Pengujian Celah Keamanan Menggunakan Metode OWASP *Web Security Testing Guide (*WSTG*)* pada *Website* XYZ

Albestty Islamyati Rafeli[1], Henki Bayu Seta[2], I Wayan Widi[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 dilakukan penyalahgunaan dengan orang yang tidak bertanggung jawab sehingga merugikan banyak orang. *Penetration Testing* merupakan cara untuk menggambarkan metode yang digunakan oleh orang 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* dengan kategori medium pada *website* XYZ.

Keyword : *Website, Penetration Testing*, WSTG.

1 Pendahuluan

Perkembangan teknologi kian hari semakin meningkat, diantaranya bidang 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 TIK pengembang merekomendasikan untuk melakukan riset secara *online* agar dapat memperbaiki kekurangan riset secara konvensional dan memberikan kesempatan bagi *reseacher* untuk mengembangkan metode penelitian dengan 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 pada bagian *client* diberikan *addons no script* dan dibagian server digunakan *frame iller*, *X frame options.*

1.2 *Penetration Testing*

Penetration Testing adalah cara untuk mengetahui kerentanan pada *system*, *identification of poor system configurations, hardware and software defects and technical weaknesses in the tested information system*. Bertujuan mencari celah keamanan yaitu sebagai mengidentifikasi. [6].

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, Pengumpulan Informasi, Pengujian Manajemen Konfigurasi dan Penerapan, Pengujian Manajemen Identitas, Pengujian Otentikasi, Pengujian Otorisasi, Pengujian Manajemen Sesi, Pengujian Validasi Input, Pengujian Untuk Penanganan Kesalahan, Pengujian Untuk Kriptografi Lemah, Pengujian Logika Bisnis, Pengujian Sisi Klien, Pengujian API.

2.2 *Tools* yang Digunakan

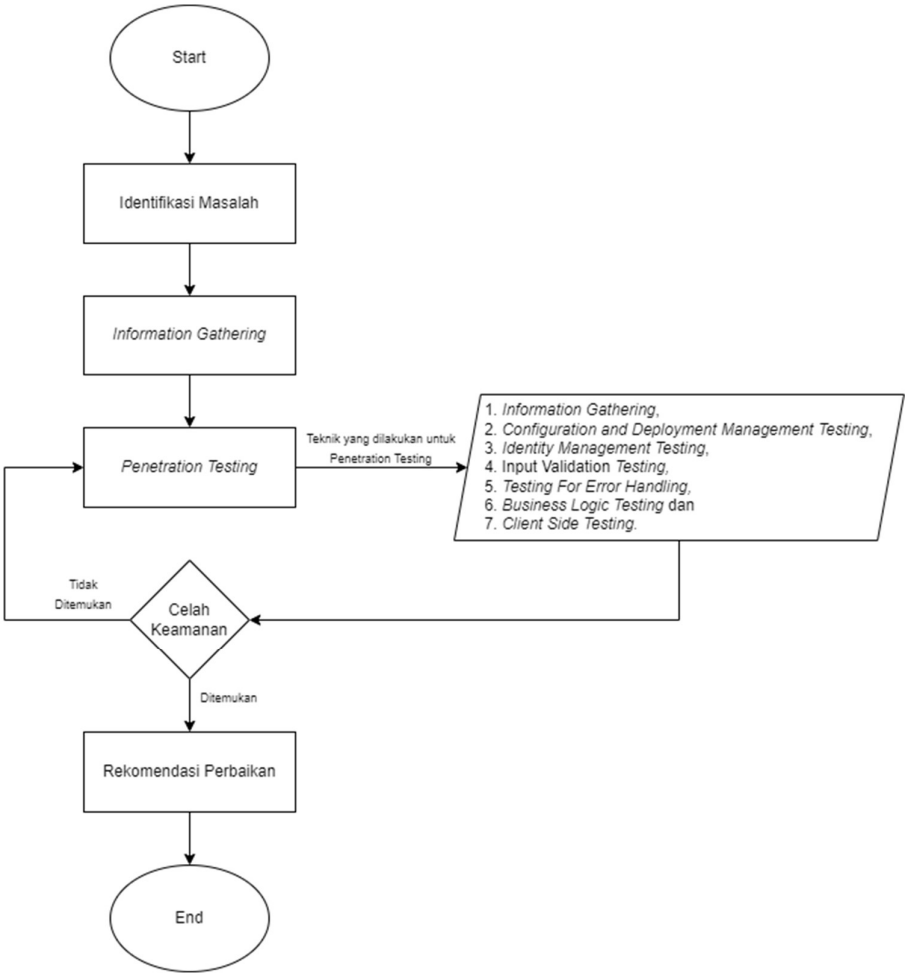
BURP *Tools*, dapat memberi gambaran umum tentang fungsionalitas dan konten aplikasi *web* target di mana ini berisi peta situs yang memberikan informasi terperinci tentang target sehingga memungkinkan untuk menetapkan ruang lingkup pengujian *penetrasi testing.*
Dirb, adalah pemindai konten *Web*, yaitu 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

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 (Pengumpulan Informasi, Pengujian Manajemen Konfigurasi dan Penerapan, Pengujian Manajemen Identitas, Pengujian Validasi Input, Pengujian Untuk Penanganan Kesalahan, Pengujian Logika Bisnis, dan Pengujian Sisi Klien) 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 menjadikan peneliti melakukan *penetration testing* untuk tema penelitian 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***
Pengumpulan Informasi berfungsi untuk menemukan komponen dan fungsionalitas dengan mengikuti URL *page* lain atau melihat peta situs *web*.

- **Melakukan Pengintaian Penemuan Mesin Pencari untuk Kebocoran Informasi**
  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.
  ***Server Web* Sidik Jari**
  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*.
- **Tinjau *Metafile Server Web* untuk Kebocoran Informasi**
  Tinjau *Metafile Server Web* untuk Kebocoran Informasi *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***
Pengujian Manajemen Konfigurasi dan Penerapan bertujuan untuk meninjau seluruh keamanan infrastruktur untuk menjaga keamanan seperti perangkat lunak *server web, server database back-end*, atau otentikasi *server.*

- **Tinjau Cadangan Lama dan *File* Tidak Direferensikan untuk Informasi Sensitif**
  Tinjau Cadangan Lama dan *File* Tidak Direferensikan untuk Informasi Sensitif 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.
- **Uji Metode HTTP**
  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***
Pengujian Manajemen Identitas 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.*

- **Uji Proses Pendaftaran Pengguna**
  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***

Pengujian Validasi Input bertujuan untuk apakah *website* rentan terhadap jenis serangan atau tidak.

- **Pengujian Untuk Skrip Lintas Situs Tersimpan**
  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***

Pengujian Untuk Penanganan Kesalahan adalah kesalahan yang timbul dengan sengaja mengirim *string* ketika *integer* diharapkan. *Input user* yang dapat diterima kode tetapi tidak dapat ditangani.

- **Pengujian Untuk Penanganan Kesalahan yang Tidak Tepat**
  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***

Pengujian Logika Bisnis tidak jauh berbeda dengan jenis pengujian yang digunakan oleh fungsional yang berfokus pada keadaan logis atau batas pengujian.

- **Uji Integritas Periksa**
  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***

Pengujian Sisi Klien adalah cara untuk mengujikan menggunakan *code injection attack* dengan menyisipkan kode berbahaya berbentuk *javascript* atau *client script code.*

- **Pengujian Untuk Skrip Situs Lintas Berbasis DOM**
  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.*
- **Menguji Berbagi Sumber Daya Lintas Asal**
  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

Penelitian ini menggunakan metode OWASP *Web Security Testing Guide* (WSTG) dan skema *black box testing* sehingga tidak semua teknik digunakan pada penelitian ini. *Authentication Testing, Authorization Testing, Session Management Testing,* tidak dapat dilakukan pengujian dikarenakan *fiture login* tidak dapat bekerja dengan baik. *Testing for Weak Cryptography* dikarenakan *website* tersebut sudah menggunakan HTTPS maka *website* tersebut

sudah terenkripsi. *API Testing*, *website* tersebut tidak menggunakan API dikarenakan *website* ini berfungsi sebagai layanan antar muka (*front end*), bukan merupakan layanan fungsi (*back end*) sehingga tidak dibuat dokumentasi API, selain itu *website* ini menggunakan *Litespeed server* yang bukan diperuntukan menyediakan API *Service* sehingga tidak dapat dilakukan API *Testing.*

Information Gathering, digunakan *BURP suite* dan *search engine google. Configuration and Deployment Management Testing* menggunakan *dirb, search engine google* dan *BURP suite. Identity Management Testing* dan Input Validation *Testing* hanya menggunakan *search engine google. Testing for Error Handling, Business Logic Testing,* dan *Client Side Testing* hanya menggunakan tools *Burp Suite.* Berikut hasil penelitian yang telah dilakukan ada *website* XYZ.

Tabel 1. Hasil dan pembahasan penelitian

Level *Risk/Score*	Metode	Hasil Temuan	Status
	Pengumpulan Informasi	Melakukan Pengintaian Penemuan Mesin Pencari untuk Kebocoran Informasi	Tidak ditemukan
5.3/10 (Medium)	Pengumpulan Informasi	*Server Web* Sidik Jari	Ditemukan
	Pengumpulan Informasi	Tinjau *Metafile Server Web* untuk Kebocoran Informasi	Tidak ditemukan
5.3/10 (Medium)	Pengujian Manajemen Konfigurasi dan Penerapan	Tinjau Cadangan Lama dan *File* Tidak Direferensikan untuk Informasi Sensitif	Ditemukan
	Pengujian Manajemen Konfigurasi dan Penerapan	Uji Metode HTTP	Tidak ditemukan
6.3/10 (Medium)	Pengujian Manajemen Identitas	Uji Proses Pendaftaran Pengguna	Ditemukan
5.3 (Medium)	Pengujian Validasi Masukan	Pengujian Untuk Skrip Lintas Situs Tersimpan	Ditemukan
5.3/10 (Medium)	Pengujian Untuk Penanganan Kesalahan	Pengujian Untuk Penanganan Kesalahan yang Tidak Tepat	Ditemukan
5.3/10 (Medium)	Pengujian Logika Bisnis	Uji Integritas Cek (Register Tanpa Checklist)	Ditemukan
5.3/10 (Medium)	Pengujian Logika Bisnis	Test Integrity Checks (Tidak Ada Validasi Input)	Ditemukan
6.5/10 (Medium)	Pengujian Logika Bisnis	Uji Integritas Cek (Wizard Pertanyaan)	Ditemukan
	Pengujian Sisi Klien	Pengujian Untuk Skrip Situs Lintas Berbasis DOM	Tidak ditemukan
	Pengujian Sisi Klien	Menguji Berbagi Sumber Daya Lintas Asal	Tidak ditemukan

5 Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil pengujian *penetration testing* di *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 Pengumpulan informasi, Pengujian Manajemen Konfigurasi dan

Penerapan, Pengujian Manajemen Identitas, Pengujian Validasi Input, Pengujian Untuk Penanganan Kesalahan, Pengujian Logika Bisnis, dan Pengujian Sisi Klien 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] First.org. (2022). Common Vulnerability Scoring System Version 3.1 Calculator. https://www.first.org/cvss/calculator/3.1. Date Accessed : 21-04-2022

[3] 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

[4] 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

[5] 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

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

[7] 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/