Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN "Veteran" Yogyakarta

Implementasi Uji Penetrasi Pada *Website* Untuk Peningkatan Keamanan Aset Informasi UPN ”Veteran” Yogyakarta

Herry Sofyan[1], **Meilan Sugiarto[2]**, **Bagus Muhammad Akbar[3]**

[1,3] Informatika, Universitas Pembangunan Nasional Veteran Yogyakarta, Indonesia
[2] Administrasi Bisnis, Universitas Pembangunan Nasional Veteran Yogyakarta, Indonesia

[1]herrysofyan@upnyk.ac.id, [2]meilan@upnyk.ac.id, [3*]bagusmuhammadakbar@upnyk.ac.id
**: Penulis korenspondensi* (*corresponding author*)

Informasi Artikel
Received: September 2022
Revised: May 2023
Accepted: June 2023
Published: June 2023

Abstract

Purpose: This study aims to implement penetration testing on the website https://fit.upnyk.ac.id owned by Telematics UPN "Veteran" Yogyakarta to determine whether there are vulnerabilities or security holes in the web server. Then make an analysis based on the results of penetration testing on the web server using penetration testing tools (penetration testing scanner) so that recommendations for improvements are obtained to close security holes that can be used as a way for hackers to enter the system, as well as provide risk mitigation recommendations.

Design/methodology/approach: This study uses the penetration test method which consists of five stages, namely literature study, information gathering, identification of system vulnerabilities, penetration testing and analysis. Penetration tests were carried out using acunetix tools and analysis using the OWASP and ISAAF methods.

Findings/result: Based on research conducted on the website https://fit.upnyk.ac.id/ using the OWASP method, several vulnerabilities were found, including one vulnerability with a high level (high), three with a medium level and six with a low level (low), so that it can be it can be concluded that in general the level of vulnerability of the website is at the medium level

Originality/value/state of the art: Penetration testing on the website can be done by identifying system vulnerabilities, penetration testing and analysis. The OWASP method can be used to find vulnerabilities on a website

Keywords:one; two; three
Kata kunci: satu; dua; tiga

Abstrak

Tujuan: penelitian ini bertujuan untuk mengimplementasikan *penetration testing* pada *website* https://fit.upnyk.ac.id milik Telematika UPN "Veteran" Yogyakarta untuk mengetahui adanya kerentanan atau celah keamanan pada *web server* tersebut. Kemudian membuat analisis berdasarkan hasil *penetration testing* pada web server dengan menggunakan *penetration testing tools* (*penetration testing scanner*) sehingga didapatkan rekomendasi perbaikan yang diperlukan untuk menutup celah keaamanan yang dapat digunakan sebagai jalan para hacker untuk masuk ke dalam sistem, serta memberikan rekomendasi mitigasi risiko.

Perancangan/metode/pendekatan: Penelitian ini menggunakan metode penetration test yang terdiri dari lima tahapan yaitu studi literatur, pengumpulan informasi, identifikasi kerentanan sistem, uji penetrasi dan analisis. Uji penetrasi dilakukan dengan acunetix *tools* serta analisis menggunakan metode OWASP dan ISAAF.

Hasil: Berdasarkan penelitian yang dilakukan pada *website* https://fit.upnyk.ac.id/ menggunakan metode OWASP ditemukan beberapa kerentanan antara lain satu kerentanan dengan level tinggi (*high*), tiga dengan level *medium* dan enam dengan level rendah (*low*), sehingga dapat disimpulkan bahwa secara umum tingkat kerentanan *website* tersebut berada pada level medium

Keaslian/ *state of the art*: Uji penetrasi pada *website* dapat dilakukan dengan identifikasi kerentanan sistem, uji penetrasi dan analasis. Metode OWASP mampu digunakan untuk menemukan celah kerentanan pada suatu *website*

1. Pendahuluan

Pertumbuhan teknologi yang semakin pesat memberikan dampak positif pada berbagai bidang, termasuk internet. *Website* menjadi alternatif bagi korporasi sebagai media promosi maupun media interaksi dengan pelanggan, *Website* dapat dengan mudah diakses oleh orang banyak dari manapun dan kapanpun. Pada tahun 2015, Indonesia diperkirakan akan ada lonjakan penggunaan internet sebesar 22 juta pengguna. Tren meningkatnya pengguna internet sudah terlihat sejak tahun 2009 dan diperkirakan akan terus meningkat [1].

