Implementasi Hydra, FFUF, dan WFUZZ dalam Brute Force DVWA

Muhammad Rudho Sampurna*
Sistem Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya, Palembang, Indonesia

*Korespondensi: rid.sampurna0711@gmail.com

ARTICLE INFO

Article History:
- Received 05 January 2022
- Received in revised form 12 March 2022
- Accepted 17 April 2022
- Available online 30 July 2022

ABSTRAK

Aspek penting dari suatu aplikasi web adalah keamanan dari web tersebut, web yang aman akan memastikan keamanan dari pengguna web. Sistem keamanan yang dimiki web ini harus terus dikembangkan agar web tetap aman dari serangan. Beberapa jenis serangan yang biasanya ditargetkan kepada aplikasi web adalah Brute Force, Cross Site Scripting (XSS), SQL Injection, Denial-of-service (DOS), dan masih banyak yang lain. Dalam penelitian ini kita akan berfokus terhadap serangan brute force. Dalam kriptografi, serangan brute force terdiri dari penyerang yang mengirimkan banyak kata sandi atau frasa sandi dengan harapan dapat menebak dengan benar. Penyerang secara sistematis memeriksa semua kemungkinan kata sandi dan frasa sandi sampai yang benar ditemukan. Atau, penyerang dapat mencoba menebak kunci yang biasanya dibuat dari kata sandi menggunakan fungsi derivasi kunci. Ini dikenal sebagai pencarian kunci lengkap. Untuk mempermudah simulasi serangan brute force kita akan menggunakan aplikasi web yang memang telah didesain untuk memiliki beberapa kekurangan dalam sistemnya, dalam penelitian ini kita akan menggunakan Damn Vulnerable Web App (DVWA) sebagai subjek serangan, alat yang akan digunakan dalam melakukan serangan adalah Hydra, FFUF, WFUZZ.

Kata Kunci : Brute Force, DVWA, Hydra, FFUF, WFUZZ

ABSTRACT

The essential aspect of a web application is the security it provides, ensuring the safety of web users. The security system of a web application must be continuously developed to keep the web safe from attacks. Various attacks are commonly targeted at web applications, including Brute Force, Cross-Site Scripting (XSS), SQL Injection, Denial-of-Service (DOS), etc. This research focuses on brute-force attacks. In cryptography, a brute force attack involves an attacker sending many passwords or passphrase attempts with the hope of guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker may try to guess the key, typically derived from a password, using essential derivation functions. This is known as a whole key search. To facilitate the simulation of a brute force attack, we will use a web application intentionally designed to have vulnerabilities in its system. In this study, Damn Vulnerable Web App (DVWA) will be used as the target, and the tools for the attack will include Hydra, FFUF, and WFUZZ.

Keywords: Brute Force, DVWA, Hydra, FFUF, WFUZZ

1. PENDAHULUAN

Keamanan aplikasi web adalah komponen utama dari setiap bisnis berbasis web. Sifat global Internet mengekspos properti web untuk diserang dari lokasi yang berbeda dan berbagai tingkat skala dan kompleksitas. Keamanan aplikasi web secara khusus berkaitan dengan keamanan di sekitar situs web, aplikasi web, dan layanan web seperti API.

Keamanan aplikasi web (juga dikenal sebagai Web AppSec) adalah gagasan untuk membangun situs web agar berfungsi seperti yang diharapkan, bahkan ketika sedang diserang. Konsep ini melibatkan kumpulan kontrol keamanan yang direkayasa ke dalam aplikasi Web untuk melindungi asetnya dari agen yang berpotensi jahat. Aplikasi web, seperti semua perangkat lunak, pasti mengandung cacat. Beberapa cacat ini merupakan kerentanan aktual yang dapat dieksploitasi, menimbulkan risiko bagi organisasi. Keamanan aplikasi web bertahan terhadap cacat tersebut. Ini melibatkan peningkatan praktik pengembangan yang aman dan penerapan langkah-langkah keamanan di seluruh siklus hidup pengembangan perangkat lunak (SDLC), memastikan bahwa kelemahan tingkat desain dan bug tingkat implementasi diatasi.

Pengujian keamanan web bertujuan untuk menemukan kerentanan keamanan dalam aplikasi Web dan konfigurasinya. Target utama adalah lapisan aplikasi (yaitu, apa yang berjalan pada protokol HTTP). Pengujian keamanan aplikasi Web sering kali melibatkan pengiriman berbagai jenis input untuk memicu kesalahan dan membuat sistem berperilaku dengan cara yang tidak terduga. Ini disebut "tes negatif" memeriksa apakah sistem melakukan sesuatu yang tidak dirancang untuk dilakukan.

Penting juga untuk dipahami bahwa pengujian keamanan Web tidak hanya tentang pengujian fitur keamanan (misalnya, otentikasi dan otorisasi) yang dapat diterapkan dalam aplikasi. Sama pentingnya untuk menguji bahwa fitur lain diimplementasikan dengan cara yang aman (misalnya, logika bisnis dan penggunaan validasi input dan pengkodean output yang tepat). Tujuannya adalah untuk memastikan bahwa fungsi-fungsi yang diekspos dalam aplikasi Web aman.

Pada penelitian ini akan dilakukan Uji Penetrasi. Uji Penetrasi adalah uji keamanan aplikasi manual yang terbaik untuk aplikasi kritis, terutama yang mengalami perubahan besar. Penilaian tersebut melibatkan logika bisnis dan pengujian berbasis musuh untuk menemukan skenario serangan lanjutan.

Tujuan utama penelitian ini adalah untuk melakukan simulasi serangan brute force pada suatu aplikasi web menggunakan beberapa alat berbeda terhadap tingkat keamanan yang berbeda.

2.1. Keamanan Aplikasi Web

Keamanan aplikasi web adalah komponen utama dari setiap bisnis berbasis web. Sifat global Internet mengekspos properti web untuk diserang dari lokasi yang berbeda dan berbagai tingkat skala dan kompleksitas. Keamanan aplikasi web secara khusus berkaitan dengan keamanan di sekitar situs, aplikasi web, dan layanan web seperti API.[1]

2.2. Brute Force

Serangan brute-force adalah serangan cryptanalytic yang secara teori dapat digunakan untuk mencoba mendekripsi data terenkripsi (kecuali untuk data yang dienkripsi dengan cara yang aman secara teori)[2]. Serangan semacam itu dapat digunakan ketika tidak mungkin memanfaatkan kelemahan lain dalam sistem enkripsi (jika ada) yang akan membuat tugas lebih mudah.

Saat menebak kata sandi, metode ini sangat cepat ketika digunakan untuk memeriksa semua kata sandi yang pendek, tetapi untuk kata sandi yang lebih panjang, metode lain seperti serangan kamus digunakan karena pencarian brute force terlalu lama. Kata sandi, frasa sandi, dan kunci yang lebih panjang memiliki lebih banyak kemungkinan nilai, membuatnya secara eksponensial lebih sulit untuk dipecahkan daripada yang lebih pendek.[3]

Setiap serangan brute force dapat menggunakan metode yang berbeda untuk mengungkap data sensitif Anda. Anda mungkin terkena salah satu metode brute force populer berikut ini:

1. Serangan Brute Force Sederhana
   Peretas mencoba menebak kredensial Anda secara logis — sepenuhnya tanpa bantuan perangkat lunak atau cara lain. Ini dapat mengungkapkan kata sandi dan PIN yang sangat sederhana. Misalnya, kata sandi yang ditetapkan sebagai "guest12345".

2. Serangan Kamus
   Dalam serangan standar, seorang peretas memilih target dan menjalankan kemungkinan kata sandi terhadap nama pengguna itu. Ini dikenal sebagai serangan kamus. Serangan kamus adalah alat paling dasar dalam serangan brute force. Meskipun tidak selalu menjadi serangan brute force, ini sering digunakan sebagai komponen penting untuk cracking kata sandi. Beberapa peretas menjalankan kamus lengkap dan menambahkan kata dengan karakter dan angka khusus atau menggunakan kamus kata khusus, tetapi jenis serangan berurutan ini tidak praktis.
3. Serangan Brute Force Hirbida
   Peretas ini memadukan cara luar dengan tebakan logis mereka untuk mencoba pembobolan. Serangan hybrid biasanya menggabungkan kamus dan serangan brute force. Serangan ini digunakan untuk mengetahui kata sandi kombo yang menggabungkan kata-kata umum dengan karakter acak. Contoh serangan brute force seperti ini akan mencakup kata sandi seperti NewYork1993 atau Spike1234.

