PERBANDINGAN VULNERABILITY ANALYSIS PADA WEBSITE MENGGUNAKAN TOOLS WAPITI, SKIPFISH, DAN ARACHNI

I Putu Mas Yuda Pratama, Gede Agus Supriatmaja, Komang Mahendra, I Made Edy Listartha, Gede Arna Jude Saskara

Program Studi Sistem Informasi, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha
Jln. Udayana No. 11 Singaraja 81116 Indonesia
mas.yuda@undiksha.ac.id, agus.supriatmaja@undiksha.ac.id, mahendra.2@undiksha.ac.id, listartha@undiksha.ac.id, jude.saskara@undiksha.ac.id

Abstract *- Increasingly advanced technology, The website is a very important means of information and communication media. At the same time, security on the website is also an important aspect, so an analysis of security holes is needed.In analyzing security vulnerabilities on a website, you are usually faced with various choices of security analysis methodologies on websites that are very diverse. The research used by the author is the Vulnerability Scanner method, by comparing tools Arachni, Skipfish, and Wapiti, which aims to find out which tools are more effective in identifying security holes on websites. Based on the research, it was found that the Arachni tool received more security vulnerability reports than the Skipfish and Wapiti tools and was one of the tools that used a GUI.*
Keywords - Vulnerability Analysis, Skipfish, Wapiti, and Arachni.

Abstrak **-** Perkembangan teknologi informasi yang semakin pesat, website merupakan alat media informasi dan komunikasi yang sangat penting. Seiring dengan hal itu tentunya keamanan pada website diperhatikan sehingga diperlukan analisis celah keamanannya. Dalam melakukan analisis celah keamanan pada suatu website biasanya dihadapkan dengan berbagai pilihan metodologi analisis keamanan pada website yang sangat beragam. Penelitian yang digunakan penulis adalah metode Vulnerability Scanner, dengan membandingkan tools Arachni, Skipfish, dan Wapiti, yang bertujuan untuk mengetahui tools mana yang lebih efektif dalam mengetahui celah keamanan pada website. Berdasarkan penelitian didapatkan hasil bahwa tool Arachni mendapatkan laporan kerentanan keamanan yang lebih banyak dibandingkan tools Skipfish dan Wapiti serta menjadi salah satu tools yang menggunakan GUI.
Kata Kunci - Vulnerability Analisis, Skipfish, Wapiti, dan Arachni.

I. PENDAHULUAN

Dengan era masa kini yang semakin maju data keamanan pada suatu website sangatlah penting dengan banyaknya peretasan pada sistem informasi khususnya pada website, disebabkan keamanan pada website tersebut masih terdapat celah keamanan, dimana celah tersebut dapat digunakan oleh peretas untuk mencuri, merubah maupun merusak website tersebut[1]. Website dengan banyak celah keamanan, tidak aman untuk dikunjungi, hal tersebut dapat merugikan pihak pengunjung dan pihak owner dari website[2]. Hal ini disebabkan pihak peretas dapat merekam atau mengambil setiap aktivitas pada website, database website, dan sebagainya, dengan mudah[3]. Sehingga berpotensi menjadi tindakan kejahatan, seperti pengambilan hak akses, pencurian data, manipulasi database, dan lain-lainnya[4].

Menganalisis suatu kerentanan pada sebuah website dengan menggunakan *tools scanner*, beberapa terdapat *scanner* yang lebih detail untuk aplikasi website. *Scanner* dilakukan dengan menjelajahi setiap halaman web serta melakukan penetrasi, juga mencari kesalahan pengkodean software seperti *buffer overflow*, *string* dll. Hasil penetrasi berupa laporan deteksi kerentanan seberapa tinggi kerentanan suatu website atau berapa banyak celah keamanan yang terdeteksi oleh *scanner*[5]. Penyebab adanya celah tersebut dikarenakan kelemahan validasi input, penggunaan mekanisme otentikasi yang lemah, logika, dan pengkodean tingkat rendah.

Kerentanan pada website disebabkan oleh banyak hal, salah satunya tidak melakukan testing keamanan sebelum website diluncurkan. Testing keamanan website bertujuan untuk mencari celah keamanan pada website, dimana hasil testing tersebut akan digunakan untuk evaluasi, agar keamanan pada website dapat diperbaiki dan ditingkatkan, sehingga memperkecil kemungkinan adanya tindakan peretasan oleh pihak yang tidak bertanggung jawab[6].