Kemudahan akses ini membuat banyak orang maupun instansi membangun sistem webserver tanpa memperhatikan apakah webserver yang dibangun sudah aman atau belum terhadap

gangguan. Gangguan tersebut diantaranya berupa serangan *maliciousCode* atau *malware*. *MaliciousCode* atau *malware* merupakan jenis serangan yang paling banyak menyerang *website*. *Webserver* yang paling rentan adalah *website* milik perusahaan di bidang perbankan yaitu sebesar 81%. Kerentanan tersebut hanya 50% yang berhasil diperbaiki dengan rata-rata waktu memperbaiki selama 107 hari dari data yang diambil dari *White Hat Security Report* yang terlihat pada gambar 1.

Gambar 1. White Hat Security Website Security Statistic Report

Isu kerentanan ini didukung oleh laporan yang dirilis oleh Akamai sebagai pengawas lalu lintas internet pada tahun 2013 menyebutkan bahwa .com menjadi domain yang paling banyak diserang oleh hacker [2]. Untuk mengamankan *webserver* dari serangan hacker maka sebaiknya para pemilik *webserver* melakukan *selftest* terhadap server mereka sendiri. Melalui selftest ini, para pemilik *webserver* akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode *selftest* ini adalah *penetration test.*

Metode ini sama dengan aktivitas hacking namun dilakukan secara legal. *Penetration test* (pentest) merupakan metode yang efektif untuk menguji kerentanan sistem. Dengan demikian *penetration test* adalah proses mencoba untuk mendapatkan akses ke dalam sebuah sistem tanpa ada pengetahuan tentang username, password dan akses lainnya. Jika fokusnya adalah pada sumber daya komputer, maka contoh dari penetrasi yang sukses akan mendapatkan atau menghancurkan dokumen-dokumen rahasia, basis data dan informasi lain yang dilindungi. Pengujian terhadap aplikasi web dengan metode *penetration testing* merupakan metode yang komprehensif mengidentifikasi kerentanan sistem [3]. Dalam pengujian penetrasi ada beberapa metode yang sering dipakai seperti *Information Systems Security Assessment Framework* (ISSAF), OWASP versi 4 dan OSSTMM [14]. Penelitian ini, metode implementasi *penetration test* yang akan digunakan adalah ISSAF (*Information Systems Security Assessment Framework*) dan OWASP versi 4. Keduanya dipilih karena bersifat opensource, bebas digunakan oleh siapa saja. ISSAF yang dikeluarkan oleh OSSIG (*Open System Security Information Group*) merupakan kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain.

UPN ”Veteran” Yogyakarta sebagai sebuah lembaga pendidikan yang cukup besar juga memiliki Sistem Informasi Akademik yang biasa disebut dengan istilah *Computer Base Information System* (CBIS) dan aplikasi pendukung lainnya juga pernah mengalami gangguan terhadap data yang dimiliki hingga diperlukan waktu dan usaha yang cukup besar untuk mengembalikan data ke kondisi semula. Hal yang perlu diperhatikan oleh pemangku kepentingan di lingkungan UPN ”Veteran” Yogyakarta khususnya yang berhubungan dengan pengolahan data adalah sudah seberapa handalkah *web server* yang dimilki untuk menangkal serangan para hacker yang mencoba untuk mengubah atau ingin merusak data yang dimilki. UPT Telematika sebagai Unit Pelaksana Teknik yang bertanggung jawab terhadap keamanan

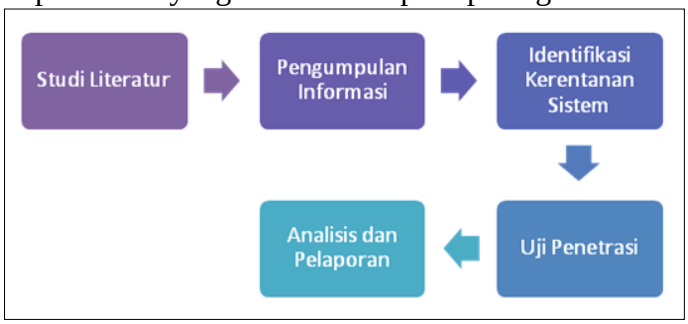
ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v20i2.7757

seluruh data dan informasi di lingkungan UPN "Veteran" Yogyakarta perlu juga melakukan pengujian dan mengamankan web server yang dimiliki oleh UPN "Veteran" Yogyakarta agar terbebas dari serangan siber dan mampu menanggulangi jika terjadi serangan siber dari pihak luar yang tidak bertanggung jawab. Mengapa hal tersebut menjadi penting karena menurut Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian selama periode Januari – Agustus 2021 telah terjadi 888.711.736 serangan siber di Indonesia (CNN Indonesia, Sep. 2021).

