Assignment 5.1.1

Course name: XSS

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. XSS detection, analysis and exploitation

Purpose: understand what is XSS, how to detect it, how to exploit it

After the work the student must

- know: what is XSS;
- be able to: exploit XSS vulnerabilities and defend from it.

Tasks:

- analyze provided web application on virtual machine 192.168.56.7 and check its' parameters.

Material of the workplace

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS)
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- BeeF

Solution:

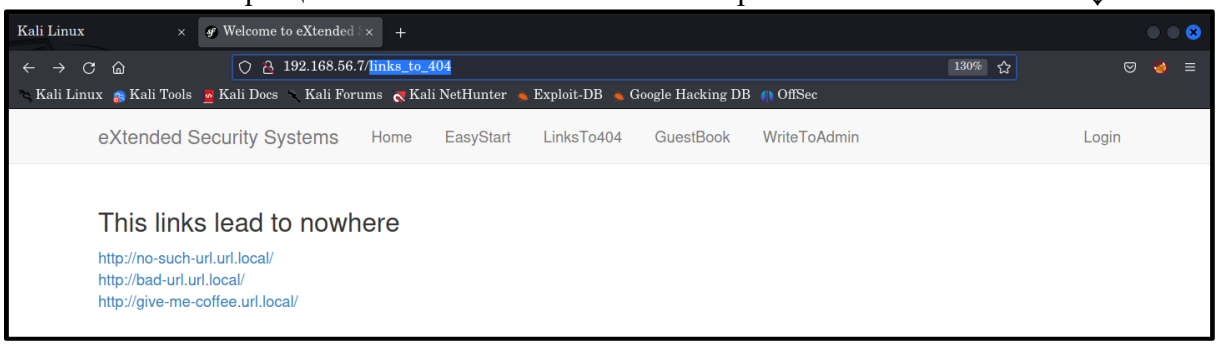
Open site in browser. Analyze HTTP-parameters for GET/POST requests. Use tools and brain for detection and exploiting XSS.