4. Serangan Brute Force Terbalik
   Seperti namanya, serangan brute force terbalik membalikkan strategi serangan dengan memulai dengan kata sandi yang diketahui. Kemudian peretas mencari jutaan nama pengguna hingga menemukan kecocokan. Banyak dari penjahat ini mulai dengan kata sandi yang bocor yang tersedia secara online dari pelanggaran data yang ada.

5. Isian Kredensial
   Jika seorang peretas memiliki kombo nama pengguna-kata sandi yang berfungsi untuk satu situs web, mereka juga akan mencobanya di banyak situs lainnya. Karena pengguna diketahui menggunakan kembali info masuk di banyak situs web, mereka adalah target eksklusif dari serangan seperti ini.[4]

2.3. DVWA

DVWA (Damn Vulnerable Web Application) adalah proyek perangkat lunak yang dengan sengaja menyertakan kerentanan keamanan dan dimaksudkan untuk tujuan pendidikan. Tujuan utamanya adalah untuk menjadi bantuan bagi profesional keamanan untuk menguji keterampilan dan alat mereka di lingkungan hukum, membantu pengembang web lebih memahami proses mengamankan aplikasi web dan membantu guru dan siswa untuk mengajar dan mempelajari keamanan aplikasi web di lingkungan ruang kelas. DVWA ini memiliki

beberapa tingkat keamanan untuk mempermudah simulasi penyerangan yang akan dilakukan yaitu:

1. Low

Tingkat keamanan ini benar-benar rentan dan tidak memiliki langkah-langkah keamanan sama sekali. Penggunaannya adalah sebagai contoh bagaimana kerentanan aplikasi web bermanifestasi melalui praktik pengkodean yang buruk dan berfungsi sebagai platform untuk mengajar atau mempelajari teknik eksploitasi dasar.

2. Medium

Pengaturan ini terutama untuk memberikan contoh kepada pengguna tentang praktik keamanan yang buruk, di mana pengembang telah mencoba tetapi gagal untuk mengamankan aplikasi. Ini juga bertindak sebagai tantangan bagi pengguna untuk memperbaiki teknik eksploitasi mereka

3. High

Opsi ini merupakan perluasan dari kesulian sedang, dengan campuran praktik buruk yang lebih sulit atau alternatif untuk mencoba mengamankan kode. Kerentanan mungkin tidak memungkinkan tingkat eksploitasi yang sama, serupa di berbagai kompetisi Capture The Flags (CTFs).

4. Imposible

Tingkat ini adalah contoh dari sistem keamanan yang baik. Pada opsi ini kerentanan yang ada pada tingkat sebelumnya itu dihapus dan diubah menjadi lebih baik, dan metode keamanan dari tingkat sebelumnya juga dikembangkan.

2.4. Hydra

Hydra adalah cracker login jaringan paralel yang dibangun di berbagai sistem operasi seperti Kali Linux, Parrot, dan lingkungan pengujian penetrasi utama lainnya. Hydra bekerja dengan menggunakan pendekatan yang berbeda untuk melakukan serangan brute force untuk menebak kombinasi nama pengguna dan kata sandi yang tepat. Hydra biasanya digunakan oleh penguji penetrasi bersama dengan serangkaian program seperti crunch, cupp dll, yang digunakan untuk menghasilkan daftar kata. Hydra kemudian digunakan untuk menguji serangan menggunakan daftar kata yang dibuat oleh program ini.

2.5. FFUF

FFUF, atau "Fuzz Faster you Fool" adalah alat fuzzing web open source, yang dimaksudkan untuk menemukan elemen dan konten dalam aplikasi web, atau server web.
FFUF adalah aplikasi berbasis baris perintah yang berjalan di Terminal Linux, atau Prompt Perintah Windows, yang berarti bahwa itu tidak berisi GUI interaktif, dan sebagai gantinya didukung oleh flag baris perintah yang dimasukkan. Meskipun ini mungkin tampak lebih membatasi pada awalnya, ini cocok untuk tingkat fleksibilitas yang lebih tinggi karena Anda dapat menggunakan alat ini sepenuhnya melalui server jarak jauh, serta "pipa" (pass ke / dari) masuk dan keluar dari FFUF dengan yang lain. alat yang digerakkan oleh baris perintah.

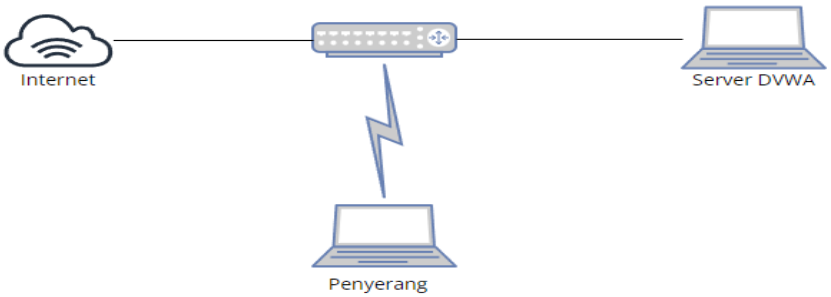
2.6. WFUZZ

Wfuzz adalah aplikasi berkode python untuk mengaburkan aplikasi web dengan banyak pilihan. Ini menawarkan berbagai filter yang memungkinkan seseorang untuk mengganti permintaan web sederhana dengan kata yang diperlukan dengan menggantinya dengan variabel "FUZZ."

3. METODELOGI PENELITIAN

3.1. Desain Topologi

Topologi jaringan yang digunakan pada penelitian ditunjukan pada Gambar 1. Pada topologi jaringan terdapat beberapa perangkat yang terdiri dari server dan penyerang.



Gambar 1. Rancangan Topologi

3.2. Pengaturan Network

Konfigurasi jaringan adalah proses menetapkan pengaturan jaringan, kebijakan, alur, dan kontrol. Dalam jaringan virtual, lebih mudah untuk membuat perubahan konfigurasi jaringan karena peralatan perangkat Jaringan fisik digantikan oleh perangkat lunak, menghilangkan kebutuhan akan konfigurasi manual yang ekstensif

Dalam penelitian ini kita harus melakukan konfigurasi jaringan dasar terhadap setiap perangkat yang digunakan, hal ini diperlukan karena untuk melakukan serangan brute force penyerang dan target serangan harus dapat berkomunikasi satu sama lain.

3.3. Konfigurasi DVWA

Pada tahap ini kita akan melakukan konfigurasi DVWA pada perangkat yang akan kita jadikan target serangan. Berikut adalah langkah-langkah yang harus dijalankan untuk menjalankan aplikasi web DVWA:

1. Download file DVWA
   Kita harus mendownload source kode DVWA dari pembuat DVWA yang bisa ditemukan di internet.
2. Konfigurasi DVWA
   Setelah file DVWA tersedia kita harus memindahkan file tersebut ke lokasi database perangkat, dilanjutkan dengan pengaturan file config DVWA untuk menentukan nama database, user, dan password database yang digunakan.
3. Konfigurasi MySQL
   Pada tahap ini kita harus membuat user baru pada MySQL dan memberi akses penuh kepada user tersebut untuk database DVWA yang telah diatur tadi

4. Konfigurasi Apache2
   Pada tahap ini kita perlu melakukan konfigurasi pada Apache2 untuk menghidupkan fitur tidak aman yang diperlukan agar DVWA dapat berjalan
5. Mulai DVWA
   Ini adalah tahap terakhir dimana kita memulai service yang menjalankan DVWA dan DVWA pun siap digunakan.

3.4. Persiapan Awal Penyerangan

Untuk dapat melakukan serangan brute force terhadap DVWA kita harus memastikan beberapa poin terlebih dahulu seperti:

1. Koneksi antara penyerang dan target serangan
   Disini kita akan melakukan pengecekan apakah penyerang bisa terhubung ke target serangan. Tahap ini bisa diselesaikan dengan percobaan ping atau akses secara normal ke aplikasi web target.
2. Hasil dari percobaan masuk normal
   Jika tahap 1 terpenuhi maka kita dapat mencoba masuk secara normal untuk melihat apakah ada pesan kesalahan, apakah ada pesan sukses. Hal diatas penting untuk mempermudah penyaringan hasil serangan yang dilakukan, dan dalam beberap kasus dapat membantu penyerang berdasarkan pesan kesalahan yang ada, sebagai contoh jika halaman masuk memberi pesan jika hanya password / username yang salah maka penyerang dapat menggunakan informasi tersebut untuk menfokuskan serangan dengan menggunakan informasi yang benar sebagai salah satu input tetap.
3. Tipe Permintaan yang terjadi ketika percobaan login
   Kita perlu melihat tipe permintaan apa yang dikirim untuk diaplikasikan kedalam serangan yang akan dilakukan, sebagai contoh DVWA Brute Force akan menggunakna tipe permintaan “http-get-form”
4. Inspeksi paket yang terkirim saat percobaan masuk normal
   Data paket terkirim dapat membantu penyerang mengumpulkan informasi tambahan terhadap proses yang dilakukan aplikasi web.
5. Pengecekan nomor sesi berjalan
   Nomor sesi biasanya adalah salah satu data cookies yang diperlukan aplikasi web untuk berjalan, dengan melihat nomor sesi yang bejalan penyerang dapat mengambil informasi dasar mengenai tingkat keamanan aplikasi web.

3.5. Penyerangan Menggunakan Hydra

Pada tahap ini kita akan menggunakan alat Hydra untuk melakukan serangan brute force ke DVWA, kita akan melakukan tiga serangan untuk merepresentasikan tiga kondisi yang berbeda.

1. Keamanan Rendah 5 User 10000 Password

Gambar 2 Serangan Hydra 1

Dapat dilihat pada gambar 2 diatas bahwa serangan berhasil dan memakan waktu real 29.89s, user 0.89s, sys 2.60s, dan dengan menggunakan 11% Cpu

2. Keamanan Rendah 5 User 1000 Password

Gambar 3 Serangan Hydra 2

Dapat dilihat pada gambar 3 diatas bahwa serangan berhasil dan memakan waktu real 11.38s, user 0.39s, sys 0.81s, dan dengan menggunakan 10% Cpu

3. Keamanan Sedang 1 User 100 Password

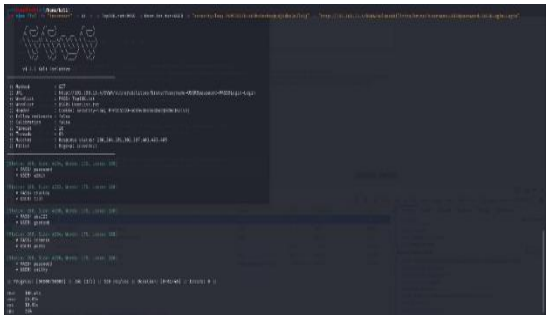
Gambar 4 Serangan Hydra 3

Dapat dilihat pada gambar 4.10 diatas bahwa serangan berhasil dan memakan waktu real 127.39, user 0.13s, sys 0.19s, dan dengan menggunakan 0% Cpu

3.6. Penyerangan Menggunakan FFUF

Pada tahap ini kita akan menggunakan alat FFUF untuk melakukan serangan brute force ke DVWA, kita akan melakukan tiga serangan untuk merepresentasikan tiga kondisi yang berbeda.

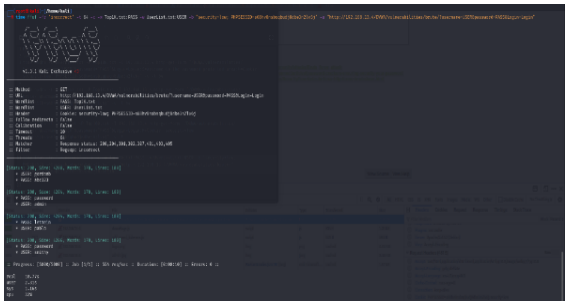
1. Keamanan Rendah 5 User 10000 Password



Gambar 5 Serangan FFUF 1

Dapat dilihat pada gambar 5 diatas bahwa serangan berhasil dan memakan waktu real 108.45s, user 25.03s, sys 10.92s, dan dengan menggunakan 33% Cpu

2. Keamanan Rendah 5 User 1000 Password



Gambar 6 Serangan FFUF 2

Dapat dilihat pada gambar 6 diatas bahwa serangan berhasil dan memakan waktu real 10.77s, user 2.32s, sys 1.16s, dan dengan menggunakan 22% Cpu

3. Keamanan Sedang 1 User 100 Password

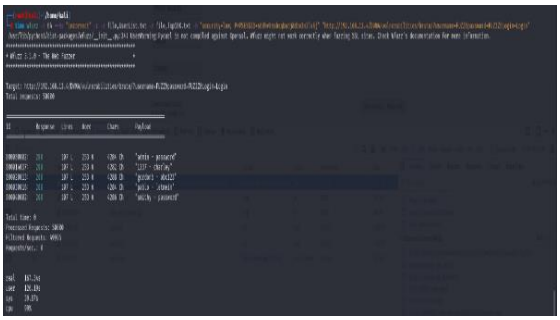
Gambar 7 Serangan FFUF 3

Dapat dilihat pada gambar 7 diatas bahwa serangan berhasil dan memakan waktu real 200.35, user 0.17s, sys 0.15s, dan dengan menggunakan 0% Cpu

3.7. Penyerangan Menggunakan WFUZZ

Pada tahap ini kita akan menggunakan alat WFUZZ untuk melakukan serangan brute force ke DVWA, kita akan melakukan tiga serangan untuk merepresentasikan tiga kondisi yang berbeda.

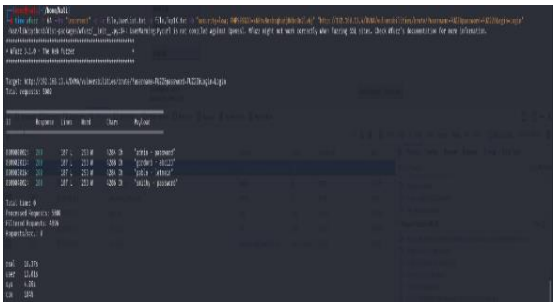
1. Keamanan Rendah 5 User 10000 Password



Gambar 8 Serangan WFUZZ 1

Dapat dilihat pada gambar 8 diatas bahwa serangan berhasil dan memakan waktu real 167.34s, user 126.19s, sys 39.87s, dan dengan menggunakan 99% Cpu

2. Keamanan Rendah 5 User 1000 Password



Gambar 9 Serangan WFUZZ 2

Dapat dilihat pada gambar 9 diatas bahwa serangan berhasil dan memakan waktu real 16.37s, user 13.01s, sys 1.06s, dan dengan menggunakan 104% Cpu

3. Keamanan Sedang 1 User 100 Password

Gambar 10 Serangan WFUZZ 3

Dapat dilihat pada gambar 10 diatas bahwa serangan berhasil dan memakan waktu real 205.03s, user 182.86s, sys 22.10s, dan dengan menggunakan 99% Cpu

4. **HASIL PENELITIAN**

Pada bagian ini kita akan melakukan analisis hasil dari tiga serangan yang telah dilakukan oleh setiap alat:

1. Serangan 1

Tabel 1 Hasil Serangan 1

DVWA Keamanan Low, dengan 5 User dan 10000 Password				
Alat	Real Time	User Time	System Time	CPU
Hydra	29.89	0.89	2.60	11
FFUF	108.15	25.13	10.92	33
WFUZZ	167.34	126.19	39.87	99

Dapat dilihat pada tabel 1 diatas perbedaan waktu yang dipakai dalam proses serangan dan berapa banyak daya CPU yang dipakai. Pada kondisi ini Hydra memiliki hasil terbaik dengan

penggunaan daya CPU yang kecil jika dibandingkan dengan FFUF yang merupakan versi lebih bagus dari WFUZZ, hal ini terjadi karena Hydra memang dibuat untuk melakukan brute force password sedangkan FFUF/WFUZZ dibuat untuk melakukan brute force direktori. Hydra akan melewati kombinasi user dan password jika ada hasil positif, sedangkan FFUF/WFUZZ akan melakukan setiap kombinasi dari user dan password.

2. Serangan 2

Tabel 2 Hasil Serangan 2

DVWA Keamanan low, dengan 5 User dan 1000 Password				
Alat	Real Time	User Time	System Time	CPU
Hydra	11.38	0.39	0.81	10
FFUF	10.77	2.32	1.16	22
WFUZZ	16.37	13.01	1.06	104

Dapat dilihat pada tabel 2 diatas perbedaan waktu yang dipakai dalam proses serangan dan berapa banyak daya CPU yang dipakai. Pada kondisi ini FFUF memiliki hasil waktu terbaik dari ketiga alat yang digunakan, hal ini terjadi karena FFUF dibuat menggunakan Bahasa pemrograman yang lebih efektif jika dibandingkan dengan Hydra dan WFUZZ.

3. Serangan 3

Tabel 3 Hasil Serangan 3

DVWA Keamanan Medium, dengan 1 User dan 100 Password				
Alat	Real Time	User Time	System Time	CPU
Hydra	127.39	0.13	0.19	0
FFUF	200.35	0.17	0.15	0
WFUZZ	205.03	182.86	22.10	99

Dapat dilihat pada tabel 3 diatas perbedaan waktu yang dipakai dalam proses serangan dan berapa banyak daya CPU yang dipakai. Pada kondisi ini hasil percobaan terbaik dimiliki oleh hydra karena hydra akan stop mencoba kombinasi baru setelah ada hasil positif.

5. KESIMPULAN

Damn Vulnerable Web Application (DVWA) adalah sebuah aplikasi web yang dirancang untuk memiliki kekurangan dalam aspek keamanan berdasarkan tingkatan tertentu. DVWA banyak digunakan sebagai alat bantu dalam teknik merancang aplikasi web dikarenakan sifatnya yang open source dan beberapa tingkat keamanan yang tersedia membantu sebagai contoh referensi keamanan aplikasi web yang biasanya digunakan, disisi lain DVWA juga digunakan dalam pembelajaran keamanan cyber sebagai alat bantu pengujian penetrasi.

Dengan adanya penelitian ini, peneliti dapat mengetahui cara melakukan serangan brute force dengan alat seperti Hydra, FFUF, dan WFUZZ. Penerapan alat-alat tersebut telah berhasil dilakukan dan memiliki hasil sesuai dengan yang diharapkan. Hydra sebagai alat yang didesain secara spesifik untuk menyerang halaman masuk memiliki hasil yang memuaskan dalam setiap tes, WFUZZ yang digunakan untuk melakukan brute force direktori memiliki hasil yang kurang memuaskan dengan daya CPU yang dipakai, FFUF yang merupakan versi lebih baik daripada WFUZZ memiliki hasil yang memuaskan dengan berapa cepat alat ini dan daya CPU yang dipakai dalam proses serangan.

DAFTAR PUSTAKA

[1] "What is web application security? | Web security | Cloudflare." https://www.cloudflare.com/learning/security/what-is-web-application-security/ (accessed Apr. 10, 2022).

[2] L. M. Adleman, P. W. K. Rothemund, S. Roweis, and E. Winfree, "On applying molecular computation to the data encryption standard," *J. Comput. Biol.*, vol. 6, no. 1, pp. 53–63, 1999, doi: 10.1089/CMB.1999.6.53.

[3] Electronic Frontier Foundation., "Cracking DES : secrets of encryption research, wiretap politics & chip design," 1998.

[4] "Brute Force Attacks: Password Protection." https://www.kaspersky.com/resource-center/definitions/brute-force-attack (accessed Apr. 10, 2022).