Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website)

I Dewa Gede Govindha Dharmawangsa[a1], Gusti Made Arya Sasmita[a2], I Putu Agus Eka Pratama[b3]
[a]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana, Bali, Indonesia
e-mail: [1]govindha@student.unud.ac.id, [2] aryasasmita@unud.ac.id, [3]eka.pratama@unud.ac.id

Abstrak

Website Pemerintah merupakan salah satu strategi di dalam melaksanakan pengembangan e-government, x instansi *mengikuti strategi ini dengan memiliki website pada alamat x, beriringan dengan perkembangan tersebut, bertambah juga serangan siber melalui website, oleh karena itu perlu dilakukan pengujian dan evaluasi berkala terhadap website dengan penetration testing. Penetration testing adalah praktik pengujian keamanan baik jaringan atau website untuk menemukan kerentanan yang dapat dieksploitasi oleh attacker. Penelitian ini didukung dengan Framework OWASP Testing Guide Versi 4.2 dengan 12 modul yang mencakup keseluruhan aspek dalam pengujian keamanan pada website. Hasil penetration testing mendapatkan celah keamanan yang selanjutnya akan dinilai kerentanannya dengan CVSS Calculator versi 3.1 kemudian diberikan saran rekomendasi setelahnya. Peneltian ini mendapatkan 32 kerentanan ,12 kerentanan diantaranya memiliki dampak pada website dengan 4 kerentanan yang memiliki risiko medium, 5 kerentanan yang memiliki risiko high dan 2 kerentanan yang memiliki risiko critical terhadap website.*

Kata kunci: *CVSS Calculator 3.1, Framework OWASP Testing Guide Versi 4.2, Penetration Testing, Website*

Abstract

Government website is one of the strategies in e-government development, x agency follows this strategy by having a website with address x, along with these developments, cyber attacks through websites also increase, therefore it is necessary to carry out periodic testing and evaluation of websites with penetration testing. Penetration testing is the security testing for network or website to find vulnerabilities that could be exploited by attackers. This research is supported by the OWASP Testing Guide Framework Version 4.2 with 12 modules covering all aspects of security testing on websites. The results of the penetration testing is found vulnerabilities then be assessed for with CVSS Calculator 3.1 and given recommendations afterward. This research finds 32 vulnerabilities, 12 of that vulnerabilities have an impact on the website with 4 vulnerabilities that have a medium risk, 5 vulnerabilities that have a high risk and 2 vulnerabilities that have a critical risk.

Keywords: *CVSS Calculator 3.1, Framework OWASP Testing Guide Version 4.2, Penetration Testing, Website*

1. Pendahuluan

Perkembangan teknologi dan internet yang telah berkembang dengan pesat di segala aspek kehidupan manusia membuat sebagian besar aktivitas dan pekerjaan mengimplementasikan internet dalam rangka untuk mendukung kinerja serta mengeluarkan hasil yang lebih baik. Implementasi internet yang dapat membantu kehidupan manusia adalah dengan penggunaan website yang akan memudahkan pekerjaan manusia karena dapat diakses kapanpun, dimanapun website memiliki peranan penting bagi setiap instansi,

perusahaan atau organisasi untuk memudahkan pihak luar dalam mengakses infomasi maupun melakukan pertukaran data. *Website* adalah kumpulan halaman web, yang menyediakan informasi visual, pendengaran dan tekstual, yang merupakan kartu kunjungan bisnis yang menyajikan organisasi atau layanan atau produk [1].

Penggunaan *website* sebagai layanan sistem informasi sudah diterapkan oleh berbagai macam kalangan termasuk dalam pemerintahan, *website* pemerintah merupakan salah satu strategi untuk mewujudkan pengembangan *e-government* secara sistematis melalui langkah yang praktis dan terukur, dimana *website* tersebut menyediakan informasi serta layanan masyarakat seperti yang dilakukan oleh x(target) instansi [2].

Keterbukaan dan kemudahan pertukaran serta pengelolaan informasi yang dilakukan pada suatu website dapat menjadi titik lemah dari suatu Lembaga pemerintahan. Informasi yang disimpan pada suatu website pemerintahan dapat berupa informasi sensitif ataupun bersifat rahasia karena menyangkut bagaimana sistem kerja pemerintahan tersebut berjalan [3]. Keamanan dan proteksi diperlukan dalam membangun suatu website untuk menjaga informasi-informasi tersebut tidak jatuh ke tangan yang salah. Terdapat berbagai cara untuk melakukan tindakan pengamanan pada suatu website oleh pihak organisasi, salah satunya dapat dilakukan dengan pengujian keamanan website dengan melakukan simulasi serangan digital terhadap website terkait, atau yang sering disebut dengan metode penetration testing [4].

