МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Захист програмного забезпечення

Лабораторна робота 6

Аналіз вразливостей Web-застосунків

Мета роботи: дізнатись, як можна атакувати програму, використовуючи поширені вразливості веб-додатків, на зразок вразливостей міжсайтового скриптингу (XSS), підробки міжсайтових запитів (XSRF), відмови в обслуговуванні, розкритті інформації або віддаленому виконанні коду.

Перевірив:

_____

Виконав:

студент III курсу

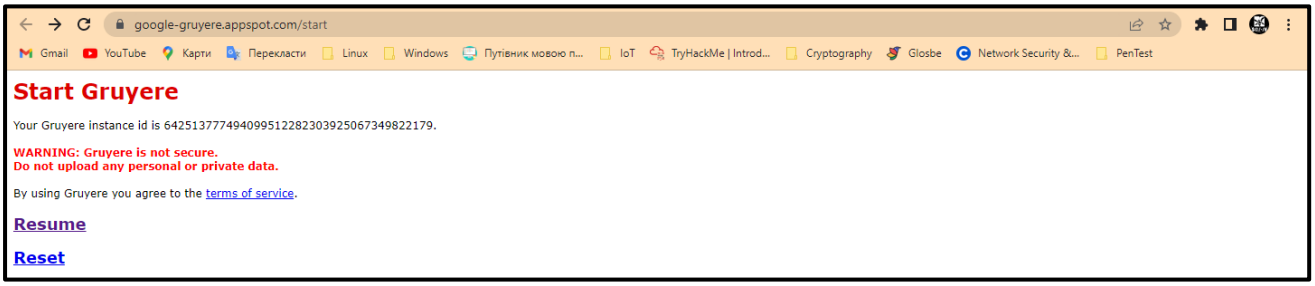
групи ФБ-01

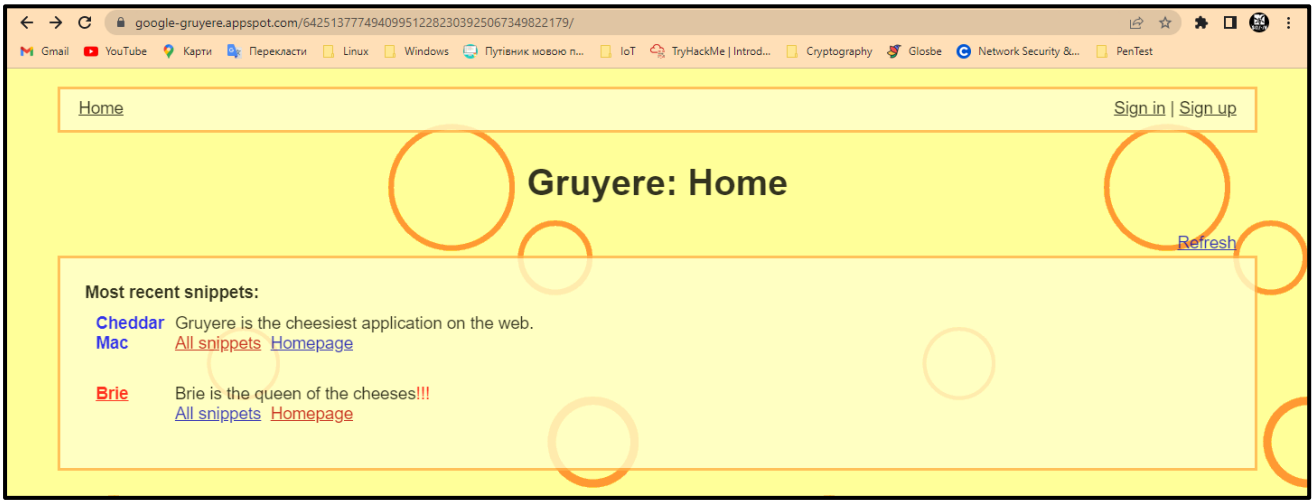
Сахній Н.Р.

