

Индивидуальный проект шаг 5

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

Задание

В этом этапе индивидуального проекта требуется использовать набор инструментов Burp Suite, чтобы найти и использовать какие-то уязвимости в DVWA.

Выполнение



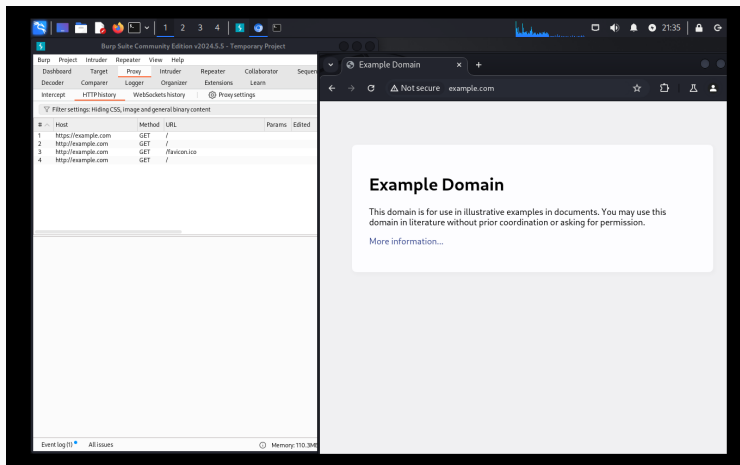


Рис. 1: Burp Proxy

POST-запрос

The image shows two overlapping windows. The background window is Burp Suite Community Edition v2024.5.5, displaying a list of HTTP requests. The foreground window is a web browser showing the 'Vulnerability: File Upload' page of the DVWA application.

Burp Suite Request List:

#	Host	Method	URL	Params	Edited	Status code	Len
3	http://example.com	GET	/favicon.ico			404	160
4	http://example.com	GET	/			304	308
5	http://localhost:4280	GET	/			200	645
7	http://localhost:4280	GET	/dwaaj/dwaajPage.js			200	134
8	http://localhost:4280	GET	/dwaaj/pradd_event_listeners.js			200	961
11	http://localhost:4280	GET	/vulnerabilities/brute/			200	456
12	http://localhost:4280	GET	/vulnerabilities/brute/?username=...			200	456
13	http://localhost:4280	GET	/vulnerabilities/weak_id/			200	378
14	http://localhost:4280	POST	/vulnerabilities/weak_id/			200	380
15	http://localhost:4280	GET	/vulnerabilities/cve/			200	571
16	http://localhost:4280	GET	/vulnerabilities/upload/			200	434
17	http://localhost:4280	POST	/vulnerabilities/upload/			200	437

Request Details (Item 11):

Request: http://localhost:4280/vulnerabilities/brute/

Response: HTTP/1.1 200 OK

Inspector: Request body parameters, Request cookies, Request headers, Response headers.

Web Application (DVWA):

Vulnerability: File Upload

Choose an image to upload:

No file chosen

Your image was not uploaded.

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload/
- <https://www.acunetix.com/websecurity/upload-forms-threat/>

Рис. 2: POST-запрос

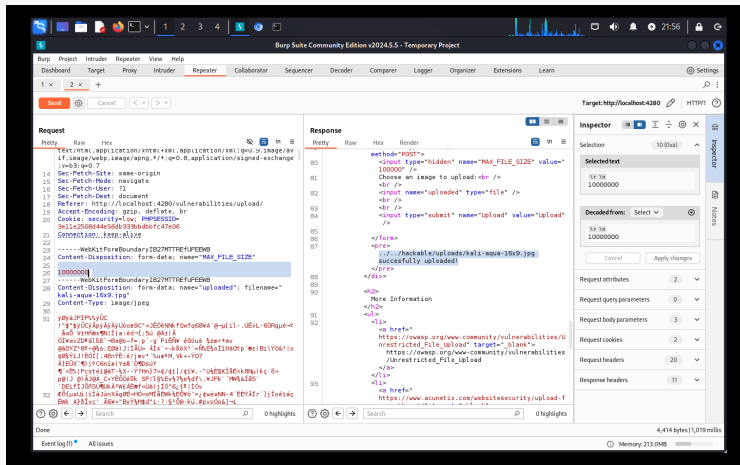


Рис. 3: MAX_FILE_SIZE

6/10

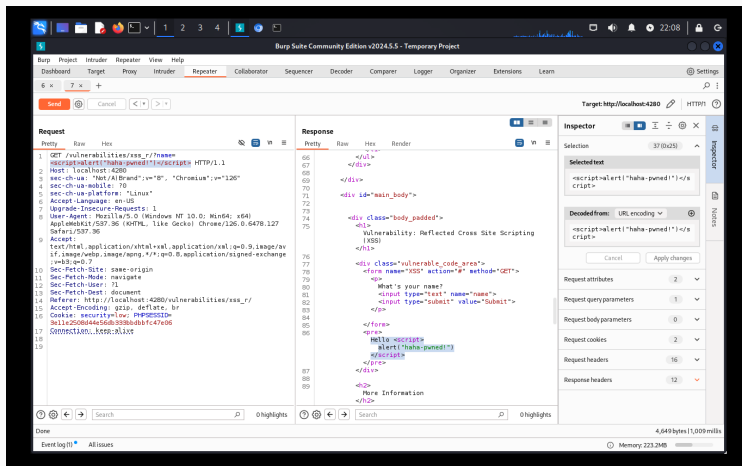


Рис. 5: XSS

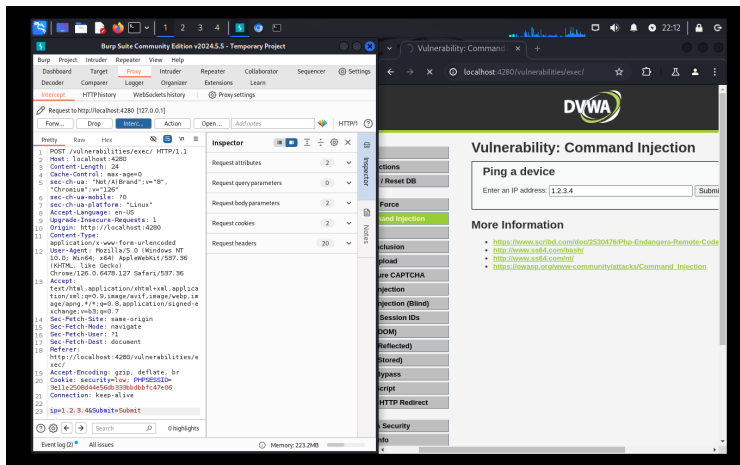


Рис. 6: Intercept

Intercept

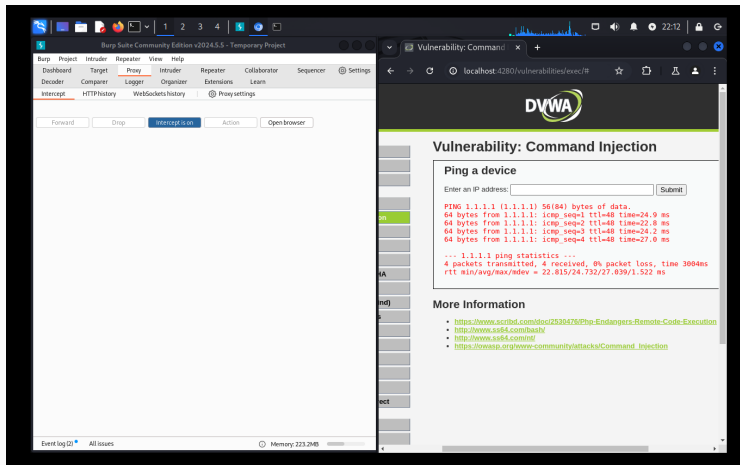


Рис. 7: Intercept

Выводы

Мы успешно использовали некоторые из утилит в Burp Suite для анализа и использования уязвимостей.