Assignment 8.1

Course name: XML attacks

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. XXE injection

Purpose: understand how to detect and exploit XXE-injection

After the work the student must

- know: how detect XXE-injection vulnerabilities;

Tasks:

- analyze provided VM (192.168.56.11);
- detect XML communication;
- exploit XXE-injection.

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- Chrome developer tools
- Mozilla developer tools

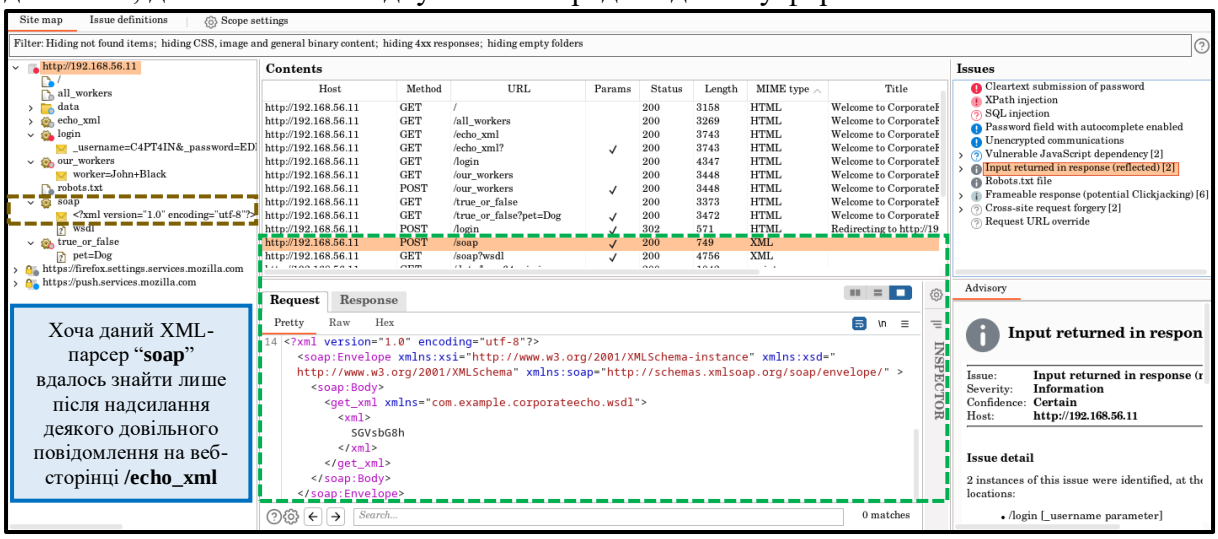
Solution:
Launch VM. Open http://192.168.56.11 in browser. Analyze HTTP-parameters for GET/POST. Find XML-based communication.

TASK 1

What page is vulnerable to XXE-injection? Prove it (screenshot).

Answer:

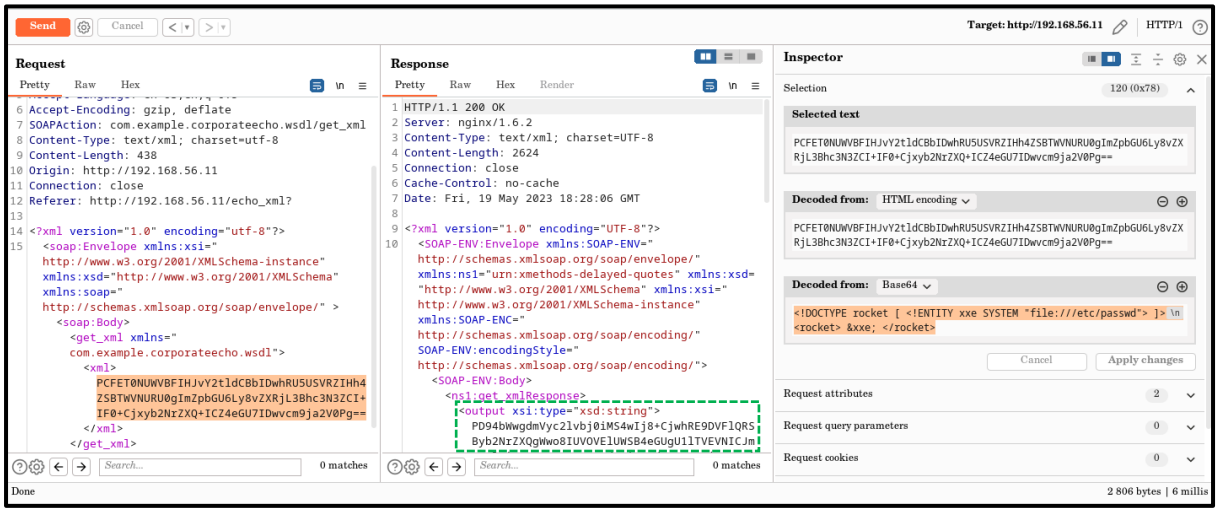
Для знаходження потенційно вразливих веб-сторінок до **XML External Entity** ін'єкції необхідно скористатися сканером веб-вразливостей **Burp Suite**, який дасть можливість дізнатися, де на веб-сайті відбувається передача даних у форматі **XML**.