Pengujian penetrasi pada website bertujuan untuk mencari celah-celah keamanan pada *website* yang nantinya dapat dikategorikan sebagai risiko kerentanan keamanan. Tahapan-tahapan yang digunakan untuk melakukan *penetration testing* pada suatu *website* terdiri dari berbagai modul yang akan disesuaikan dengan standarisasi atau *framework* yang telah tersedia. *Framework* wajib digunakan oleh penguji agar hasil pengujian bersifat valid dan dapat dipertanggung jawabkan. Terdapat dua jenis *framework* yang dapat digunakan dalam melakukan *penetration testing*, yaitu Framework ISSAF dan OWASP Testing Guide [5]. Pengujian keamanan website x menggunakan Framework OWASP. Framework pengujian sistem yang dikeluarkan oleh OWASP memiliki beberapa versi dan yang digunakan pada penelitian ini adalah Framework OWASP terbaru, yaitu OWASP Testing Guide versi 4.2 tahun 2020. *Tools* yang digunakan untuk pengujian adalah *tools* yang bersifat *open source* agar lebih memudahkan pengujian pada sisi ketersediaan.

Hasil dari pengujian tersebut akan mendapatkan kerentanan-kerentanan pada *website* (target), setelah itu dilakukan penilaian terhadap hasil pengujian dengan *Common Vulnerability Scoring System* (CVSS). Hasil pengujian keamanan tersebut nantinya ditampilkan dalam bentuk laporan evaluasi dengan saran terhadap perbaikan celah keamanan yang ditemukan. Saran yang diberikan penguji diharapkan membentuk suatu *website* yang memiliki tingkat keamanan yang tinggi.

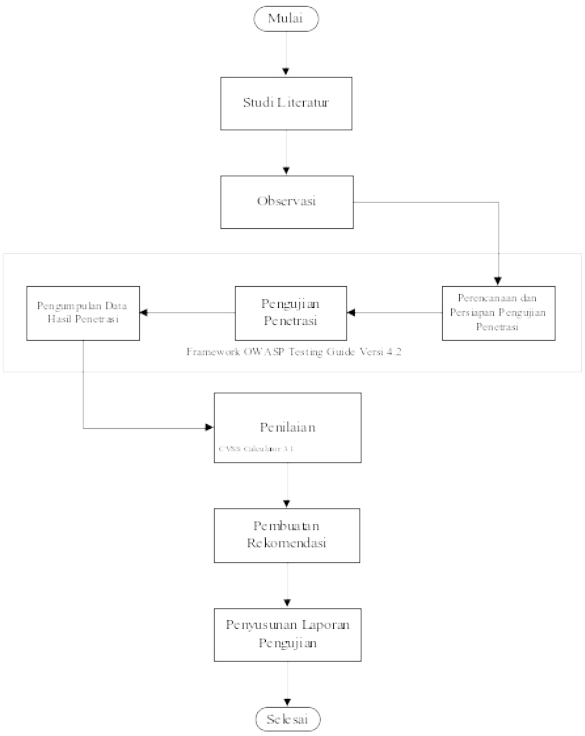
2. Metodologi Penelitian

Metode penelitian merupakan tahapan yang menjelaskan mengenai gambaran umum penelitian, gambaran umum *penetration testing*, gambaran umum website dan metode penilaian kerentanan yang dipergunakan dalam penelitian ini.

2.1. Gambaran Umum Penelitian

Gambaran umum penelitian merupakan alur proses berlangsungnya penelitian dengan output hasil penetration testing, nilai kerentanan dan rekomendasi yang diberikan.

Gambaran umum penelitian dimulai dari studi literatur, observasi, persiapan penetration testing, *penetration testing* (OWASP Testing Guide Versi 4.2), pengumpulan data hasil, penilaian kerentanan (CVSS Calculator 3.1), dan pembuatan rekomendasi serta penyusunan laporan.