Київ 2023

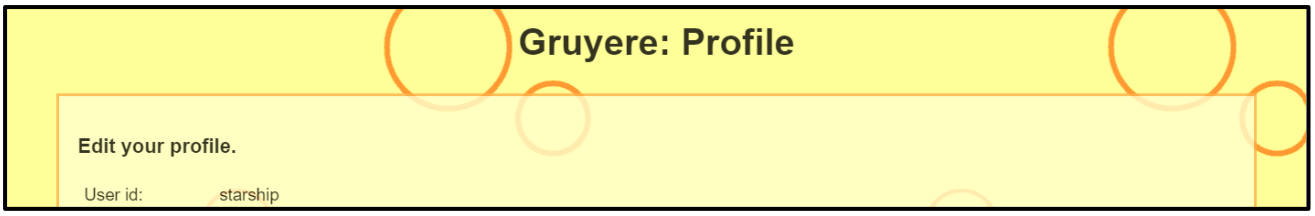
Хід виконання роботи

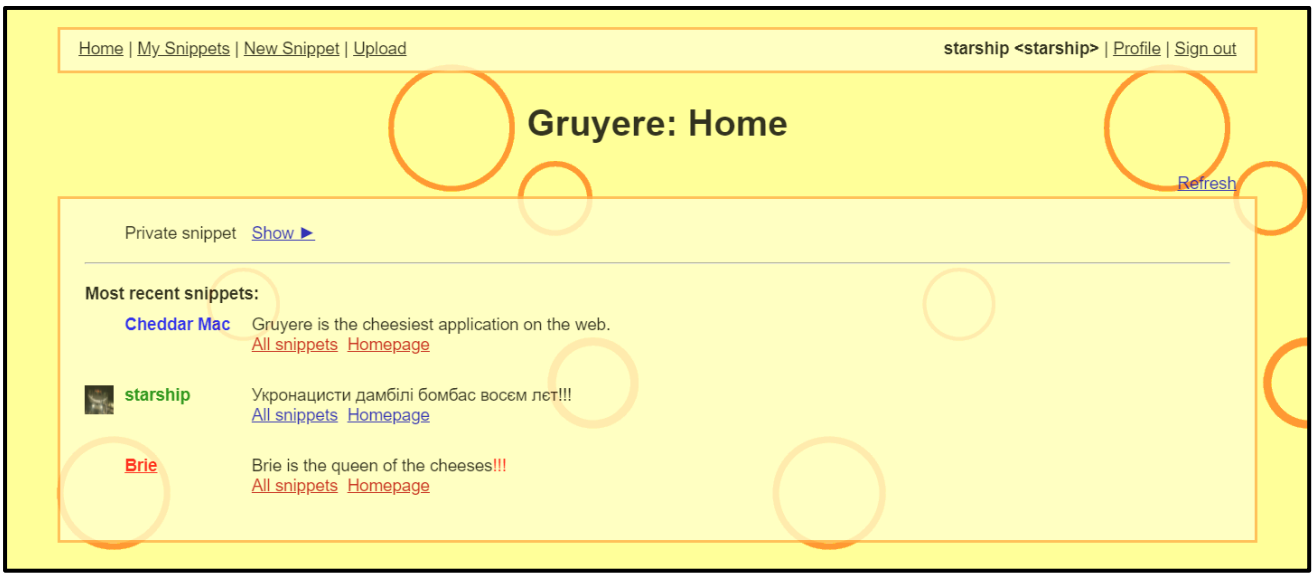
1. Початкові налаштування ==========





2. Підготовчі операції з Gruyere ==========

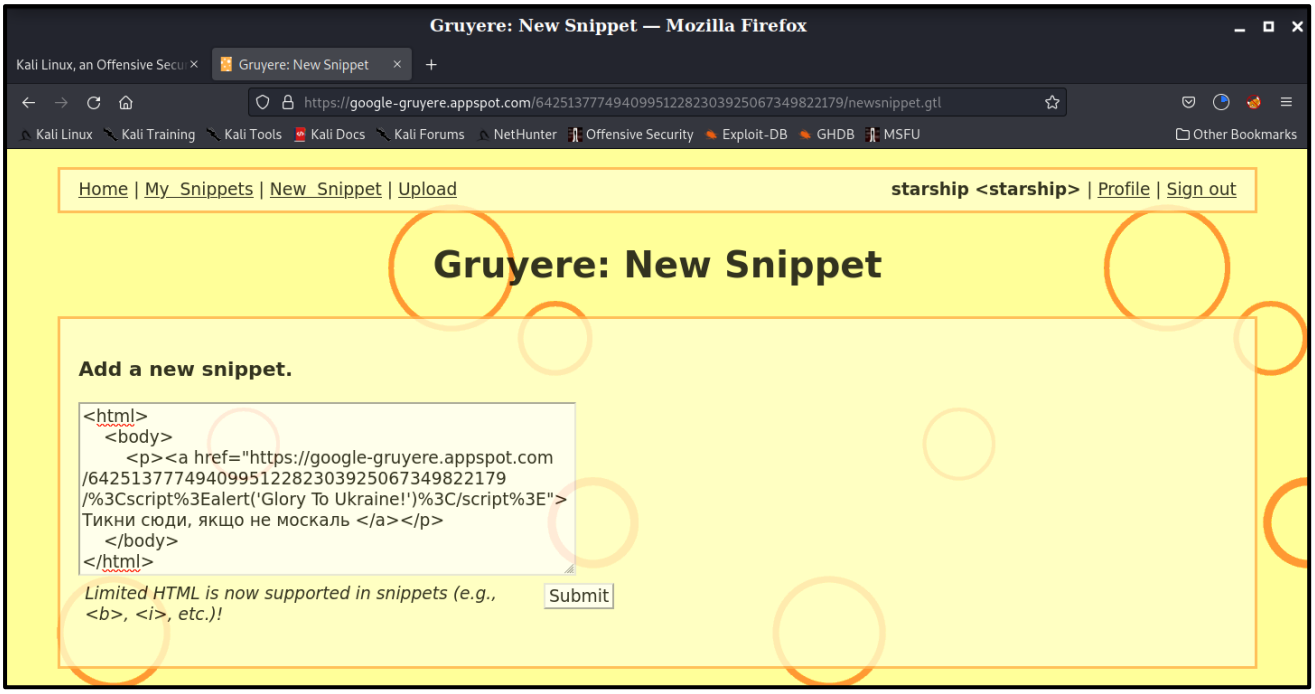


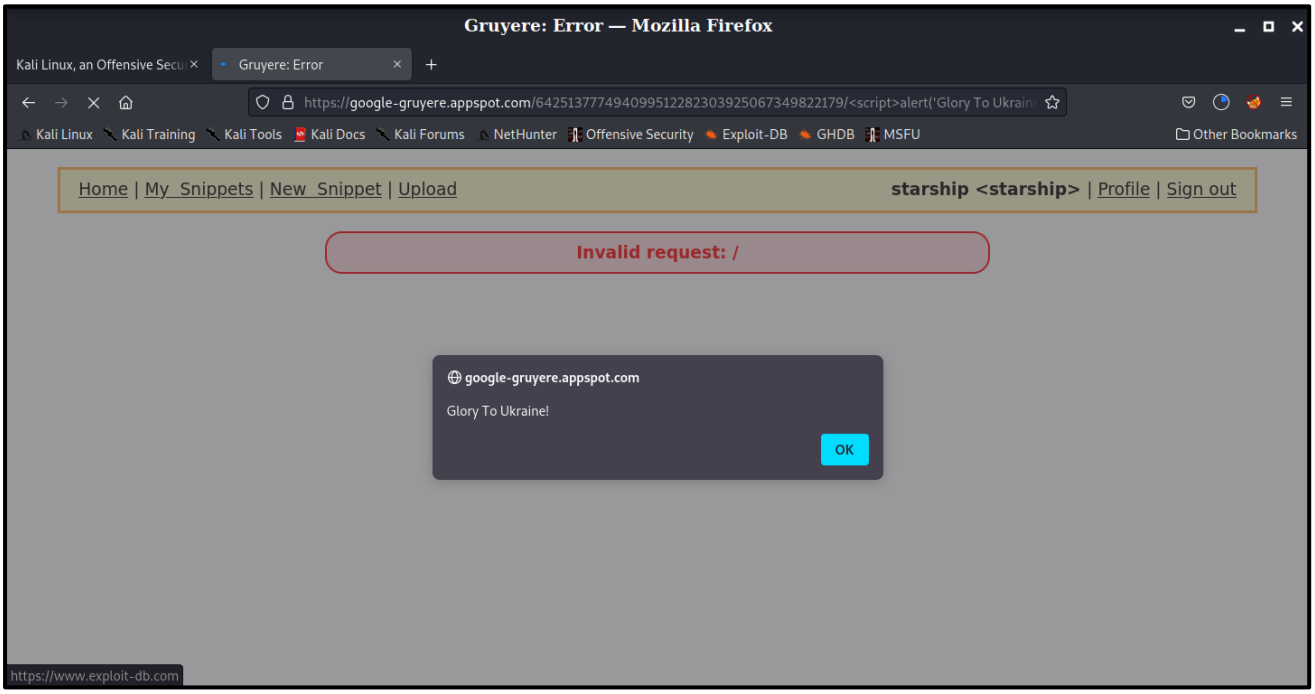


3. Аналіз вразливості до міжсайтового скриптингу (XSS) ========

3.1. Пошук вразливості до віддзеркаленого XSS

Завдання. Впровадити скрипт в сніпет, кодуючи заборонені символи.

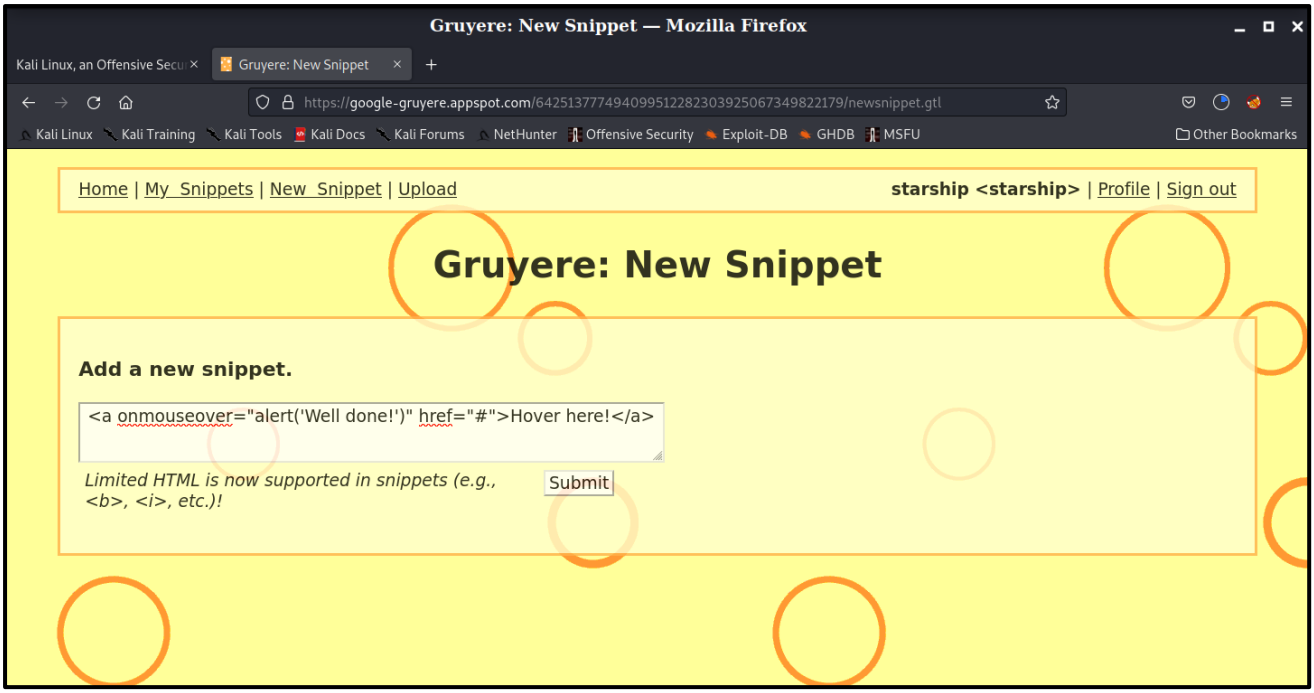


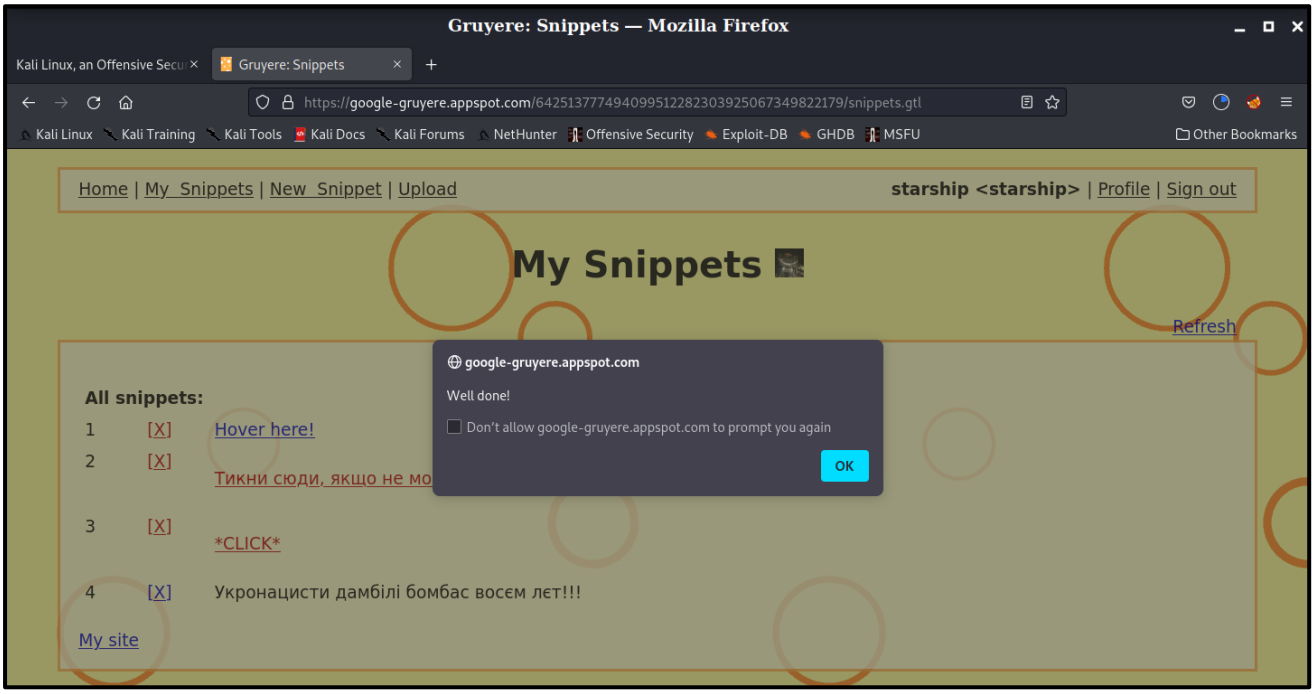


3.2. Пошук вразливості до збереженого XSS

- **Збережений XSS через сніпет**

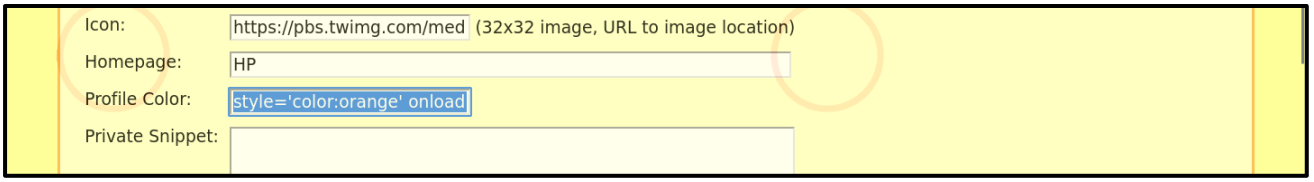
Завдання. Впровадити скрипт в сніпет, обходячи встановлені фільтри.

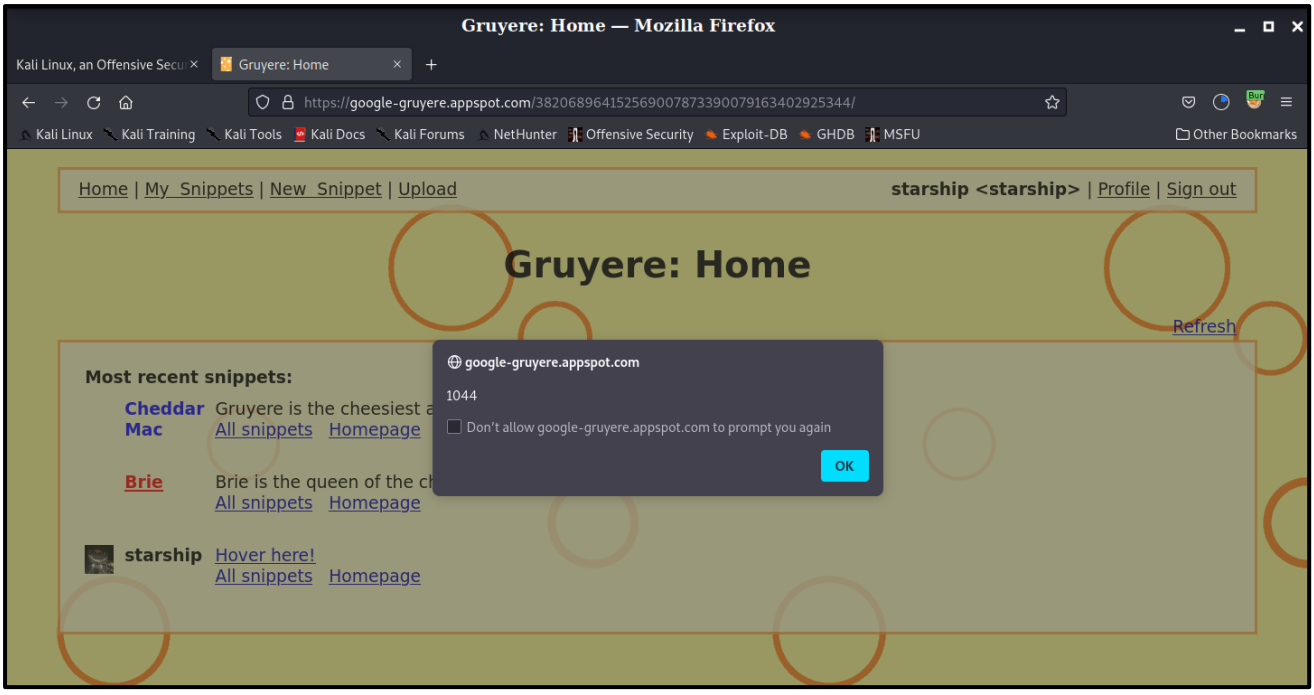




- **Збережений XSS через атрибут HTML**

Завдання. Впровадити скрипт, що активується при установці значення кольору в профілі.

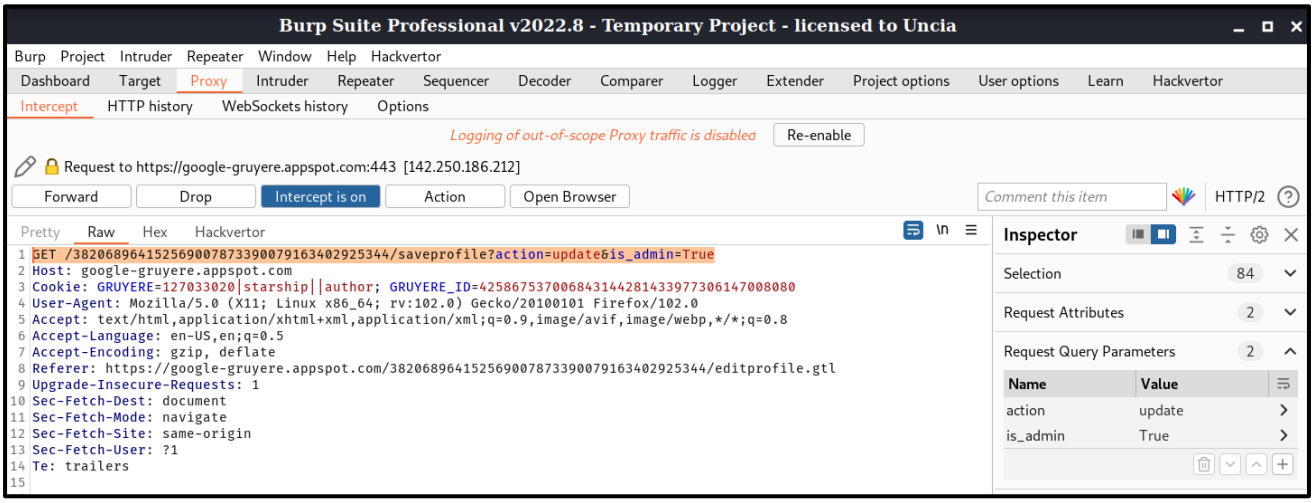




4. Аналіз вразливості до маніпуляцій зі сторони клієнта =========

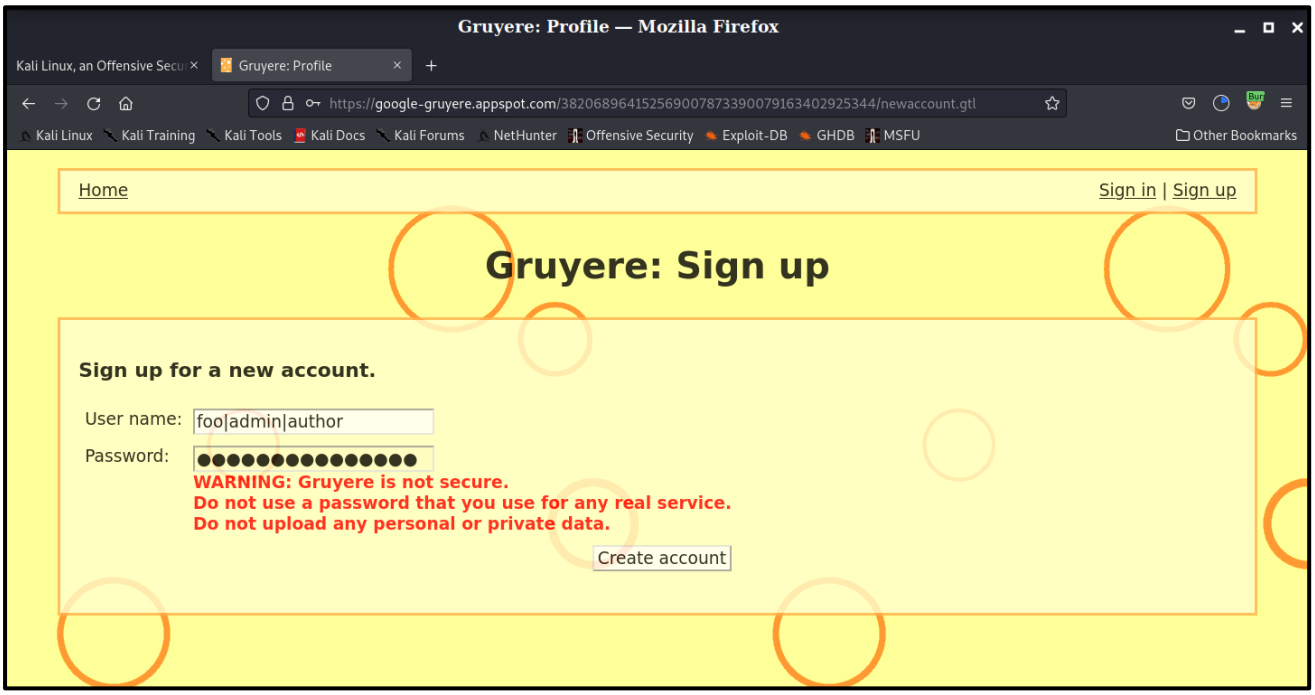
4.1. Вразливість до підвищення привілеїв

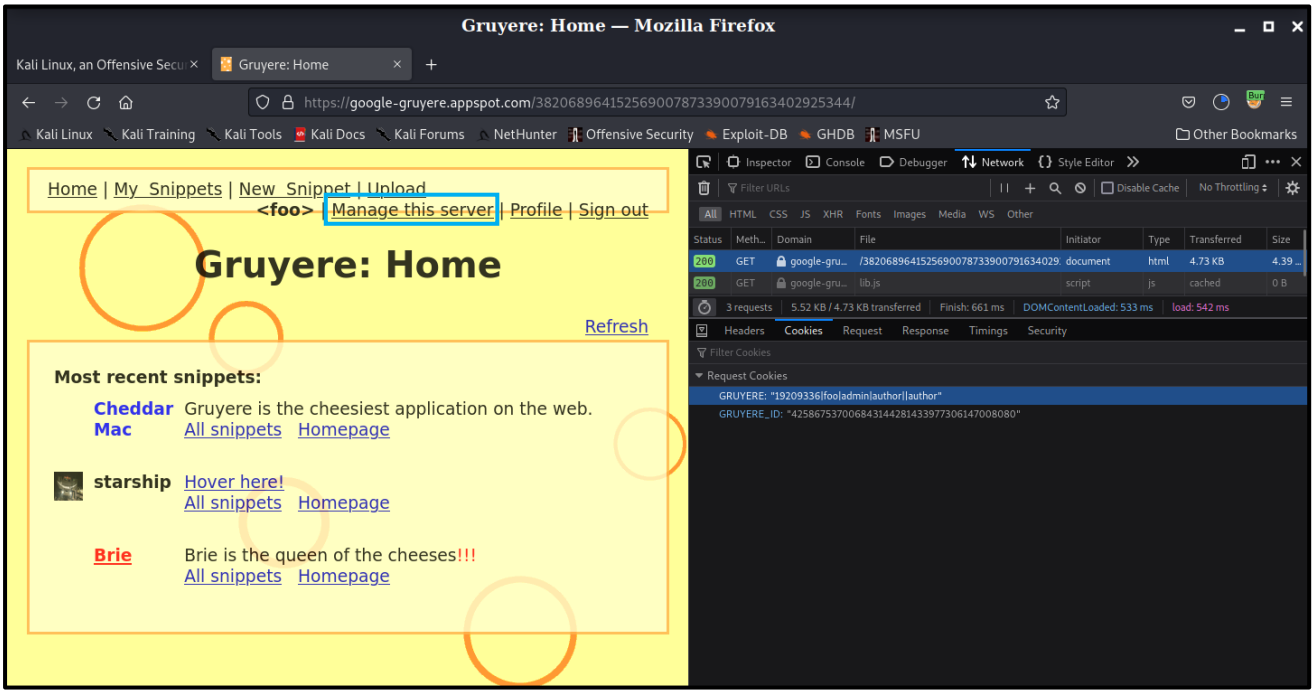
Завдання. Перетворити свій обліковий запис в обліковий запис адміністратора.



4.2. Вразливість до маніпуляції з cookie

Завдання. Отримати cookie для іншого користувача.

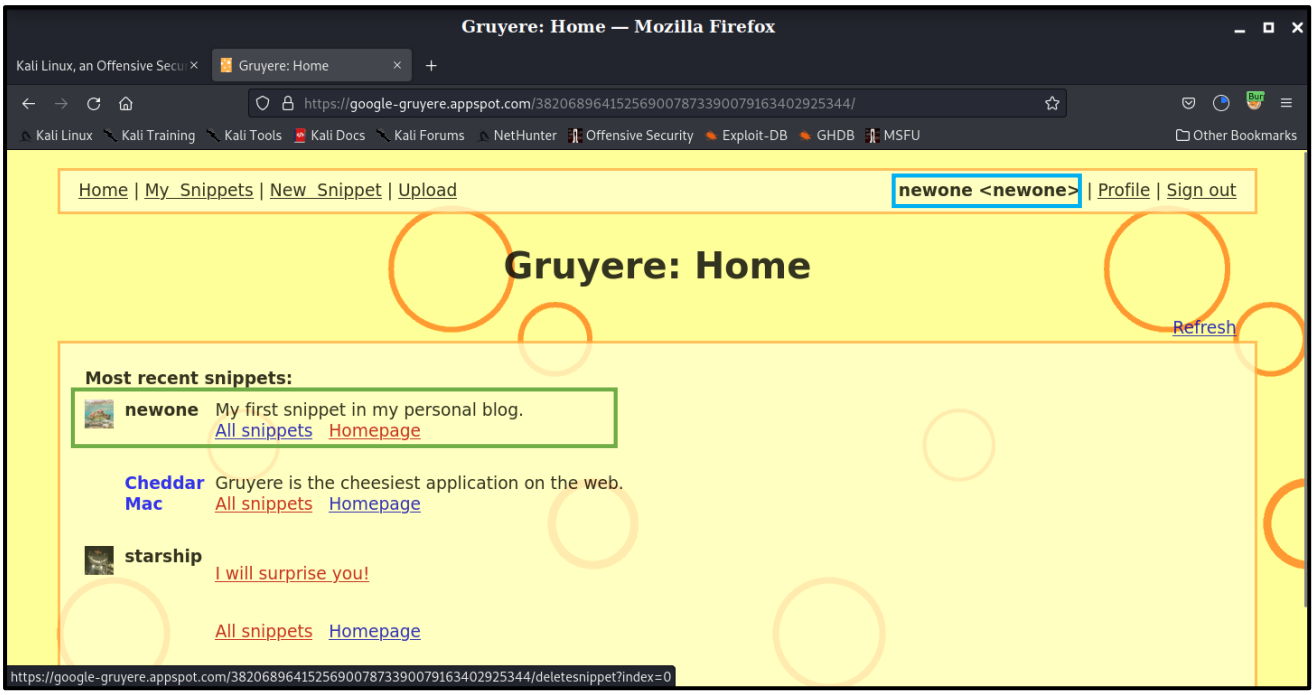




5. Аналіз вразливості до підробки міжсайтових запитів (XSRF) ===

Завдання. Знайти спосіб виконати дію по зміні облікового запису зареєстрованого користувача Gruyere без його відома.


Home | My Snippets | New Snippet | Upload
starship <starship> | Manage this server | Profile | Sign out
Gruyere: New Snippet
Add a new snippet.
<html>
<body>
<a href="https://google-gruyere.appspot.com
/382068964152569007873390079163402925344
/deletesnippet?index=0>I will surprise you!
</body>
</html>
Limited HTML is now supported in snippets (e.g., <b>, <i>, etc.)!
Submit

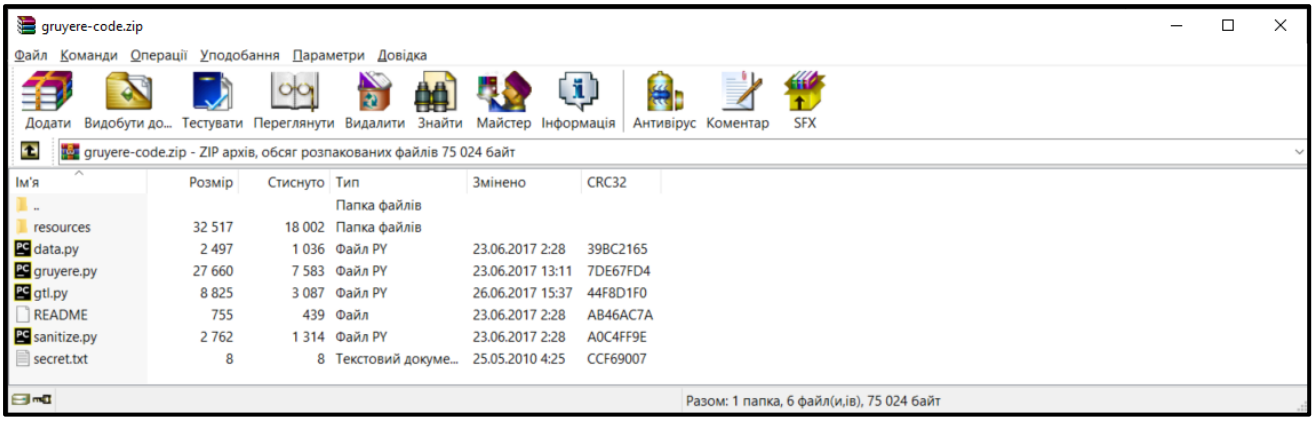

Gruyere: Home — Mozilla Firefox
Kali Linux, an Offensive Secu
Gruyere: Home
https://google-gruyere.appspot.com/382068964152569007873390079163402925344/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Other Bookmarks
Home | My Snippets | New Snippet | Upload
newone <newone> | Profile | Sign out
Gruyere: Home
Refresh
Most recent snippets:
newone My first snippet in my personal blog.
All snippets Homepage
Cheddar Mac Gruyere is the cheesiest application on the web.
All snippets Homepage
starship
I will surprise you!
All snippets Homepage
https://google-gruyere.appspot.com/382068964152569007873390079163402925344/deletesnippet?index=0


Gruyere: Snippets — Mozilla Firefox
Kali Linux, an Offensive Secu
Gruyere: Snippets
https://google-gruyere.appspot.com/382068964152569007873390079163402925344/snippets.gtl
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Other Bookmarks
Home | My Snippets | New Snippet | Upload
newone <newone> | Profile | Sign out
My Snippets
Refresh
No snippets.
My site

6. Аналіз вразливості обхідного шляху==========

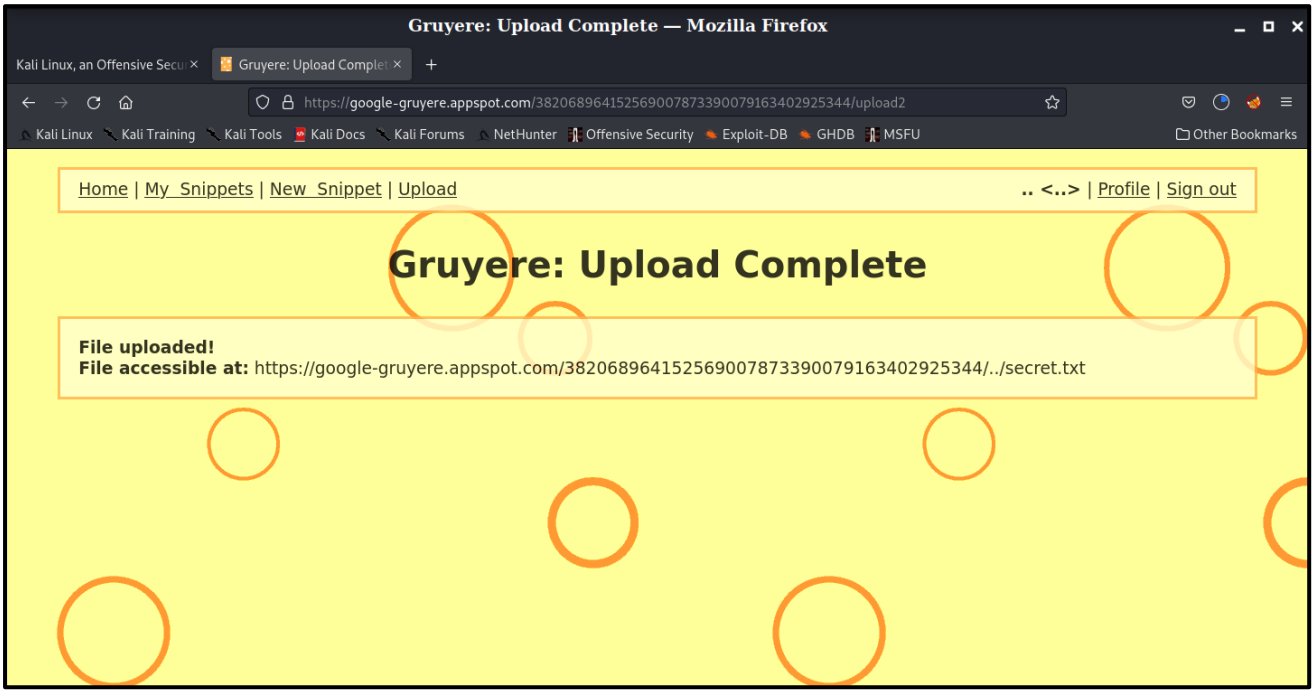
6.1. Вразливість до розкриття інформації через обхідний шлях

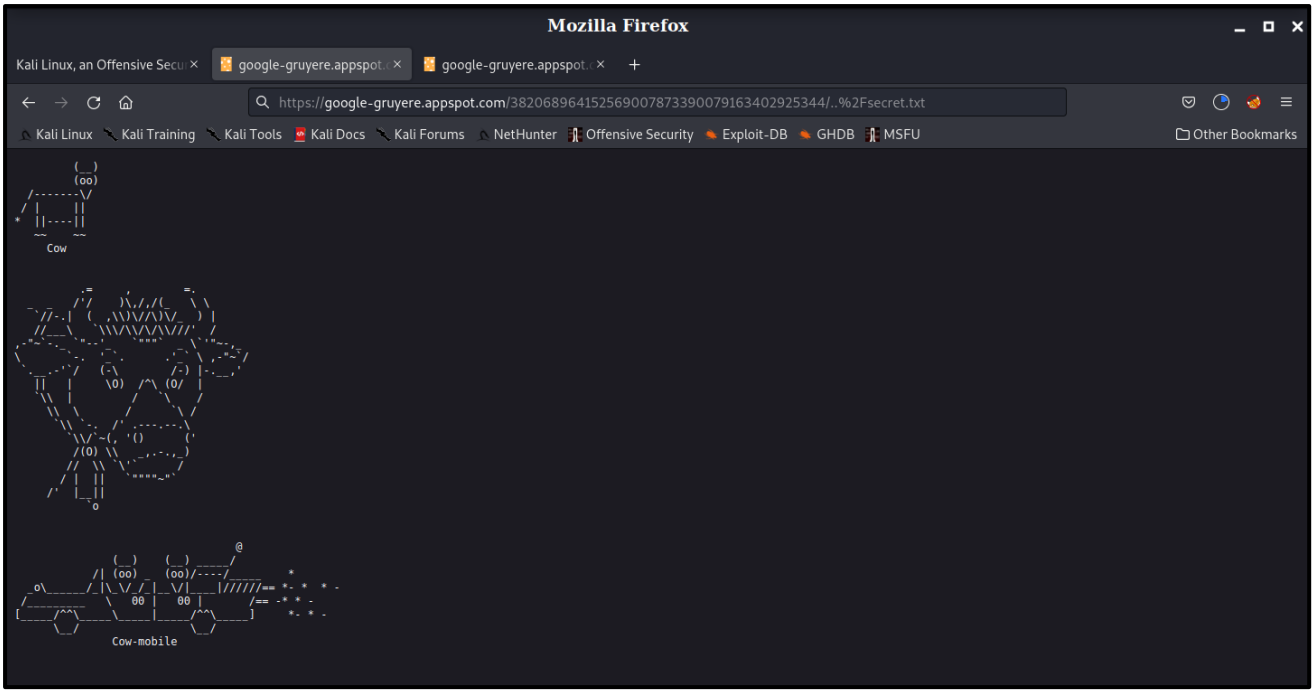
Завдання. Знайти спосіб прочитати **secret.txt** з сервера Gruyere.



6.2. Вразливість до модифікації інформації через обхідний шлях

Завдання. Знайдіть спосіб замінити файл **secret.txt** на працюючому сервері Gruyere.

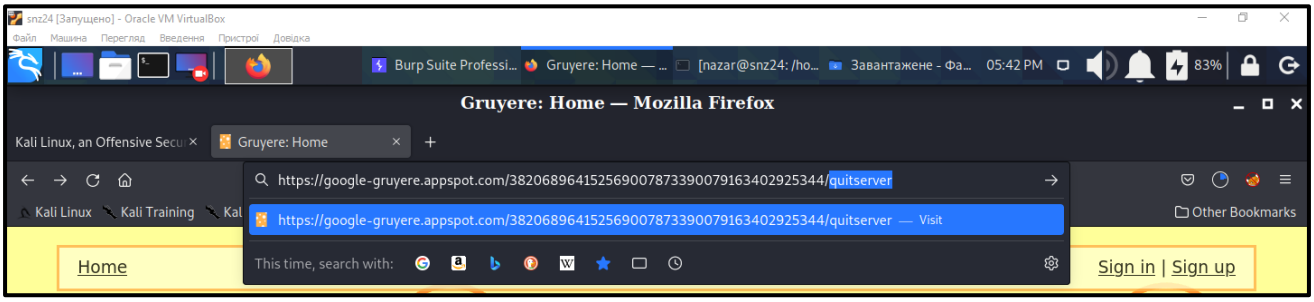


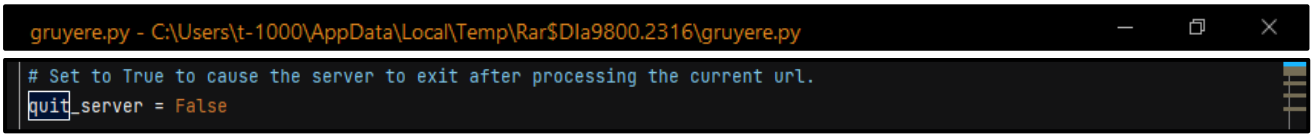


7. Аналіз вразливостей до DoS – атак ==========

7.1. Вразливість до DoS – завершення роботи сервера

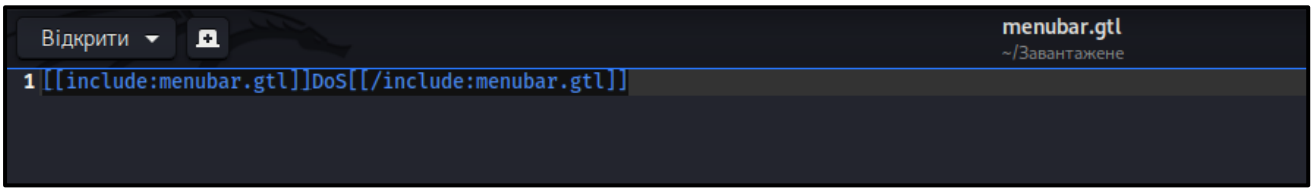
Завдання. Знайти спосіб завершити роботу сервера.

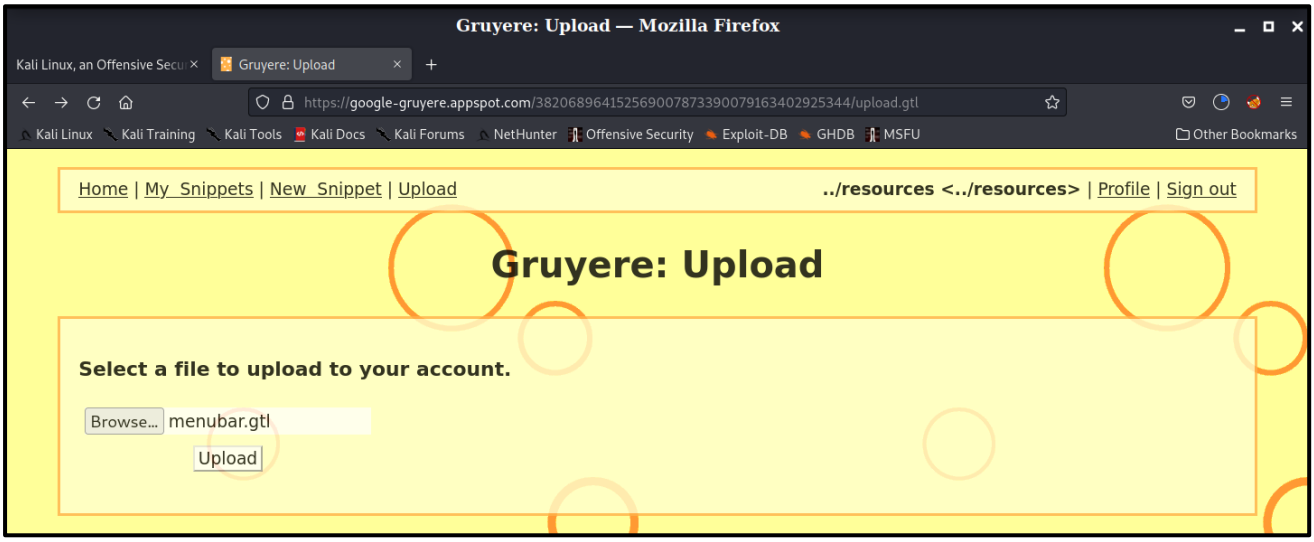




7.2. Вразливість до DoS - перевантаження сервера

Завдання. Знайти спосіб перевантажити сервер.





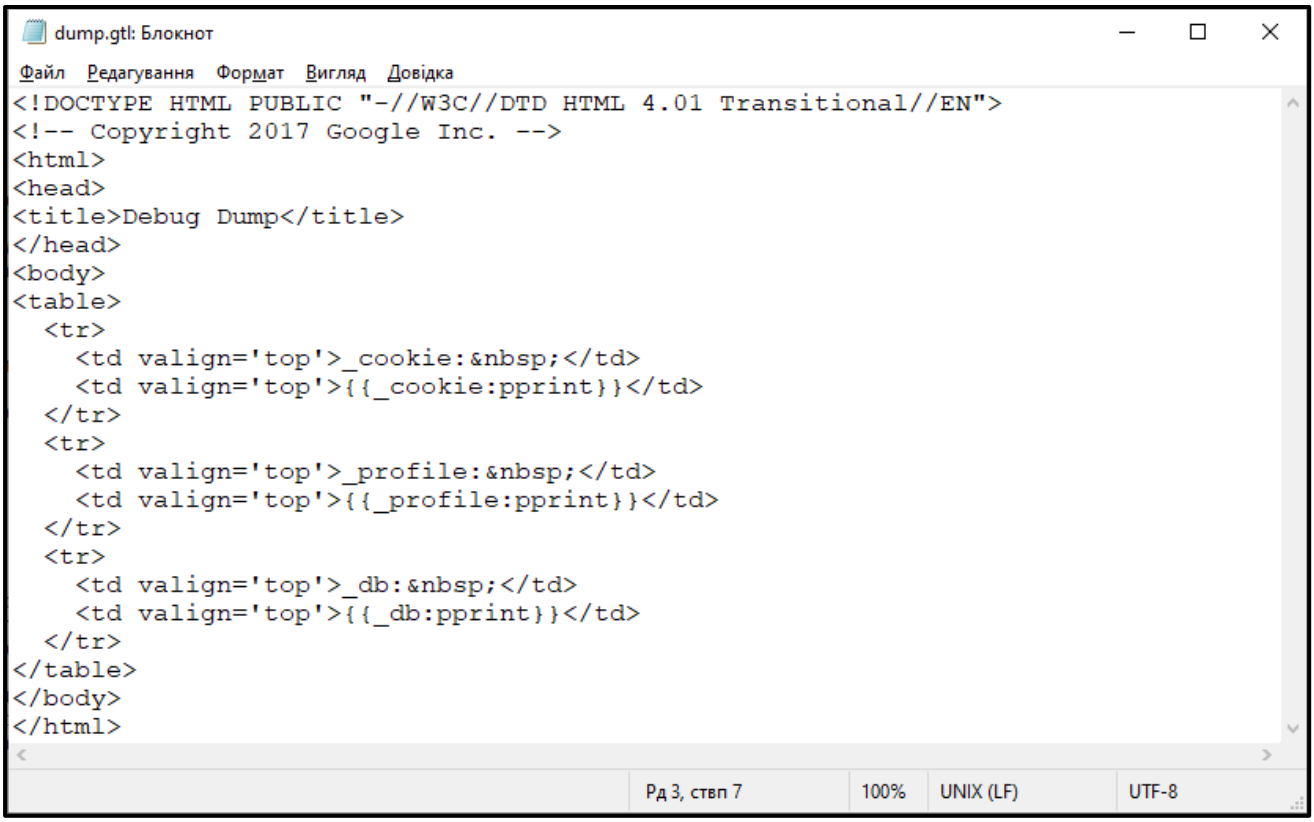
8. Аналіз вразливості до віддаленого виконання коду (RCE)=======

Завдання. Впровадити в програму файл, що дозволяє виконати код експлойта.

9. Аналіз можливості розкриття інформації через вразливості конфігурації ==========

9.1. Розкриття інформації № 1

Завдання. Зчитати вміст бази даних з працюючого сервера, скориставшись вразливістю конфігурації.



9.2. Розкриття інформації № 2

Завдання. Впровадити в конфігурацію додатка файл, що дозволяє читати інформацію.