Assignment 7.1

Name: Parameter tampering and authorization errors

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. Detect parameter tampering vulnerability

Purpose: understand how to detect parameter tampering vulnerabilities.

After the work, the student must

- know: what is parameter tampering, and how it could be performed;
- be able to: analyze the results of parameters processing.

Tasks:

- analyze provided web application on virtual machine 192.168.56.10, check its' parameters, and try to get photos from the gallery without a watermark.

Technical equipping of the workplace:

- Browser Developer Tools.

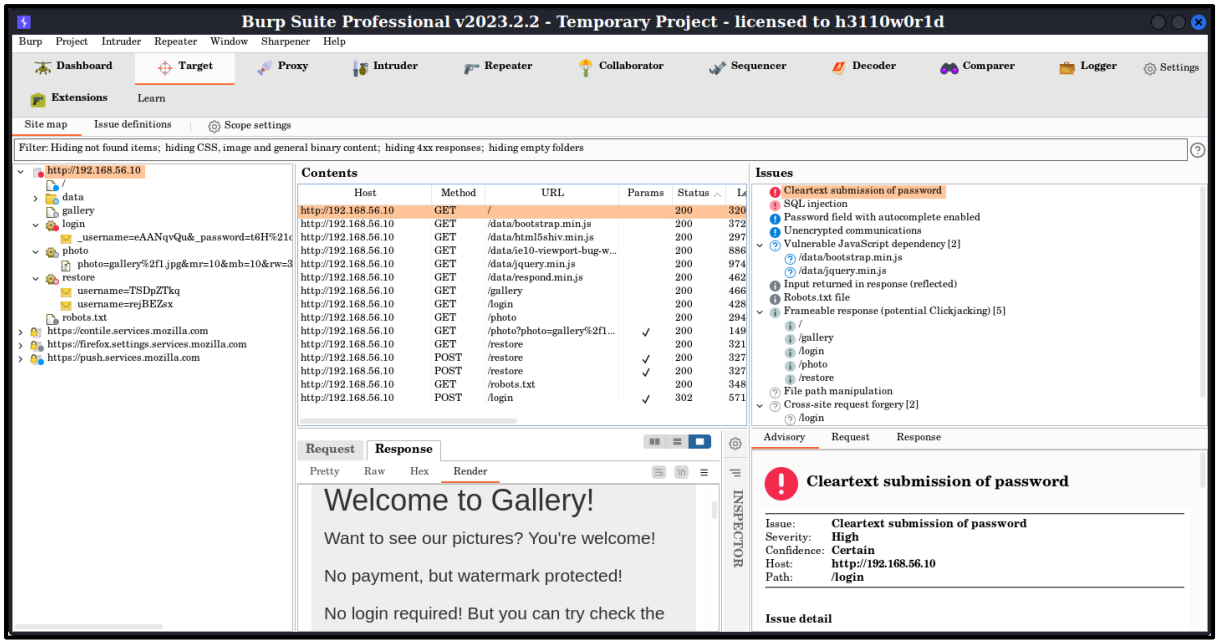
TASK 1

Which vulnerabilities provided the web application has? Prove it with a screenshot.

Answer:

Усі ті вразливості, які ми маємо знайти у цьому та наступному завданні, будуть справді присутні у даному веб-застосунку, тому нагадаємо їх ще раз (підтвердження пізніше):

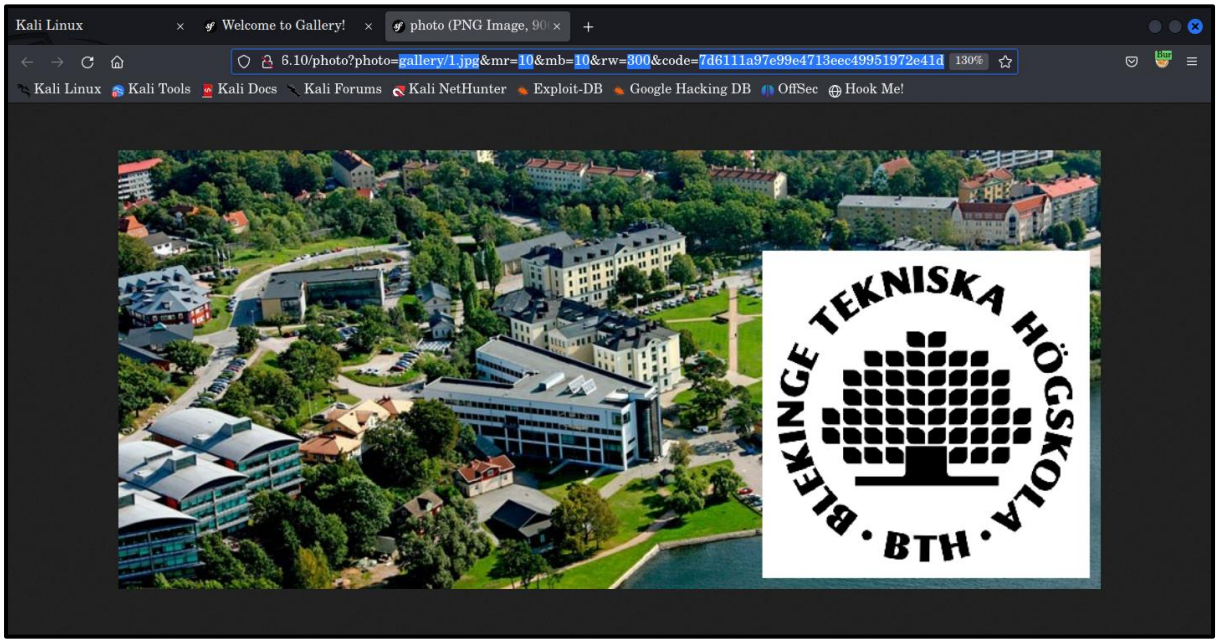
- ❖ Можливість прямого доступу без попередньої авторизації до ресурсів веб-сайту;
- ❖ Передача у відкритому вигляді параметрів генерації вотермарки для зображень;
- ❖ Використання слабкого та передбачуваного токену для функції скидання паролю;
- ❖ Надсилання облікових даних під час автентифікації у незахищеному вигляді;
- ❖ Та інші вразливості, які не входять до теми лабораторної роботи. ↓ ↓ ↓ ↓ ↓

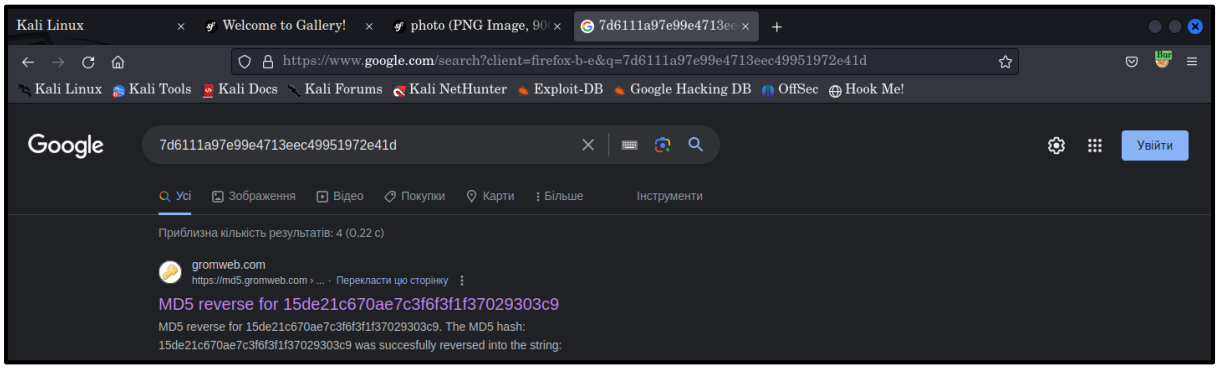


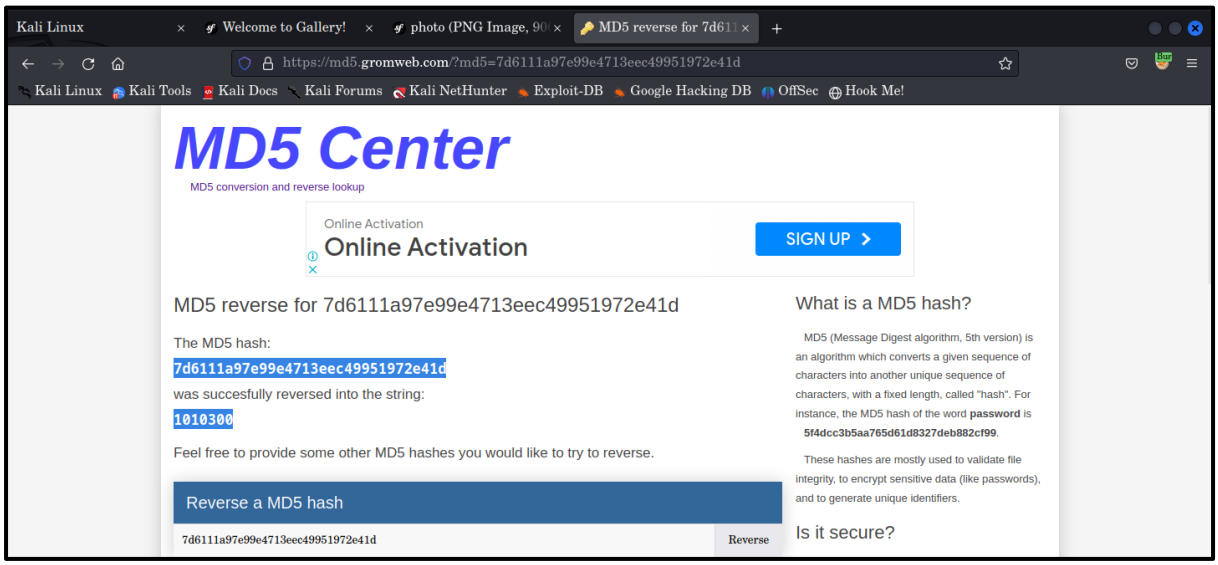
TASK 2

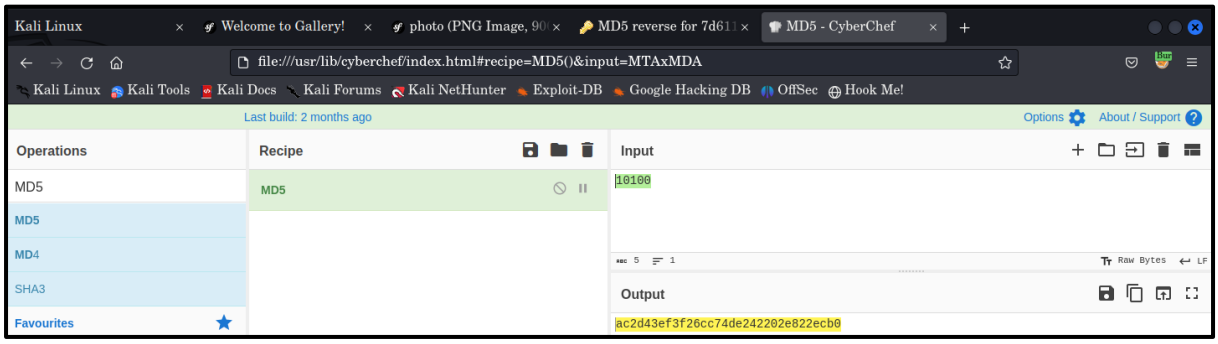
How is possible to get images without watermarks?

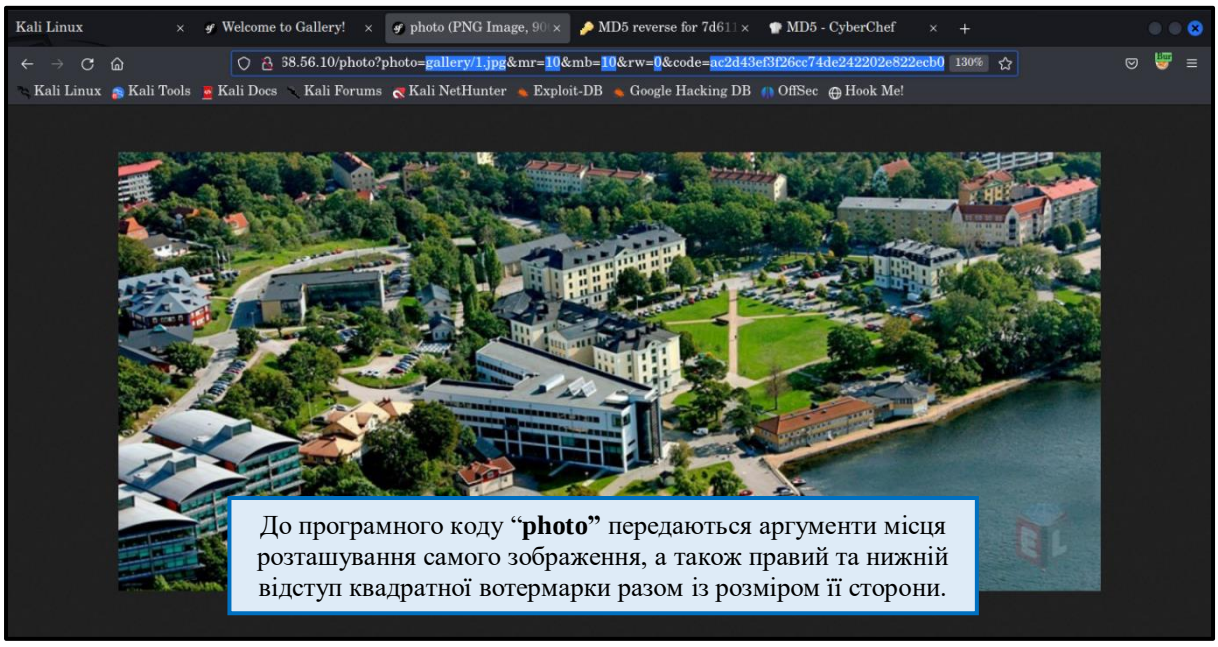
Answer:




Kali Linux
Welcome to Gallery!
photo (PNG Image, 90
7d6111a97e99e4713ec
https://www.google.com/search?client=firefox-b-e&q=7d6111a97e99e4713eec49951972e41d
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
Google
7d6111a97e99e4713eec49951972e41d
Увійти
Усі Зображення Відео Покупки Карти Більше Інструменти
Приблизна кількість результатів: 4 (0,22 с)
gromweb.com
https://md5.gromweb.com › ... · Перекласти цю сторінку
MD5 reverse for 15de21c670ae7c3f6f3f1f37029303c9
MD5 reverse for 15de21c670ae7c3f6f3f1f37029303c9. The MD5 hash:
15de21c670ae7c3f6f3f1f37029303c9 was succesfully reversed into the string:


Kali Linux
Welcome to Gallery!
photo (PNG Image, 90
MD5 reverse for 7d611
https://md5.gromweb.com/?md5=7d6111a97e99e4713eec49951972e41d
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
MD5 Center
MD5 conversion and reverse lookup
Online Activation
Online Activation
SIGN UP
MD5 reverse for 7d6111a97e99e4713eec49951972e41d
The MD5 hash:
7d6111a97e99e4713eec49951972e41d
was succesfully reversed into the string:
1010300
Feel free to provide some other MD5 hashes you would like to try to reverse.
Reverse a MD5 hash
7d6111a97e99e4713eec49951972e41d
Reverse
What is a MD5 hash?
MD5 (Message Digest algorithm, 5th version) is an algorithm which converts a given sequence of characters into another unique sequence of characters, with a fixed length, called "hash". For instance, the MD5 hash of the word password is 5f4dcc3b5aa765d61d8327deb882cf99.
These hashes are mostly used to validate file integrity, to encrypt sensitive data (like passwords), and to generate unique identifiers.
Is it secure?

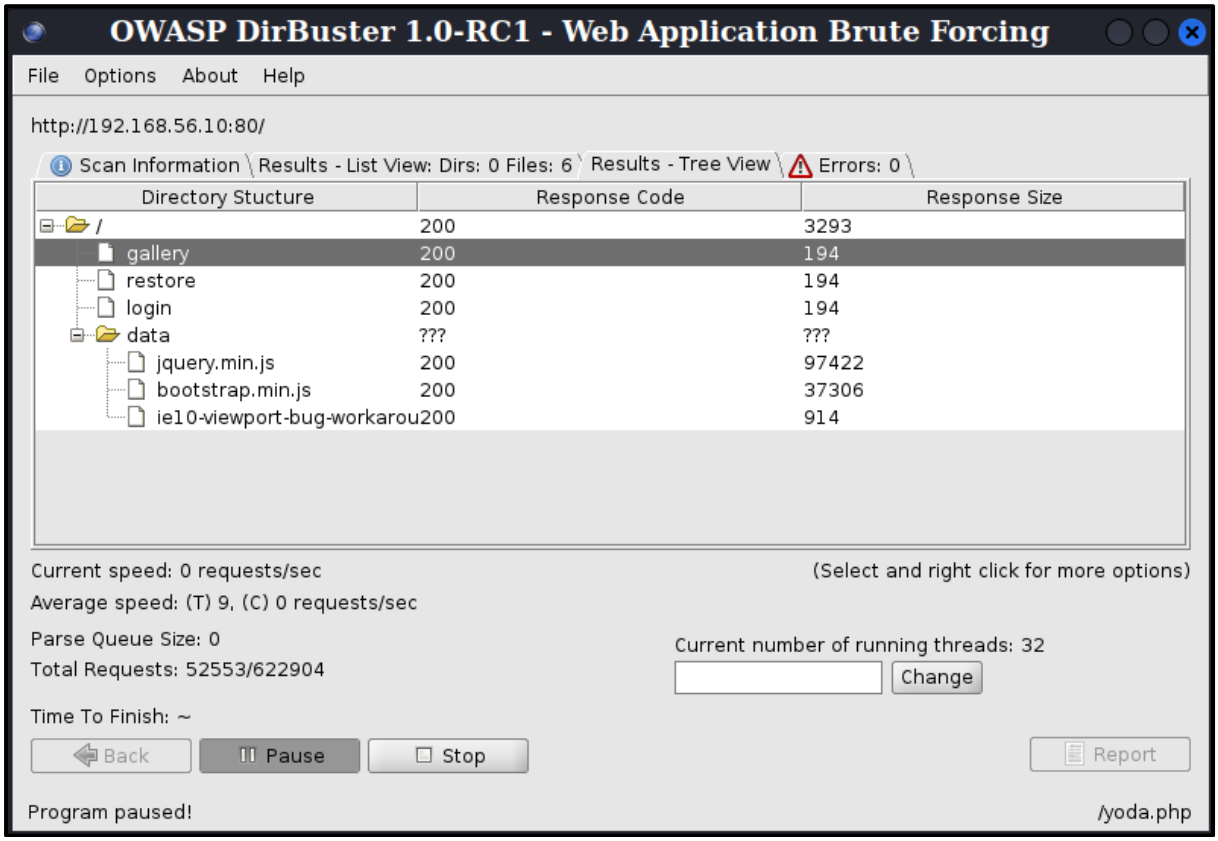

Kali Linux
Welcome to Gallery!
photo (PNG Image, 90
MD5 reverse for 7d611
MD5 - CyberChef
file:///usr/lib/cyberchef/index.html#recipe=MD5()&input=MTAxMDA
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
Last build: 2 months ago
Options
About / Support
Operations
MD5
MD5
MD4
SHA3
Favourites
Recipe
MD5
Input
10100
Raw Bytes
LF
Output
ac2d43ef3f26cc74de242202e822ecb0