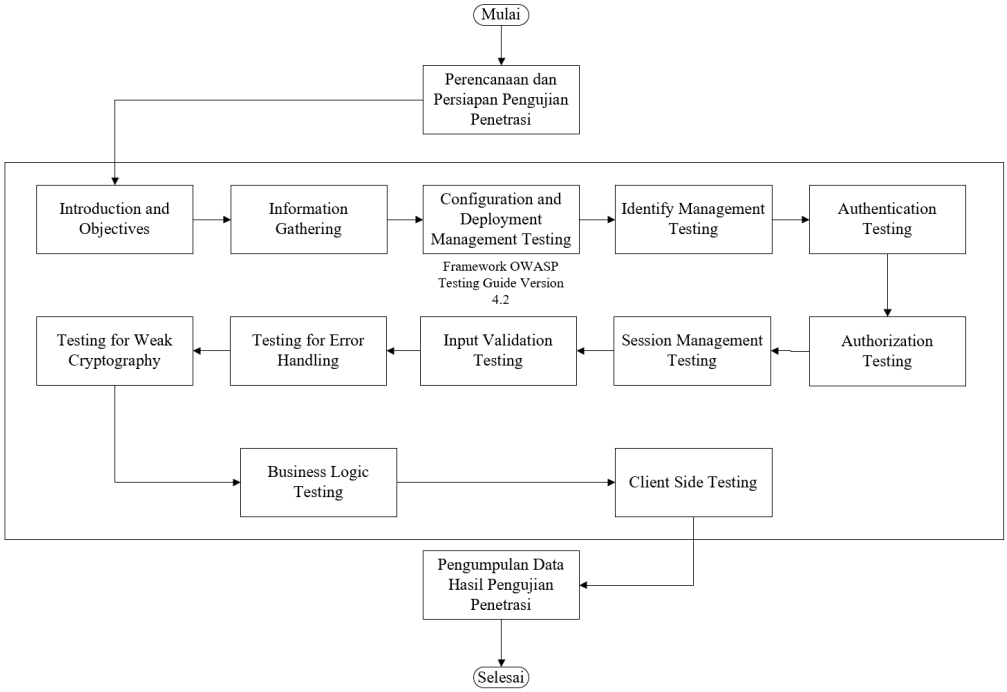


Gambar 1. Gambaran Umum Penelitian

2.2. Gambaran Umum Penetration Testing

Gambaran umum pengujian *penetration testing* merupakan proses pengujian yang dimulai dari perencanaan dan persiapan pengujian penetrasi seperti mempersiapkan *tools* untuk melakukan pengujian serta melakukan penetration testing dengan 12 modul pengujian pada *Framework* OWASP Testing Guide versi 4.2 kemudian dilakukan pencatatan mengenai hasil tersebut. Gambaran umum *penetration testing* dapat dilihat pada Gambar 2.

Penetration testing dimulai dari melakukan *Information Gathering* dilakukan dengan maksud untuk pengumpulan informasi penting mengenai komponen yang digunakan website, *Configuration and Deployment Management Testing* dengan tujuan untuk mengevaluasi konfigurasi dan manajemen protokol komunikasi, *Identity Management Testing* dengan tujuan untuk mengevaluasi syarat serta informasi yang dibutuhkan oleh *website* ketika menyimpan akun *user*, *Authentication Testing* dengan tujuan untuk melakukan uji skema otentikasi yang digunakan oleh *website* target, *Authorization Testing* dengan tujuan untuk menguji skema otorisasi pengguna, *Session Management Testing* dengan tujuan untuk menguji aspek fungsionalitas penggunaan *session*, *Input Validation Testing* dengan tujuan untuk menguji keamanan *input* dari pengguna, *Testing for Error Handling* dengan tujuan mengetahui bagaimana penanganan, pengelolaan, dan penampilan *error* yang terjadi, *Testing for Weak Cryptography* dilakukan dengan tujuan menguji tingkat keamanan dari kriptografi *website* target, *Business Logic Testing* dengan tujuan untuk menguji kerentanan yang terdapat pada mekanisme website menyelesaikan fungsionalitasnya, *Client Side Testing* dengan tujuan untuk menguji keamanan eksekusi sistem dan kode yang berjalan pada sisi klien, dan API Testing menguji API yang digunakan website.

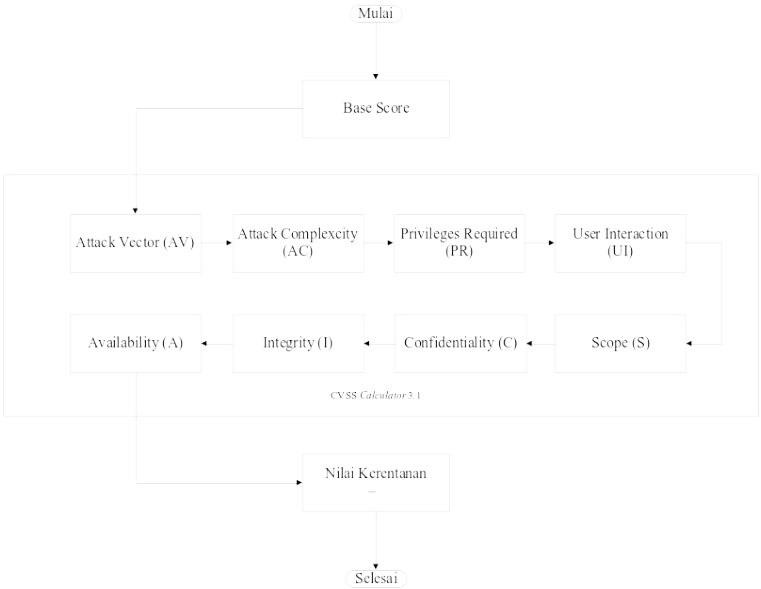


Gambar 2. Gambaran Umum Penetration Testing

2.3. Gambaran Umum Penilaian Kerentanan

Setelah dilakukan *penetration testing* untuk mencari celah kerentanan, penilaian dari celah kerentanan yang ditemukan dilakukan, untuk memberi nilai kerentanan dari *website* yang telah diuji menggunakan CVSS *calculator* versi 3.1. Gambaran umum penilaian kerentanan dapat dilihat pada Gambar 3.

