PENGUJIAN CELAH KEAMANAN MENGGUNAKAN METODE OWASP *WEB SECURITY TESTING GUIDE (*WSTG*)* PADA *WEBSITE* XYZ

Albestty Islamyati Rafeli[1], Henki Bayu Seta, S.Kom, MTI[2], I Wayan Widi P., S.Kom, MTI[3]
Program Studi Informatika, Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
JL. RS Fatmawati No. 1, Pondok Labu, Jakarta Selatan, DKI Jakarta12450
albestty@gmail.com[1], henkiseta@upnvj.ac.id[2], wayan.widi@upnvj.ac.id[3]

Abstrak. XYZ sebagai *website research* tentunya memiliki banyak data sensitif seperti data pribadi pengguna baik *researcher* ataupun responden dan data hasil *research*. Data ini rentan akan kebocoran data ataupun dicuri dan disalah gunakan oleh oknum yang tidak bertanggung jawab dan merugikan banyak pihak. *Penetration Testing* merupakan cara untuk mensimulasikan metode yang sekiranya akan digunakan oleh penyerang atau oknum tidak bertanggung jawab untuk dapat mengakses data secara ilegal kedalam sistem. WSTG merupakan singkatan dari *Web Security Testing Guide*, yaitu sebuah panduan *project* pengujian keamanan *Cyber* terutama dibidang pengembang aplikasi *web* dan keamanan professional. Pada penelitian ini dilakukan tujuh teknik yaitu *Information gathering, Configuration and Deployment Management Testing*, *Identity Management Testing, Input Validation Testing, Testing For Error Handling*, *Business Logic Testing* dan *Client Side Testing.* Pada penelitian ini ditemukan delapan *vulnerability* pada *website* XYZ. Setelah dilakukan penilaian resiko secara menyeluruh resiko dari *vulnerability* pada *website* XYZ termasuk dalam kategori *medium.*

Keyword : *Website, Penetration Testing*, WSTG.

1 Pendahuluan

Perkembangan teknologi kian hari semakin berkembang pesat, salah satunya dibidang TIK atau Teknologi Informasi dan Komunikasi. Riset yang dilakukan secara konvensional membutuhkan banyak biaya karena memerlukan banyak *hardcopy* seperti kertas kuesioner dan ekspedisi. Seiring dengan perkembangan teknologi informasi ini para pengembang merekomendasikan untuk melakukan riset secara *online* agar dapat memperbaiki kekurangan riset secara konvensional dan memberikan kesempatan bagi *reseacher* untuk mengembangkan metode penelitiannya melalui riset *online* mulai dari merancang, menjalankan dan bahkan menganalisis data. menganalisis data.

Website riset *online* menjadi salah satu pilihan bagi *researcher*, karena dapat menutup kekurangan riset secara konvensional, tetapi riset *online* memiliki kekurangan yaitu kebocoran data berisi informasi pribadi yang dilakukan oknum yang tidak bertanggung jawab. Menurut Kepala Badan Siber dan Sandi Negara (BSSN), Hinsa Siburian mengatakan, selama tahun 2021 ini tercatat ada 888.711.736 serangan siber (Jakarta, Kompas.com 2021). Oleh karena itu perlu dilakukan *penetration testing* terhadap *website* riset untuk melindungi data pribadi user *website* riset dan mengurangi kejahatan siber yang bisa menembus sistem keamanan yang ada.

1.1 Studi Literatur

Pada penelitian ini terdapat referensi yang digunakan penulis dalam melakukan penelitian. Pertama, Penelitian berjudul "*Hardening Web* Aplikasi Dengan Menggunakan OWASP *Security Testing Guide* (WSTG) Pada *Website* ABC" yang dilakukan oleh Rezshal Hidayah pada tahun 2021 menjelaskan bahwa penelitian ini menggunakan metode OWASP dilakukan untuk mendapatkan *vulnerability* pada *website* ABC menggunakan tiga teknik yaitu *information gathering, data validation testing* dan *client side testing* dan tidak dilakukan *penetration testing* secara menyeluruh dikarenakan