Oleh karena itu, penelitian ini dilakukan dengan mengimplementasikan *penetration testing* pada *website* https://fit.upnyk.ac.id milik Telematika UPN "Veteran" Yogyakarta untuk mengetahui adanya kerentanan atau celah keamanan pada *web server* tersebut. Kemudian membuat analisis berdasarkan hasil *penetration testing* pada web server dengan menggunakan *penetration testing tools* (*penetration testing scanner*) sehingga didapatkan rekomendasi perbaikan yang diperlukan untuk menutup celah keaamanan yang dapat digunakan sebagai jalan para *hacker* untuk masuk ke dalam sistem, serta memberikan rekomendasi mitigasi risiko.

2. Metode/Perancangan

Tahap-tahapan metode penelitian yang dilakukan seperti pada gambar berikut:



Gambar 2. Tahap-tahapan penelitian

2.1. Studi Literatur

Menurut hasil penelitian pengujian kerentanan web server dengan menarapkan metode ISSAF dan OWASP versi 4 untuk pengamanan web server dari serangan hacker maka sebaiknya para pemilik web server melakukan *self test* terhadap server mereka sendiri [2]. Melalui *self test* ini, para pemilik web server akan mengetahui letak kerentanan dari sistem yang ada [13]. Salah satu metode *self test* ini adalah *penetration testing* [15]. Metode ini sama dengan aktivitas hacking namun dilakukan secara legal [10].

Dalam penelitian lain yang dilakukan oleh Zainal Ali Abidin yang berjudul *penetration testing* Menggunakan Metode OWASP *(Open Web Application Security Project*) disebutkan bahwa OWASP dapat digunakan sebagai acuan dalam melakukan pengujian pada suatu sistem lebih sepesifiknya untuk web application dengan demikian OWASP bisa dijadikan sebagai dasar dalam pengujian keamanan terhadap *web application* [1]. Dalam penelitian tersebut target yang diserang adalah web SIMSON (Manejemen Skripsi Online) milik Universitas Islam Indonesia. *Open Web Application Security Project* (OWASP) adalah sebuah organisasi internasional yang bersifat non-profit, didirikan oleh OWASP foundation pada 21 April

2004 di Amerika Serikat. OWASP fokus pada peningkatan keamanan perangkat lunak dan didedikasikan untuk memungkinkan organisasi dalam mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi terpercaya untuk menjamin keamanan yang dibuat atau dikembangkan. OWASP memiliki misi untuk mengamankan *software*, sehingga orang-orang dan organisasi dapat membuat keputusan terhadap risiko keamanan yang benar.

OWASP merupakan vendor netral yang tidak berafiliasi dengan perusahaan teknologi manapun, tidak mendukung atau merekomendasikan produk atau layanan komersial. Proyek yang sudah dibuat dan dipublikasikan ada 363 proyek dan semua berkaitan dengan keamaan aplikasi, diantara proyek tersebut yaitu OWASP *Top Ten Project*, OWASP ASVS *Assessment tool*, OWASP Zed Attack Proxy Project, OWASP Testing Guide [11]. OWASP ZAP adalah sebuah *tools vulnerabilities scanner* yang dibuat oleh organisasi OWASP tools ini adalah suatu proyek dari OWASP yang paling aktif karena terus dikembangkan *tools* ini bersifat *opensource* sehingga siapa saja juga bisa mengembangkan *tools* ini. [12]

b. Pengumpulan Informasi

Tahap pengumpulan informasi merupakan proses mengumpulkan informasi secara umum berkaitan dengan target yang akan diuji. Informasi yang dikumpulkan berupa data mengenai IP target, *registrant* dan admin, informasi mengenai reverse DNS dan IP lookup, dan informasi lainnya yang diperlukan.