Pengujian yang dinilai adalah pengujian yang yang berhasil dilakukan dan serangan tersebut tergolong serangan aktif (serangan yang mempunyai dampak langsung terhadap sistem aplikasi) dan bukan serangan pasif (hanya berupa informasi yang tidak terkait langsung ke sistem). *Input* diberikan pada CVSS *calculator* versi 3.1 dengan keluaran dari kalkulator berupa nilai kerentanan dengan rentang 0.0 sampai 10 yang akan keluar setelah semua inputan dimasukkan ke kalkulator.



Gambar 3. Gambaran Umum Penilaian Kerentanan

3. Kajian Pustaka

Kajian pustaka atau teori-teori yang digunakan sebagai penunjang dalam pelaksanaan penelitian ini dijabarkan sebagai berikut.

3.1. Website

Website sebagai layanan yang menyajikan informasi dengan konsep *hyperlink* (tautan), sehingga mempermudah pengguna internet. *Website* dapat memberikan *highlight* konten yang disajikan dalam sebuah dokumen untuk ditautkan ke media lain. *Website* dapat menghubungkan dari berbagai lokasi dalam sebuah dokumen atau gambar ke berbagai lokasi di dokumen lain. Dengan sebuah *browser*, tautan dapat di hubungkan ke tujuannya dengan mengklik tautan tersebut [6].

3.2. Penetration Testing

Penetration testing adalah praktik pengujian keamanan baik jaringan atau website untuk menemukan kerentanan yang dapat dieksploitasi oleh *attacker* dengan memberikan tahapan serangan sistem ke sistem yang sedang berjalan [7]. *Penetration testing* dilakukan dengan serangan nyata untuk menilai kerentanan pada target uji, selain itu penguji juga mengeksploitasi kerentanan tersebut untuk menilai apa yang mungkin didapat oleh penyerang [8].

3.3. OWASP

Open Web Application Security Project (OWASP) adalah organisasi *non-profit* yang berfokus pada peningkatan keamanan perangkat lunak. Misi OWASP adalah membuat keamanan perangkat lunak diperhatikan, sehingga individu dan organisasi dapat membuat keputusan yang tepat. OWASP ada untuk memberikan informasi praktis dan tidak memihak tentang *appsec* kepada individu, perusahaan, universitas, lembaga pemerintah, dan organisasi lain di seluruh dunia. Beroperasi sebagai komunitas profesional yang berpikiran sama, OWASP mengeluarkan alat perangkat lunak dan dokumentasi berbasis pengetahuan tentang keamanan aplikasi [9].

OWASP sudah banyak dijadikan standar keamanan dalam melakukan penilaian terhadap sebuah aplikasi yang dibuat oleh berbagai macam organisasi, termasuk lembaga pemerintahan, universitas, perusahaan startup, dll. OWASP juga memiliki projek aplikasi keamanan yang digunakan pada kali linux yaitu OWASP ZAP dan OWASP Dirbuster. Selain aplikasi OWASP juga membuat penelitian mengenai isu-isu security, salah satunya *Top 10 Application Risk* yang terakhir kali diupdate pada tahun 2019 [9].

3.4. CVSS

Common Vulnerability Scoring System (CVSS) adalah open *framework* untuk menilai karakteristik dan tingkat kerentanan perangkat lunak, perangkat keras, dan *firmware* dalam bentuk kalkulator *online* yang memberikan keluaran nilai tingkat kerentanan sistem. CVSS dimiliki dan dimanajemen oleh FIRST.Org,Inc. First adalah perusahaan *non-pofit* dari Amerika yang misinya membantu dalam hal keamanan komputer [10]. CVSS menilai beberapa aspek dalam kerentanan yang dibagi menjadi 8 bagian, yaitu: *Attack Vector, Attack Complexity, Privilege Required, User Interaction, Scope, Confidentiality, Integrity, dan Availability.* CVSS menilai kerentanan dari rentang 0.0 sampai 10.0 yang dibagi menjadi 4 level, yakni *Low* (0.0 sampai 3.9), *Medium* (4.0 sampai 6.9), *High* (7.0 sampai 8.9), dan *Critical* (9.0 sampai 10.0)

4. Hasil dan Pembahasan

Hasil dan pembahasan membahas secara rinci mengenai hasil penetration testing dengan OWASP Testing Guide Versi 4.2 dan penilaian kerentanan dengan CVSS Calculator 3.1.