hanya mengambil metode yang merupakan bagian dari OWASP TOP 10 dan selain itu penelitian ini bertujuan untuk penguatan konfigurasi *server* (*hardening*) bukan pembaharuan aplikasi.
Kemudian berdasarkan penelitian kedua, penelitian ini berujudul "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" oleh Yum Thurfah Afifa Rosallah pada tahun 2021 dan hasil penelitian yang didapatkan yaitu:

a. *Broken Authentication* menggunakan *hydra*, rekomendasi yang diberikan yaitu membuat kombinasi *password* yang rumit, adanya *limit log in*, menggunakan *captcha* dan memanfaatkan *two factor authentication*.
b. *Sensitive Data Exposure* menggunakan *dirb*, rekomendasi yang diberikan yaitu melakukan pengecekan dan penyetingan lebih ketat di *direktori website* untuk mengurangi adanya penyerang mengambil informasi *sensitive*.
c. *Security Misconfiguration* yaitu melakukan *scanning* pada *open port* SSL dan mencek konfigurasi SSL, rekomendasi yang diberikan men*disabled port* 443 atau SSL/HTTPS secepat mungkin untuk keamanan *port* SSL.
d. *Clickjacking* didapatkan dari hasil *scanning vulnerability*, rekomendasi yang diberikan yaitu melakukan pencegahan di sisi *client* ditambahkan *addons no script* dan pada *server* menggunakan *frame iller*, *X frame options.*

1.2 *Penetration Testing*

Penetration Testing merupakan metode yang digunakan untuk menguji kerentanan pada sistem, identifikasi konfigurasi sistem yang buruk, kecacatan perangkat keras dan perangkat lunak serta kelemahan teknis pada sistem informasi yang diujikan. Tujuan utama pengujian *penetration testing* yaitu sebagai mengidentifikasi keamanan sistem (I Gede Ary Suta Sunjaya, dkk, 2020).

1.3 *Website* yang Digunakan

Website yang digunakan yaitu *Website* demo.XYZ.id merupakan suatu *website research* yang bertujuan untuk membantu para *customer* dalam pembuatan riset yang interaktif dan responsif dengan disediakan berbagai macam template, jenis pertanyaan dan jenis jawaban. Pembuatan riset bertujuan untuk keperluan bisnis maupun pendidikan dan lainnya sesuai dengan kebutuhan *researcher* dan dapat memberikan manfaat untuk mewujudkan tujuan dari masing-masing keperluan.

2 Tinjauan Pustaka

2.1 *Web Security Testing Guide* (WSTG)

Web Security Testing Guide atau WSTG merupakan panduan untuk melakukan tes keamanan pada *website*, untuk mengevaluasi dan melibatkan analisisi aktif dari aplikasi untuk setiap kelemahan, baik kelemahan teknis ataupun kerentanan. Terdapat beberapa teknik pada WSTG diantaranya, *Information Gathering, Configuration dan Deployment Management Testing, Identity Management Testing, Authentication Testing, Authorization Testing, Session Management Testing,* Input Validation *Testing, Testing For Error Handling, Testing For Weak Crypthography, Business Logic Testing, Client Side Testing,* API *Testing.*

