

## Задание выполнил студент группы 2345 Романенко Кирилл

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

На сайте <http://192.168.56.11/dvwa/vulnerabilities/csrf/> отсутствует проверка соответствия Host - Referer

### Где найдена уязвимость

Уязвимость расположена по адресу

<http://192.168.56.11/dvwa/vulnerabilities/csrf/>

Наименование продукта: Metasploitable 3 Linux virtual machine.

### Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить на странице

<http://192.168.56.11/dvwa/vulnerabilities/csrf/>

Ввел в форму ввода 123 и перехватил запрос в Burp Suite:

The screenshot shows the Burp Suite interface. On the left, the 'Instructions' panel is visible with 'CSRF' highlighted. The main window displays the 'Change your admin password' form with fields for 'New password' and 'Confirm new password', both containing three dots. Below the form is a 'Change' button. The bottom panel shows the intercepted HTTP request in the 'Raw' tab. The request is a GET request to [http://192.168.56.11/dvwa/vulnerabilities/csrf/?password\\_new=123&password\\_conf=123&Change=Change](http://192.168.56.11/dvwa/vulnerabilities/csrf/?password_new=123&password_conf=123&Change=Change). The headers include Host: 192.168.56.11, User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, Connection: close, Referer: http://192.168.56.11/dvwa/vulnerabilities/csrf/?password\_new=password&password\_conf=password&Change=Change, Cookie: security=medium; security\_level=1; PHPSESSID=an4tuk8uqe2df82j85aqp72lg7, and Upgrade-Insecure-Requests: 1.

Заменяю Referer

ДО: <http://192.168.56.11/dvwa/vulnerabilities/csrf/>

ПОСЛЕ: 127.0.0.1

Forward

## Vulnerability: Cross Site Request Forgery

Change your admin password:

New password:

Confirm new password:

Change

Password Changed

### 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.
- FireFox Extended Support Release 102.5.0esr (64-bit).