Yang menjadi acuan dalam penelitian ini didasarkan pada beberapa contoh penelitian sebelumnya yang membahas mengenai perbandingan tools dalam melakukan *vulnerability analysis* yaitu dengan membandingkan tingkat keamanan website menggunaakan *tools* Nmap dan Nikto[7]. Dijelaskan bahwa dari pengujian yang dilakukan *tools* Nmap dapat melakukan vulnerability analysis paling baik dibandingkan dengan *tools* Nikto dikarenakan lebih lengkap dalam laporan celah keamnan yang didapat saat melakukan *vulnerability scanning* pada suatu website[8].

Dalam penelitiannya peneliti melakukan pengujian network dan port *scanning* menggunakan *tools* Nmap dan Nikto mencakup tingkat kerentanan setiap keamanan website yang diuji[9]. Metode yang digunakan adalah *Ethical Hacking*, yakni dengan menekankan pada *Footprinting* dan *Vulnerability Scanning*. Hasil dari penelitian tersebut menjelaskan bahwa tools Nmap mampu melakukan vulnerability assessment lebih baik dari pada tool nikto.

Berdasarkan penelitian sebelumnya dalam praktek *scanning* keamanan pada website kali ini menggunakan sistem operasi Kali Linux. Pada operasi sistem Kali Linux menyediakan berbagai *tools* untuk melakukan *vulnerability sanning* keamanan pada suatu website. *Tools* yang digunakan pada praktek kali ini yaitu Arachni, Wapiti, dan Skipfish. Scanning keamanan pada website ini nantinya dapat membantu dalam menemukan celah keamanan yang ada pada website, jelasnya cara kerja ketiga *tools* tersebut mendeteksi halaman website lalu mencari celah keamanannya.

A. Wapiti

Wapiti adalah *tool* yang digunakan untuk *scanning* keamanan website dimana *tools* ini bekerja dengan melakukan pengecekan keamanan pada suatu website yang diinginkan, dimana diawali dengan memindai halaman website dengan melakukan scan kemudian mendapatkan daftar data dan selanjutnya *tools* akan menyuntikkan data untuk mengecek apakah terjadi kerentanan pada website[10]. Dengan itu wapiti ini pada saat *scanning* menjalankan modulnya keseluruh halaman website yang dituju sehingga membutuhkan relatif banyak waktu tergantung dari kompleksitas dari web yang di scan[11].

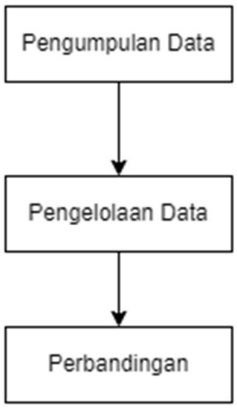
B. Skipfish

Skipfish merupakan salah satu *tool* yang dibuat oleh Google, dimana *tool* ini berfungsi untuk mendeteksi atau mengintai kerentanan keamanan sebuah aplikasi website. *Tool* ini memiliki cara kerja *crawl* dan *dictionary-based probes*, dimana merayap ke dalam direktori file pada website tersebut satu per satu lalu memeriksa keamanannya[5]. Output dari hasil testing menggunakan *tool* ini yaitu berupa web html, dimana dalam web HTML tersebut akan memperlihatkan kerentanan yang didapat, dimana setiap kerentanan akan memiliki tingkatan resiko yang berbeda-beda, tingkatan rentanan dapat dilihat dengan warnanya[12].

C. Arachni

Arachni adalah *tool opensource* yang dikembangkan untuk menyediakan penetrasi *testing environment.* Tool ini dapat mendeteksi berbagai *vulnearbility web application* seperti XSS, SQL *Injection, Local File Inclusion, Remote file inclusion, unvalidated redirect,* dll[13]. Arachni ini multi-platform, mendukung semua sistem operasi utama (MS Windows, Mac OS dan Linux) dan didistribusikan melalui paket portabel yang memungkinkan penyebaran instan. Arachni memiliki *command-line interface* dan juga GUI Web. Paket ini tersedia untuk Linux (32-bit dan 64-bit), macOS (64-bit), dan Windows (64-bit)[14]. Halaman Unduhan Arachni merekomendasikan versi Linux dan macOS daripada implementasi Windows.