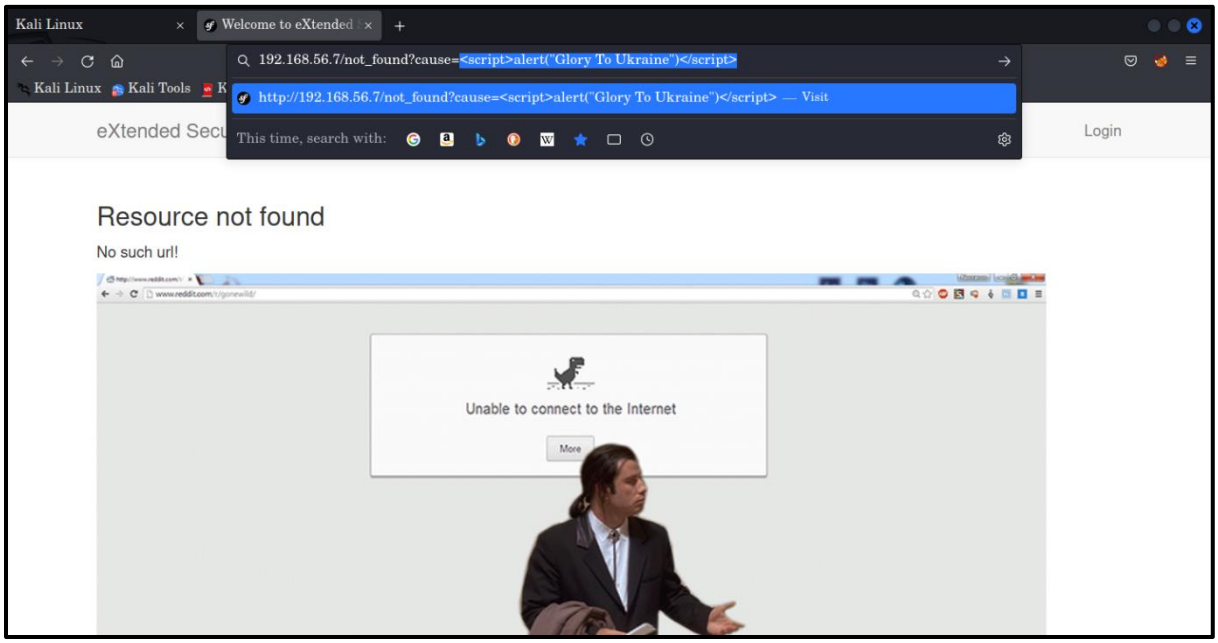
TASK 1

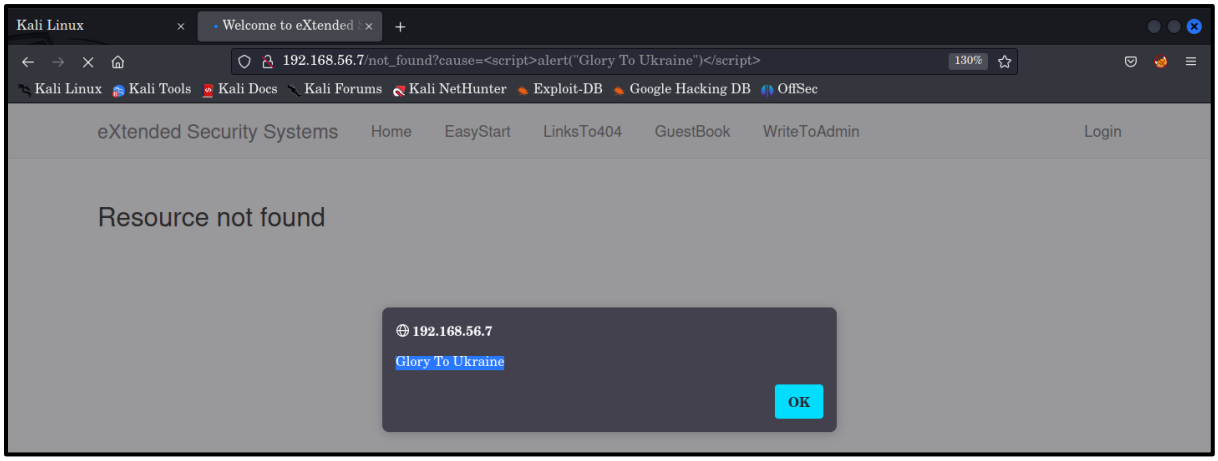
For provided sites, you need to answer: are there XSS-vulnerabilities? How did you find it? Prove it (screenshot).

Answer:

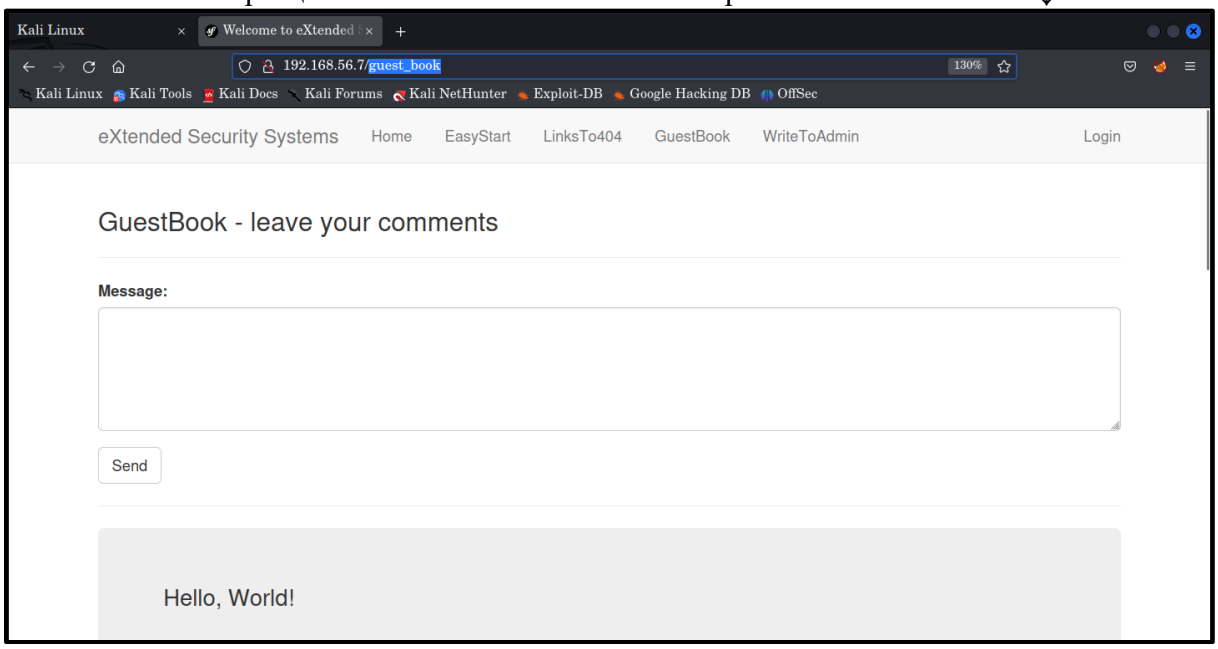
– На веб-сторінці “**LinksTo404**” ми можемо скористатися **Reflected XXS** ↓