4.1 Hasil Penetration Testing

Tabel 1 menunjukkan hasil penetration testing website (target) dengan OWASP Testing Guide Versi 4.2. Dari 12 modul, 97 total submodul diujikan dan mendapatkan hasil 21 submodul sukses dijalankan, 34 submodul gagal, dan 42 submodul dilewati

Tabel 1. Hasil Penetration Testing

Modul	Jumlah Submodul	Hasil Pengujian
Information Gathering	10	4 Sukses, 6 Gagal
Configuration and Deployment Management Testing	11	1 Sukses, 6 Gagal, 4 Dilewati
Identity Management Testing	5	3 Gagal, 2 Dilewati
Authentication Testing	10	4 Sukses, 6 Dilewati
Authorization Testing	4	4 Dilewati
Session Management Testing	9	1 Sukses, 4 Gagal, 4 Dilewati
Input Validation Testing	19	3 Sukses, 6 Gagal, 10 Dilewati
Testing for Error Handling	2	2 Sukses
Testing for Weak Cryptography	4	1 Sukses, 2 Gagal, 1 Dilewati
Business Logic Testing	9	2 Sukses, 4 Gagal, 3 Dilewati
Client Side Testing	13	3 Sukses, 3 Gagal, 7 Dilewati
API Testing	1	1 Dilewati

4.2 Penilaian Kerentanan

Penilaian kerentanan dilakukan dengan CVSS *calculator* versi 3.1, pengujian yang dinilai adalah pengujian yang yang berhasil dilakukan dan serangan tersebut tergolong serangan aktif (serangan yang mempunyai dampak langsung terhadap sistem aplikasi) dan bukan serangan pasif (hanya berupa informasi yang tidak terkait langsung ke sistem).

4.2.1 Test Network Infrastructure Configuration (WSTG-CONF-01)

Sistem gagal pada pengujian WSTG-CONF-01 karena ditemukan *vulnerability* pada servis (versi lama) yang digunakan pada *website* target.

4.2.1.1 Halaman x

Halaman x dengan url x dan IP x memiliki 2 *vulnerability* yang dapat dilihat pada tabel 2. Tabel 2 menunjukan versi dari aplikasi yang digunakan halaman x berserta *vulnerability* dari servis tersebut dengan nilai CVSS dari NVD (National Vulnerability Database).

Tabel 2. Tabel Vulnerability Halaman x

Servis	Port	Versi	Vulnerability	Nilai CVSS
Apache	80, 443	Apache 2.4.6 (CentOS)	CVE-2014-0118	4,3 (Medium)
SSH	22	OpenSSH 7.4 (protocol 2.0)	CVE-2017-15906	5,3 (Medium)

4.2.1.2 Halaman x

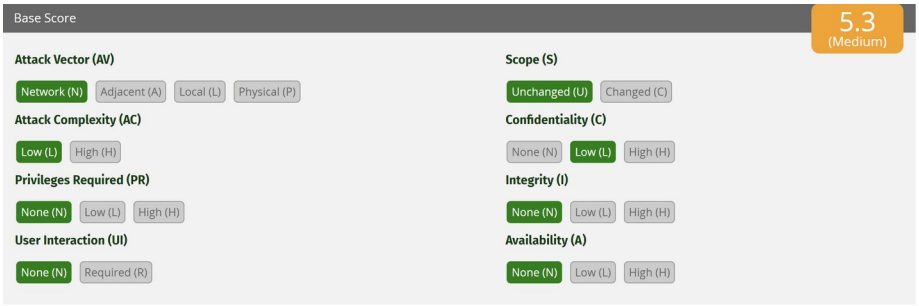
Halaman x dengan url x dan IP x memiliki 2 *vulnerability* yang dapat dilihat pada tabel 3. Tabel 3 menunjukan versi dari aplikasi yang digunakan halaman x berserta *vulnerability* dari servis tersebut beserta nilai CVSS dari NVD (National Vulnerability Database).

Tabel 3. Tabel Vulnerability Halaman x

Servis	Port	Versi	Vulnerability	Nilai CVSS
Domain	53	PowerDNS Authoritative Server 4.4.1	CVE-2021-27227	Belum di publish
SSH (Closed)	22	OpenSSH 7.4 (protocol 2.0)	CVE-2017-15906	5,3 (Medium)

4.2.2 Testing for Credentials Transported over an Encrypted Channel (WSTG-ATHN-01)

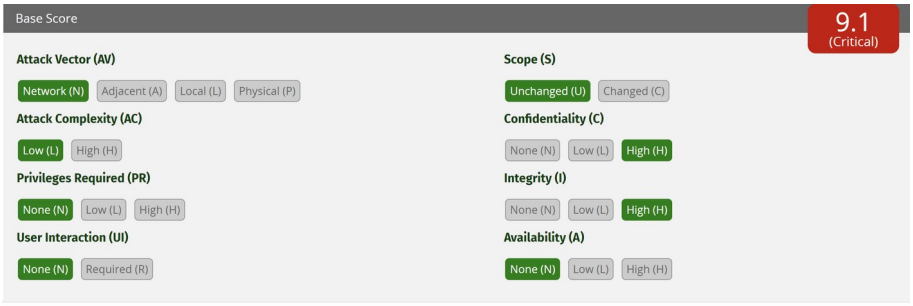
Sistem gagal pada pengujian WSTG-ATHN-001 karena data yang dikirim ke server tidak di enkripsi, sehingga jika ada yang melakukan *sniffing* pada lalu lintas pertukaran data, data yang dikirim dapat dilihat. Nilai kerentanan pengujian WSTG-ATHN-01 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 5.3 (Medium) yang dapat dilihat pada Gambar 4.



Gambar 4. Nilai WSTG-ATHN-01

4.2.3 Testing for Default Credentials (WSTG-ATHN-02)

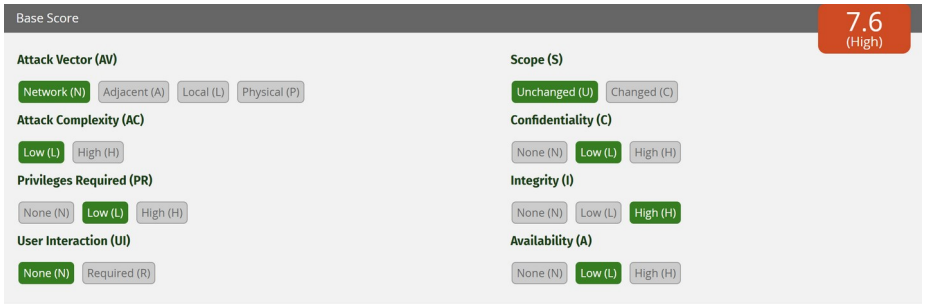
Sistem gagal pada pengujian WSTG-ATHN-02, tidak ditemukan pada sistem yang menggunakan *tools third* dengan *default credentials* seperti “admin”, “user” dan *default credentials* lainnya, namun pada saat pengujian didapati beberapa sub domain yang terdapat *login page* masih menggunakan *default credentials*. Nilai kerentanan pengujian WSTG-ATHN-02 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 9.1 (Critical) seperti pada Gambar 5.



Gambar 5. Nilai WSTG-ATHN-02

4.2.4 Testing for Reflected Cross Site Scripting (WSTG-INPV-01)

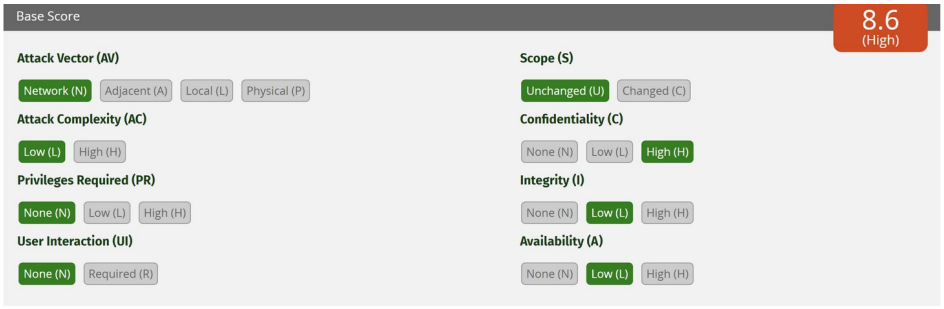
Sistem gagal pada pengujian WSTG-INPV-01 karena inputan pengguna berupa kode html tetap diterima oleh *website* target dan tetap di refleksikan kembali sebagai kode html seperti yang diinginakn penguji (namun tidak disimpan di *database*). Nilai kerentanan pengujian WSTG-INPV-01 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 7.6 (Critical) seperti pada gambar 6.



Gambar 6. Nilai WSTG-INPV-01

4.2.5 Testing for Stored Cross Site Scripting (WSTG-INPV-02)

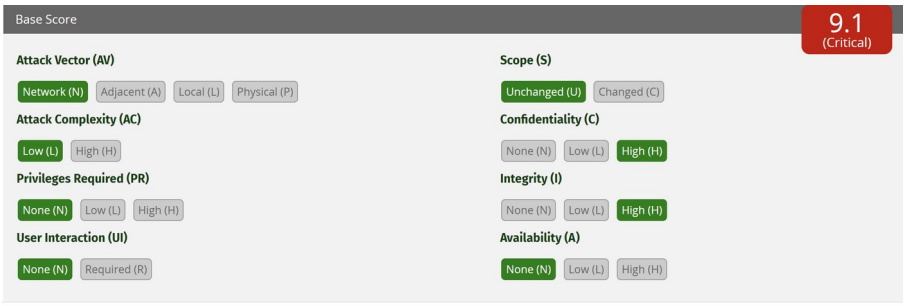
Pengujian gagal karena inputan pengguna berupa kode html tetap diterima oleh *website* target dan tetap di refleksikan kembali sebagai kode html sesuai keinginan penguji dan disimpan di database. Nilai kerentanan pengujian WSTG-INPV-02 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 8.6 (Critical) seperti pada gambar 7.



Gambar 7. Nilai WSTG-INPV-02

4.2.6 Testing for SQL Injection (WSTG-INPV-05)

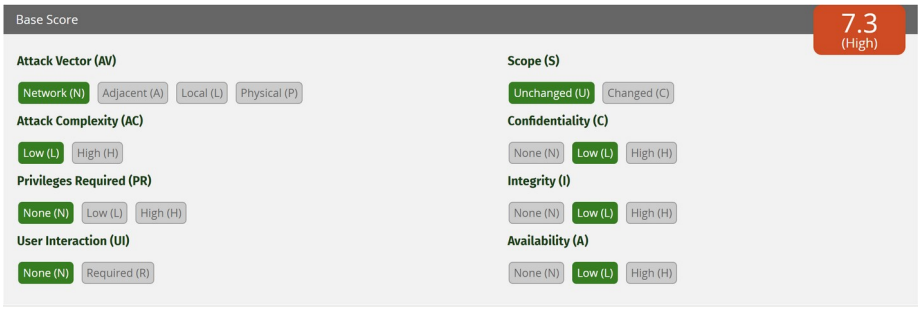
Sistem gagal pada pengujian WSTG-INPV-05, karena SQL Injection berhasil dilakukan, sehingga *bypass* login berhasil dilakukan. Nilai kerentanan pengujian WSTG-INPV-05 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 9.1 (Critical) seperti pada gambar 8.



Gambar 8. Nilai WSTG-INPV-05

4.2.7 Testing for Improper Error Handling (WSTG-ERRH-01)

Sistem gagal pada pengujian WSTG-ERRH-01, karena error yang terjadi pada website target terlihat jelas alasannya dengan kata lain website target tidak melakukan penanganan error dengan baik. Nilai kerentanan pengujian WSTG-ERRH-01 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 7.3 (High) seperti pada gambar 9.



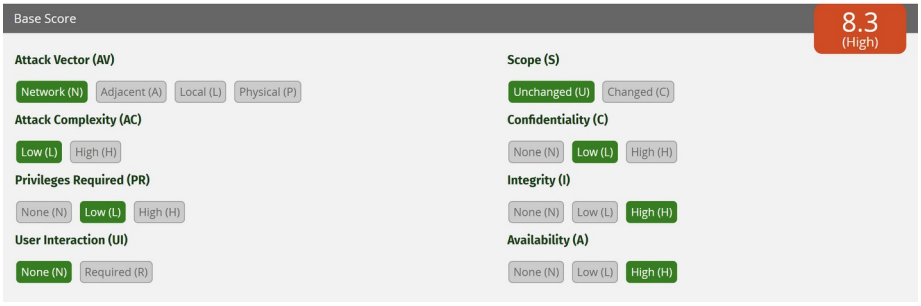
Gambar 9. Nilai WSTG-INPV-05

4.2.8 Testing for Weak Transport Layer Security (WSTG-CRYP-01)

Sistem gagal pada pengujian WSTG-CRYP-01 karena hasil scanning tool Nessus di Halaman x dengan url x sertifikat SSL tidak bisa dipercaya, dengan hasil penilaian CVSS Calculator 3.1 di pengujian WSTG-CRYP-01 adalah 6.4 (Medium).

4.2.9 Testing for DOM-Based Cross Site Scripting (WSTG-CLNT-01)

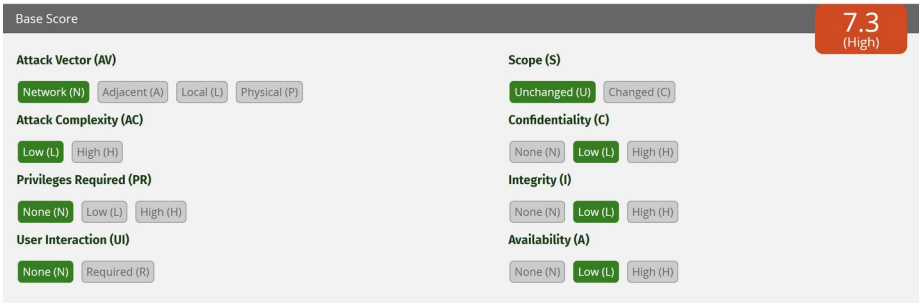
Sistem gagal pada pengujian WSTG-CLNT-01, karena inputan user dapat merubah DOM (Document Object Model) yang berisi kode html (tag Doctype, tag html, tag head, dan tag body). Nilai kerentanan pengujian WSTG-CLNT-01 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 8.3 (High) seperti pada gambar 10.



Gambar 10. Nilai WSTG-CLNT-01

4.2.10 Testing for HTML Injection (WSTG-CLNT-03)

Sistem gagal pada pengujian WSTG-CLNT-03, karena pengujian XSS (Cross-site scripting) dengan memasukkan kode javascript ke dalam elemen HTML melalui parameter yang terdapat di URL berhasil dilakukan. Nilai kerentanan pengujian WSTG-CLNT-03 yang dihitung menggunakan CVSS Calculator 3.1 mendapatkan hasil akhir 7.3 (High) seperti pada gambar 11.



Gambar 11. Nilai WSTG-CLNT-01

5. Kesimpulan

Berdasarkan hasil *penetration testing* yang dilakukan dengan OWASP Testing Guide Versi 4.2, dari dua belas modul yang telah diuji dengan 97 submodul, didapatkan hasil *website* gagal melewati 21 pengujian, *website* berhasil melewati 34 pengujian, dan 42 pengujian dilewati karena *website* tidak memenuhi kriteria pengujian. Pengujian yang berhasil dilakukan kemudian dipilih yang memiliki dampak untuk dinilai dengan CVSS *Calculator* 3.1. Terdapat 4 kerentanan yang memiliki risiko *medium*, 5 kerentanan yang memiliki risiko *high* dan 2 kerentanan yang memiliki risiko *critical* terhadap *website*. Pemberian saran diberikan berdasarkan hasil *penetration testing* dengan OWASP Testing Guide Versi 4.2 dan penilai kerentanan dengan CVSS *Calculator* 3.1. Secara ringkas, saran yang dapat diberikan kepada pihak instansi x yang mengelola *website* adalah melakukan *update* menggunakan versi terbaru dari servis yang digunakan, melakukan tambahan validasi pada setiap halaman *login* dengan OTP, menambahkan fitur batasan untuk mencoba melakukan login, jeda waktu yang diberikan jika user selalu gagal melakukan login, melakukan enkripsi disisi client sebelum request dikirimkan, menghapus default credentials pada database user, menambahkan proteksi Cross Site Request Forgery (CSRF), melakukan filterisasi pada inputan pengguna sesuai dengan inputan yang diharapkan, melakukan encode data pada output dalam bentuk respon HTTP, menggunakan Content-Type dan X-Content-Type-Options headers untuk memastikan bahwa browser menginterpretasikan respon sesuai keinginan kita, menggunakan Content Security Policy (CSP) untuk mengurangi kerentanan XSS yang masih terjadi, memperbaiki syntaq SQL pada halaman yang berhasil dilakukan SQL injection, melakukan penanganan error dengan baik tanpa memperlihatkan kesalahan kode program pada preview error¸ mengganti sertifikasi SSL yang digunakan, dan menonaktifkan fungsi penting saat serangan diindikasikan.

Daftar Pustaka

[1] Margarita Isooraite. (2020). Internet Website Analysis. *International Journal of Trend in Scientific Research and Development*, *5*(1), 9–12.

[2] KOMINFO. (2018). *Website Pemerintah Daerah Sangat Penting*. https://kominfo.bone.go.id/2018/12/05/website-pemerintah-daerah-sangat-penting/

[3] Trull, J. (2012). Security Through Effective Penetration Testing. *ISACA Journal*, *2*, 1–5.

[4] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

[5] Shanley, A., & Johnstone, M. N. (2015). Selection of penetration testing methodologies: A comparison and evaluation. Australian Information Security Management Conference, AISM 2015, 2015, 65–72. https://doi.org/10.4225/75/57b69c4ed938d

[6] Susilo, M. (2018). Rancang Bangun Website Toko Online Menggunakan Metode Waterfall. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *2*(2), 98–105. https://doi.org/10.30743/infotekjar.v2i2.171

[7] Yeboah-Ofori, A. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 87–98. https://doi.org/10.17781/p002378

[8] Azis, H., & Fattah, F. (2019). Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing. *ILKOM Jurnal Ilmiah*, *11*(2), 167–174. https://doi.org/10.33096/ilkom.v11i2.447.167-174

[9] OWASP. (2021). *OWASP Web Security Testing Guideo Title*. https://owasp.org/www-project-web-security-testing-guide/

[10] First. (2019). *CVSS v3.1User Guide*. 1–22. https://www.first.org/cvss/