security knowledge in practice." Associate Publisher's Choice, 801, 30. 2002.
[15] Saad, E., & Mitchell, R. "Web Security Testing Guide", 2020.
[16] Sasongko, et al. "Panduan Keamanan WebServer Informatika", Ed. Jakarta: Direktorat Keamanan Informasi Dirjen Aplikasi Informatika Kemenkominfo, 2011.