

Индивидуальный проект. Этап 5

Использования Burp Suite

Парфенова Е. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньвна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

Важность понимания, как происходит перехват http-запросов, для поднятия уровня безопасности используемых систем, веб-сайтов и так далее

Цель: Обретение практических навыков использования Burp Suite

Задачи:

- Осуществить перехват запроса для веб-сервера DVWA
- Перехватить запрос аутентификации, попробовав изменить передаваемые данные

Теоретическое введение

Burp Suite – это мультитул для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многое другое. Сам инструмент представляет из себя проксирующий механизм, перехватывающий и обрабатывающий все поступающие от браузера запросы.

Основные модули:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender

Выполнение пятого этапа проекта

Запуск сервера и открытие Burp Suite

```
(eeparfenova@eeparfenova)-[~]  
$ sudo service apache2 start  
[sudo] password for eeparfenova:  
  
(eeparfenova@eeparfenova)-[~]  
$ service mariadb start  
  
(eeparfenova@eeparfenova)-[~]  
$ burpsuite  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Your JRE appears to be version 23-ea from Debian  
Burp has not been fully tested on this platform and you may experience problems.  
□
```

Рис. 1: Запуск сервера и открытие Burp Suite

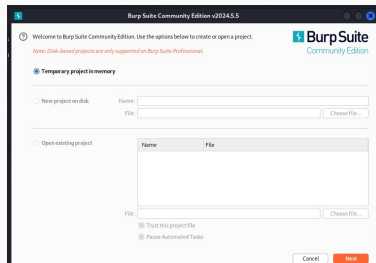


Рис. 2: Создание проекта в Burp Suite

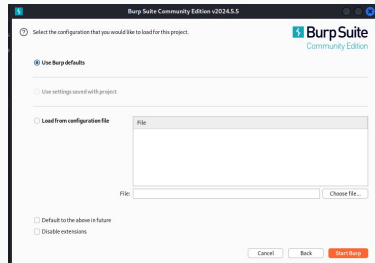


Рис. 3: Настройки проекта в Burp Suite

Запуск перехвата

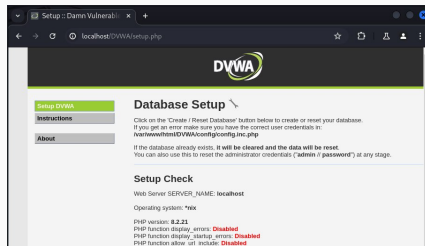


Рис. 4: Открытие DVWA через Burp-браузер

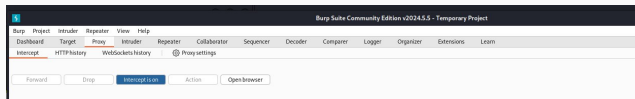


Рис. 5: Запуск перехвата

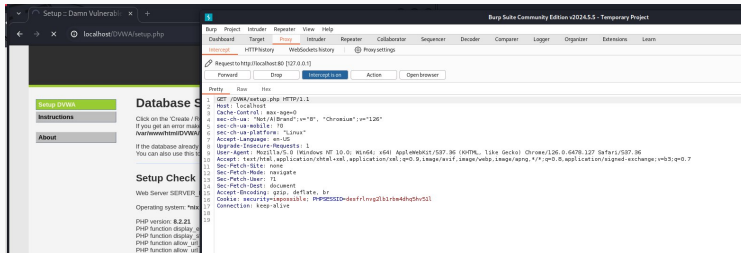


Рис. 6: Перехваченный запрос

Перехват запроса авторизации

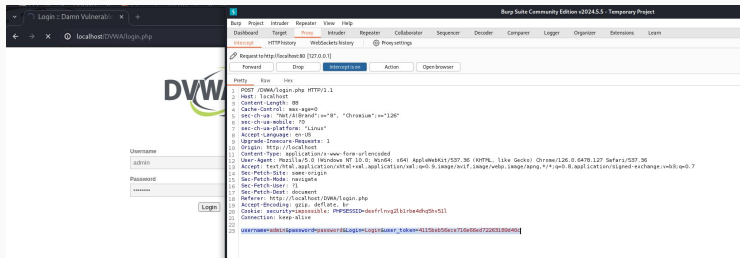


Рис. 7: Перехваченный запрос авторизации

История запросов

78	http://localhost	GET	/DWWA/login.php	200	7870	HTML	php	Login: DamnVulnerable...	127.0.0.1	20:24:27.0...	8080	20
81	http://localhost	POST	/DWWA/login.php	✓	302	476	HTML	php	PHPSESSID=...	20:24:41.0...	8080	30
82	http://localhost	GET	/DWWA/index.php	200	6435	HTML	php	Welcome: DamnVulnerable...	127.0.0.1	20:27:37.0...	8080	19
83	http://localhost	GET	/DWWA/vulnerabilities/routes/	✓	200	4875	HTML	Vulnerability: Brute Force...	127.0.0.1	20:28:04.0...	8080	34
84	http://localhost	POST	/DWWA/vulnerabilities/routes/	✓					127.0.0.1	20:29:29.0...	8080	

Request

Pretty

Raw

Hex

1

POST /DWWA/login.php HTTP/1.1

2

Host: localhost

3

Content-Length: 88

4

Cache-Control: max-age=0

5

sec-ch-ua: "msie";v="120", "Chromium";v="120"

6

sec-ch-ua-mobile: ?0

7

sec-ch-ua-platform: "Linux"

8

Accept-Language: en-US

9

Upgrade-Insecure-Requests: 1

10

Origin: http://localhost

11

Content-Type: application/x-www-form-urlencoded

12

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6479.127 Safari/537.36

13

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14

Sec-Patch-Site: same-origin

15

Sec-Patch-Mode: navigate

16

Sec-Patch-User: ?

17

Sec-Patch-User: document

18

Referer: http://localhost/DWWA/login.php

19

Accept-Encoding: gzip, deflate, br

20

Cookie: security=impossible; PHPSESSID=...

21

Connection: keep-alive

22

23

24

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 Found

2

Date: Wed, 09 Oct 2024 17:27:37 GMT

3

Server: Apache/2.4.62 (Debian)

4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

5

Cache-Control: no-store, no-cache, must-revalidate

6

Pragma: no-cache

7

Set-Cookie: PHPSESSID=...; path=/; HttpOnly; SameSite=Strict

8

GMT: Mon, 09 Oct 2024 17:27:37 GMT

9

Location: index.php

10

Content-Length: 0

11

Keep-Alive: timeout=5, max=100

12

Connection: Keep-Alive

13

Content-Type: text/html; charset=UTF-8

14

Inspector

Request attributes

2

Request body parameters

4

Request cookies

2

Request headers

20

Response headers

11

user=...&id=...&password=...&login=...&token=...

4115eb56ce716e66d72269389480c

Рис. 8: Данные о запросе в истории запросов

Изменение данных перехваченного запроса

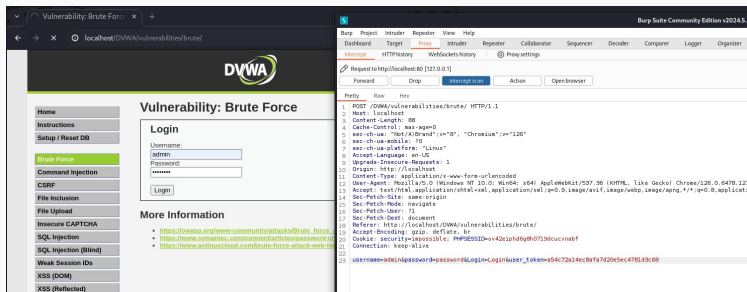


Рис. 9: Перехват логина и пароля с Brute Force

Изменение данных перехваченного запроса

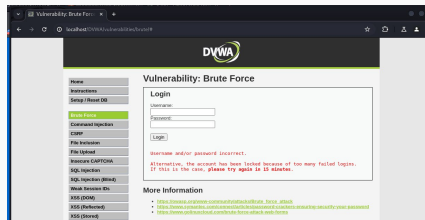


Рис. 10: Неудачная из-за измененных данных авторизация

34	http://localhost	POST	DVWA/vulnerability/brute/	✓	✓	200	5019	HTML	Vulnerability: Brute For...	127.0.0.1	PHP/5.6.40-gem...	20292990c...	8080	2115
----	------------------	------	---------------------------	---	---	-----	------	------	-----------------------------	-----------	-------------------	--------------	------	------

Рис. 11: Запись об авторизации в истории запросов

Вывод

Мы обрели практические навыки использования Burp Suite, осуществив перехват запроса для веб-сервера DVWA и перехватив запрос аутентификации с изменением его данных