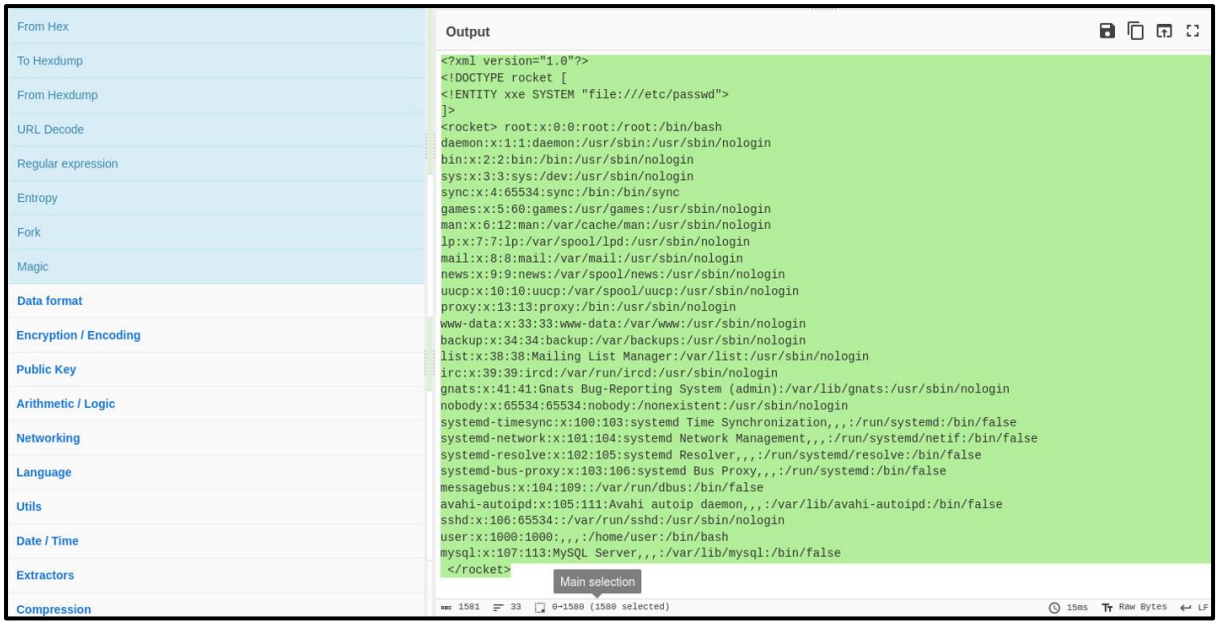


TASK 2

How can you exploit XXE-injection? Prove it (screenshot).

Answer:





Task 2. WSDL testing

Purpose: understand how to detect and work with WSDL schemas

After the work the student must

- know: how detect and use XML schemes (WSDL);

Tasks:

- analyze provided VM (192.168.56.11);
- detect WSDL schema definition;
- analyze announced methods;
- use methods.

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- Chrome developer tools
- Mozilla developer tools
- Boomerang - SOAP & REST Client
  - https://chrome.google.com/webstore/detail/boomerang-soap-rest-clien/eipdnjedkpcnlmmdfdkgfpljanehloah)

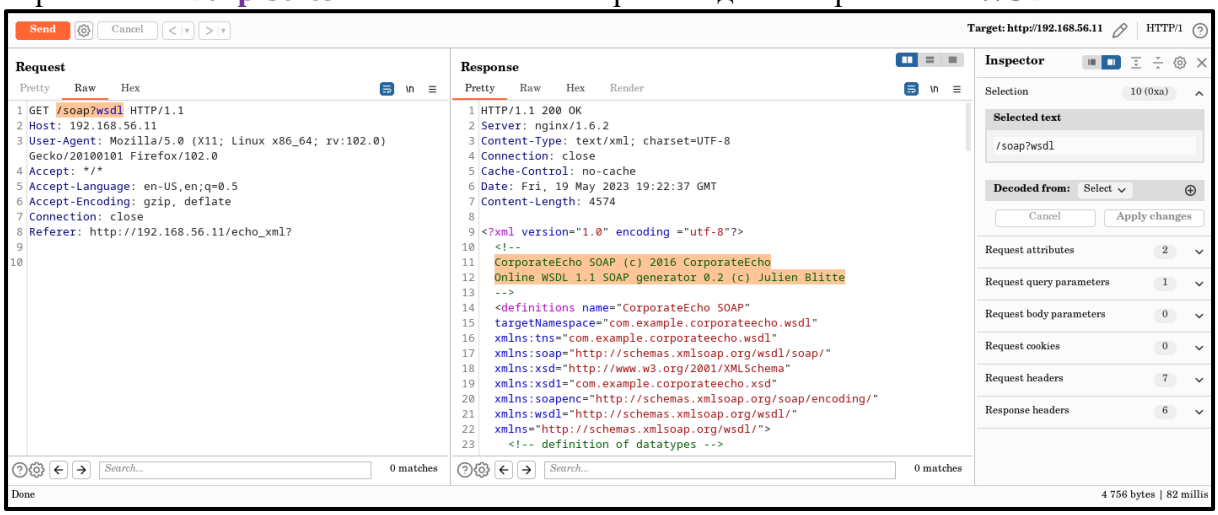
Solution:
Launch VM. Open http://192.168.56.11 in browser. Analyze HTTP-parameters for GET/POST. Find WSDL. Analyze results. Detect worked methods.

TASK 1

What page announces WSDL? Prove it (screenshot).

Answer:

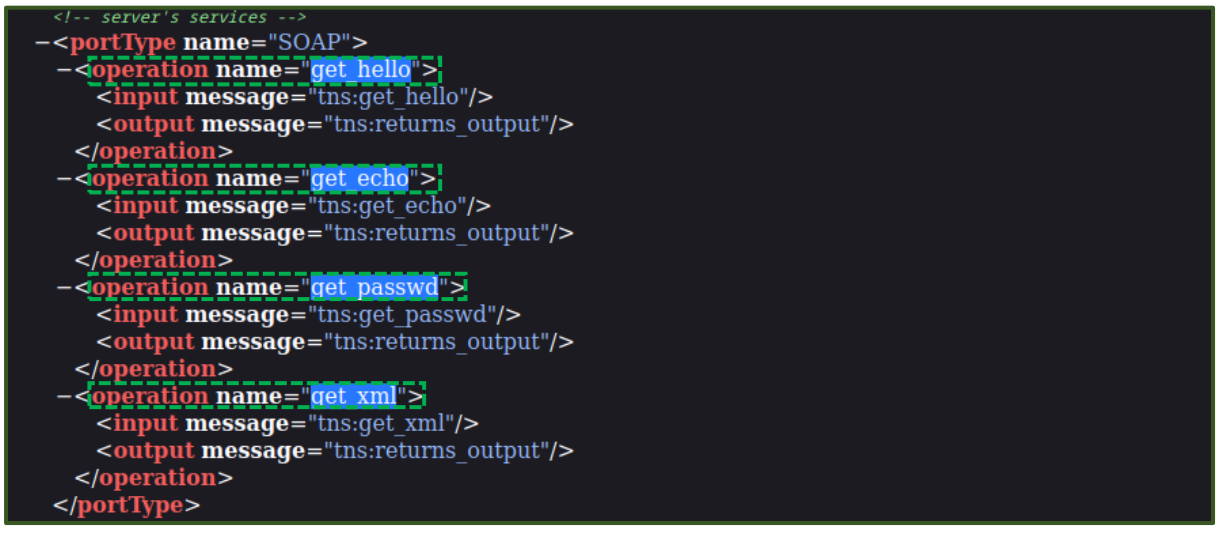
Так само, тільки якщо надіслати деякий запит до веб-сторінки **/echo_xml**, то в історії перехоплень **Burp Suite** можна помітити звернення до мови розміток "**WSDL**".



TASK 2

Which methods are announced via WSDL? Prove it (screenshot).

Answer:



TASK 3

What method is possible to execute? Prove it (screenshot).

Answer: