**JURNAL INFORMATIKA DAN TEKONOLOGI KOMPUTER**
Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/jitek
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

DOI : https://doi.org/10.55606/jitek.v3i2.908

# ANALISIS PERBANDINGAN *VULNERABILITY SCANNING* PADA *WEBSITE* DVWA MENGGUNAKAN OWASP NIKTO DAN BURPSUITE

**Ni Putu Ana Rainita [a], Anak Agung Istri Callysta Athalia[b], Made Diva Putera Ananta [c], I Ketut Pratista Tri Pramana[d], Gede Arna Jude Saskara [e], I Made Edy Listartha[f]**

[a] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, ana.rainita@undiksha.ac.id, Universitas Pendidikan Ganesha
[b] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, anak.agung.istri.11@undiksha.ac.id Universitas Pendidikan Ganesha
[c] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, diva.putera@undiksha.ac.id, Universitas Pendidikan Ganesha
[d] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika pratista@undiksha.ac.id, Universitas Pendidikan Ganesha
[e] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, jude.saskara@undiksha.ac.id, Universitas Pendidikan Ganesha
[f] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, listartha@undiksha.ac.id, Universitas Pendidikan Ganesha

## ABSTRACT

*Information technology from time to time is growing rapidly and has become part of human life in this modern era, with these developments, websites have an important role, however, existing developments also have an impact on the security of a website, testing web servers is very important. important thing to do, this test aims to test whether the web server is safe or not from the crimes of hackers. Appropriate methods and techniques are needed to see possible vulnerabilities in components, libraries and systems that underlie web applications used in anticipating this, OWASP, Nikto, and Burp Suite tools can be used to test website security vulnerabilities. Each tool has differences in terms of speed or duration, results, or scanned objects. The research objective of this article is how to analyze a comparison of tools in testing website security vulnerabilities. Therefore, the results of detection or analysis of website vulnerabilities are then compared based on scanned objects, duration, and results to then suggest tools that are effective and efficient in their use.*

**Keywords**: Vulnerability Scanning, OWASP, Nikto, Burp Suite, Ethical Hacking.

## Abstrak

Teknologi informasi dari waktu ke waktu semakin berkembang pesat dan sudah menjadi bagian dari kehidupan manusia di era modern ini, dengan adanya perkembangan tersebut, *website* memiliki peran penting, namun, perkembangan yang ada juga memiliki dampak terhadap keamanan dari suatu *website*, pengujian terhadap *web server* sangatlah penting dilakukan, pengujian ini bertujuan untuk menguji apakah *web server* sudah aman atau belum dari tindak kejahatan para *hacker*. Metode dan teknik yang tepat diperlukan dalam melihat kemungkinan-kemungkinan kerentanan pada komponen, pustaka dan sistem yang mendasari aplikasi web yang digunakan dalam mengantisipasi hal tersebut, *tools OWASP*, Nikto, dan Burp Suite dapat dimanfaatkan untuk menguji celah keamanan *website.* Masing-masing *tools* memiliki perbedaan dari segi kecepatan atau durasi, hasil, ataupun objek *scan.* Adapun tujuan penelitian artikel ini adalah bagaimana menganalisis perbandingan *tools* dalam menguji celah keamanan *website.* Maka dari itu, hasil deteksi atau analisis kerentanan *website* kemudian dibandingkan berdasarkan objek scan, durasi, dan hasil untuk kemudian menyarankan *tools* yang efektif dan efisien dalam penggunaannya.

**Kata Kunci**: *Vulnerability Scanning, OWASP, Nikto, Burp Suite, Ethical Hacking.*

*Received Desember 30, 2022; Revised Januari 22, 2023; Accepted Juli 15, 2023*

## 1. PENDAHULUAN

Teknologi informasi dari waktu ke waktu berkembang dengan pesat dan sudah menjadi bagian dari kehidupan manusia di era modern saat ini. Pesatnya perkembangan teknologi informasi telah memberikan dampak positif di berbagai bidang, dan salah satu bidang yang mendapat manfaat dari perkembangan teknologi informasi adalah teknologi internet. Selaras dengan kemajuan atau perkembangan tersebut, sebagian besar orang telah lumrah dengan keberadaan teknologi informasi salah satunya *website* dan berbanding lurus dengan intensitas yang tinggi dari pengguna layanan internet yang juga berkembang pesat, menurut laporan digital yang dibuat oleh *We Are Social (Hootsuite),* pengguna internet pada awal Januari 2021 sudah mencapai 202,6 juta pengguna, dan di Indonesia pertumbuhan pengguna yang mengakses internet sebesar 274,9 juta jiwa, artinya penetrasi internet di Indonesia telah mencapai 73,7% pada awal tahun 2021 (Ramadhan, 2020). Dengan semakin bertambahnya pengguna internet di Indonesia menandakan bahwa masyarakat Indonesia lebih banyak memperoleh informasi melalui internet. Website dapat diartikan sebagai kumpulan halaman yang menampilkan informasi data teks, data gambar, data animasi, suara, video dan gabungan dari semuanta, baik yang bersifat status maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait, dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink)* [1] Website menyediakan sumber data dan informasi yang dapat diakses oleh siapa saja melalui internet dengan menggunakan perangkat lunak browser seperti Internet Explorer, Mozilla Firefox Browser Opera dan Google Chrome. Jumlah website yang berhasil tercipta dan jumlah pengakses dari suatu website tersebut yang terhitung banyak karena kemudahan dalam pengaksesan suatu website membuat website yang ada rentan untuk diretas dan tidak dapat dipungkiri, aspek keamanan sebuah website dapat dimanfaatkan oleh orang yang tidak bertanggung jawab dengan melakukan peretasan. Didukung dengan adanya teori CIA Triad. CIA Triad yang terdiri dari aspek kerahasiaan (*Confidentiality)*, integritas (*Integrity),* dan ketersediaan (*Avaibality),* keamanan dari suatu website dapat dianalisa dengan cara-cara tertentu dalam menjaga dan meningkatkan keamanan dari suatu website [2]

Salah satu cara yang dapat digunakan dalam tindakan awal sebelum proses analisis yaitu dengan *vulnerability scanning.* Cara ini merupakan tindakan yang menghasilkan *output* berupa kelemahan-kelemahan dari *website* yang dipindai disertai dengan informasi lainnya yang bergantung dengan apa yang ditawarkan di dalam suatu *tools* artikel ini bertujuan untuk membandingkan *tools* yang ada di dalam kali linux yaitu Nikto, *OWASP*, dan Burp Suite. Adapun objek atau target pada penelitian ini yaitu *website* yang memang disediakan guna melaksanakan *ethical hacking* dalam kata lain digunakan untuk pendidikan, *website* ini bernama DVWA. Ketiga *tools* tersebut digunakan untuk mengenali kerentanan yang ada dalam web, untuk mengetahui kerentanan yang terdapat pada *website* ini bernama DVWA. Ketiga *tools* tersebut digunakan untuk mengenali kerentanan yang ada dalam web, untuk mengetahui kerentanan yang terdapat pada *website* dapat dilakukan dengan cara *vulnerability scanning*, dengan vulnerability ini akan menjadi pertimbangan bagi developer untuk mengambil tindakan pencegahan dan mengetahui cara kerja dari *attackers* [3[3]

## 2. TINJAUAN PUSTAK

### 2.1. Keamanan Informasi

G. J. Simons mengemukakan bahwa Keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating)* atau bisa mendeteksi adanya adanya penipuan pada sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalan suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information),* informasi dipegang oleh orang yang berwenang (*right people),*

### 2.2. *Vulnerability Scanning*

*Vulnerability* merupakan suatu poin kelemahan dimana suatu sistem rentan terhadap serangan. Sebuah ancaman (*threats*) adalah suatu hal yang berbahaya bagi keberlangsungan system. *Vullnerability scanning* adalah proses mendefinisikan, mengidentifikasi, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dan memberikan organisasi melakukan penilaian dengan pengetahuan, kesadaran, dan latar belakang risiko yang diperlukan untuk memahami ancaman terhadap lingkungannya dan bereaksi dengan tepat.

### 2.3. *Website*
Website dapat diartikan sebagai kumpulan halaman yang menampilkan informasi data teks, data gambar, data animasi, suara, video dan gabungan dari semuanta, baik yang bersifat status maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait, dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink*[1] *Website* menyediakan sumber data dan informasi yang dapat diakses oleh siapa saja melalui internet dengan menggunakan perangkat lunak *browser* seperti *Internet Explorer, Mozilla Firefox Browser Opera* dan *Google Chrome.*

### 2.4. Kerentanan *Website*
Kerentanan website merupakan celah keamanan yang bisa diakses oleh pihak yang tidak bertanggung jawab dan memungkinkan peretas untuk masuk ke dalam sistem.

### 2.5. OWASP (*Open Web Application Security)*
*OWASP* adalah komunitas terbuka yang memungkinkan organisasi untuk mengembangkan, membeli dan memlihara aplikasi yang dapat dipercaya. *OWASP* tidak terafilisi dengan perusahaan maupun, dan merupakan komunitas non-profit yang memastikan kesuksesan jangka panjang proyek [4] Berdasarkan standar yang dikeluarkan oleh OWASP terdapat sebelas langkah yang dapat dilakukan untuk menilai dan menguji keamanan pada sebuah website, berupa : *Information Gathering, Configuration Management, Secure Transmission, Authentication, Session Management, Authorization, Cryptography, Data Validation, Denial of Service, Error Handling*[5]. Mendeteksi kerentanan keamanan aplikasi website menggunakan metode Owasp untuk pneliaian *risk rating* membantu pengelola dan pengembang sistem untuk penilaian *risk rating* [5]

### 2.6. Burp Suite
Burp suite bekerja dengan membangun proxy dan melakukan interupsi ke setiap request dan respon dari komunikasi dengan aplikasi web. Brup suite memiliki banyak alat yang diintegrasikan dan dapat bekerja dalam mode pasif maupun aktif, mode ini memungkinkan pengujian kerentanan berjalan pada seluruh proses pengujian aplikasi web mulai dari proses identifikasi dan eksploitasi kerentanan. [6]

### 2.7. Nikto
Nikto adalah sebuah webserver paket FIN, URG, dan PUSH ke *port* sasaran. Berdasarkan RCF 739, sistem sasaran akan mengembalikan suatu RST untuk RST untuk semua port yang tertutup [7[7]

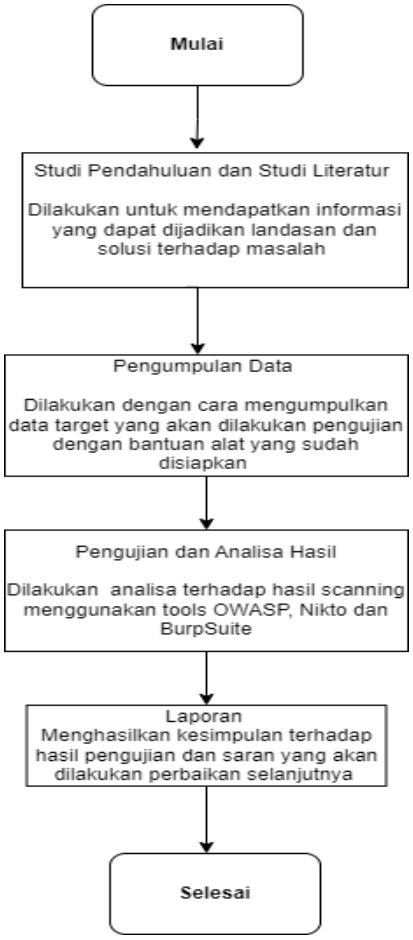
### 2.8. *Damn Vulnerable Web Application* (DVWA)
*Damn vulnerable web application* (DVWA) adalah aplikasi spesial untuk uji celah keamanan, berjalan menggunakan service apache web server yang berjalan pada protokol HTTP [8]