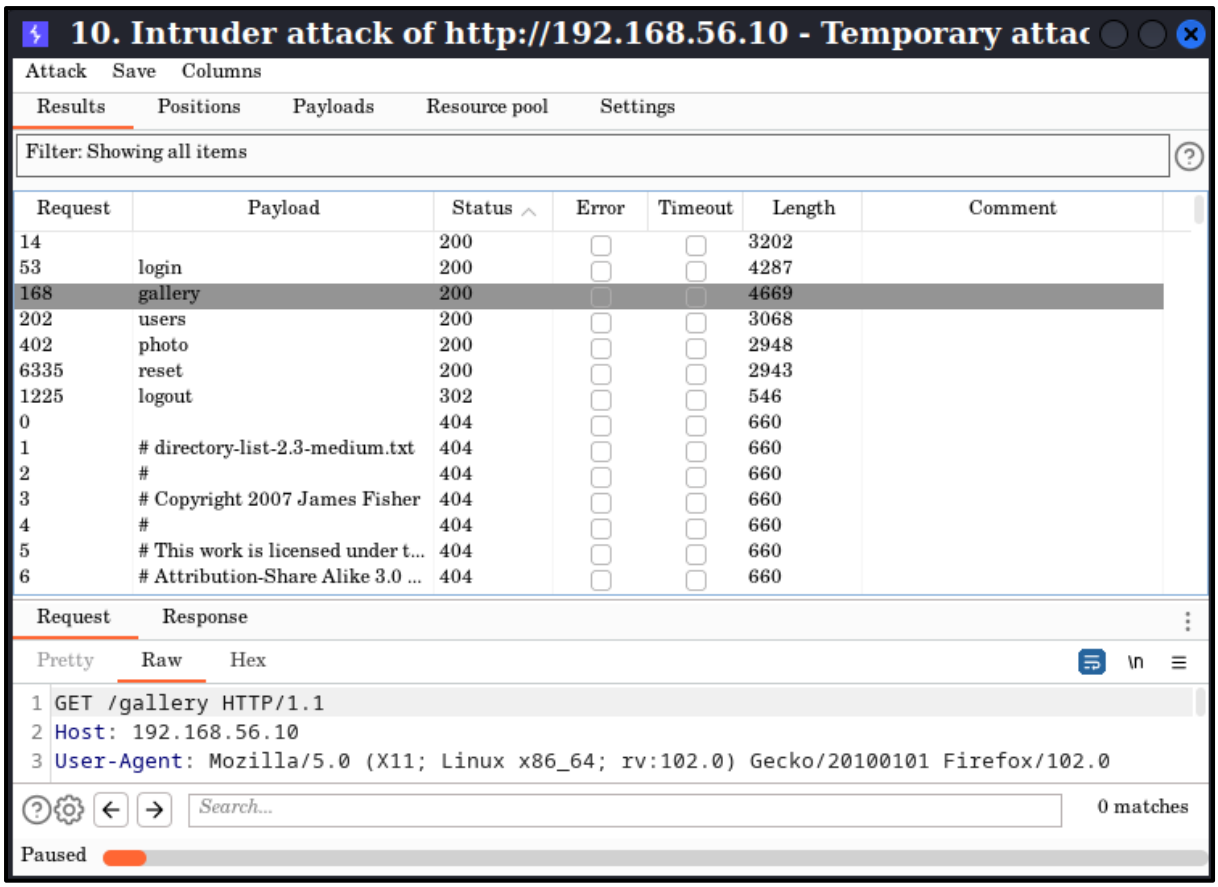

Kali Linux
Welcome to Gallery!
photo (PNG Image, 90
MD5 reverse for 7d611
MD5 - CyberChef
58.56.10/photo?photo=gallery/1.jpg&mr=10&mb=10&rw=0&code=ac2d43ef3f26cc74de242202e822ecb0
130%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
До програмного коду “photo” передаються аргументи місця розташування самого зображення, а також правий та нижній відступ квадратної вотермарки разом із розміром її сторони.