c. Identifikasi Kerentanan Sistem

Identifikasi kerentanan sistem atau *vulnerability assessment* adalah proses identifikasi dan kuantifikasi kerentanan keamananan pada suatu lingkungan keamanan sistem infomasi. Dapat diartikan juga sebagai suatu evaluasi mendalam terhadap keamanan sistem infomasi yang aktif digunakan.

d. Uji Penetrasi

Uji penetrasi (*penetration testing*) atau peretasan etis, adalah praktik pengujian aset teknologi informasi untuk menemukan kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Pengujian penetrasi dapat diotomatisasi dengan perangkat lunak atau dilakukan secara manual.

e. Analisis dan Pelaporan

Pada tahap ini biasanya dilaporkan tentang langkah kerja yang dilakukan, celah keamanan yang ditemukan serta usulan perbaikan. Tahapan selanjutnya biasanya tindak lanjut, yang biasanya harus dilakukan bersama-sama dengan admin untuk memperbaiki sistem.

3. Hasil dan Pembahasan

Hasil dan pembahasan berisi tentang langkah-langkah penelitian yang dilakukan beserta hasilnya. Berikut ini uraian hasil penelitian:

3.1. Pengumpulan Informasi

Tahap pengumpulan informasi (*information gathering*) bertujuan untuk mengumpulkan informasi umum mengenai *website* yang menjadi target menggunakan perangkat (*tool*) Whois Domain, dengan memasukkan domain *website* https://fit.upnyk.ac.id sebagai target. Hasil informasi yang didapat dilihat pada Tabel 1 berikut ini.

Tabel 1. Target IP dan Registrant

Domain ID	PANDI-DO152316
Domain Name	upnyk.ac.id
Create On	1996-12-15 13:09:12
Expiration Date	2023-10-01 00:09:10
IP Address	103.236.192.6
IP Location	Yogyakarta - Depok - Universitas Pembangunan Nasional Veteran Yogyakarta
Name Servers	NS1.UPNYK.AC.ID (has 1 domains) NS2.UPNYK.AC.ID (has 1 domains)
Registration ID	-
Registrant Name	-
Registrant Organization	-
Admin ID	-
Admin Name	-
Admin Organization	-

Tahap selanjutnya adalah mengumpulkan informasi mengenai jaringan *website* target secara spesifik. Proses pengumpulan informasinya dilakukan dengan cara memindai port *website* taget menggunakan perangkat Nmap. Berikut hasil pemindaian seperti pada Tabel 2.

Tabel 2. Port scanning menggunakan Nmap

Port	State	Service
21	Open	FTP
22	Closed	SSH
23	Filtered	Telnet
25	Open	SMTP
80	Open	HTTP
110	Open	Pop3
139	Filtered	NetBios-SSN
443	Open	HTTPs
445	Filtered	Microsoft-DS
3389	Filtered	MS-WBT_Server

Berdasarkan Tabel 2 tersebut, terlihat hasil pemindaian memperlihatkan bahwa ada beberapa port TCP yang penting pada *website* target masih terbuka. Hal tersebut cukup berbahaya karena beberapa *port* tersebut dapat dijadikan celah bagi hacker untuk dapat melakukan penyerangan.

3.2. Identifikasi Kerentanan Sistem dan Uji Penetrasi

Proses identifikasi kerentanan dilakukan dengan memindai kerentanan keamanan pada *website* http://fit.upnyk.ac.id. Alat OWAPS TOP 2021 digunakan untuk memindai kerentanan di domain utama situs web target. Hasilnya seperti terlihat pada Tabel 3. Berdasarkan pemindaian kerentanan menggunakan standar OWASP TOP 2021 Ada

beberapa kriteria yang digunakan oleh OWASP untuk menilai tingkat kerentanan suatu *website.*

a. *Broken Access Control*

Website http://fit.upnyk.ac.id berpotensi terkena serangan *Clickjacking*. Serangan clickjacking adalah semua jenis serangan pada aplikasi web yang menyebabkan korban secara tidak sengaja mengklik elemen halaman web yang tidak ingin mereka klik. Ini paling sering diterapkan pada halaman web dengan menempatkan konten berbahaya pada halaman tepercaya. Untuk mengatasinya, Anda dapat menambahkan header X-Frame-Options untuk mencegah serangan *Clickjacking*.

Table 3. Hasil Identifikasi Kerentanan

No	Jenis	Kerentanan	Level
1	Broken Access Control	Clickjacking attacks	High
2	Cryptographic Failures	Sensitif Information	Low
3	Injection	Cross site scripting (XSS) Attack	Medium
4	Insecure Design	Design page security	Medium
5	Security Misconfiguration	Cookie security configurations	Low
6	Vulnerable and Outdated Components	Folder listing	Medium
7	Identification and Authentication Failures	The HTTPS protocol not used	Low
8	Software and Data Integrity Failures	Software and Data Integrity Failures	Low
9	Security Logging and Monitoring Failures	Security Logging and Monitoring Failures	Low
10	Server-Side Request Forgery	Security Logging and Monitoring Failures	Low

b. *Cryptographic Failures*

Website http://fit.upnyk.ac.id relatif baik karena kredensial di *website* sudah mencukupi. Hal yang masih menjadi kerentanan adalah masih ada informasi sensitif yaitu file index.php.

c. Injection

Website https://fit.upnyk.ac.id berpotensi terkena serangan *Cross site scripting* (XSS) Attack karena terdapat celah keamanan pada input data berbasis SQL. Untuk mengatasi masalah ini, dapat dilakukan dengan menambahkan Filter XSS pada kondisi input data menggunakan SQL.

d. Insecure Design

Website https://fit.upnyk.ac.id belum memiliki keamanan halaman desain karena tidak memiliki header XFO yang aman di setiap halaman web. Untuk mengatasinya, dapat ditambahkan *Content Security Policy* (CSP) pada setiap halaman web yang digunakan.

e. Security Misconfiguration

Untuk penanganan konfigurasi keamanan cookie pada *website* fit UPN sudah cukup baik. Perbaikan yang disarankan pada indikator ini adalah masih ada daftar folder terbuka yang memungkinkan serangan terhadap folder terbuka terjadi.

f. Vulnerable and Outdated Components

Pada indikator komponen rentan dan ketinggalan jaman pada *website* FIT UPN terdapat beberapa kerentanan yang perlu diperbaiki yaitu beberapa listing folder masih dapat diakses, sehingga perlu dilakukan perubahan permission pada listing folder agar tidak dapat diakses

oleh pihak yang tidak berwenang dan penggunaan *library javascript* (jquery) yang masih menggunakan versi yang rentan terhadap serangan cyber.

g. Identification and Authentication Failures

Untuk penanganan identifikasi dan autentikasi (kredensial) sudah cukup. Tapi, ada kerentanan karena belum menggunakan protokol HTTPS.

h. Software and Data Integrity Failures

Pada indikator kegagalan integritas perangkat lunak dan data, respon kerentanan cukup baik. Hal yang perlu ditingkatkan adalah menghilangkan URL yang tidak digunakan terutama google *webfonts*.

i. Security Logging and Monitoring Failures

Dalam indikator *Security Logging and Monitoring Failures* tidak ada catatan perbaikan terkait dengan kerentanan. Hal ini dapat dikatakan sangat baik pada indikator.

j. Server-Side Request Forgery

Dalam indikator Pemalsuan permintaan *Server-Side* tidak ada catatan perbaikan yang terkait dengan kerentanan. Hal ini dapat dikatakan sangat baik pada indikator.

3.3. Analisis dan Pelaporan

Berdasarkan hasil identifikasi kerentanan dapat disimpulkan hasil pengujian terhadap celah keamanan terhadap *website* adalah sebagai berikut.

Tabel 4. Hasil Identifikasi Kerentanan

No	Level Risiko	Jumlah Alert
1	*High*	1
2	*Medium*	3
3	*Low*	6

Pada Tabel 4 terlihat ada satu celah keamanan yang berisiko tinggi (*high*) dan tiga berisiko sedang (*medium*). Untuk itu beberapa saran untuk perbaikan pada *website* akan direkomendasikan dan ulasannya ditampilkan pada Tabel 5.

Tabel 5. Saran Perbaikan Website

No	Jenis Kerentanan	Rekomendasi Perbaikan
1	Broken Access Control	1. Lakukan pemerikasaan dan pengujian kontrol akses secara berkelanjutan. 2. Tolak Akses secara default 3. Membatasi Penggunaan CORS (Cross-Origin Resource Sharing) 4. Aktifkan kontrol akses berbasis peran pengguna 5. Aktifkan kontrol akses berbasis izin terhadap 6. Aktifkan kontrol akses berdasarkan mandat pada pengguna
2	Injection (XSS Attack)	1. Filter seketat mungkin input (masukan) yang valid dari pengguna 2. Ubah data output sedemikian rupa untuk mencegah ditafsirkannya sebagai konten aktif. 3. Gunakan header respons yang sesuai. 4. Terapkan kebijakan keamanan informasi
3	Insecure Design	1. Gunakan siklus hidup pengembangan sistem yang aman. 2. Gunakan pengujian per unit dan terintegrasi secara berkelanjutan.

		3. Tetapkan unsur-unsur manajemen sumberdaya dan kebutuhan. 4. Menerapkan pemisahan system layer dan jaringan.
4	Vulnerable and Outdated Components	1. Hapus redundansi. 2. Periksa versi dan selalu perbaharui komponen 3. Selalu memindai kerentanan 4. Gunakan sumber daya yang resmi 5. Selalu memantau aktifitas.

4. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan pada *website* https://fit.upnyk.ac.id/ menggunakan metode OWASP ditemukan beberapa kerentanan antara lain satu kerentanan dengan level tinggi (*high*), tiga dengan level *medium* dan enam dengan level rendah (*low*), sehingga dapat disimpulkan bahwa secara umum tingkat kerentanan *website* tersebut berada pada level medium. Terdapat beberapa kerentanan yang harus segera mendapatkan perhatian dan pebaikan segera antara lain adalah *Broken Access Control*, *Injection* (*XSS Attack*), *Insecure Design* dan *Vulnerable and Outdated Components*. Hal tersebut harus segera dilakukan karena sangat rentan oleh serangan para *hacker*.

Daftar Pustaka

[1] Abidin, A., Zainal, *Penetration testing* Menggunakan Metode Owasp (Open Web Application Security Project), https://dspace.uii.ac.id

[2] Dirgahayu, R.T, Prayudi, Fajaryanto, Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server, Networking Engineering Research Operation Vol 1, No 3 (2015).

[3] Fauzan, R. H. (2019). Pengujian Keamanan Sistem Informasi Akademik Menggunakan Metode *Penetration testing*. Studi Kasus: Institut Pertanian Stiper Yogyakarta.

[4] I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, D. M. S. A. (2020). Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration testing* Menggunakan Framework ISSAF. Jurnal Ilmiah Merpati, Vol. 8, No(2), 113–124.

[5] Jofie yordan, muhammad fikrie. (2019, February 17). BSSN Bikin *Website* Pemantau Serangan Siber di Indonesia. https://kumparan.com/kumparantech/bssn-bikin-*website*-pemantau-serangan-siber-di-indonesia-1549535309181754057/full

[6] KOMINFO (2011), Panduan Keamanan Web Server, Direktorat Keamanan Informasi, KOMINFO RI.

[7] Nazwita, S. R. (2017). Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata. Seminar Nasional Teknologi Informasi Komunikasi Dan Industri, 0(0), 2579–5406. http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368

[8] OWASP, "The ten Most Critical Web Application Security Risk," http://www.owasp.org, 2017

[9] Rheno Widianto, S., & Abdullah Azzam, I. (2018). Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server. Elektra, 3(2), 19–28.

[10] Fahmi Fachri , Abdul Fadlil & Imam R. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. Jurnal Informatika, 3(2), 183-190

[11] Reza Vidi A., Edi Surya N. (2022). Pemindai Kerentanan Terhadap *Website* Jago Masak Dengan Metode Pengujian Penetrasi OWASP ZAP. Jurnal Mantik, 6(3), 3406-3412

[12] Bhaskara, V. T., Ari K., & Yahya, W.. (2017) Analisis Perbandingan *Penetration testing* Tool Untuk Aplikasi Web. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 1(3), 206-214.

[13] Yulia Fauzan, Fadilla & Syukhri. (2021). Analisis Metode Web Security PTES (*Penetration testing* Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. Jurnal Vocational Teknik Elektronika dan Informatika, 9(2).

[14] I Gede A. S., Gusti Made A., Dewa Made S.. (2020). Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration testing* Menggunakan Framework ISSAF. Jurnal Ilmiah Merpati, 8(2).

[15] Marzuki H., & Andi Marwan E. (2022). *Penetration testing* Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box Studi Kasus Web Server Diva Karaoke.co.id. Jurnal Teknik Informatika, 1(4).