Assignment 5.1.2

Course name: CSRF

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. CSRF

Purpose: understand what CSRF is

After the work the student must

- know: CSRF;
- be able to: recognize, analyze and exploit CSRF.

Tasks:

- analyze provided web application on virtual machine 192.168.56.8 and check its' parameters.

Material of the workplace

- http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery
- https://owasp.org/www-community/attacks/csrf
- https://owasp.org/www-project-code-review-guide/reviewing-code-for-csrf-issues

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- WEb developer tools

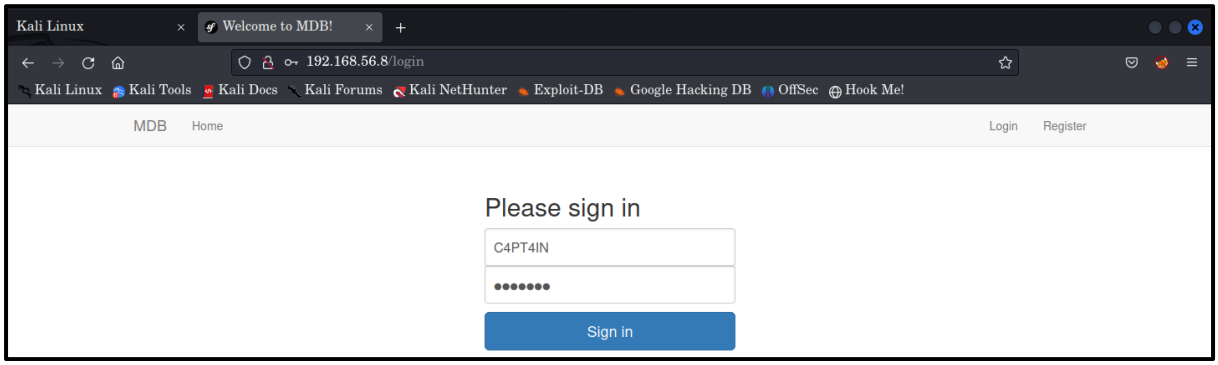
Solution:

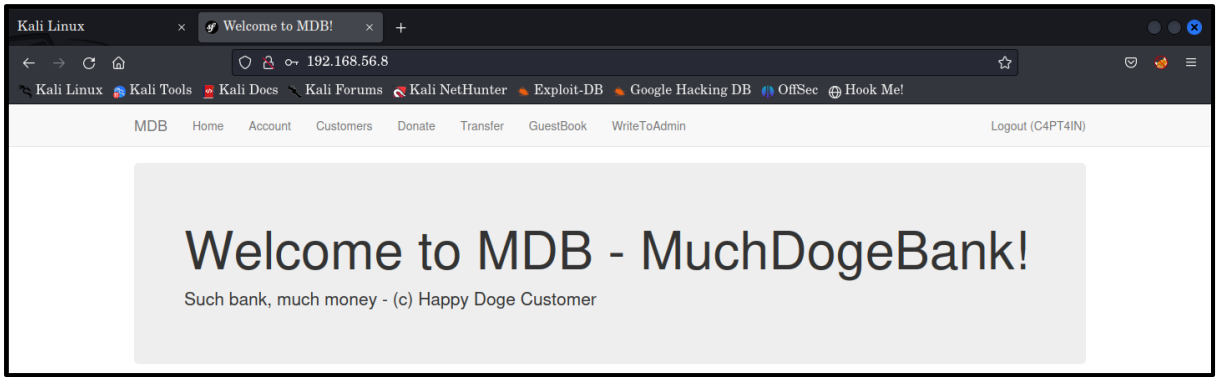
Open each site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for detection and exploiting CSRF.

TASK 1

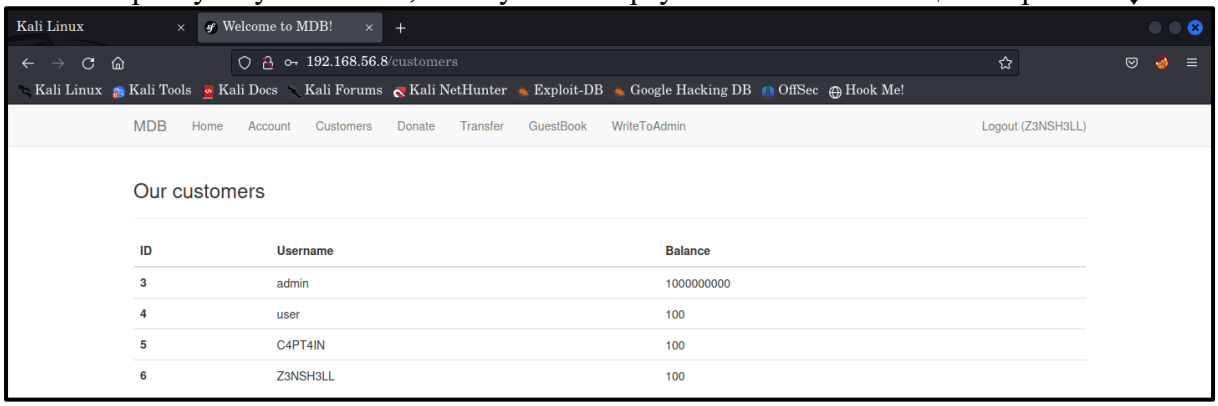
For provided sites you need to answer: is there CSRF present? How did you find it? Prove it (screenshot).