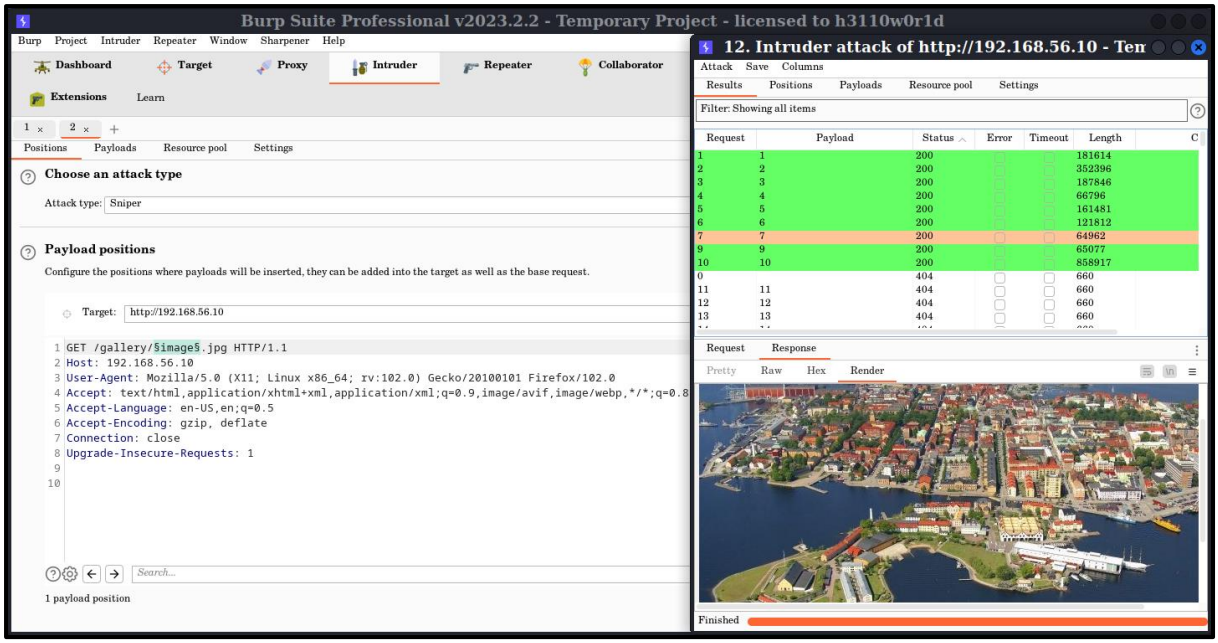
TASK 3

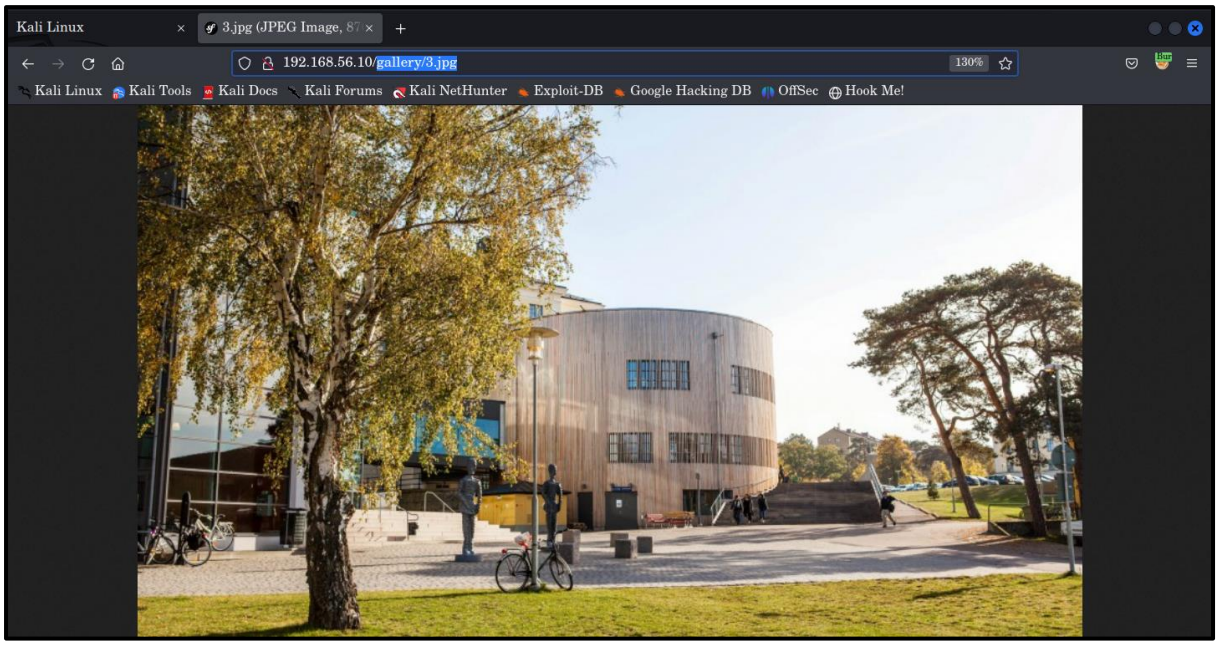
Are there direct access vulnerabilities? Prove it.

Answer:







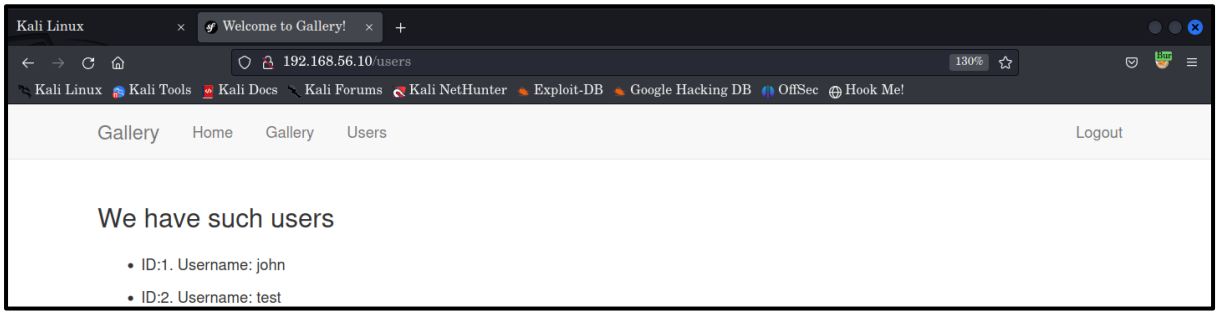


Task 2. Password reset vulnerably

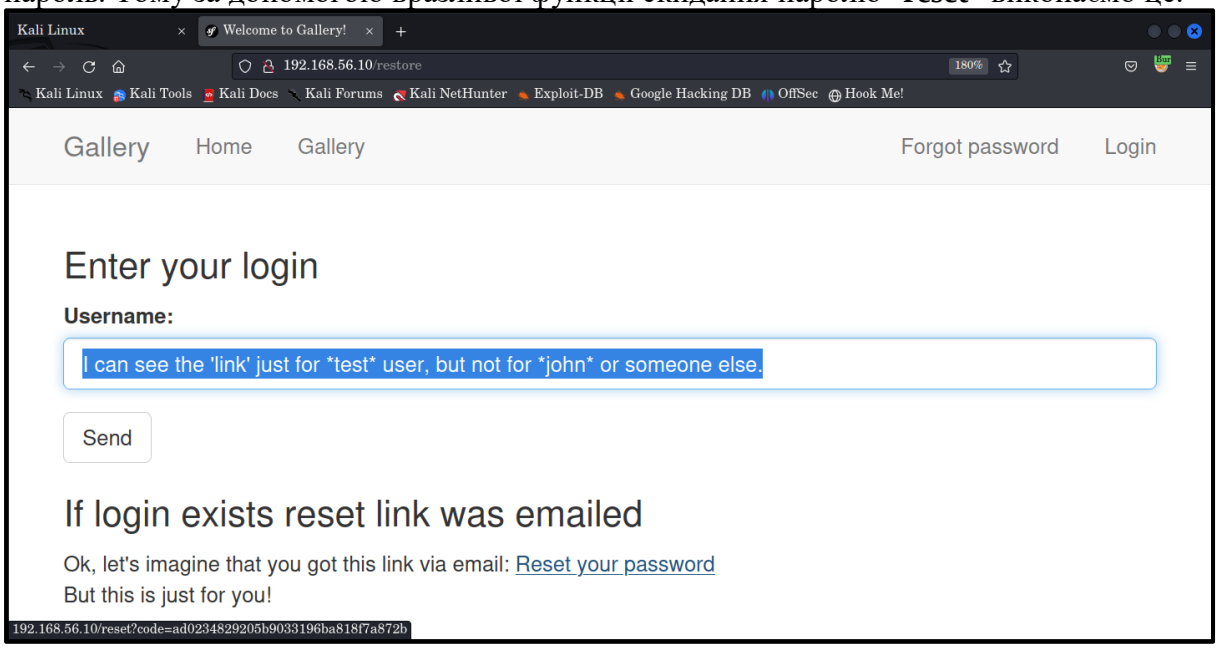
TASK 1

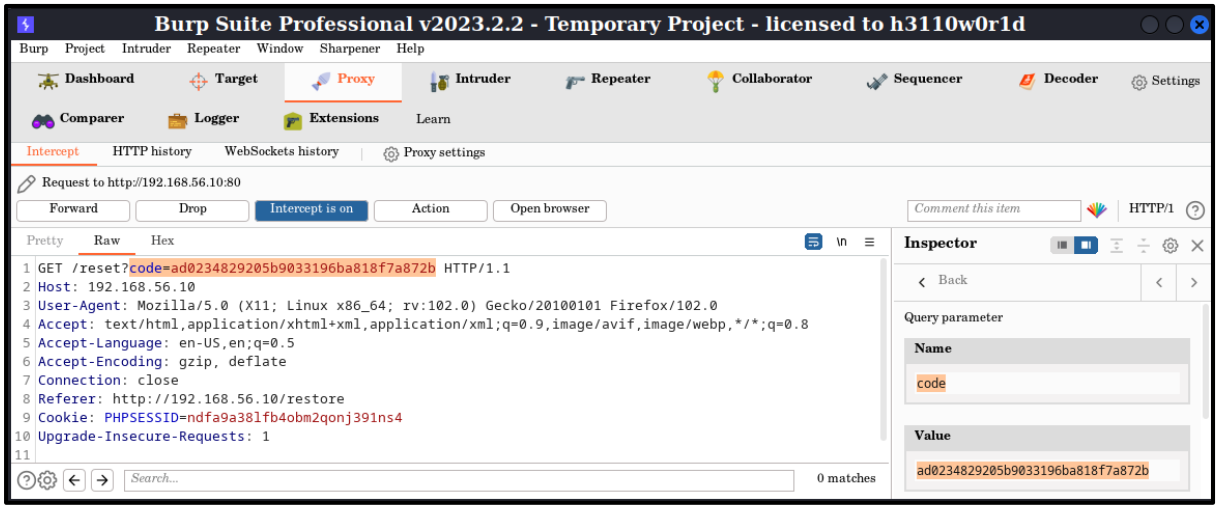
Is it possible to steal a user's account? Prove it.

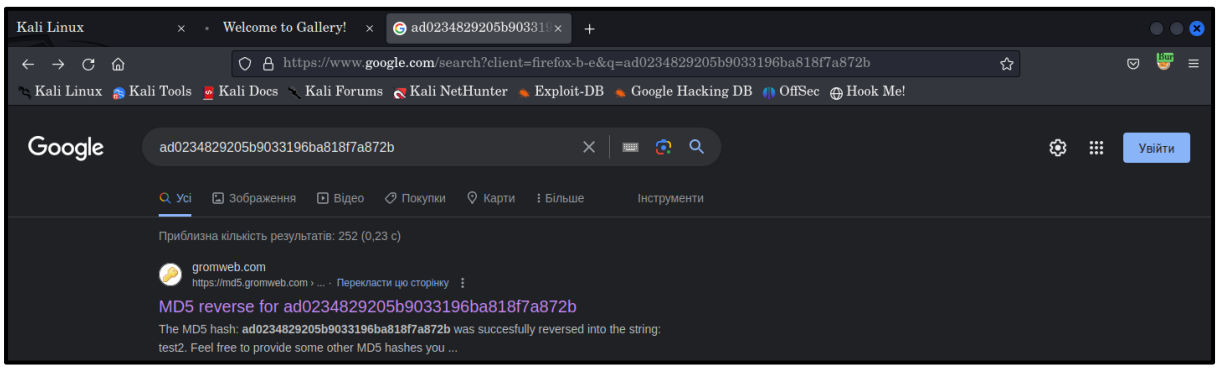
Answer:

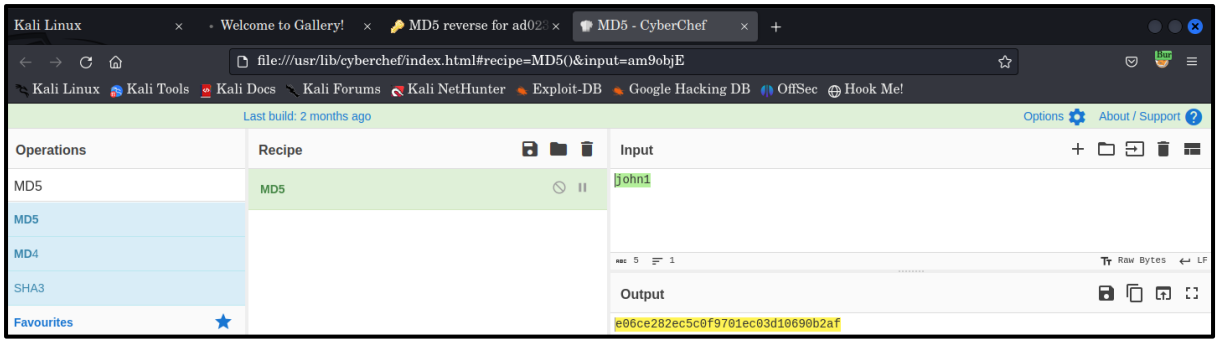


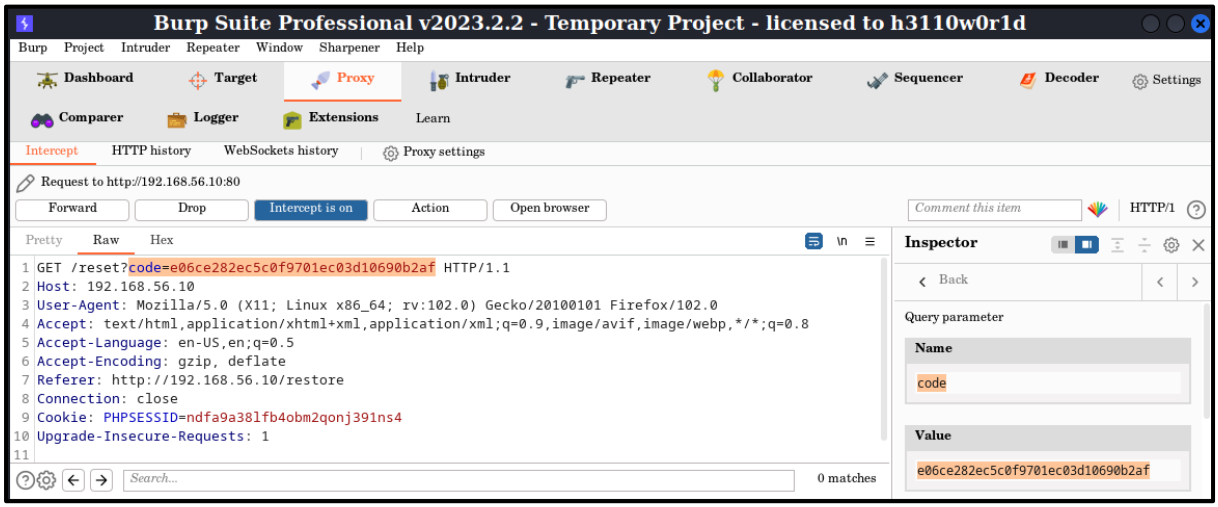
Як наведено вище на фото, на веб-сторінці “**users**” розташований список усіх, хоча можливо лише деяких, користувачів. Тобто можна спробувати отримати доступ до профілю користувача **john**, для якого, на відміну від користувача **test**, ми не знаємо пароль. Тому за допомогою вразливої функції скидання паролю “**reset**” виконаємо це.

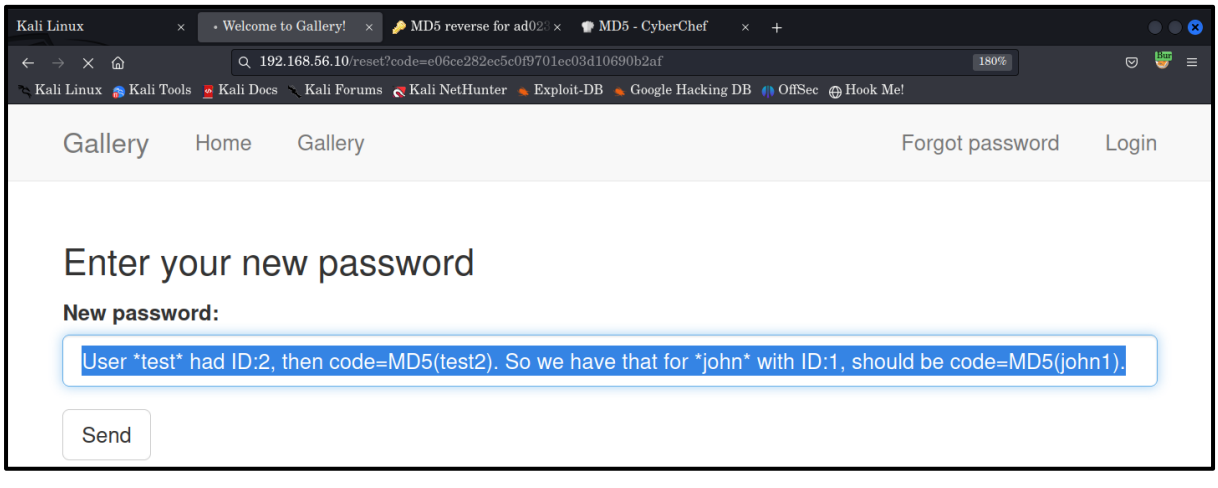


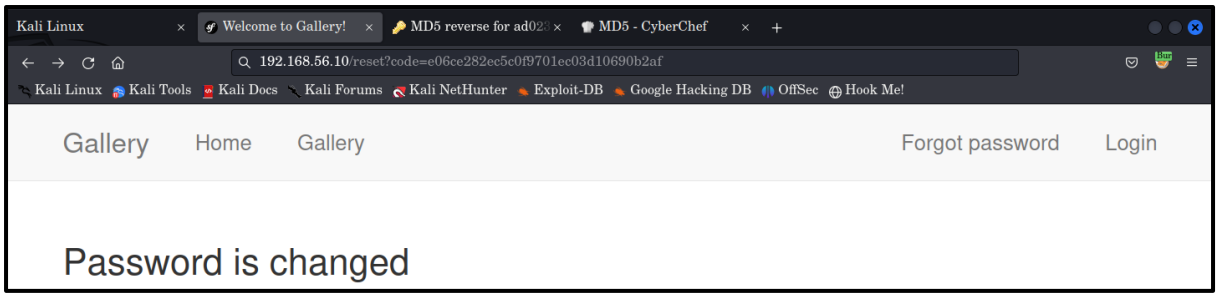




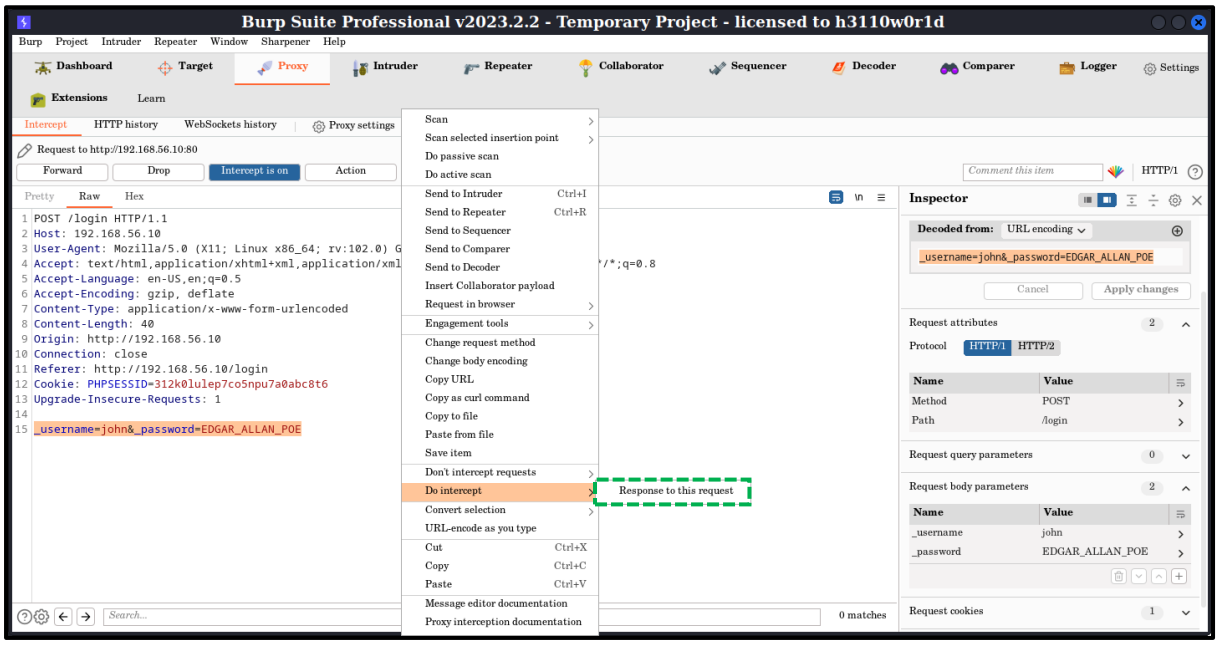

Kali Linux
Welcome to Gallery!
MD5 reverse for ad023
MD5 - CyberChef
file:///usr/lib/cyberchef/index.html#recipe=MD5()&input=am9objE
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
Last build: 2 months ago
Options
About / Support
Operations
MD5
MD5
MD4
SHA3
Favourites
Recipe
MD5
Input
john1
Output
e06ce282ec5c0f9701ec03d10690b2af

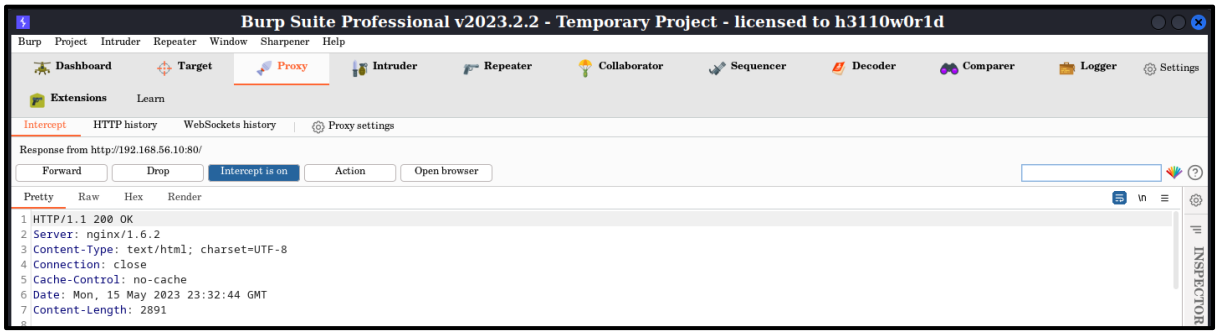

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Sharpener Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.56.10:80
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
1 GET /reset?code=e06ce282ec5c0f9701ec03d10690b2af HTTP/1.1
2 Host: 192.168.56.10
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 Referer: http://192.168.56.10/restore
8 Connection: close
9 Cookie: PHPSESSID=ndfa9a38lfb4obm2qonj391ns4
10 Upgrade-Insecure-Requests: 1
11
Search...
0 matches
Inspector
Back
Query parameter
Name
code
Value
e06ce282ec5c0f9701ec03d10690b2af

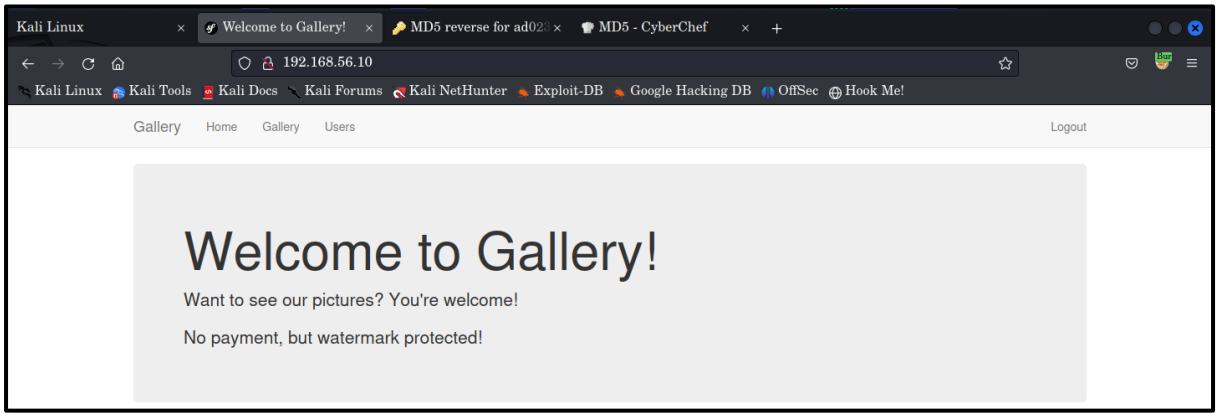

Kali Linux
Welcome to Gallery!
MD5 reverse for ad023
MD5 - CyberChef
192.168.56.10/reset?code=e06ce282ec5c0f9701ec03d10690b2af
180%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
Gallery
Home
Gallery
Forgot password
Login
Enter your new password
New password:
User *test* had ID:2, then code=MD5(test2). So we have that for *john* with ID:1, should be code=MD5(john1).
Send


Kali Linux
Welcome to Gallery!
MD5 reverse for ad023
MD5 - CyberChef
192.168.56.10/reset?code=e06ce282ec5c0f9701ec03d10690b2af
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!
Gallery
Home
Gallery
Forgot password
Login
Password is changed


Please sign in
john
Sign in







TASK 2

How to mitigate this vulnerability?

Answer:

Необхідно переконатися, що відповідний процес скидання пароля відповідає безпечним практикам, таким як: обмеження спроб скидання пароля, реалізація багатофакторної автентифікації (**MFA**), використання складніших методів генерації **reset**-токенів та застосування надійніших функцій їх хешування. Хоча взагалі, не варто передавати у **GET**-запиті будь-який хеш, який стосується інформації про користувача. Якось так ツ