### 2.9. *Vulnerability Asesment*
*Vulnerability asesment* ialah keranga kegiatan abstrak global yang seleksi, tercantum arti kegiatan abstrak global yang seleksi, tercantum arti kerentanan yang memastikan resiko buat pengukuran. Perihal ini pula terkait pada tujuan konsumen hasil evaluasi yang bisa berkisar dari hasrat buat menginformasikan kebijaksanaan global ataupun buat merunjuk aksi ditingkat publik[[9]]

### 2.10. *Ethical Hacking*
*Ethical hacking* adalah suatu metode meliputi penggunaan aplikasi hacking, trik-trik dan teknik untuk mengidentifikasi vulnerability dari sistem guna memastikan keamanannya [[10]]

## 3. METODOLOGI PENELITIAN
Metode penelitian laporan ini dapat digambarkan sebagaimana pada gambar 1. Berdasarkan skema pada gambar 1 dapat dijelaskan bahwa metode penelitian ini menggunakan teknik studi literatur dan teknik pengumpulan data dalam hal ini menggunakan observasi non partisipan yang mana, teknik ini menempatkan diri sebagai pengamat yang tidak secara langsung terlibat di dalam sistem. Berdasarkan hasil pengamatan dilakukan pengujian dengan teknik dan bantuan alat yang sudah disiapkan, untuk gambaran umum pengujian, dapat dijelaskan bahwa langkah pengujian menggunakan *tools* Nikto dimulai dari informasi yang didapatkan terkait dengan IP dari *website* DVWA, informasi IP ini berkaitan dengan target pengujian selanjutnya

melakukan pengujian menggunakan *tools* Burp Suite, sedangkan untuk *tools OWASP* menggunakan *automated scan* dengan menggunakan tautan *website.* target pengujian selanjutnya yaitu melakukan *scanning* dan membuktikan adanya kerentanan dari masing-masing bagian. Tahapan paling terakhir adalah pembuatan laporan hasil pengujian *vulnerability scanning* dari *tools OWASP*, Nikto dan Burp Suite.



Gambar 1. Alur Penelitian

## 4. HASIL DAN PEMBAHASAN

Tahap awal dalam melakukan pengujian celah keamanan menggunakan ketiga *tools* ini adalah dengan melakukan persiapan dengan membuka DVWA untuk selanjutnya mengumpulkan informasi dari target yang dapat berupa IP yang tahapan selanjutnya yaitu membuka IP tersebut pada *browser* sehingga mendapatkan *link* atau tautan yang selanjutnya akan melaksanakan tahapan *scanning.* Tahapan selanjutnya yaitu melakukan proses pemindaian atau *scanning* terhadap informasi baik berupa IP ataupun *link* pada masing-masing *tools.*

### 4.1 *Hasil Scanning* Menggunakan *Tools* Nikto

| 10.10.47.95 / 10.10.47.95 port 80 | |
|---|---|
| **Target IP** | 10.10.47.95 |
| **Target hostname** | 10.10.47.95 |
| **Target Port** | 80 |
| **HTTP Server** | Apache/2.4.10 (Debian) |
| **Site Link (Name)** | http://10.10.47.95:80/ |
| **Site Link (IP)** | http://10.10.47.95:80/ |

| | |
|---|---|
| **URI** | / |
| **HTTP Method** | GET |
| **Description** | The anti-clickjacking X-Frame-Options header is not present. |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | / |
| **HTTP Method** | GET |
| **Description** | The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | / |
| **HTTP Method** | GET |
| **Description** | The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | / |
| **HTTP Method** | GET |
| **Description** | Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 587d26e84300b, mtime: gzip |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |

Gambar 2. Hasil *Scanning Tools* Nikto

| | |
|---|---|
| **URI** | / |
| **HTTP Method** | HEAD |
| **Description** | Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch. |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | / |
| **HTTP Method** | OPTIONS |
| **Description** | Allowed HTTP Methods: GET, HEAD, POST, OPTIONS |
| **Test Links** | http://10.10.47.95:80/<br>http://10.10.47.95:80/ |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | /phpmyadmin/changelog.php |
| **HTTP Method** | GET |
| **Description** | Uncommon header 'x-ob_mode' found, with contents: 0 |
| **Test Links** | http://10.10.47.95:80/phpmyadmin/changelog.php<br>http://10.10.47.95:80/phpmyadmin/changelog.php |
| **OSVDB Entries** | OSVDB-0 |
| **URI** | /icons/README |
| **HTTP Method** | GET |
| **Description** | /icons/README: Apache default file found. |
| **Test Links** | http://10.10.47.95:80/icons/README<br>http://10.10.47.95:80/icons/README |
| **OSVDB Entries** | OSVDB-3233 |
| **URI** | /phpmyadmin/ |
| **HTTP Method** | GET |
| **Description** | /phpmyadmin/: phpMyAdmin directory found |
| **Test Links** | http://10.10.47.95:80/phpmyadmin/<br>http://10.10.47.95:80/phpmyadmin/ |
| **OSVDB Entries** | OSVDB-0 |

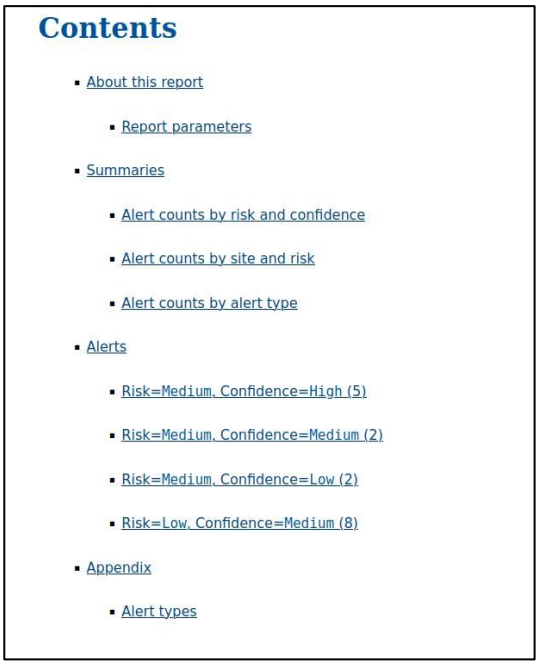
Gambar 3. Hasil *Scanning Tools* Nikto

| Host Summary | |
|---|---|
| **Start Time** | 2022-11-22 00:25:39 |
| **End Time** | 2022-11-22 00:26:47 |
| **Elapsed Time** | 68 seconds |
| **Statistics** | 8041 requests, 0 errors, 9 findings |

| Scan Summary | |
|---|---|
| **Software Details** | Nikto 2.1.6 |
| **CLI Options** | -output hasil_scan_dvwa.html -h 10.10.47.95 |
| **Hosts Tested** | 1 |
| **Start Time** | Tue Nov 22 00:25:39 2022 |
| **End Time** | Tue Nov 22 00:26:47 2022 |
| **Elapsed Time** | 68 seconds |

Gambar4. Hasil *Scanning Tools* Nikto

### 4.2 *Hasil Scanning Menggunakan Tools OWASP*




Gambar 4. Hasil *Scanning Tools OWASP*

| | | Confidence | | | | |
|---|---|---|---|---|---|---|
| | | User Confirmed | High | Medium | Low | Total |
| Risk | High | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) |
| | Medium | 0 (0.0%) | 5 (29.4%) | 2 (11.8%) | 2 (11.8%) | 9 (52.9%) |
| | Low | 0 (0.0%) | 0 (0.0%) | 8 (47.1%) | 0 (0.0%) | 8 (47.1%) |
| | Informational | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) |
| | Total | 0 (0.0%) | 5 (29.4%) | 10 (58.8%) | 2 (11.8%) | 17 (100%) |