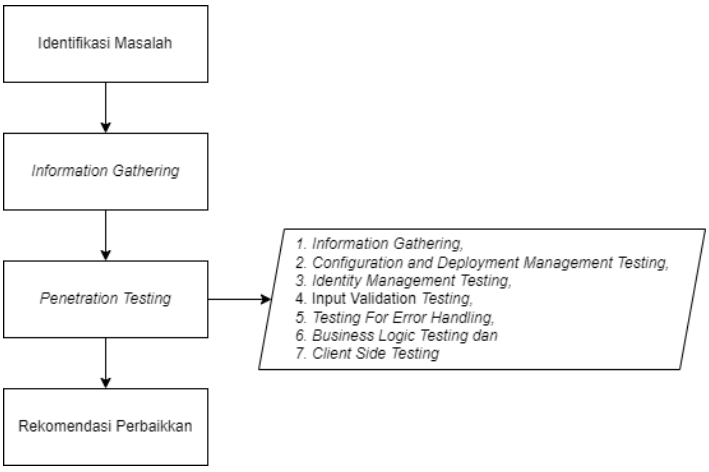
2.2 *Tools* yang Digunakan

BURP *Tools*, dapat memberi gambaran umum tentang fungsionalitas dan konten aplikasi *web* target di mana ini berisi peta situs yang memberikan informasi terperinci tentang target sehingga memungkinkan untuk menetapkan ruang lingkup pengujian *penetrasi testing.*
Dirb, adalah pemindai konten *Web*, yaitu mencari objek *web* yang ada atau tersebunyi. *Dirb* berkerja dengan meluncurkan serangan berbasis *dictionary* terhadap *server web* dan menganalisis tanggapan. *Dirb* bertujuan untuk membantu audit aplikasi *web* profesional. *Dirb* bekerja dengan memindai direktori dan kemudian melintasi di dalam *direktori* tersebut untuk memindai lebih banyak *subdirektori*.
Common Vulnerability Scoring Sysem atau **CVSS,** adalah sebuah *framework* yang dapat digunakan oleh publik untuk mengkomunikasikan dan kerentanan perangkat lunak. CVSS terdiri dari tiga bagian bagian, yaitu *Base Score*, *Temporal Score* dan *Environmental Score. Base Score* yaitu mewakili kualitas intrinsik kerentanan yang konstan sepanjang waktu dan diseluruh lingkungan pengguna, *Temporal Score* menggambarkan karakteristik kerentanan yang berubah seiring waktu dan *Environmental score* mewakili karakteristik kerentanan unik bagi pengguna lingkungan.

3. Metodologi Penelitian

3.1 Implementasi Penelitian

Pada penelitian ini digunakan *website* demo.xyz.id menggunakan metode OWAPS *Web Security Testing Guide* (WSTG) dan *tools* yang digunakan untuk mengeksploitasi yaitu BURP *Suite* dan *Dirb* sedangkan untuk menghitung nilai kerentanan yaitu *Common Vulnerability Scoring System.* Proses ini terdiri dari identifikasi masalah, *information gathering, penetration testing* dengan menggunakan beberapa teknik yaitu (*Information Gathering, Configuration and Deployment Management Testing, Identity Management Testing,* Input Validation *Testing, Testing For Error Handling, Business Logic Testing dan Client Side Testing*) dan rekomendasi perbaikan.



Gambar. 1. Alur penelitian diawali dari identifikasi masalah, information gathering, penetration testing, dan rekomendasi perbaikan.

Identifikasi Masalah

Bahayanya kebocoran data dari *website research* yang berisikan pengguna *website* hingga hasil *research* yang telah dilakukan membuat peneliti tertarik menjadikan *penetration testing* sebagai tema penelitian ini dan sebagai salah satu upaya meminimalisir permasalahan seperti kurangnya kesadaran akan keamanan terhadap pengamanan terhadap *website* hingga pencurian data yang mengakibatkan kerugian.

Penetration Testing

a. ***Information Gathering***
Information Gathering berfungsi untuk menemukan komponen dan fungsionalitas dengan mengikuti URL *page* lain atau melihat peta situs *web*.

- ***Conduct Search Engine Discovery Reconnaissance for Information Leakage***
  Pengujian ini dilakukan untuk mengetahui apakah terdapat informasi sensitif dari *website* yang dapat diakses dengan menggunakan *search engine.* Pengujian ini dilakukan dengan melakukan pencarian *search engine google* dengan menggunakan operasi pencarian "site:" agar hasil pencarian hanya menampilkan situs yang ditentukan saja yakni website XYZ. Dari penelitian yang dilakukan tidak terdapat indikasi terjadinya kebocoran informasi.
- ***Fingerprint Web Server***
  Web Server bertujuan untuk mengetahui apakah versi dan tipe dari aplikasi beserta komponen yang digunakan oleh situs *web* XYZ dapat diketahui, jika dapat diketahui oleh khalayak umum maka hal ini mengindikasikan terjadinya kebocoran data. Pengujian ini dilakukan dengan mengakses website XYZ seraya menangkap *request* yang dikirimkan serta *response* yang diterima menggunakan burp *suite.* Dari penelitian yang dilakukan ditemukan versi PHP 8.0.19 dan *server Litespeed* yang digunakan pada *website*.
- ***Review Web Server Metafiles for Information Leakage***
  Review Web Server Metafiles for Information Leakage bertujuan untuk mengidentifikasi adanya fungsi dan lokasi yang tersembunyi atau tersamarkan dengan melakukan analisa terhadap *file - file metadata.* Pemeriksaan dilakukan dengan melakukan percobaan penelusuran *file - file* tersebut di dalam *website* dengan memasukkan nama *file* diatas kedalam URL. Dari penelitian yang dilakukan tidak terdapat indikasi terjadinya kebocoran informasi.

b. ***Configuration dan Deployment Management Testing***
Configuration dan Deployment Management Testing bertujuan untuk meninjau seluruh keamanan infrastruktur untuk menjaga keamanan seperti perangkat lunak *server web, server database back-end*, atau otentikasi *server.*

- ***Review Old Backup and Unreferenced Files for Sensitive Information***
  Review Old Backup and Unreferenced Files for Sensitive Information bertujuan untuk mengetahui apakah terdapat *file* lama, *file back up,* dan *file* yang tidak direferensikan yang bisa diakses didalam *website* tersebut. Pengujian dilakukan dengan menggunakan *tool dirb* untuk memeriksa direktori dan *file* apa saja dan mana saja yang dapat diakses pada *website.* Dari penelitian yang dilakukan diketahui *direktori* yang ditemukan dan dapat diakses secara eksternal.
- ***Test HTTP Methods***
  Pengujian terhadap *testing* pada *HTTP Method*, *testing* ini bertujuan untuk mengetahui apakah *website* sudah menjamin *method* yang digunakan pada saat *request* hanya satu tidak lebih. Cara melakukan pengetesan ini adalah dengan mengubah *request* dengan *method get* menjadi *put.* Dari

penelitian yang dilakukan HTTP Method sudah berhasil diimplementasi dengan baik, tetapi *website* mengeluarkan *Stack Trace* dan *Error Handling.*

c. *Identity Management Testing*

Identity Management Testing bertujuan untuk mengelola fungsionalitas aplikasi, auditor untuk meninjau transaksi aplikasi dan memberikan laporan rinci, teknisi dapat membantu untuk mendebug dan memerbaiki masalah pada akun *users.*

- ***Test User Registration Process***

  Test User Registration Process bertujuan untuk memverifikasi proses *registration.* Pengujian ini dilakukan dengan cara mencoba membuat akun pada *website* XYZ dan memasukkan data – data yang diminta oleh *website* XYZ. Dari penelitian yang dilakukan *website* mengeluarkan *error* dengan menampilkan *codingan laravel* yang menandakan adanya kebocoan informasi.

d. *Input Validation Testing*

Input Validation Testing bertujuan untuk apakah *website* rentan terhadap jenis serangan atau tidak.

- ***Testing For Stored Cross Site Scripting***

  Testing For Stored Cross Site Scripting bertujuan untuk mengidentifikasi input tersimpan yang tercermin pada sisi *client*, mengetahui nilai input yang diterima dan jika ada pengkodean yang diterapkan saat kembali. Pengujian dilakukan dengan mencoba mengisi fitur register pada *website* dengan memasukkan *e-mail* yang tidak benar. Dari penelitian yang dilakukan dapat membuat akun dengan menggunakan email yang salah dan hal itu menandakan adanya *vulnerability* pada *website.*

e. *Testing For Error Handling*

Testing For Error Handling adalah kesalahan yang timbul dengan sengaja mengirim *string* ketika *integer* diharapkan. *Input user* yang dapat diterima kode tetapi tidak dapat ditangani.

- ***Testing For Improper Error Handling***

  Testing For Improper Error Handling bertujuan untuk memeriksa apakah terdapat pengendalian *error* yang kurang baik sehingga dapat memberikan informasi yang seharusnya tidak diketahui oleh publik. *Pengujian* dilakukan dengan mencoba berbagai fitur yang tersedia di dalam situs *web*. Dari penelitian yang dilakukan *website* menggeluarkan *error handling* dengan menampilkan *codingan larevel* dan hal itu menandakan adanya *vulnerability* pada *website.*

f. *Business Logic Testing*

Business Logic Testing tidak jauh berbeda dengan jenis pengujian yang digunakan oleh fungsional yang berfokus pada keadaan logis atau batas pengujian.

- ***Test Integrity Check***

  Test Integrity Check Merupakan pengujian pemeriksaan integritas logika bisnis dan dilakukan dengan menggunakan logika bisnis pada *website* XYZ. Dari hasil penelitia yang dilakuakn ditemukan *vulnerability* sebagai berikut :

  1. *Register* tanpa Checklist = Dapat membuat akun tanpa menceklis syarat dan ketentuan.
  2. Tidak Ada Validasi Input = Dapat menginput apa saja pada *field box* yang tersedia.
  3. *Question Wizard* = Dapat berpindah kepertanyaan yang diiginkan tanpa menjawab pertanyaan sebelumnya.

g. *Client-side Testing*

Client-side Testing Client Side Testing merupakan salah satu bentuk pengujian menggunakan *code injection attack* dengan menyisipkan kode berbahaya berbentuk *javascript* atau *client script code.*

- ***Testing For DOM-Based Cross Site Scripting***

  Testing For DOM-Based Cross Site Scripting bertujuan untuk mengetahui apakah *website* XYZ dari skrip sisi *client* untuk pengguna memberikan data ke DOM (*Document Object Model*). Cara melakukan pengetesan ini adalah dengan menambahkan kode *javascript.* Dari penelitian yang dilakukan tidak terdapat indikasi adanya *vulnerability DOM-Based Cross Site Scripting.*

- ***Testing Cross Origin Resource Sharing***

  Testing Cross Origin Resource Sharing bertujuan untuk memastikan konfigurasi CORS aman atau tidak berbahaya. Dari penelitian yang dilakukan tidak terdapat indikasi adanya *vulnerability Cross Origin Resource Sharing.*

4 Hasil dan Pembahasan

Berikut hasil penelitian yang telah dilakukan ada *website* XYZ.

Tabel 1. Hasil dan pembahasan penelitian

Level *Risk/Score*	Metode	Hasil Temuan	Status
	Information Gathering	*Conduct Search Engine Discovery Reconnaissance for Information Leakage*	Tidak ditemukan
5.3/10 (Medium)	*Information Gathering*	*Fingerprint Web Server*	Ditemukan
	Information Gathering	*Review Web Server Metafiles for Information Leakage*	Tidak ditemukan
5.3/10 (Medium)	*Configuration and Deployment Management Testing*	*Review Old Backup and Unreferenced Files for Sensitive Information*	Ditemukan
	Configuration and Deployment Management Testing	*Test* HTTP *Method*	Tidak ditemukan
6.3/10 (Medium)	*Identity Management Testing*	*Test User Registration Process*	Ditemukan
5.3 (Medium)	*Input Validation Testing*	*Testing For Stored Cross Site Scripting*	Ditemukan
5.3/10 (Medium)	*Testing For Error Handling*	*Testing For Improper Error Handling*	Ditemukan
5.3/10 (Medium)	*Business Logic Testing*	*Test Integrity Checks (Register* Tanpa *Checklist)*	Ditemukan
5.3/10 (Medium)	*Business Logic Testing*	*Test Integrity Checks* (Tidak Ada Validasi Input)	Ditemukan
6.5/10 (Medium)	*Business Logic Testing*	*Test Integrity Checks (Question Wizard)*	Ditemukan
	Client Side Testing	*Testing For DOM-Based Cross Site Scripting*	Tidak ditemukan
	Client Side Testing	*Testing Cross Origin Resource Sharing*	Tidak ditemukan

5 Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian *penetration testing* pada *website* XYZ yang telah dilakukan menggunakan metode OWASP *Web Security Testing Guide* (WSTG) dengan tools BURP *Suite*, *Dirb* dan CVSS untuk mengukur tingkat kerentanan dan menggunakan tujuh teknik yaitu *Information gathering, Configuration and Deployment Management Testing, Identity Management Testing, Input Validation Testing, Testing For Error Handling, Business Logic Testing* dan *Client Side Testing* dan ditemukan delapan *vulnerability* dengan kategori medium.