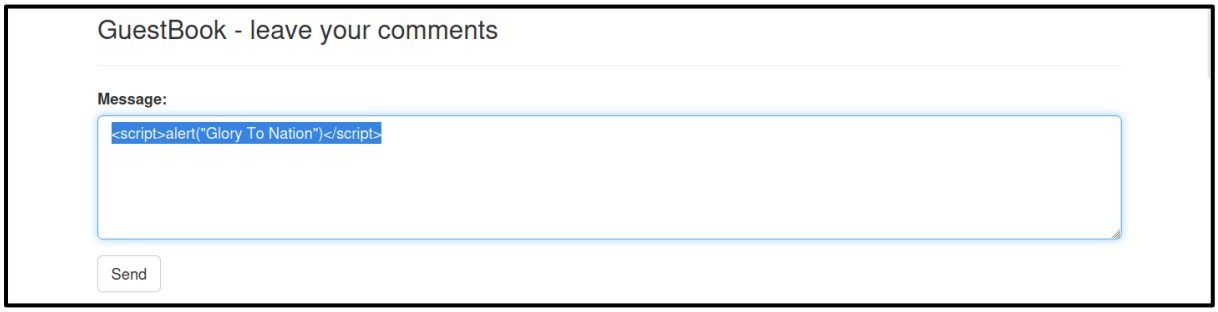


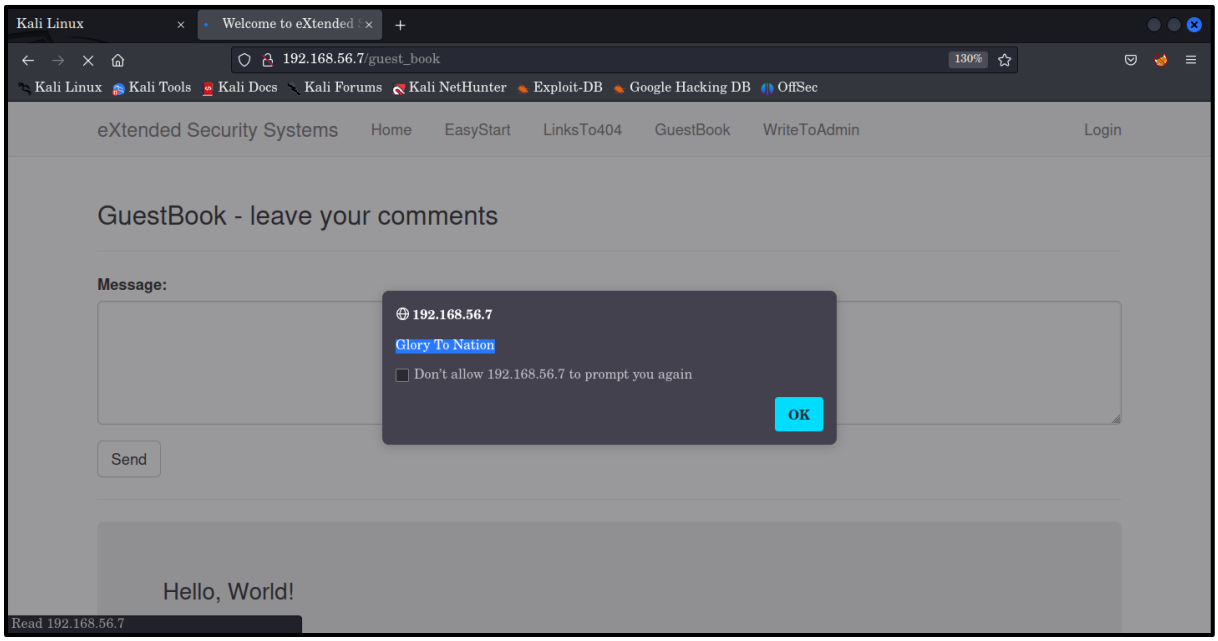


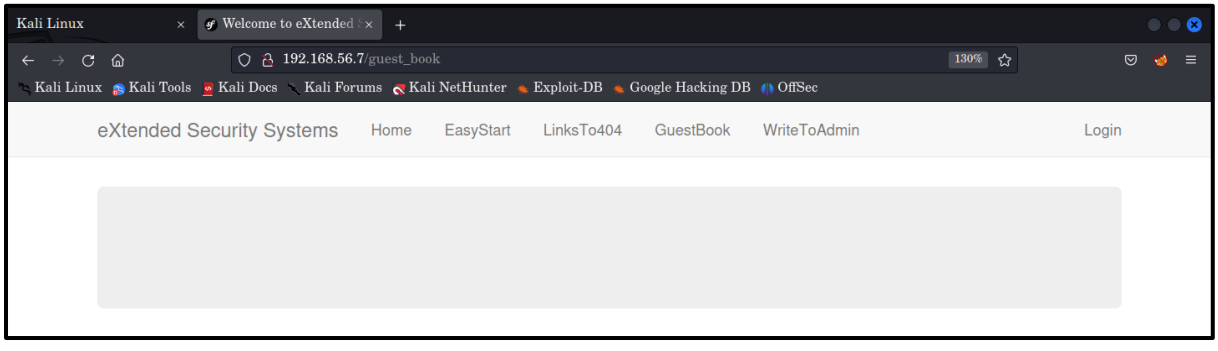


– На веб-сторінці “**GuestBook**” ми можемо скористатися **Stored XXS** ↓