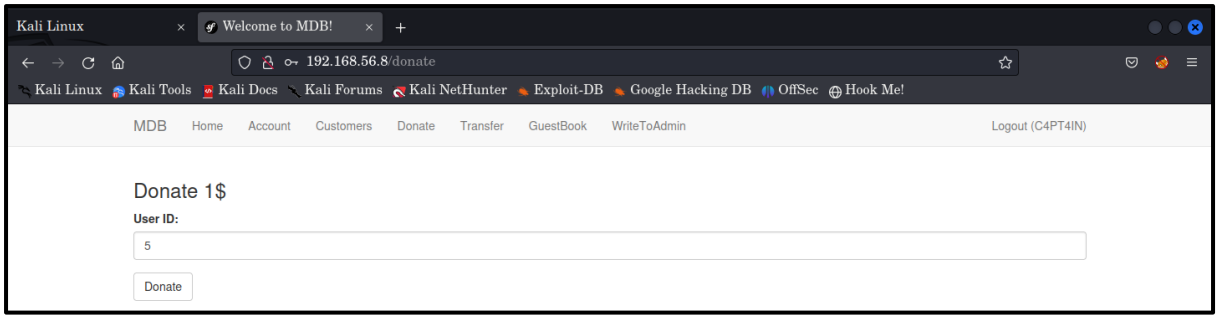
Answer:

