Analisis Perbandingan Kinerja *Tool Website Directory Brute Force* dengan Target *Website* DVWA

I Made Putra Utama[1], Kadek Rosila Putri[2], Anak Agung Eka Wirayuda[3], Varelly Arletta Tyora Putri Herlambang[4], I Made Edy Listartha[5], Gede Arna Jude Saskara[6]
Sistem Informasi / Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
putra.utama@undiksha.ac.id[1]*, rosila@undiksha.ac.id[2], anak.agung.eka@undiksha.ac.id[3], varelly@undiksha.ac.id[4], listartha@undiksha.ac.id[5], jude.saskara@undiksha.ac.id[6]

Abstrak. Seiring dengan perkembangan teknologi yang semakin meningkat, banyak ditemukan penemuan baru yang dapat mempermudah kehidupan manusia, salah satunya yaitu situs *website*. Banyaknya situs *website* di internet mengakibatkan tingkat keamanannya semakin menurun. Hal tersebut mengakibatkan *website* menjadi rentan untuk diretas dan diambil alih orang yang tidak bertanggung jawab. Salah satu cara peretas untuk menyerang *website* adalah dengan mencari direktori web yang memiliki celah keamanan. Serangan tersebut dikenal dengan *website directory brute force*. Penelitian ini menggunakan metode eksperimental dengan membandingkan kinerja dari *tools* Gobuster, FFUF, dan Dirb dengan tujuan menemukan *tool* yang memiliki kinerja paling baik untuk melakukain serangan web directory brute force dengan target serangan website DVWA. Aspek yang diuji dari ketiga *tools* tersebut yaitu kecepatan, kemampuan, dan efektivitas. Hasil penelitian menunjukkan bahwa *tool* Gobuster memiliki kinerja paling baik jika aspek kecepatan menjadi prioritas, sedangkan *tool* FFUF menjadi *tool* dengan kinerja terbaik jika aspek kemampuan yang menjadi prioritas.

Kata Kunci: *Website, Directory, Brute force,* Gobuster, FFUF, Dirb.

1 Pendahuluan

Perkembangan teknologi informasi semakin berkembang pesat dan banyak membawa perubahan di dunia ini. Karena perkembangan teknologi yang semakin meningkat, banyak ditemukan penemuan-penemuan baru yang dapat mempermudah kehidupan manusia, salah satunya yaitu situs *website*. *Website* adalah kumpulan halaman situs yang terdapat dalam sebuah domain atau subdomain yang berada pada *world wide* di dalam jaringan internet [1]. Dengan hadirnya situs *website* ini dapat mempermudah pencarian informasi terkait suatu hal. Saat ini situs *website* semakin berkembang dan semua orang dapat membuat *website* untuk menyampaikan berbagai informasi. Beberapa situs *website* yang sering diakses diantaranya *search engine*, *e-commerce*, *social networking*, forum, portal berita, dan lain-lain [2]. Selain itu, *website* juga digunakan untuk membantu perkembangan bisnis sebuah perusahaan. *Website* menjadi cara alternatif sebagai media promosi maupun media interaksi antara perusahaan dengan pelanggan [3]. Karena semakin meningkatnya jumlah *website* yang ada, maka tak heran jika tingkat keamanan informasi situs *website* semakin menurun. Keamanan informasi sebuah *website* dapat diartikan suatu kebutuhan akan adanya perlindungan terhadap informasi sebagai sebuah aset yang tersedia di dalam *website*, seperti mengatur akses informasi, mengatur identitas pengguna dan sebagainya [4]. Dengan penurunan tingkat keamanan tersebut, situs *website* menjadi rentan untuk diretas dan diambil alih oleh orang yang tidak bertanggung jawab. Salah satu cara peretas untuk menyerang *website* yaitu dengan mencari direktori web yang disembunyikan dan memiliki celah keamanan. Serangan tersebut dikenal dengan *website directory brute force*. Peretas akan berusaha melakukan serangan dengan memasukkan kemungkinan nama-nama direktori pada alamat situs *website* target.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan memberikan gambaran bagaimana peretas menemukan direktori tersembunyi dengan menggunakan tiga *tools web directory brute force*, yaitu Gobuster, FFUF, dan Dirb serta menemukan *tool* yang memiliki kinerja paling baik untuk melakukan serangan *web directory brute force* dengan target serangan *website* DVWA. Hasil dari penelitian ini dapat digunakan sebagai acuan untuk para pengembang *website* dalam mengamankan situs *web* yang dimilikinya dan sebagai sarana edukasi bagi pelajar.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