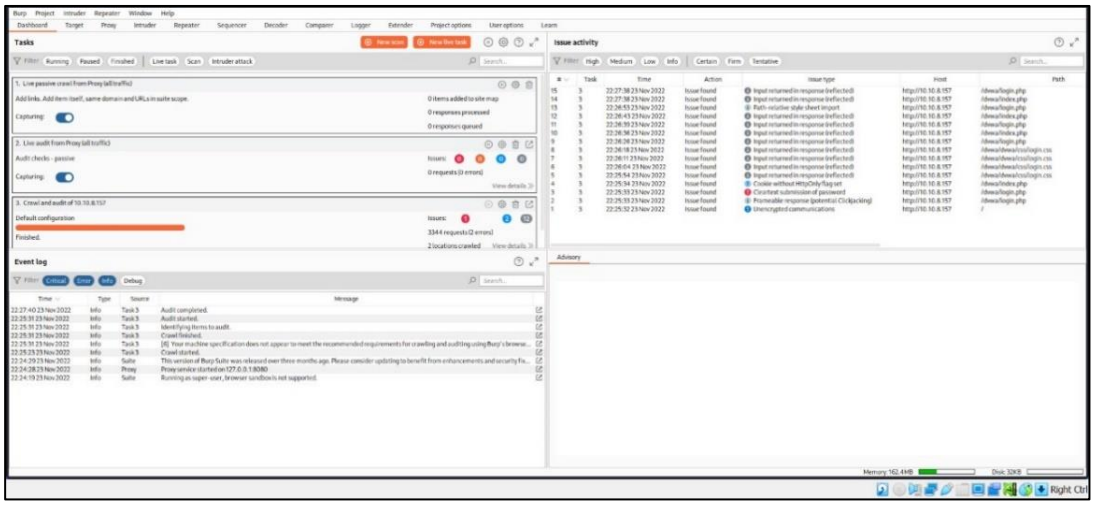
Gambar 5. Hasil *Scanning Tools OWASP*

| | | Risk | | | |
|---|---|---|---|---|---|
| | | High (= High) | Medium (>= Medium) | Low (>= Low) | Informational (>= Informational) |
| Site | http://10.10.47.95 | 0 (0) | 9 (9) | 8 (17) | 0 (17) |

Gambar 6. Hasil *Scanning Tools OWASP*

| Alert type | Risk | Count |
|---|---|---|
| Absence of Anti-CSRF Tokens | Medium | 2 (11.8%) |
| Content Security Policy (CSP) Header Not Set | Medium | 5 (29.4%) |
| Missing Anti-clickjacking Header | Medium | 2 (11.8%) |
| Cookie No HttpOnly Flag | Low | 1 (5.9%) |
| Cookie without SameSite Attribute | Low | 2 (11.8%) |
| X-Content-Type-Options Header Missing | Low | 5 (29.4%) |
| Total | | 17 |

Gambar 7. Hasil *Scanning Tools OWASP*



Gambar 8 Hasil *Scanning* Menggunakan *Tools* Buirp Suite

Setelah melakukan *vulnerability scanning*, didapatkan hasil perbandingan dari *tools OWASP*, Burp Suite, dan Nikto pada tabel di bawah ini:

Tabel 1. Perbandingan *Tools OWASP*, Burp Suite, dan Nikto

| **Parameter** | ***OWASP*** | **Burp Suite** | **Nikto** |
|---|---|---|---|
| **Objek *Scan*** | Tautan atau *link website* DVWA | Tautan atau *link website* DVWA | Tautan atau *link website* DVWA dan juga dapat menggunakan IP dari *website* |
| **Durasi** | *Tools OWASP* menghabiskan durasi selama 02.23 dalam melakukan *scanning* pada *website* DVWA | *Tools* Burp Suite menghabiskan durasi selama 2 menit dalam melakukan *scanning* pada *website* DVWA | *Tools* Nikto menghabiskan durasi kurang lebih 4 jam dalam melakukan *scanning* pada website DVWA sedangkan, jika menggunakan IP menghabiskan durasi kurang lebih 4 menit 30 detik |
| ***Result*** | Informasi yang diberikan jelas dengan dikelompokkan berdasarkan rangkuman, pemberitahuan baik dari tingkat risiko, situs dan peringatan. | Informasi yang ada pada hasil scan berisikan detail aktivitas masalah yang mana, kita dapat mengetahui secara lebih mendetail mengenai masalah, latar belakang masalah, dan juga klasifikasi *vulnerability* | Hasil *scan* memperlihatkan informasi terkait kesalahan konfigurasi, direktori web, serta sejumlah kerentanan aplikasi web lainnya. |