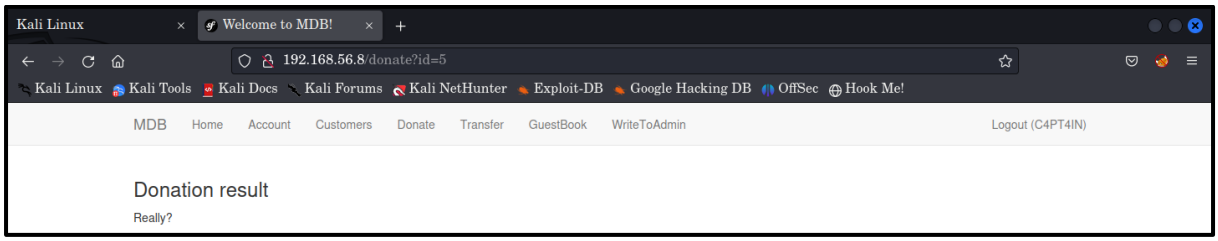


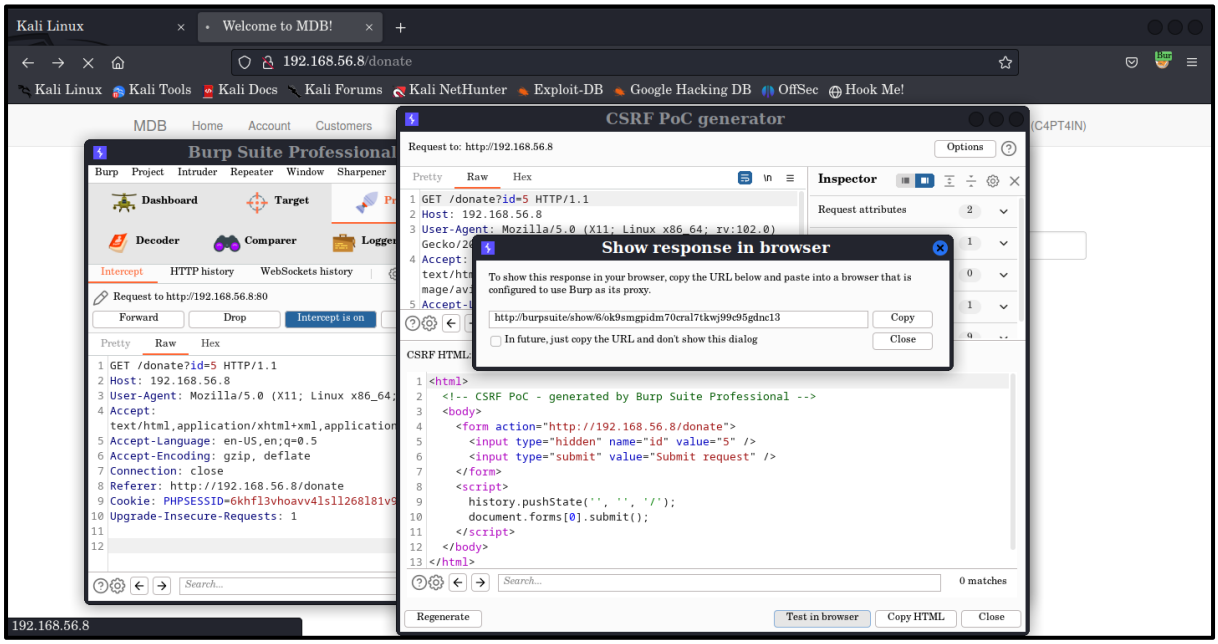


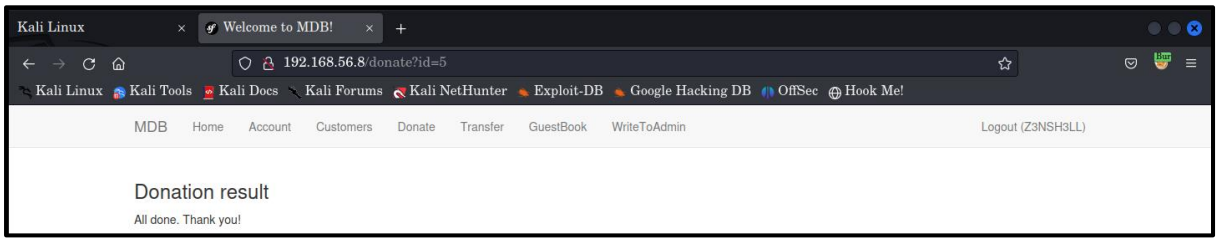
– На веб-сторінці “**Donate**” ми можемо скористатися **CSRF** вразливістю, щоб деякий користувач **Z3NSH3LL** випадковим чином, будучи вже авторизованим на веб-сайті, перейшов за попередньо створеним посиланням та пожертвував 1$ користувачу **C4PT4IN**, який у свою чергу не може сам собі цього зробити ↓

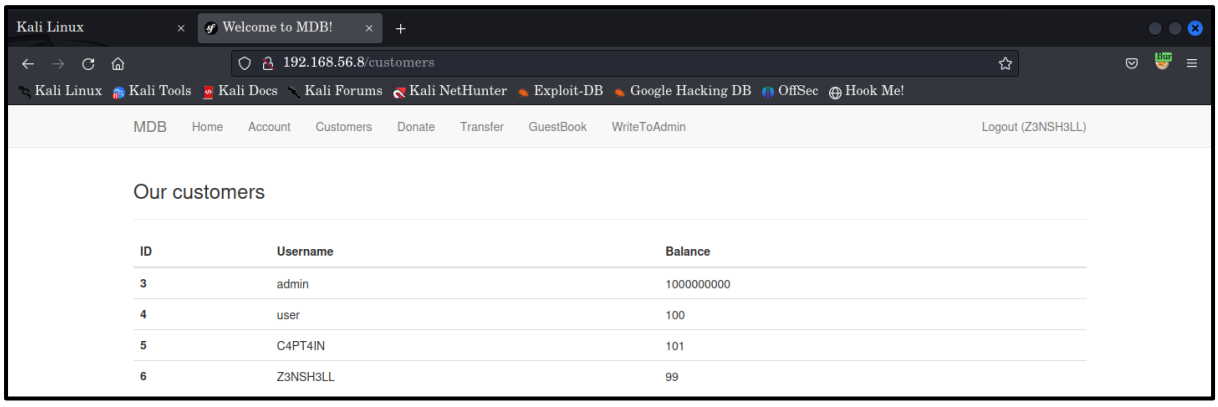



Kali Linux
Welcome to MDB!
192.168.56.8/donate
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
MDB Home Account Customers Donate Transfer GuestBook WriteToAdmin Logout (C4PT4IN)
Donate 1$
User ID:
5
Donate

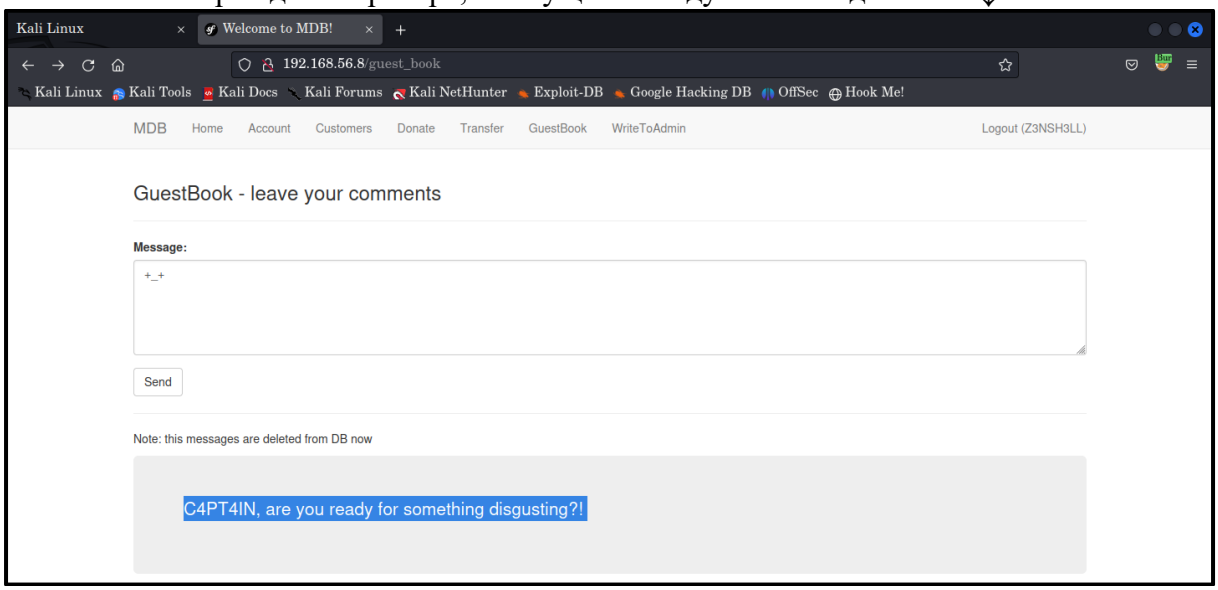

Kali Linux
Welcome to MDB!
192.168.56.8/donate?id=5
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
MDB Home Account Customers Donate Transfer GuestBook WriteToAdmin Logout (C4PT4IN)
Donation result
Really?