II. METODE PENELITIAN



Gambar 1 Metode Penelitian

Pengambilan metode penelitian yang dilakukan oleh penulis berdasarkan penggunaan data dari penelitian sebelumnya, membaca beberapa jurnal lalu dibandingkan dengan cara menjabarkannya secara berurut sesuai dengan *vulnerbility* analisis. Metode penelitian saat ini menggunakan *Ethical Hacking Vulnerability* website ini merupakan suatu aktivitas pengujian tingkat kerentanan keamanan sebuah website guna menjaga website dari pihak peretas yang tidak bertanggung jawab[15]. Penelitian ini diawali dengan melakukan studi literatur mengenai pengujian yang dilakukan dengan mencari informasi yang berkaitan dengan penelitian ini, proses dalam penelitian ini dilaksanakan dengan langkah sebagai berikut.

1. Metode Pengumpulan Data
   Metode ini dilakukan dengan membaca beberapa penelitian, artikel, dan buku yang berhubungan dengan penelitian.
2. Metode Mengolah Data
   Pada metode ini dilakukan pengelolaan data yang telah dikumpulkan. Hal ini bertujuan agar data dapat digunakan sebagai acuan dalam penelitian. Sehingga mempermudah dalam melakukan perbandingan *tools* pada *vulnerability* analisis.
3. Melakukan perbandingan
   Pada tahap ini dilakukan perbandingan menggunakan setiap *tools vulnerability* analisis, seperti Skipfish, Aranchi, dan Wapiti, dengan menggunakan alamat website http://testphp.vulnweb.com/. Sehingga menghasilkan laporan hasil scanning setiap *tools*,

agar mendapatkan *tools* yang dapat memberikan informasi celah keamanan paling banyak.

Pada penelitian ini menggunakan laptop dengan sistem operasi Kali Linux dan beberapa *tools* dalam melakukan pengujian website target.
Informasi Hardware.

Tabel 1 Informasi Hardware

No	Alat	Keterangan Spesifikasi
1	Laptop Lenovo IdeaPad Slim 5	- Processor Ryzen 5 - Ram 8 GB - SSD 512 GB
2	Jaringan Seluler	- Kecepatan Jaringan 1.68 Mbps

Informasi Software.

Tabel 2 Informasi Software

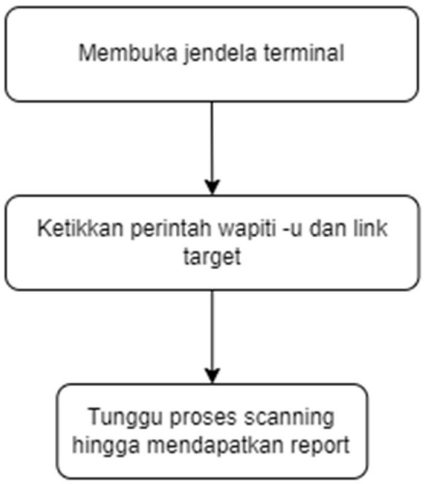
No	Nama	Spesifikasi
1	Virtual Box Kali Linux	- 1 CPU - Ram 2GB - Memory 20 GB

III. HASIL DAN PEMBAHASAN

Untuk menguji setiap *tools*, scan dilakukan dengan menggunakan sebuah halaman website khusus yaitu http://testphp.vulnweb.com/ ketiga *tools* tersebut di jalankan menggunakan sistem operasi kali linux dengan perbandingan yang dihasilkan menggunakan perangkat dan jaringan yang sama sehingga hasil dari *scanning* dapat dibandingkan secara optimal.

A. Vulnerability Scanner Menggunakan Wapiti

Pada saat melakukan *scan* menggunakan *tools* wapiti dapat dijalankan dengan urutan sebagai berikut.



Gambar 2 Langkah Kerja Tools Wapiti

Langkah kerja dalam pengujian analisis suatu website dengan menggunakan Wapiti ini dijalankan pada virtualbox kali linux, dimulai dengan menginstall Wapiti lalu memilih target website yang akan di *scanning*, proses *scanning* dilakukan dengan cara menginputkan perintah wapiti -u dan url yang di tuju pada terminal kali linux[16]. Dari perintah tersebut akan menghasilkan laporan berupa beberapa data informasi dari target website yang di *scanning* oleh *tools* wapiti.

Gambar 3 Proses Awal Scanning Wapiti

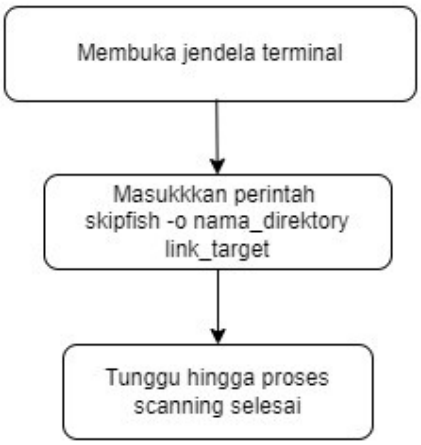
Gambar 3 merupakan proses *scanning* pada website yang telah ditargetkan. Pada saat itu wapiti *tools* ini akan menajalankan berbagai modul yang berfungsi untuk menemukan kerentanan pada website yang dianalisis. Wapiti terus melakukan *scanning* hingga selesai maka selanjutnya akan terdapat laporan berupa file HTML yang tersimpan di direktori home/user/.wapiti/generated_report/nama website yang menjadi target. Hasil laporan data dari *scanning* Wapiti adalah berbentuk file HTML, file ini bisa dibuka di browser untuk dapat melihat laporan lengkap dari hasil *scanning*.

Gambar 4 Hasil Scanning Wapiti

Dalam file HTML yang telah dibuka terdapat informasi tambahan mengenai kerentanan dari website yang di analisis, untuk detailnya dijelaskan pada tabel 1 berikut.

B. Vulnerability Scanner Menggunakan Skipfish

Pada saat melakukan scan menggunakan *tools* skipfish dapat di jalankan dengan urutan cara sebagai berikut:

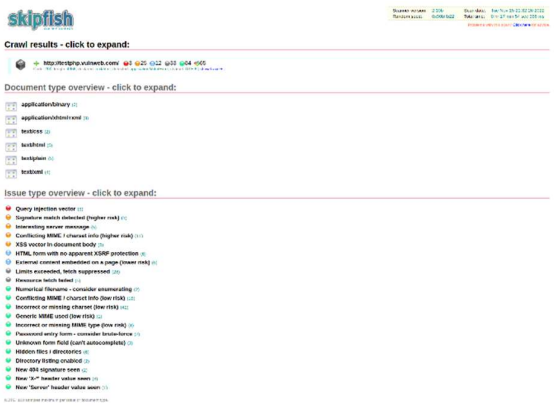


Gambar 5 Langkah Kerja Tools Skipfish

Dalam kasus ini website yang menjadi target adalah http://testphp.vulnweb.com dan folder tempat menyimpan laporan hasil *scanning*. Jadi perintah yang digunakan adalah skipfish -o vulnwebphp http://testphp.vulnweb.com, untuk perintah -o artinya folder yang akan menjadi tempat menyimpan hasil *scanning*. Dalam melakukan *scanning* akan membutuhkan waktu yang relatif lama, tergantung koneksi internet dan keamanan website target. Berikut gambar proses *scanning tools* skipfish.

Gambar 6 Proses Scanning Skipfish

Dalam proses scanning, *tool* ini melakukan permintaan-permintaan pada web server target. Setelah selesai melakukan *scanning*, hasil laporan akan disimpan pada folder yang telah ditentukan sebelumnya. Laporan hasil dari *scanning* berbentuk file HTML.

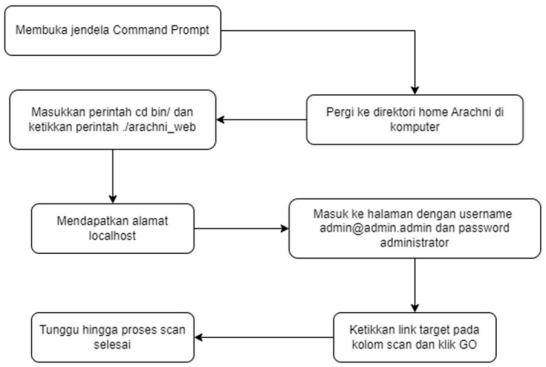


Gambar 7 Hasil Scanning Tools Skipfish

Gambar 7 merupakan hasil *scanning* yang dihasilkan dari *tools* skipfish, laporan berisi informasi mengenai celah keamanan yang di temukan oleh *tools* Skipfish.

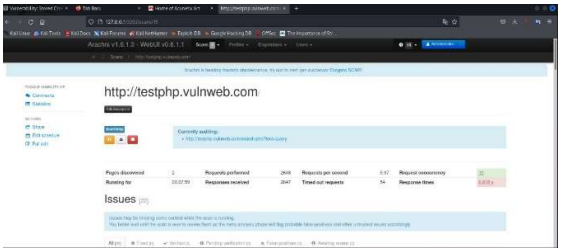
C. *Vulnerability Scanner Menggunakan Arachni*

Pada saat melakukan scan menggunakan *tools* arachni dapat di jalan kan dengan urutan cara sebagai berikut:



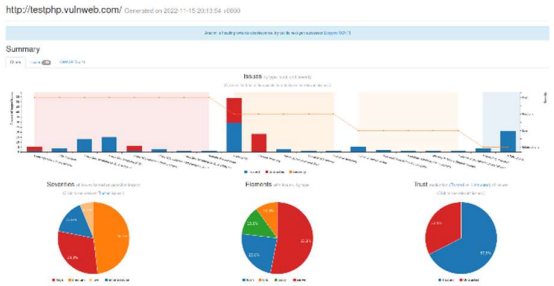
Gambar 8 Langkah Kerja Tools Arachni

Untuk menjalankan GUI, yang perlu dilakukan adalah membuka jendela *Command Prompt*, pergi ke direktori home Arachni di komputer tempat disimpannya file arachni yang telah di unduh sebelumnya, dan masuk ke direktori bin kemudian ketikkan perintah ./arachni_web. Maka akan diperlihatkan pesan yang memberi tahu bahwa program sedang berjalan di localhost: berisikan nomor <port> yang dapat dibuka di browser (mis., http://127.0.0.1:9292). Link tersebut akan menuju halaman interface web GUI, kemudian masuk dengan username admin@admin.admin dan password administrator. Berikut gambar proses *scanning* tools Arachni.



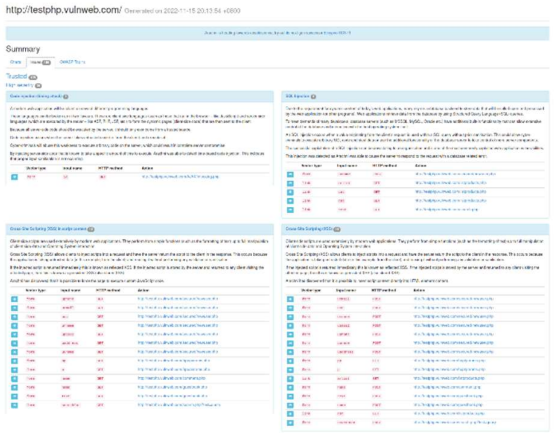
Gambar 9 Proses Scanning Arachni

Gambar 9 merupakan kondisi sedang berlangsungnya proses scanning menggunakan *tools* Arachni, *tools* ini dapat digunakan sebagai utilitas pemindai baris perintah sederhana atau dikonfigurasi dalam kotak pemindai kinerja tinggi untuk mendukung rutinitas pengujian keamanan berskala besar.



Gambar 10 Hasil Scanning Tools Arachni

Gambar 10 merupakan hasil *scanning tools* arachni yang divisualisasikan dalam bentuk chart dengan informasi celah keamanan yang berhasil didapat dari proses *scanning*. Selain itu informasi detail lainnya juga dapat diakses di laporan tersebit berikut gambar hasil summary yang ditampilkan secara detail.



Gambar 11 Hasil Summary Tools Arachni

Informasi hasil celah keamanan yang didapatkan melalui scan masing-masing *tools* di paparkan pada tabel berikut ini.

Tabel 3 Hasil Laporan Scanning

Tools	Kerentanan	Jumlah
Skipfish	Query Injection Vector	3
	Signature match detected	1
	Intersting Server Massage	5
	Conflicting MIME	29
	XSS vector in document body	8
	HTML form with no apparent XSRF protection	6
	External content embedded on a page	6
	Limits exceeded, fetch suppressed	26
	Resource fetch failed	5
	Numerical filename	2
	Incorrect or missing charset	42
	Generic MIME used	1
	Incorrect or missing MIME type	8
	Password entry form	2
	Unknown form field	3
	Hidden files / directories	6
	Directory listing enabled	2
	New 404 signature seen	2
	New “X-” header value seen	3
	New ‘Sever’ header value seen	1
Arachni	Cross-Site Scripting(XSS)	28
	SQL Injection	13
	Remote File Inclusion	1
	Code injection	5
	Common directory	1
	Backup file	54
	Unencrypted password form	3
	Unvalidated redirect	1
	Backup directory	18
	Missing ‘X-Frame-Options’ header	1
	Insecure cross-domain policy	1
	Common sensitive file	5
	Directory listing enabled	2
	New 404 signature seen	2
	New “X-” header value seen	3
	New ‘Sever’ header value seen	1
Wapiti	Blind SQL Injection	8
	Content Security Policy Configuration	1
	Path Traversal	2
	HTTP Secure Headers	4
	SQL Ijection	9
	Cross Site Scripting	15

Berdasarkan Informasi hasil scanning dari ketiga *tools* yang diuji diatas didapatkan hasil perbandingan pada tabel berikut.

Tabel 4 Hasil Perbandingan Ketiga Tools

Tools	Durasi	Kerentanan	Laporan	GUI	Status
Wapiti	01:34:57	38	Ada	-	Berhasil
Skipfish	00:17:54	157	Ada	-	Berhasil

Arachni	01:12:54	159	Ada	✓	Berhasil

Pada tabel 4 diatas dapat diketahu perbedaan hasil yang didapat dari masing-masing *tools* yang digunakan sebagai alat uji pada penelitian ini. Untuk data diatas *tools* arachni mendapatkan celah keamanan terbanyak yakni dengan 159 celah keamanan yang ditemukan.

IV. KESIMPULAN

Dapat disimpulkan bahwa dari ketiga *tools* yang di uji dalam scanning suatu website khusus, di perlihatkan masing-masing laporan hasil scan yang berbeda beda sesuai kemampuan *tools* tersebut. Maka dapat dinyatakan sebagai berikut.

1. Pada durasi waktu dalam proses *scanning tools* Skipfish memiliki kemampuan *scanning* tercepat yakni selesai dengan waktu 18 menit di halaman web yang sama dengan kedua tools lainnya.
2. *Tools* Arachni memiliki kemampuan dengan temuan celah terbanyak yakni 159 celah keamanan di sebuah halaman web yang sama dari kedua *tools* lainnya.
3. Dalam penelitian ini Arachni merupakan satu satunya *tools* yang memiliki tampilan GUI (Graphical User Interface), laporan berbentuk diagram chart dan tampilan detail informasi celah keamanan yang didapat dalam *scannig.*
4. Dalam penelitian ini ketiga *tools* yang digunakan *opensource* dan tidak ada biaya maupaun pembayaran yang dilakukan dalam melakukan *scanning*.

DAFTAR PUSTAKA

[1] I. Kamilah and A. Hendri Hendrawan, "Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika," 2019.

[2] R. Alamsyah, "Jurnal Sistem Keamanan dalam Sebuah Sistem Informasi."

[3] N. Sulisrudatin, "ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT," 2018. [Online]. Available: www.detikinet.com,

[4] G. A. Utomo, "ETHICAL HACKING," 2019. [Online]. Available: www.cyberriskanalytics.com

[5] D. Sagar, S. Kukreja, J. Brahma, S. Tyagi, and P. Jain, "STUDYING OPEN SOURCE VULNERABILITY SCANNERS FOR VULNERABILITIES IN WEB APPLICATIONS." [Online]. Available: www.iioab.org

[6] J. S. Komputer, K. Buatan, M. A. Adiguna, and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)."

[7] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, pp. 354–361, Jun. 2020, doi: 10.1109/ICOEI48184.2020.9143018.

[8] 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."

[9] B. Tasya Kumala Dewi and M. Andri Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web."

[10] S. Suroto and A. Asman, "ANCAMAN TERHADAP KEAMANAN INFORMASI OLEH SERANGAN CROSS-SITE SCRIPTING (XSS) DAN METODE PENCEGAHANNYA," 2021. [Online]. Available: http://www.hackers.com?yid=

[11] B. Vito Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," 2017. [Online]. Available: http://j-ptiik.ub.ac.id

[12] O. : Aufan and I. Rosadi, "ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN WEB PENETRAION TESTING."

[13] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," *Electronics 2022, Vol. 11, Page 2991*, vol. 11, no. 19, p. 2991, Sep. 2022, doi: 10.3390/ELECTRONICS11192991.

[14] A. Stasinopoulos, C. Ntantogian, and C. Xenakis, "Commix: automating evaluation and exploitation of command injection vulnerabilities in Web applications," *International Journal of Information Security 2018 18:1*, vol. 18, no. 1, pp. 49–72, Feb. 2018, doi: 10.1007/S10207-018-0399-Z.

[15] 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/

[16] B. Gomez, "Complete Guide to Using Wapiti Web Vulnerability Scanner to Keep Yo...," 2022. https://linuxsecurity.com/features/complete-guide-to-using-wapiti-web-vulnerability-scanner-to-keep-your-web-applications-websites-secure (accessed Nov. 23, 2022).