5.2 Saran

Berdasarkan hasil penelitian *penetrasi testing* pada *website* XYZ diperlukan melakukan pengujian celah keamanan rutin yang lebih mendalam dan detail guna mencari kelemahan terbaru atau tidak disadari oleh pihak pengembang *website* XYZ.

Referensi

[1] Burp Suite. (2021). *How to use Burp Suite for penetration testing*. Burp Suite. https://portswigger.net/burp/documentation/desktop/penetration-testing. Date Accessed : 02-08-2022

[2] Dewanto, A. P. (2018). Penetration Testing padaDomain uii.ac.id Menggunakan OWASP 10. Https://Dspace.Uii.Ac.Id/. https://dspace.uii.ac.id/bitstream/handle/123456789/11281/13523025-Adetya Putra D-laporan skripsi.pdf?sequence=1&isAllowed=y

[3] First.org. (2022). *Common Vulnerability Scoring System Version 3.1 Calculator*. https://www.first.org/cvss/calculator/3.1. Date Accessed : 21-04-2022

[4] Hall, G., & Watson, E. (2016). *Hacking_ Computer Hacking, Secu - Gary Hall.pdf*. http://index-of.es/Varios-2/Hacking Computer Hacking Security Testing Penetration Testing and Basic Security.pdf

[5] Joshi, C., & Kumar, U. (2016). Security Testing and Assessment of Vulnerability Scanners in Quest of Current Information Security Landscape. *International Journal of Computer Applications*, *145*(2), 1–7. https://doi.org/10.5120/ijca2016910563

[6] Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., Ibrahim, I. M., Ahmed, A. M., Rashid, Z. N., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. *Asian Journal of Research in Computer Science*, *July*, 13–32. https://doi.org/10.9734/ajrcos/2021/v10i330242

[7] Mailkuloan. (2022). *Vulnerability Charts*. https://maikuolan.github.io/Vulnerability-Charts/php.html. Date Accessed : 18-05-2022

[8] Mashabi, S. (2021, September). BSSN: Hingga Agustus 2021 tercatat 888 Juta Serangan Siber. *Kompas.Com*. https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber. Date Accessed : 24-09-2021

[9] Mell, P., Scarfone, K., & Romanosky, S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. *FIRSTForum of Incident Response and Security Teams*, 1–23. https://www.first.org/cvss/cvss-v2-guide.pdf

[10] OWASP. (2022). *WSTG*. https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/02-Testing_for_Stack_Traces. Date Accessed : 18-05-2022

[11] RedHat. (2022). *CVE-2021-21708*. https://access.redhat.com/security/cve/cve-2021-21708. Date Accessed : 18-05-2022

[12] Rezshal Hidayah. (2021). *Hardening Web Aplikasi Dengan Menggunakan OWASP Security Testing Guide (WSTG) PADA WEBSITE ABC*. https://repository.telkomuniversity.ac.id/pustaka/174937/hardening-web-aplikasi-dengan-menggunakan-owasp-security-testing-guide-wstg-pada-*website*-abc.html. Date Accessed : 24-05-2022

[13] Saad, E., & Mitchell, R. (2020). WEB SECURITY TESTING GUIDE. https://github-releases.githubusercontent.com/91277330/87c4c000-357b-11eb-8c88-e5664025b5bc?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20211124%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211124T063815Z&X-Amz-Expires=300&X-A

[14] Sanjaya, I. G. A. S. (2020). Evaluasi Keamanan *Website* Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati*, *8*(2), 113–124.

[15] Sirait, F., & Sofyan Putra, M. K. (2018). Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. *Universitas Mercu Buana ISSN*, *9*(1), 16.

[16] Yum Thurfah Afifa Rosallah. (2021). *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*. https://repository.upnvj.ac.id/11253/