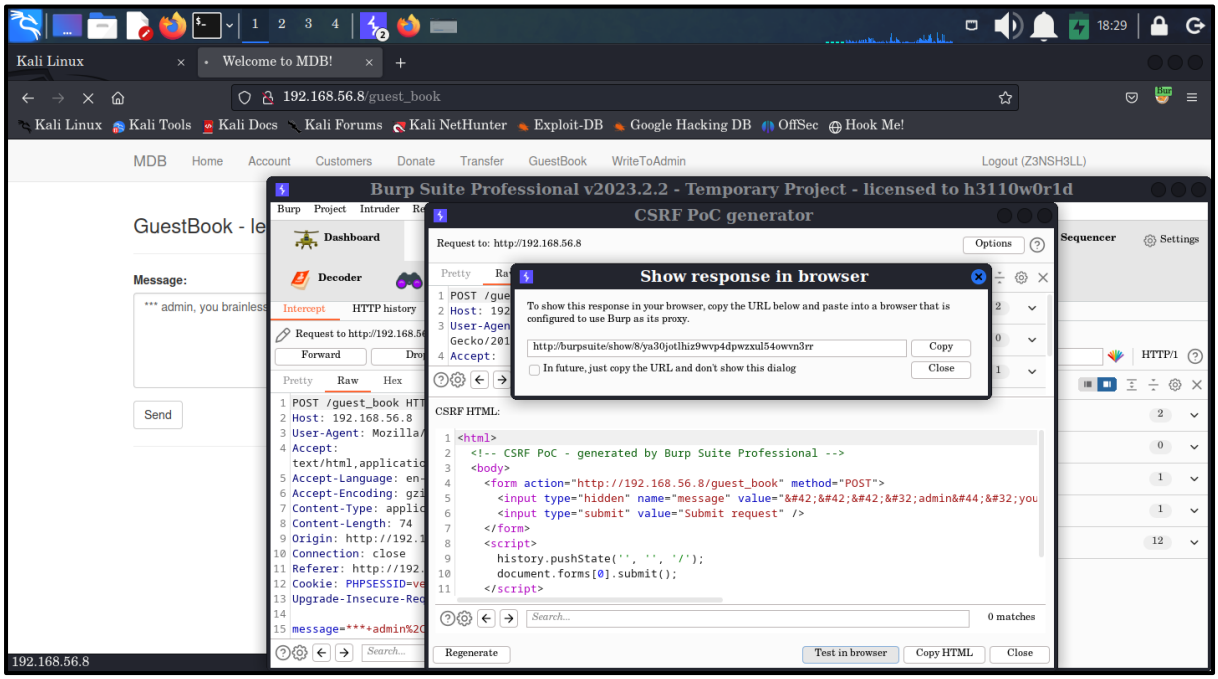

Kali Linux
Welcome to MDB!
192.168.56.8/donate
Burp Suite Professional
CSRF PoC generator
Request to: http://192.168.56.8
Show response in browser
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.
http://burpsuite/show/6/ok9smgpidm70cral7tkwj99c95gdnc13
Copy
Close
In future, just copy the URL and don't show this dialog
Regenerate
Test in browser
Copy HTML
Close
192.168.56.8

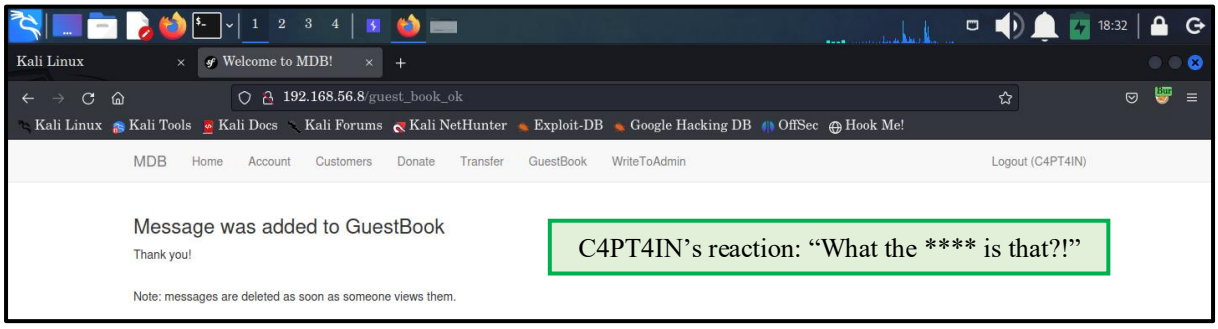

Kali Linux
Welcome to MDB!
192.168.56.8/donate?id=5
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
MDB Home Account Customers Donate Transfer GuestBook WriteToAdmin Logout (Z3NSH3LL)
Donation result
All done. Thank you!


Kali Linux
Welcome to MDB!
192.168.56.8/customers
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
MDB Home Account Customers Donate Transfer GuestBook WriteToAdmin Logout (Z3NSH3LL)
Our customers
ID Username Balance
3 admin 1000000000
4 user 100
5 C4PT4IN 101
6 Z3NSH3LL 99

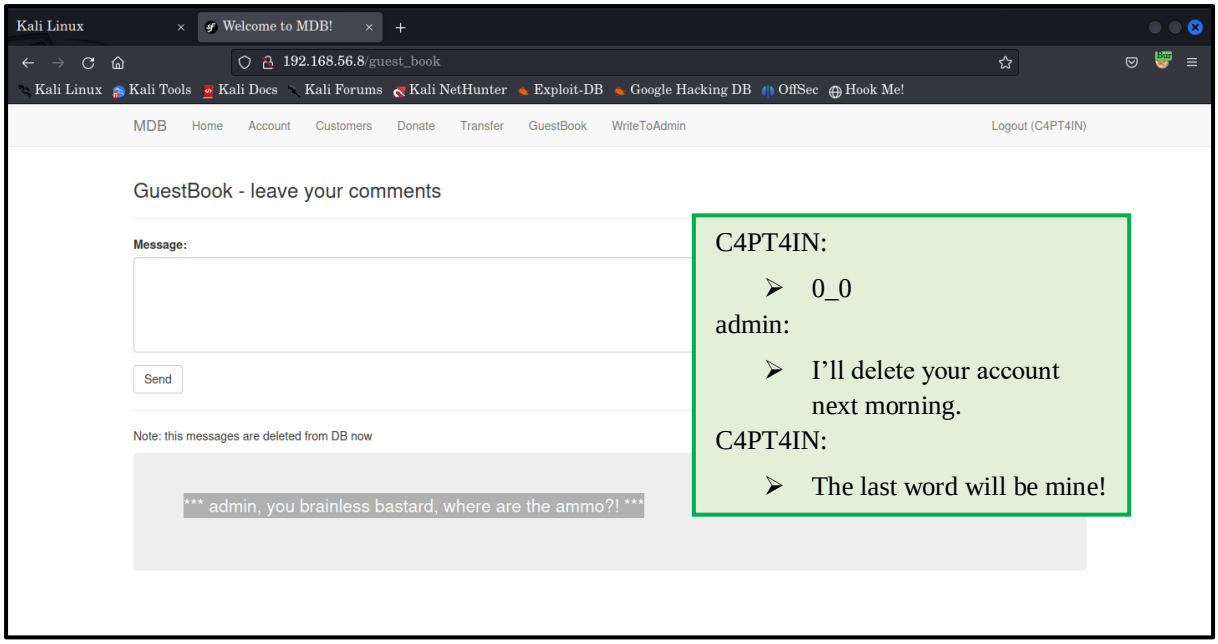
– Однак користувач **Z3NSH3LL** також знає про вразливість сайту до **CSRF**-атак, тому зараз він заставить користувача **C4PT4IN** написати на веб-сторінці “погані слова” про адміністратора, якому це може дуже не сподобатися ↓





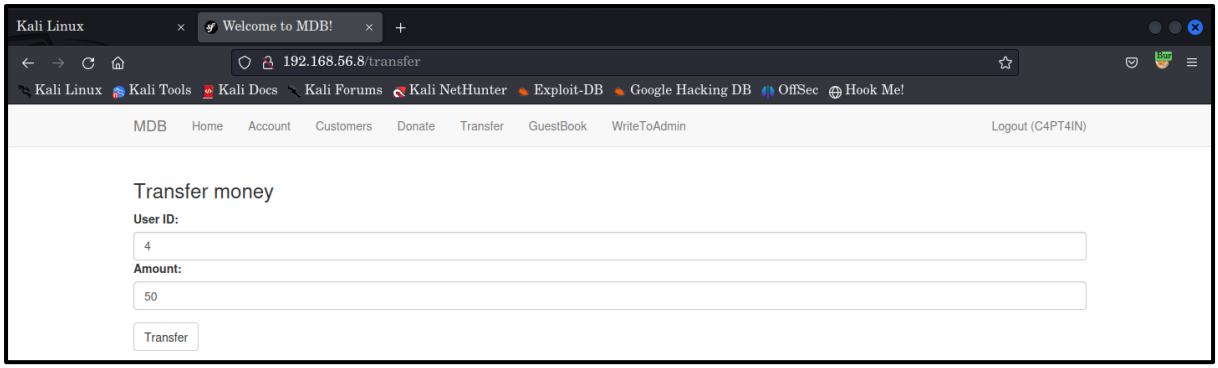


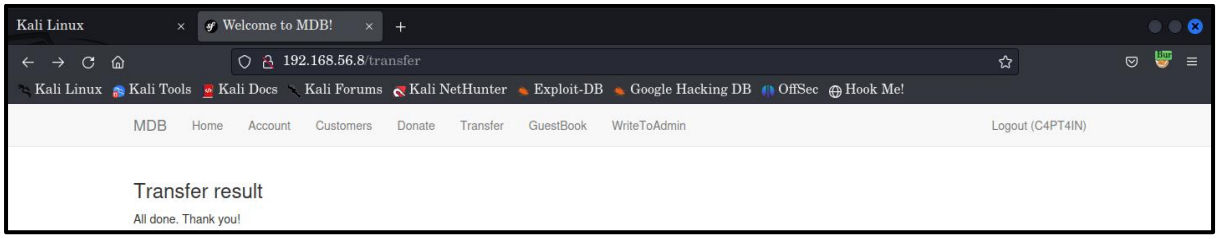
C4PT4IN’s reaction: “What the **** is that?!”