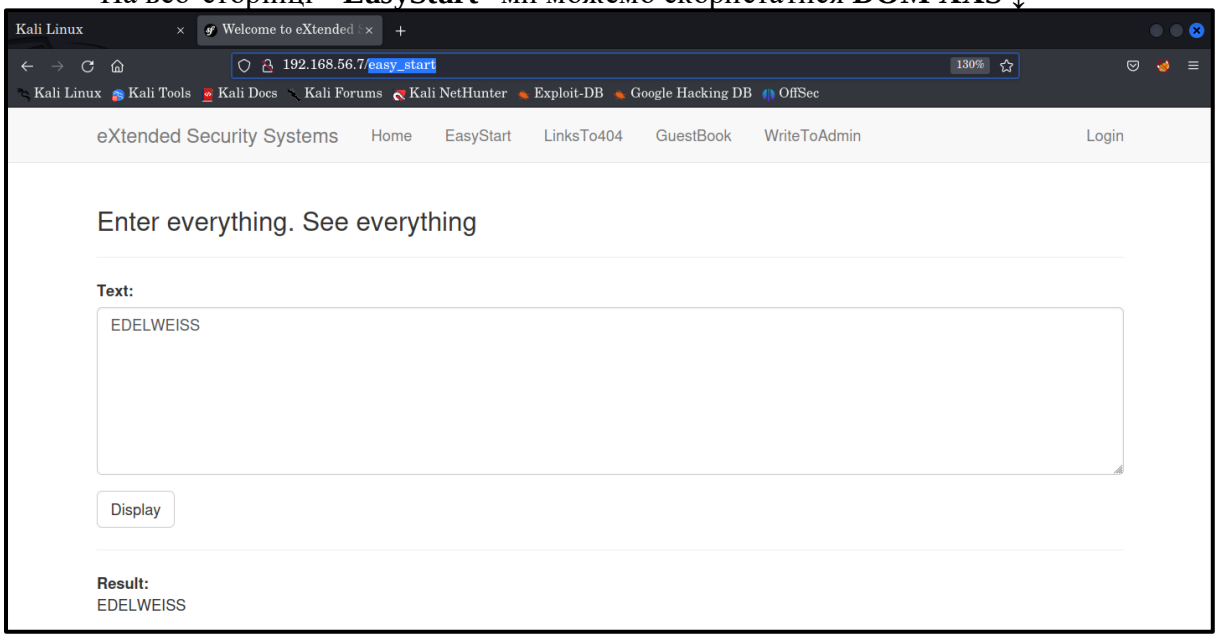


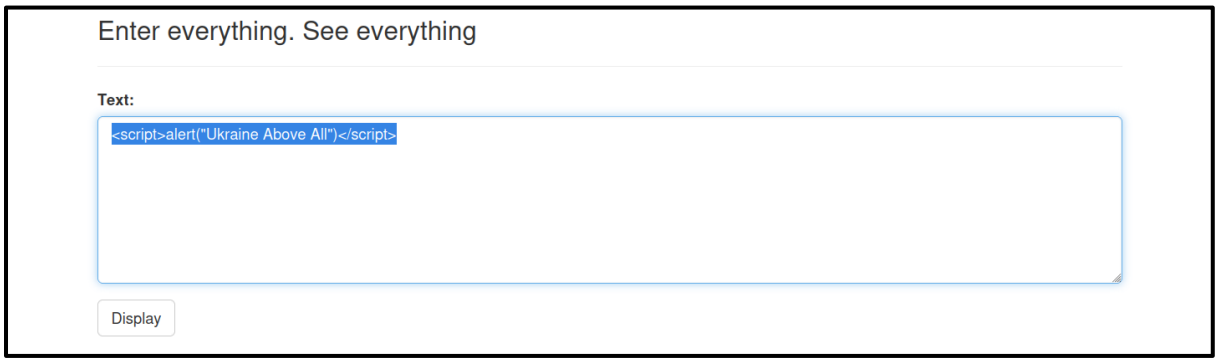


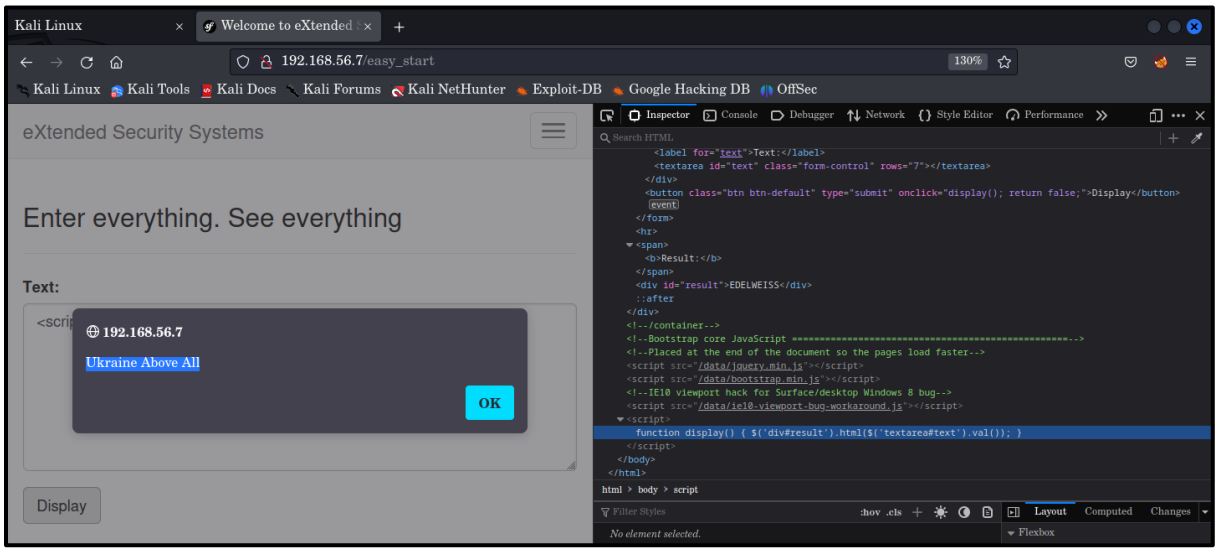


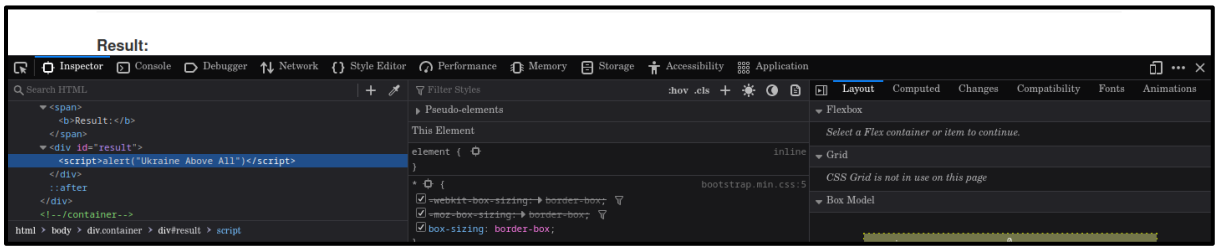


– На веб-сторінці “**EasyStart**” ми можемо скористатися **DOM XXS** ↓





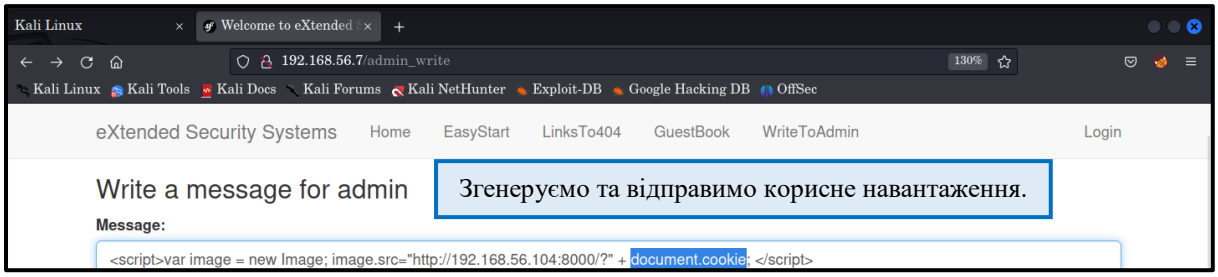


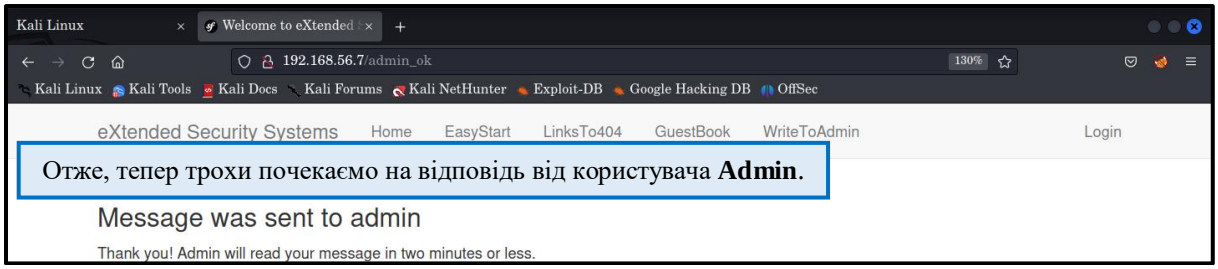


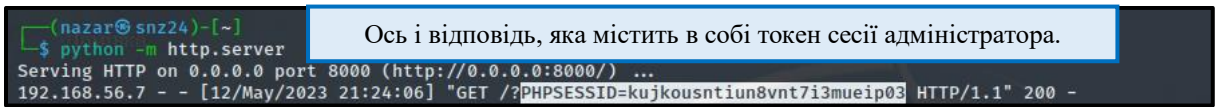