2 Kajian Pustaka

2.1 *Website*

Website merupakan kumpulan halaman *web* yang saling terhubung serta file-filenya saling terkait yang dapat disertai dengan file gambar, video ataupun file-file yang lain, baik bersifat statis maupun bersifat dinamis. Informasi atau file-file yang tersedia pada *website* tersimpan di dalam sebuah *server web* [5]. *Website* dibangun dengan menggunakan format HTML (*Hypertext Markup Language*) dan memanfaatkan protokol komunikasi HTTP yang terletak pada *application layer* pada referensi OSI *layer* [6].

2.2 *Website Directory Brute Force*

Directory brute force merupakan teknologi aplikasi *website* yang digunakan untuk menemukan dan mengidentifikasi kemungkinan direktori tersembunyi dalam sebuah *website* [7].

2.3 *Wordlist*

Wordlist merupakan file yang berisi daftar ribuan kemungkinan nama direktori dan file yang terdapat dalam sebuah *website*. File ini yang akan digunakan oleh *tool directory brute force* untuk memindai *website* target [7].

2.4 *Website* DVWA

Damn Vulnerable Web Application (DVWA) merupakan aplikasi web yang menggunakan layanan Apache *web server* dan berjalan pada protokol HTTP [8]. Tujuan dari aplikasi web ini yaitu untuk membantu para profesional keamanan dalam menguji *skill* dan *tool hacking* pada lingkungan yang legal, memahami proses pengamanan *website* bagi pengembang, serta sebagai sarana edukasi bagi para pelajar [9].

2.5 Kali Linux

Kali Linux merupakan sistem operasi berbasis Debian Linux serta hasil pembangunan kembali (*rebuild*) dari sistem operasi Backtrack. Kali Linux sendiri dikembangkan dengan tujuan sebagai sistem operasi *penetration testing* yang dilengkapi dengan berbagai *tools hacking*. Sistem operasi ini dirilis pertama kali pada tanggal 13 Maret 2013 dan dikembangkan oleh Offensive Security, yaitu perusahaan pelatihan sertifikasi bidang *IT Security* [10]. Fitur-fitur yang terdapat dalam sistem operasi ini yaitu berisi lebih dari 300 *tools* untuk *penetration testing*, bersifat *open source* atau gratis, mengikuti FHS *compliant*, dukungan perangkat *wireless* yang luas, lingkungan pengembangan yang aman, serta tersedia dalam banyak bahasa [11].

2.6 Gobuster

Gobuster adalah *tool* yang digunakan untuk *brute force* URL (direktori dan file) pada situs *website*, subdomain DNS, nama host virtual, dan membuka bucket Amazon S3 [12].

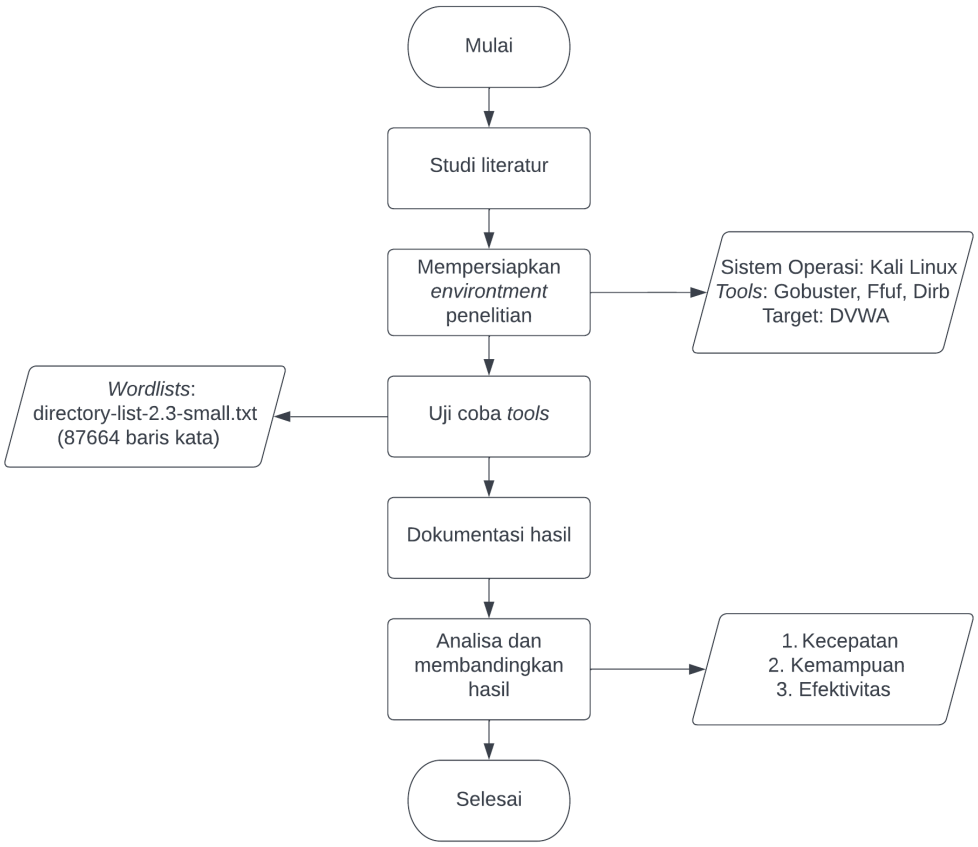
2.7 FFUF

FFUF (*Fuzz Faster U Fool)* adalah alat *web fuzzing* yang *open source,* dimana alat ini memiliki fungsi untuk menemukan elemen dan konten tersembunyi dalam aplikasi atau server *web* [13]. FFUF merupakan aplikasi berbasis baris perintah (*command line*) yang berjalan di terminal Linux atau *command prompt* Windows, yang berarti *tool* FFUF tidak menyediakan GUI interaktif dalam pengoperasiannya [14].

2.8 Dirb

Dirb merupakan alat pemindai konten *web*. Dirb akan mencari objek *web* yang ada dan tersembunyi dengan meluncurkan serangan *bruteforce* berbasis *wordlists* terhadap server *web* dan menganalisis responsnya. Alat ini telah menyediakan *wordlists* secara *default* yang berisi kemungkinan nama direktori dan file yang telah dikonfigurasi sebelumnya untuk melakukan serangan [15].

3 Metodologi Penelitian



Gambar .1. Diagram alir metodologi penelitian.

3.1 Studi Literatur

Pada tahap ini peneliti menggali informasi yang bersumber dari internet, jurnal, dan buku serta mempelajari literatur yang berkaitan dengan topik penelitian.

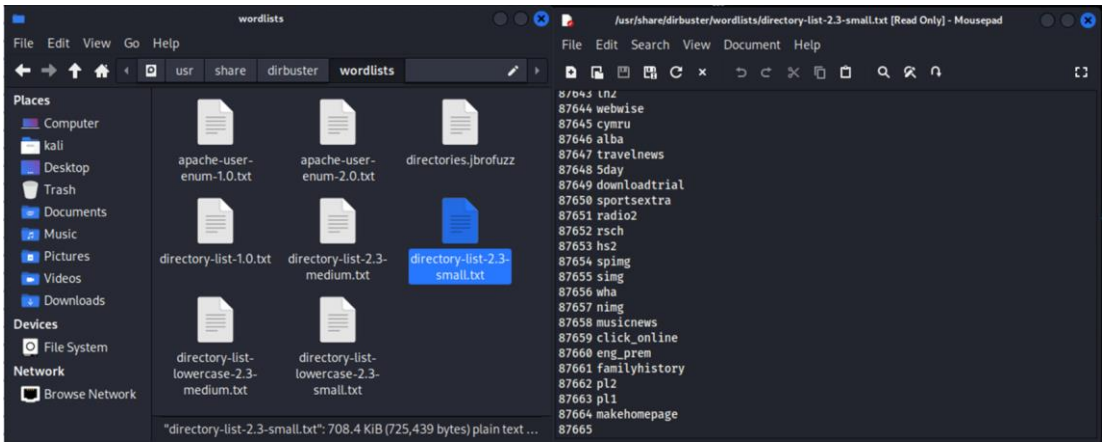
3.2 Mempersiapkan Environment Penelitian

Environment yang digunakan pada penelitian ini yaitu sistem operasi Kali Linux versi 2022.3 yang dapat diunduh pada laman https://www.kali.org/get-kali/#kali-platforms, *tool* Gobuster yang dapat diunduh dengan menuliskan perintah *sudo apt install gobuster* pada terminal Kali Linux, *tool* FFUF dan Dirb yang secara *default* tersedia pada sistem operasi Kali Linux versi 2022.3, serta *website* DVWA.

3.3 Uji Coba *Tool*

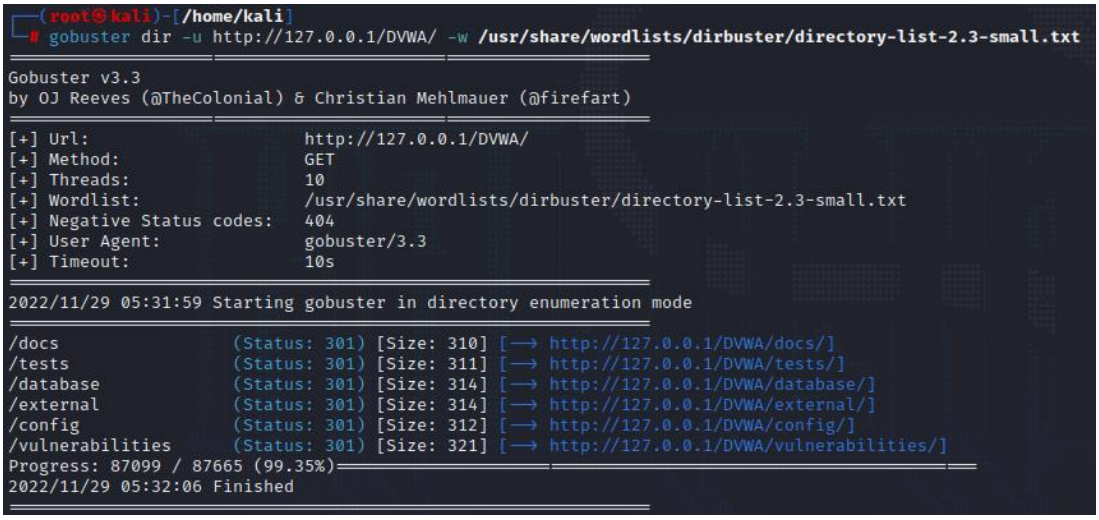
Ketiga *tools* yang telah dipilih akan diuji untuk melakukan serangan web directory brute force dengan target website DVWA yang memiliki alamat URL http://127.0.0.1/DVWA. Wordlists yang digunakan dalam melakukan serangan adalah directory-list-2.3-small.txt dengan total 87664 baris kata (termasuk komentar) yang berlokasi pada direktori /usr/share/wordlists/dirbuster.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)



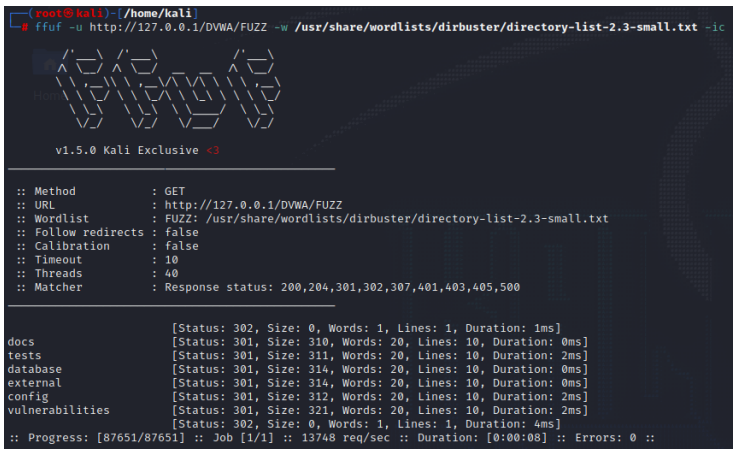
Gambar. 2. Lokasi dan jumlah baris kata dari *wordlists* yang digunakan untuk melakukan serangan.

Untuk melakukan serangan menggunakan *tool* Gobuster dapat dilakukan dengan menjalankan perintah *gobuster dir -u [alamat URL dari target] -w [file wordlists yang digunakan untuk melakukan serangan]*.



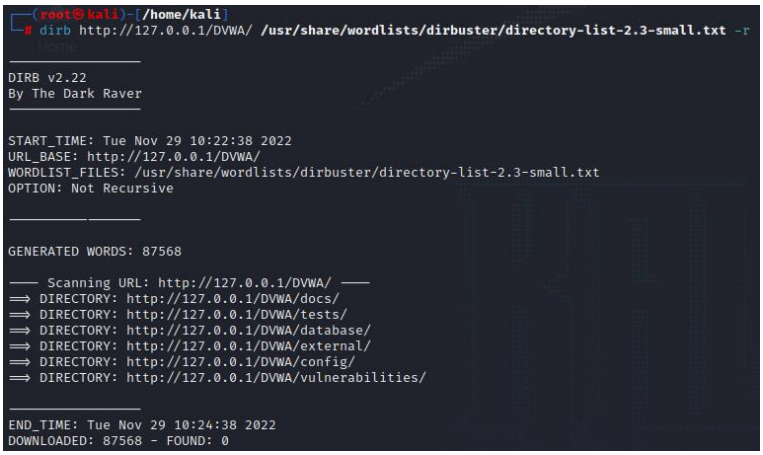
Gambar. 3. Baris perintah dan *output* dari *tool* Gobuster.

Untuk melakukan serangan menggunakan *tool* FFUF dapat dilakukan dengan menjalankan perintah *ffuf -u [alamat URL dari target/FUZZ] -w [file wordlists yang digunakan untuk melakukan serangan] -ic. Command -ic (ignore comment)* memiliki fungsi mengabaikan dan tidak mengeksekusi komentar pada *wordlists*.



Gambar . 4. Baris perintah dan *output* dari *tool* FFUF.

Untuk melakukan serangan menggunakan *tool* Dirb dapat dilakukan dengan menjalankan perintah *dirb [alamat URL dari target] [file wordlists yang digunakan untuk melakukan serangan] -r. Command -r* berarti serangan tidak dilakukan secara rekursif.



Gambar. 5. Baris perintah dan *output* dari *tool* Dirb.

3.4 Dokumentasi Hasil

Hasil dari setiap percobaan yang telah dilakukan didokumentasikan dan disimpan pada Microsoft Excel untuk selanjutnya dilakukan perbandingan dan operasi matematika yang dibutuhkan.

3.5 Analisa dan Membandingkan Hasil

Aspek yang akan dianalisa dan dijadikan perbandingan dari ketiga *tools* yang diuji adalah kecepatan, kemampuan, dan efektivitas. Aspek kecepatan ditentukan dengan mencari rata-rata waktu yang dibutuhkan *tool* untuk melakukan serangan hingga menemukan direktori dari *website* target. Waktu diukur dengan Linux *time command* yang diletakkan pada bagian awal baris perintah untuk melakukan serangan. Aspek kemampuan dilihat dari kemampuan *tool* untuk mengeksekusi baris kata di dalam *wordlists* yang digunakan untuk melakukan serangan. Aspek efektivitas ditentukan dari direktori yang berhasil ditemukan oleh *tool,* apakah *tool* berhasil menemukan direktori yang tersembunyi dan rentan atau tidak.

4 Hasil dan Pembahasan

Berdasarkan uji coba *tools website directory brute force* yang telah dilakukan menggunakan *wordlists* directory-list-2.3-small.txt dengan total 87664 baris kata (termasuk komentar) diperoleh hasil untuk masing-masing *tool* sebagai berikut.

4.1 Gobuster

Tabel 1. Hasil uji coba *tool* Gobuster

Percobaan ke-	Durasi (detik)	Progress	Jumlah direktori
1	6,4	93,54 %	6
2	5,81	94,23 %	6
3	5,51	91,27 %	6
4	5,43	91,76 %	6
5	5,67	96,99 %	6
6	5,48	91,39 %	6
7	6,12	98,02 %	6
8	5,65	97,45 %	6
9	5,71	96,24 %	6
10	5,67	97,21 %	6
Rata-rata:	5,745	94,81 %	6

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Pada sepuluh kali percobaan *web directory brute force* menggunakan *tool* Gobuster, diperoleh rata-rata waktu yang dibutuhkan untuk melakukan serangan adalah selama 5,745 detik. Rata-rata *progress* yang berhasil dieksekusi dalam sepuluh kali percobaan tersebut adalah sebesar 94,81%. Pada percobaan ini, *tool* Gobuster dengan *wordlists* directory-list-2.3-small.txt berhasil menemukan enam direktori yang memberikan respon terhadap serangan yang dikirimkan. Direktori tersebut diantaranya yaitu /docs, /tests, /database, /external, /config, dan /vulnerabilities.

4.2 FFUF

Tabel 2. Hasil uji coba *tool* FFUF

Percobaan ke-	Durasi (detik)	Progress	Jumlah direktori
1	6,83	100 %	6
2	6,7	100 %	6
3	6,59	100 %	6
4	6,59	100 %	6
5	6,96	100 %	6
6	6,84	100 %	6
7	6,95	100 %	6
8	6,94	100 %	6
9	6,85	100 %	6
10	7,07	100 %	6
Rata-rata:	6,832	100 %	6

Pada percobaan menggunakan *tool* FFUF diperoleh rata-rata waktu yang dibutuhkan dalam melakukan serangan adalah selama 6,832 detik atau 1,087 detik lebih lama dari Gobuster, semua baris kata pada *wordlists* berhasil dieksekusi atau *progress* eksekusi mencapai 100%, dan direktori yang berhasil ditemukan berjumlah enam direktori dengan nama-nama direktori sama dengan yang berhasil ditemukan oleh *tool* Gobuster, yaitu /docs, /tests, /database, /external, /config, dan /vulnerabilities.

4.3 Dirb

Tabel 3. Hasil uji coba *tool* Dirb

Percobaan ke-	Durasi (detik)	Progress	Jumlah direktori
1	102,41	100 %	6
2	103,8	100 %	6
3	110,13	100 %	6
4	116,51	100 %	6
5	206,54	100 %	6
6	124,03	100 %	6
7	230,01	100 %	6
8	136,9	100 %	6
9	129,44	100 %	6
10	118,82	100 %	6
Rata-rata:	137,859	100 %	6

Berdasarkan sepuluh kali percobaan menggunakan *tool* Dirb, diperoleh rata-rata waktu yang dibutuhkan untuk menemukan direktori *website* target adalah 137,859 detik atau sekitar 20 kali lipat dari *tool* FFUF. Sama halnya dengan FFUF, Dirb juga dapat mengeksekusi seluruh baris kata dalam *wordlists* saat melakukan serangan. Jumlah serta nama direktori yang berhasil ditemukan oleh *tool* ini sama dengan dua *tool* sebelumnya, yaitu sebanyak enam direktori yang terdiri dari direktori /docs, /tests, /database, /external, /config, dan /vulnerabilities.

4.4 Perbandingan Ketiga Tools

Ketiga *tools* yang telah diuji kemudian dilakukan perbandingan berdasarkan aspek kecepatan melakukan serangan, kemampuan dalam mengeksekusi *wordlists*, dan efektivitas (ditemukan atau tidak ditemukan direktori). Perbandingan tersebut dituangkan pada Tabel 4 di bawah.

Tabel 4. Perbandingan tools berdasarkan aspek yang diuji

Aspek yang diuji	Nama *tools*		
	Gobuster	FFUF	Dirb
Kecepatan	Paling cepat, dengan rata-rata waktu untuk melakukan serangan selama 5,745 detik	Cepat, dengan rata-rata waktu untuk melakukan serangan selama 6,832 detik	Paling lambat, dengan rata-rata waktu untuk melakukan serangan selama 137,859 detik
Kemampuan	Tidak mampu mengeksekusi seluruh baris kata dalam *wordlists*, dengan rata-rata *progress* eksekusi *wordlists* sebesar 94,81 %	Mampu mengeksekusi seluruh baris kata dalam *wordlists*	Mampu mengeksekusi seluruh baris kata dalam *wordlists*
Efektivitas	Berhasil menemukan direktori yang rentan	Berhasil menemukan direktori yang rentan	Berhasil menemukan direktori yang rentan

5 Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, ketiga *tools* yang diuji (Gobuster, FFUF, dan Dirb) memiliki kelebihan dan kekurangannya masing-masing. Ketiga *tools* berhasil menemukan direktori yang rentan pada target *website* DVWA. Gobuster unggul dalam aspek kecepatan, namun kalah dalam aspek kemampuan. FFUF unggul dalam aspek kemampuan, namun kalah cepat dibandingan Gobuster. Dirb sangat kurang dalam aspek kecepatan, namun unggul pada aspek lainnya. Berdasarkan penjelasan tersebut, dapat ditarik kesimpulan bahwa *tool* Gobuster memiliki kinerja yang paling baik diantara ketiga *tools* yang diuji jika aspek kecepatan menjadi prioritas utama, sedangkan jika aspek kemampuan yang menjadi prioritas utama, maka *tool* FFUF yang memiliki kinerja paling baik diantara dua *tools* lainnya dengan aspek kecepatan yang jauh melebihi *tool* Dirb.

5.2 Saran

Saran yang dapat diberikan untuk penelitian selanjutnya yaitu serangan *web directory brute force* selain untuk menemukan direktori dapat juga digunakan untuk menemukan file-file tersembunyi dan rentan dari sebuah *website*, uji coba serangan dapat menggunakan *wordlists* dengan jumlah baris kata yang lebih banyak untuk mendapatkan hasil yang maksimal, serta serangan dapat dilakukan secara *recursive*, yaitu melakukan serangan kembali pada alamat direktori yang telah ditemukan sebelumnya untuk menemukan direktori dan file rentan secara lebih mendalam.

Referensi

[1] A. Adelheid, Cara Cepat Membuat Segala Jenis Website. Jakarta: PT Elex Media Komputindo, 2013.

[2] L. M. Gultom dan M. Harahap, "Analisis Celah Keamanan Website Instansi Pemerintahan di Sumatera Utara," *Jurnal Teknovasi*, vol. 02, no. 2, hal. 1–7, 2015.

[3] R. T. Dirgahayu, Y. Prayudi, dan A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *Jurnal Ilmiah NERO*, vol. 1, no. 3, 2015.

[4] A. M. Tania, D. Setiyadi, dan F. N. Khasanah, "Keamanan Website Menggunakan Vulnerability Assessment," *Informatics for Educators and Professionals*, vol. 2, no. 2, hal. 171–180, 2018.

[5] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection untuk Keamanan Website," *Jurnal Teknologi Informasi*, vol. VII, Mar 2013.

[6] T. Feri Efendi, "Pengembangan Website Smk Negeri 3 Sukoharjo," *SENASIF*, ISSN: 2597-4696, 2017.

[7] C. Ibeakanma, "What Is Directory Bursting and How Does It Work?" *makeuseof*.com. Apr 19, 2022. https://www.makeuseof.com/what-is-directory-bursting/ (diakses Des 1, 2022).

[8] A. Putra Armadhani, D. Nofriansyah, dan K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *Jurnal Sains Manajemen Informatika dan Komputer*, vol. 21, no. 2, hal. 80–88, 2022.

[9] Digininja, "Damn Vulnerable Web Application (DVWA)." *Github*.com https://github.com/digininja/DVWA (diakses Des 1, 2022).

[10] M. Doel, "Panduan Hacking Website dengan Kali Linux," dalam *Jakarta: PT Elex Media Komputindo*, 2016.

[11] M. I. Rusdi dan D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," dalam *SEMANTIK*, 2019, hal. 260-268.

[12] O. Reevers, "Gobuster." *Github*.com, https://github.com/OJ/gobuster (diakses Des 01, 2022).
[13] Codingo, "Everything you need to know about FFUF," *Coding*.io, Sep 17, 2020. https://codingo.io/tools/ffuf/bounty/2020/09/17/everything-you-need-to-know-about-ffuf.html (diakses Des 1, 2022).
[14] M. R. Sampurna, "Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA," *NetPLG Journal of Network and Computer Applications*, vol. 1, no. 2, 2022.
[15] Kali, "Dirb Kali Linux Tools," Agu 5, 2022. *Kali*.org, https://www.kali.org/tools/dirb/ (diakses Des 1, 2022).