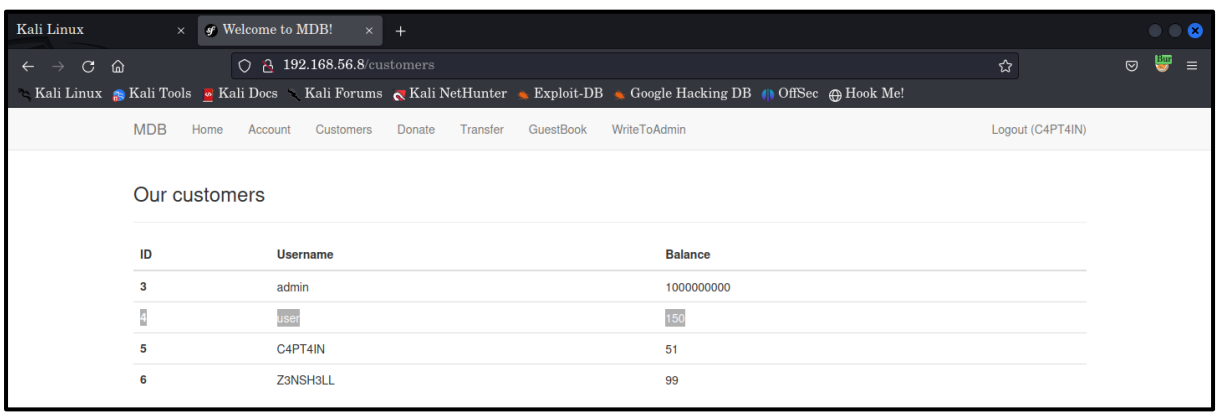


TASK 2
You need to steal 1000000 from admin account? Do and prove it (screenshot).

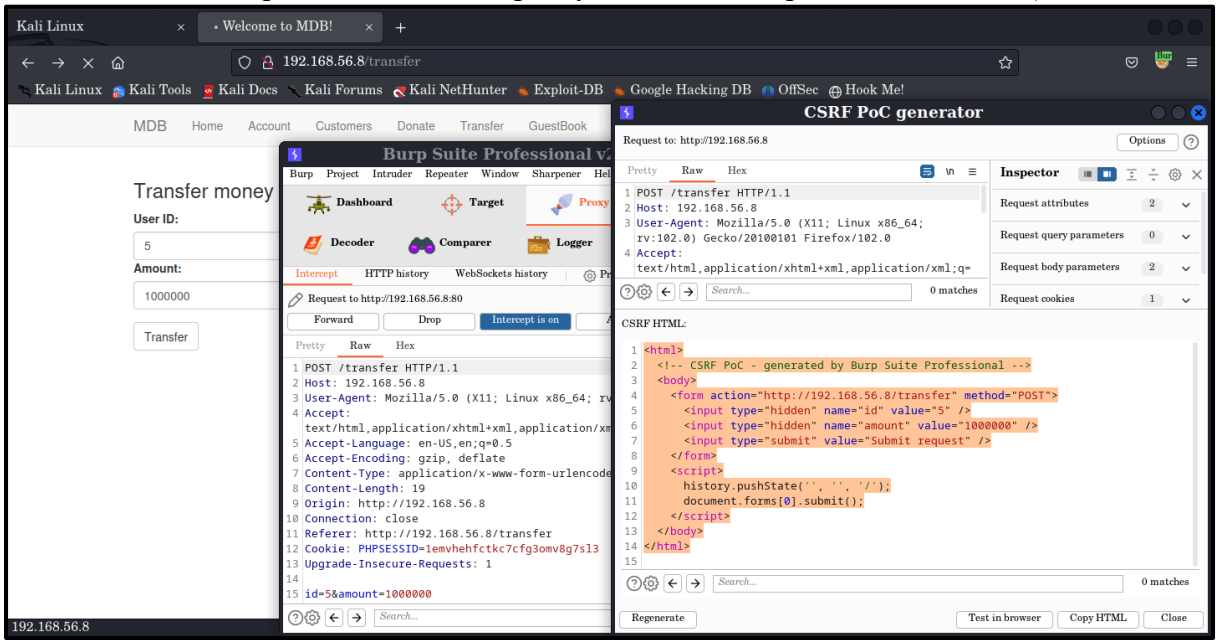
Answer:

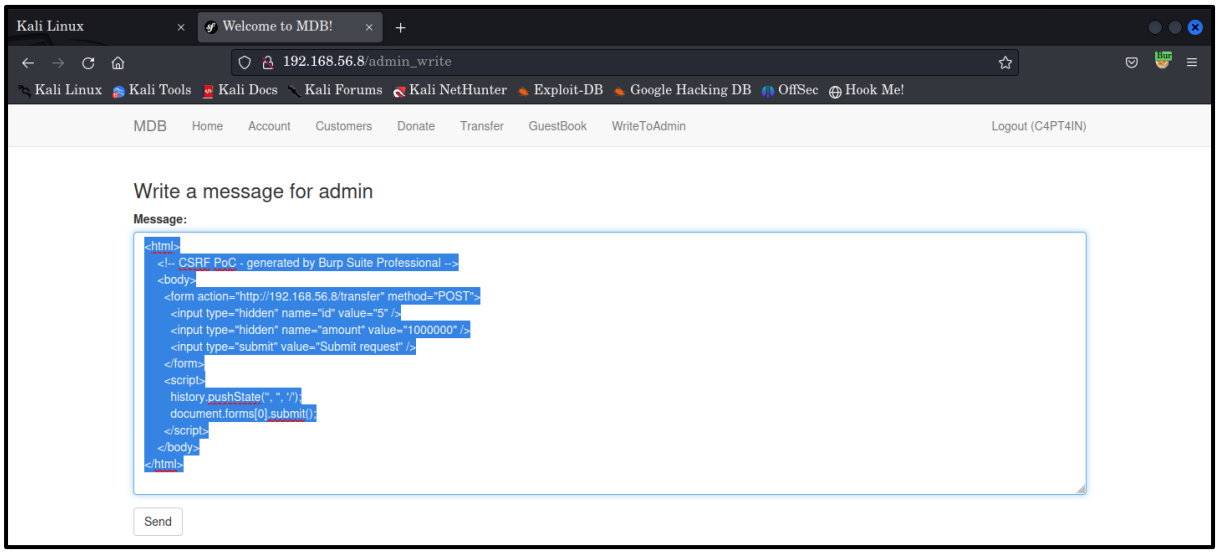


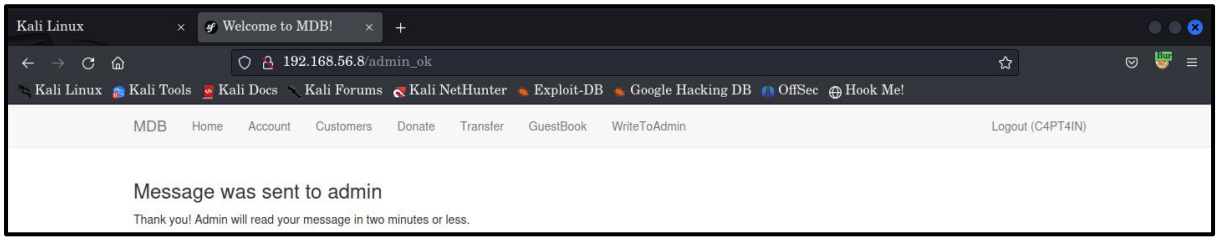


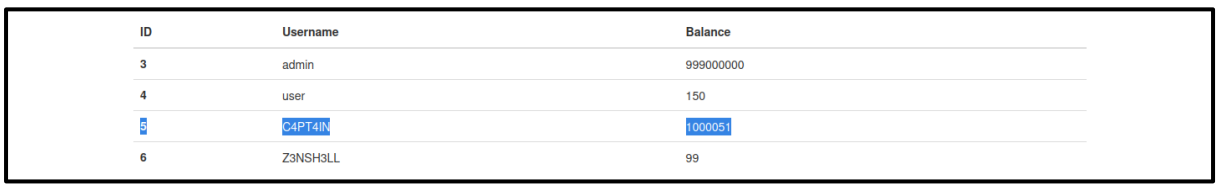


– Дуже цікавий функціонал знайшов **C4PT4IN** на сторінці “**Transfer**”, надсилаючи одному простому користувачу 50$. Якщо казати конкретніше, то через те, що веб-сайт, як ми вже бачили, повністю вразливий до **CSRF**-атак, звідси можна припустити, що ця веб-сторінка, схоже що не виняток. Тому, на останок, заставимо привілейованого користувача **admin** переслати 1000000$↓

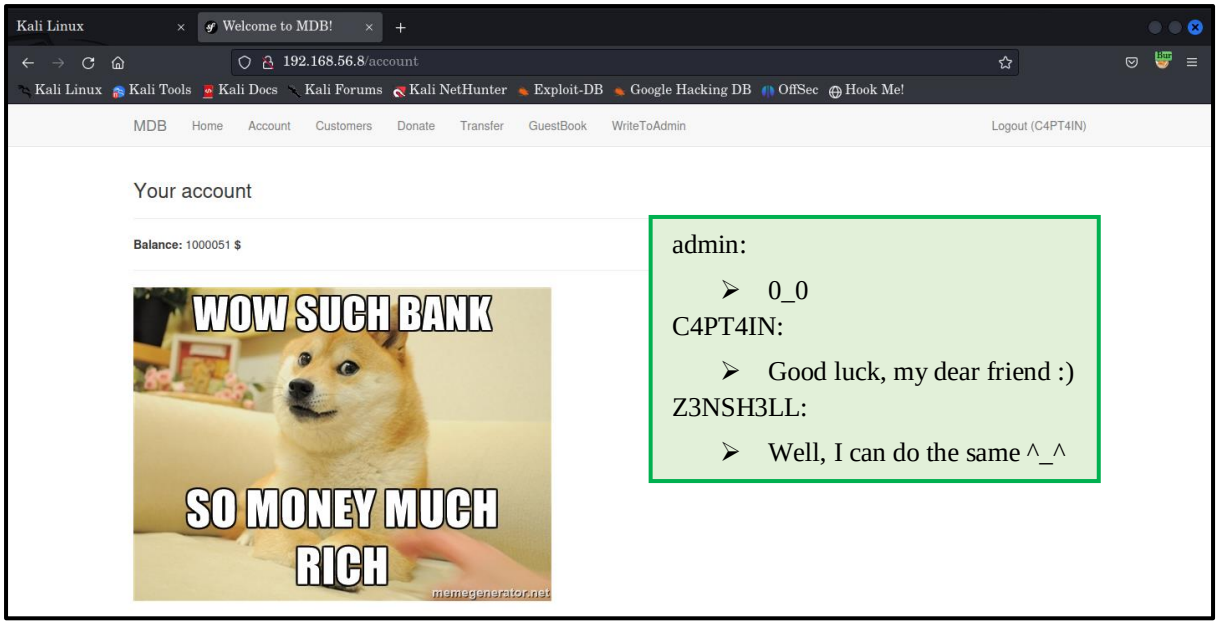








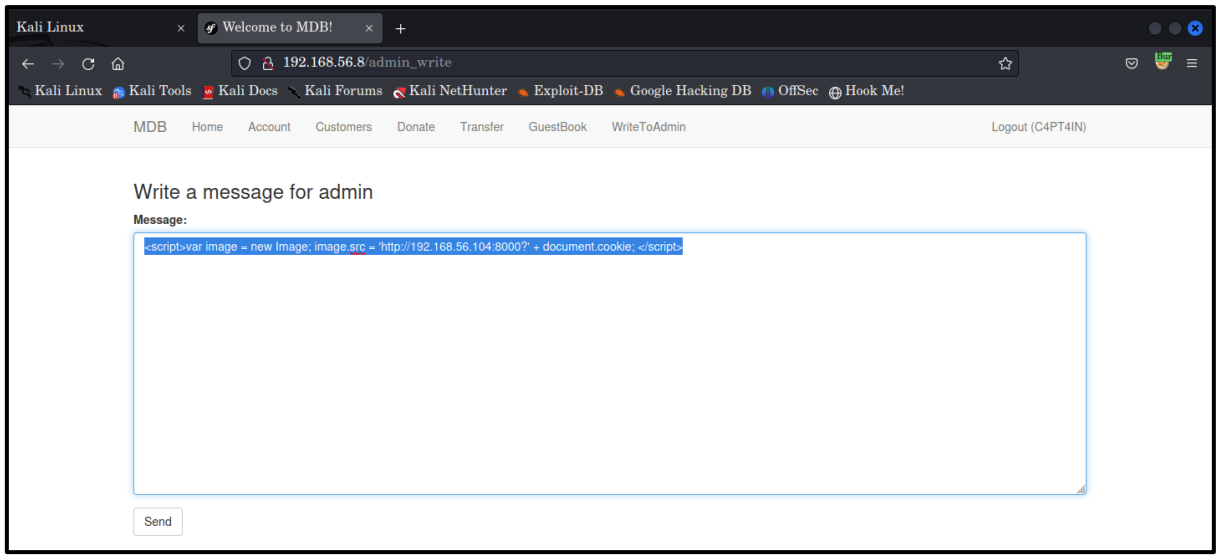
ID	Username	Balance
3	admin	999000000
4	user	150
5	C4PT4IN	1000051
6	Z3NSH3LL	99



TASK 3
Could you steal admin session? How? Prove it (screenshot).

Answer:
CSRF сам по собі не дозволяє викрасти файл ідентифікатор сесії. Натомість **CSRF** дозволяє зловмиснику лише надсилати запит до домену cookie, який містить cookie, так само, як це роблять запити до домену cookie, надіслані справжнім користувачем. Таким чином, це дозволяє надсилати запити з ідентичністю справжнього користувача в браузері користувача, але не викрадати ідентифікаційні дані для використання поза вихідним середовищем браузера.

У цілому файл cookie може бути викрадений зловмисником, який виконує власний сценарій у домені файлів cookie, але це буде XSS, а не **CSRF**. Файл cookie може бути вкрадено шляхом перехоплення трафіку між браузером і доменом файлів cookie, але це буде атака MITM, а не **CSRF**. Значення cookie може бути якимось чином розкрито сервером, на який надсилається файл cookie, але це буде витік інформації, а не **CSRF**.



```
┌──(nazar㉿snz24)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether [redacted]
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 466sec preferred_lft 466sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(nazar㉿snz24)-[~]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.56.8 - - [13/May/2023 20:13:29] "GET /? HTTP/1.1" 200 -
```