## 5. KESIMPULAN DAN SARAN

Pengujian *tools* dengan menggunakan *OWASP*, Nikto, dan Burp Suite yang merupakan suatu *vulnerability scanning* menghasilkan keterangan-keterangan mengenai kelemahan dari suatu *website* dengan tampilan dan cara yang berbeda-beda. Semua *tools* digunakan dalam mengetahui kelemahan dengan perbandingan antara masing-masing *tools* yang dibandingkan dalam aspek objek *scan*, durasi, kemudahan, dan informasi.

Berdasarkan penelitian dan pengujian *tools* yang telah dilakukan terdapat beberapa saran yang dapat diterapkan dan dikembangkan pada untuk penelitian berikutnya. Selain itu, juga untuk *website Damn Vulnerable Web Application* sebagai objek penelitian, antara lain:

a. Pengujian kerentanan pada *website Damn Vulnerable Web Application* dapat dilakukan dengan metode lain untuk menampilkan hasil berbeda.
b. Menggunakan lebih banyak *tools* untuk mendeteksi jenis kerentanan lain yang belum dapat terdeteksi oleh *tools* yang digunakan dalam penelitian ini.

Perlu diadakannya perbaikan celah kerentanan yang ditemukan untuk peningkatan keamanan pada *website Damn Vulnerable Web Application*.

**DAFTAR PUSTAKA**

[1] R. Meilano, F. Damanik, P. Jambi Jl Lingkar Barat, and L. Veteran Alam Barajo Kota Jambi, "ELTI Jurnal Elektronika, Listrik dan Teknologi Informasi Terapan Pengembangan Sistem Informasi Persediaan Barang dengan Metode Waterfall," 2019. [Online]. Available: https://ojs.politeknikjambi.ac.id/elti

[2] A. Maliq Ibrahim, T. Defisa, H. Bayu Seta, and I. P. Wayan Widi, "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT)," 2022.

[3] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi*, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[4] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)." [Online]. Available: http://jurnal.itg.ac.id/

[5] L. Costaner and dan Musfawati, "ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)."

[6] E. Listartha, G. Arna, J. Saskara, D. Gede, and S. Santyadiputra, "I Made," *ScientiCO : Computer Science and Informatics Journal*, vol. 4, no. 2, 2021.

[7] Y. Muhyidin, M. Hafid Totohendarto, E. Undamayanti, and S. Tinggi Teknologi Wastukancana, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods."

[8] A. Putra Armadhani, D. Nofriansyah, K. Ibnutama, S. Informasi, and S. Triguna Dharma, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *Jurnal Sains Manajemen Informatika dan Komputer*, vol. 21, no. 2, pp. 80–88, 2022, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jis

[9] P. M. Purba, A. Cipta Amandha, R. H. Purnama, and A. Ikhwan, "ANALISIS KEAMANAN WEBSITE PRODI SISTEM INFORMASI UINSU MENGGUNAKAN METODE APPLICATION SCANNING," 2022. [Online]. Available: https://si.uinsu.ac.id/

[10] Kurniawan, D., Maulana, P. A., & Zusrony, E. (2021). ANALYSIS OF E-COMMERCE CONSUMER SATISFACTION LEVEL WITH THE TECHNOLOGY ACCEPTANCE MODEL (TAM) APPROACH. International Journal of Economics, Business and Accounting Research (IJEBAR), 5(4).

[11] Irawadi Alwi and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," 2020.