TASK 2

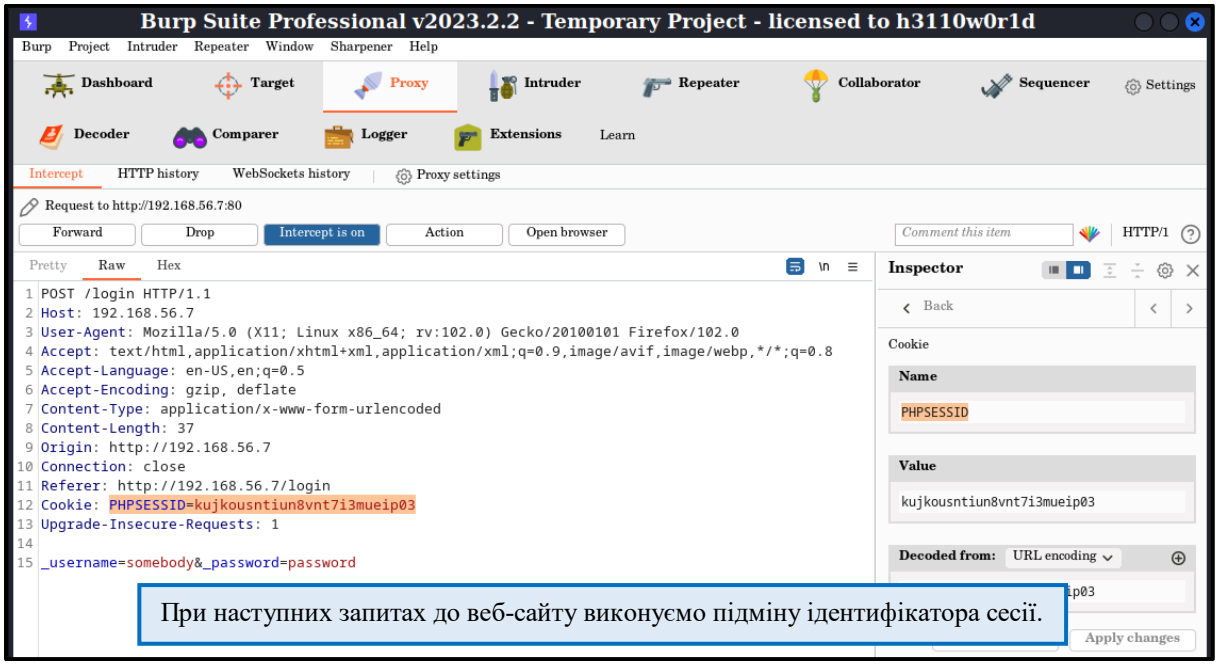
Can you use XSS to hijack administrator session? Prove it (screenshot).

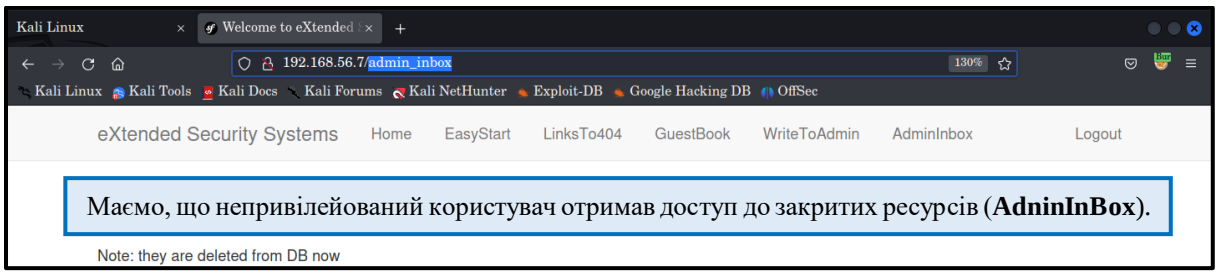
Answer:

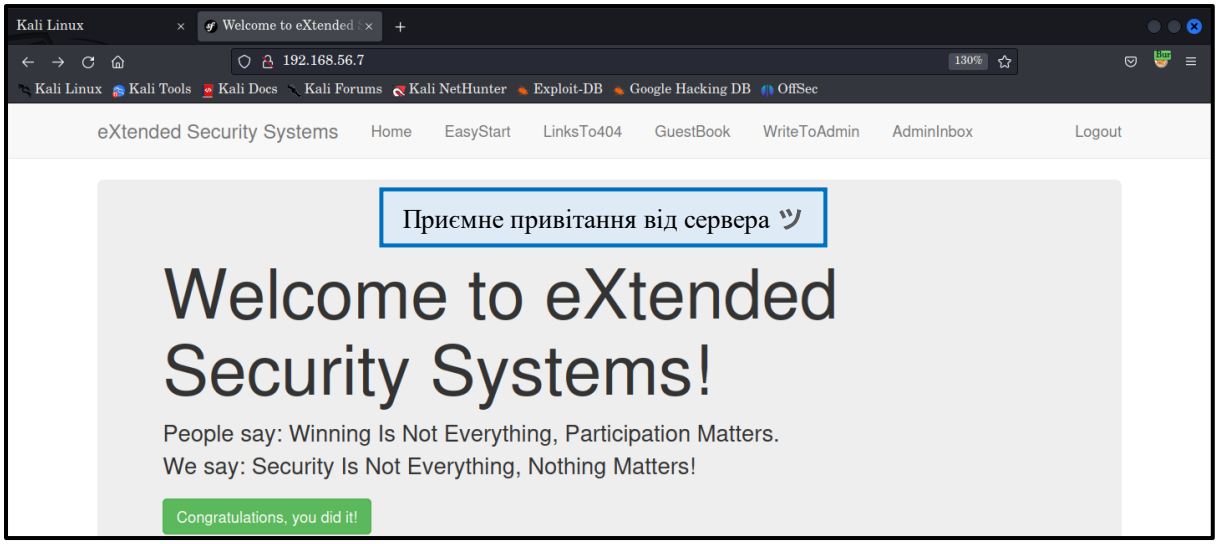








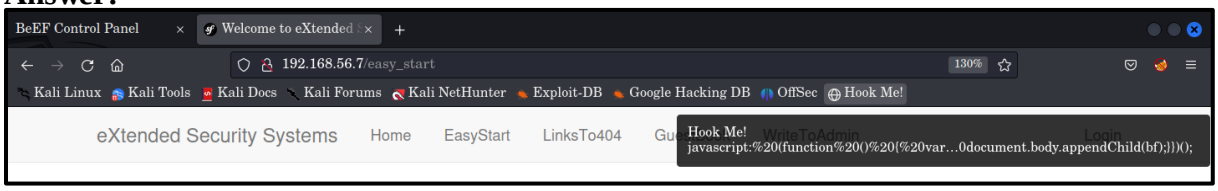


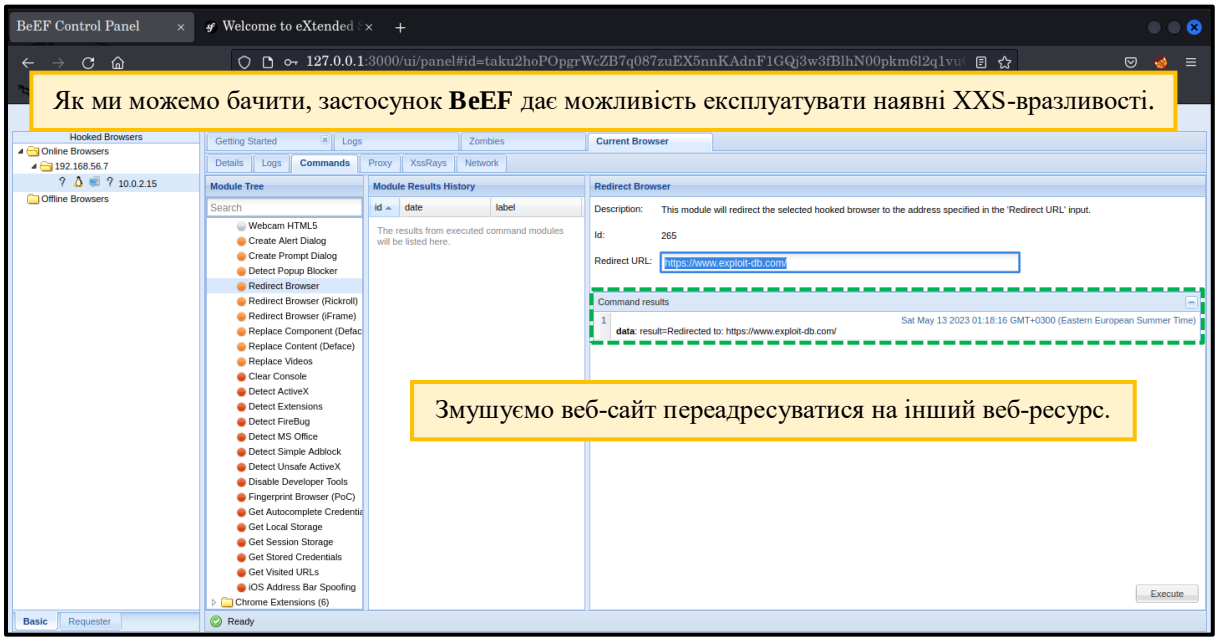


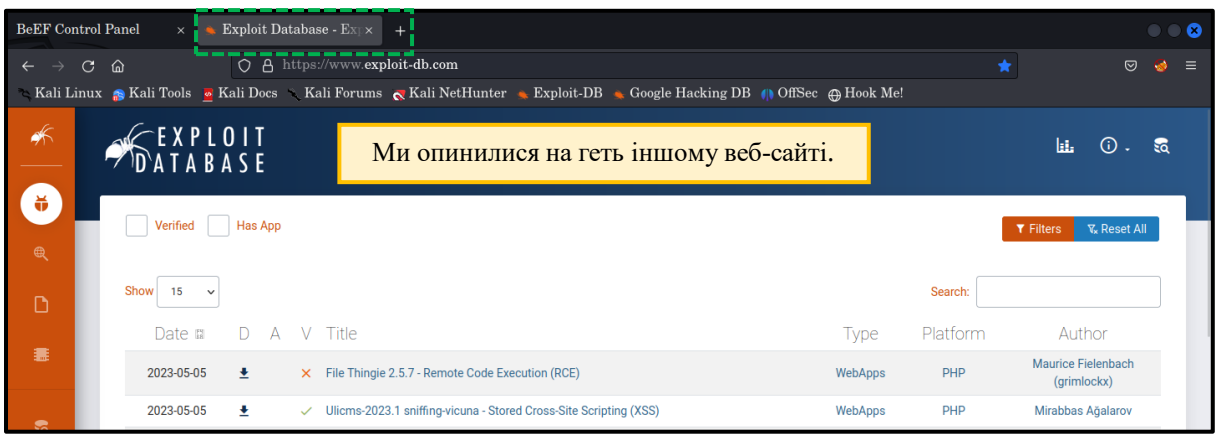
TASK 3

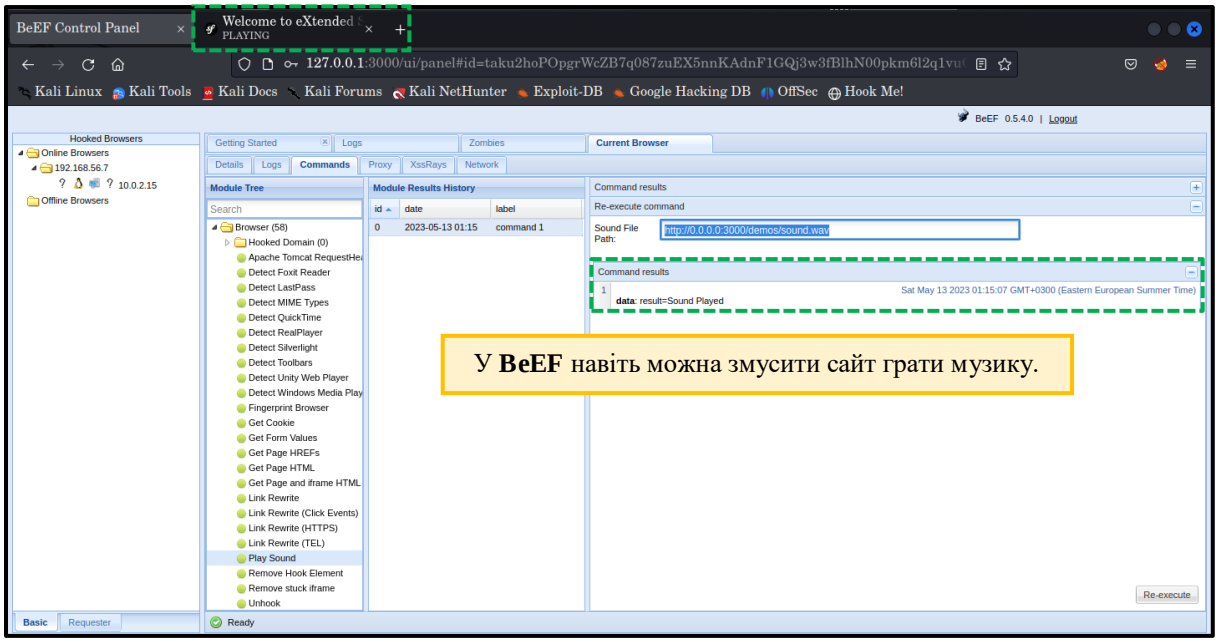
Can you use provided vulnerabilities to compromise host machine with BeeF? Prove it (screenshot).

Answer:









TASK 4

What BeeF functions are working on host machine? Prove it (screenshot).

Answer: