MAJOR PROJECT

Bug hunting on any target of openbugbounty

TEAM MEMBER:

Yogaraj.S

SURUTHILAYA D V

Prajit k

MARK JOHN MHANDO

Nanda Kishore E S

DURGA NANTHINI DEVI.S

Harson Dasouni

Introduction:

The rapid growth of digital technologies has transformed the way we live, work, and communicate. However, it has also increased the risk of cyber threats such as hacking, data breaches, and identity theft. As a result, there is a growing need for enhanced online security measures to protect individuals and organizations from these risks.

The Bug hunting on any target of openbugbounty aims to address this need by identifying and reporting vulnerabilities on websites listed on the Open Bug Bounty platform. Open Bug Bounty is a non-profit organization that facilitates coordinated disclosure of website security vulnerabilities by connecting security researchers with website owners. The platform enables researchers to identify vulnerabilities and report them to the website owner, allowing them to take necessary measures to address the issues.

The Bug hunting on any target of openbugbounty involves a community of security researchers who use a range of tools and techniques to systematically search for security weaknesses on websites. By identifying and reporting vulnerabilities, the project helps website owners to improve their website's security and prevent potential attacks or breaches.

Testing Methodology:

- Choose a target from openbugbounty platform
- Manual Testing
- Exploitation
- Reporting
- Varification

Choose a target from openbugBounty platform:

1. First create an account on openbugbounty in order to participate in their bug bounty program.
2. Now, here we are choosing https://lescontamines.net/ that was listed on OpenBugBounty as a target for our bug hunting.
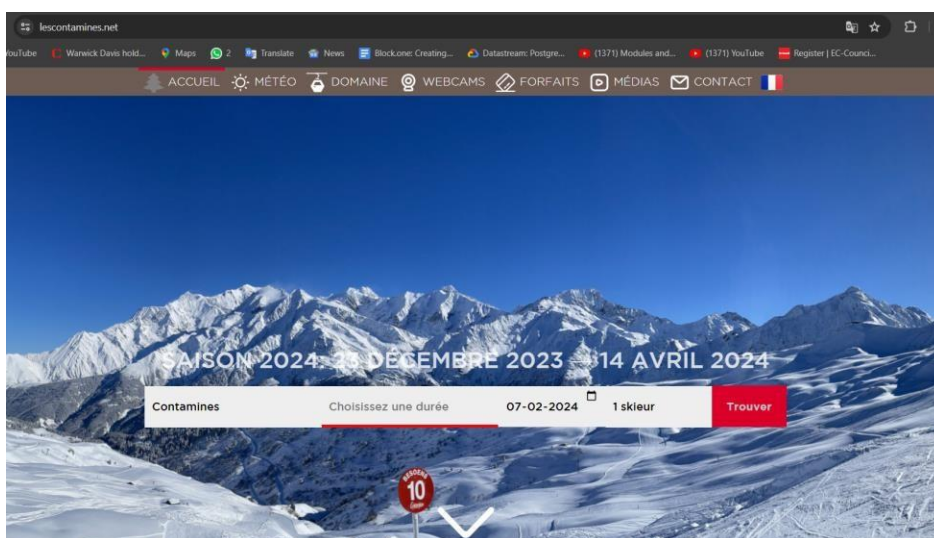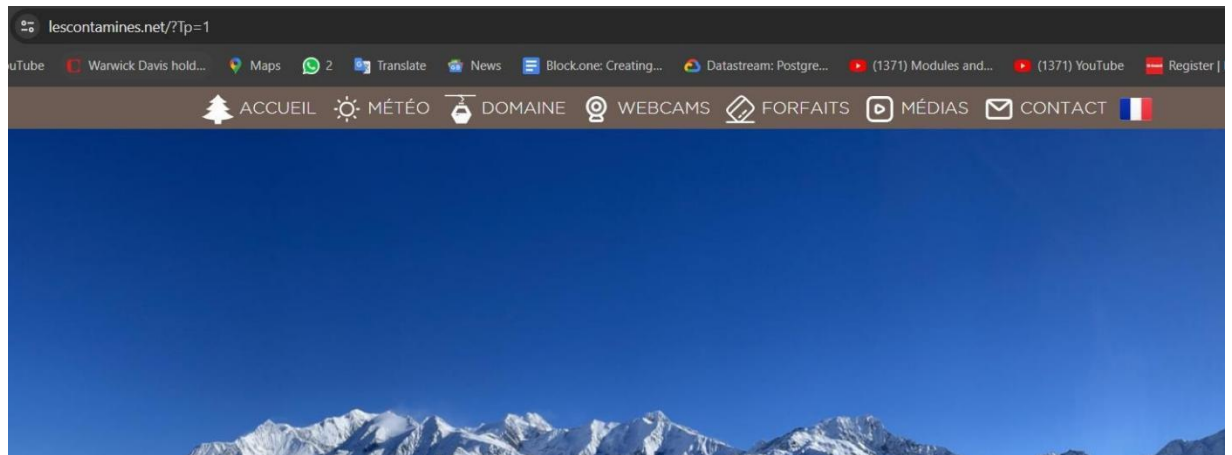

Manual Testing:

3. Next, conduct manual testing to identify vulnerabilities.

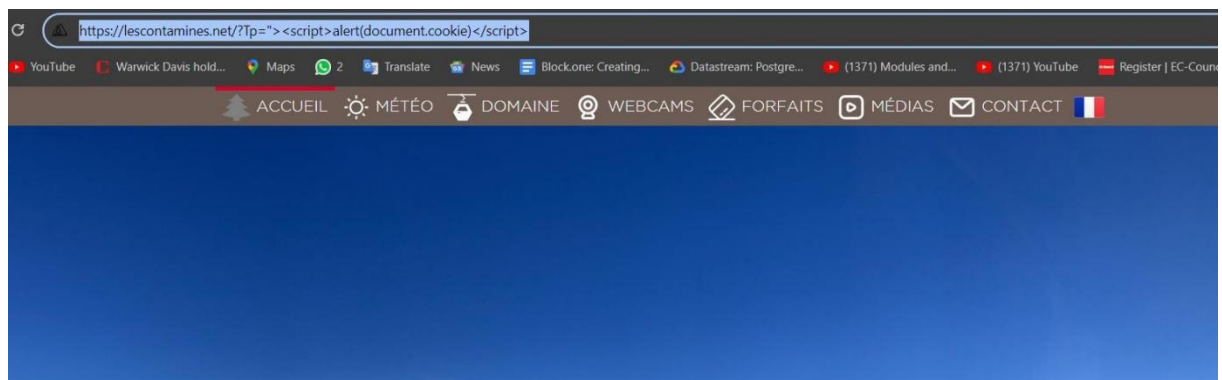Vulnerable found: CWE-79: Cross-site scripting (XSS)
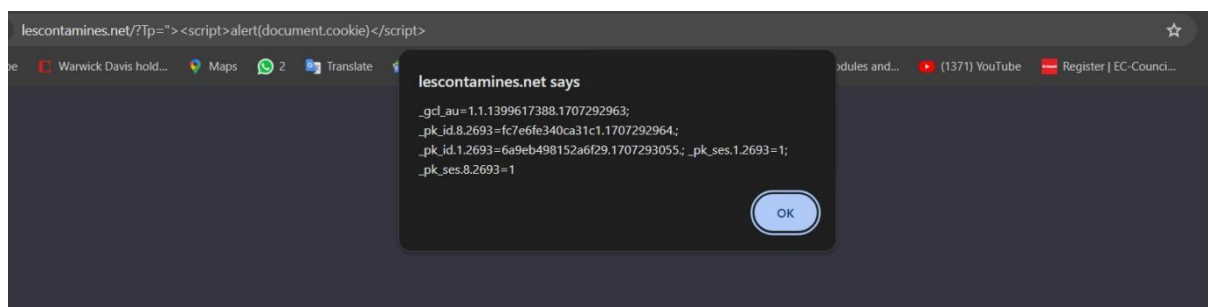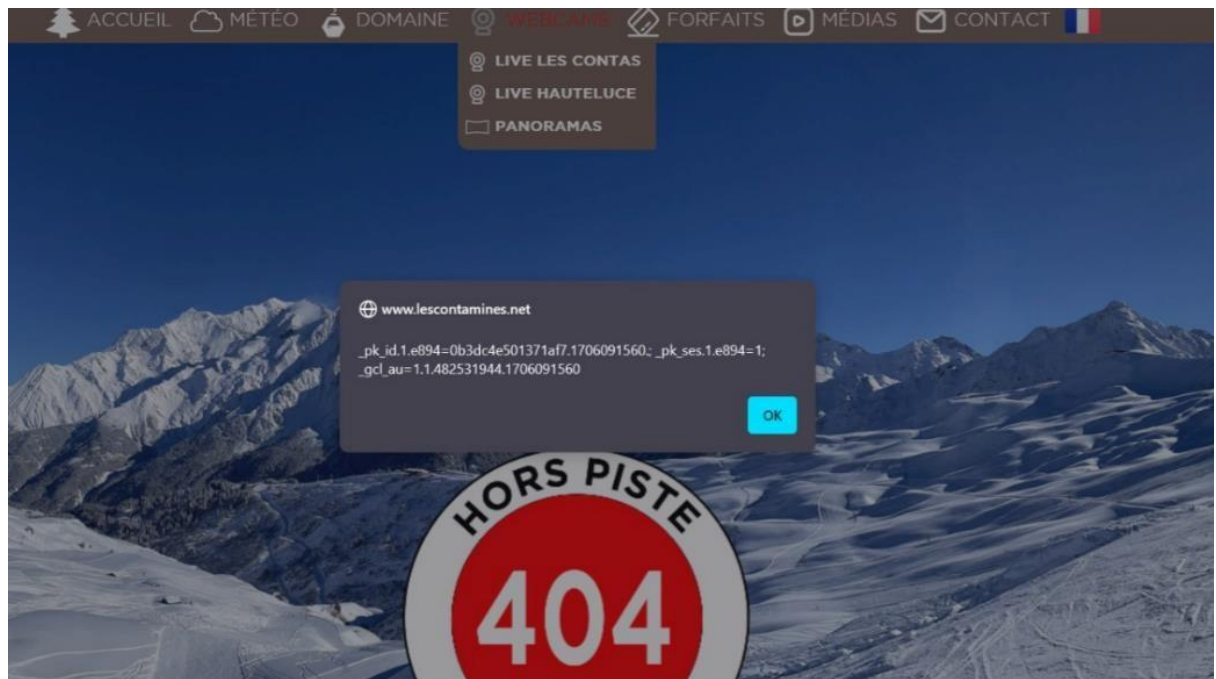Type: Critical

XSS:

Exploitation:

4. Exploit the vulnerability by injecting the following script into the URL:
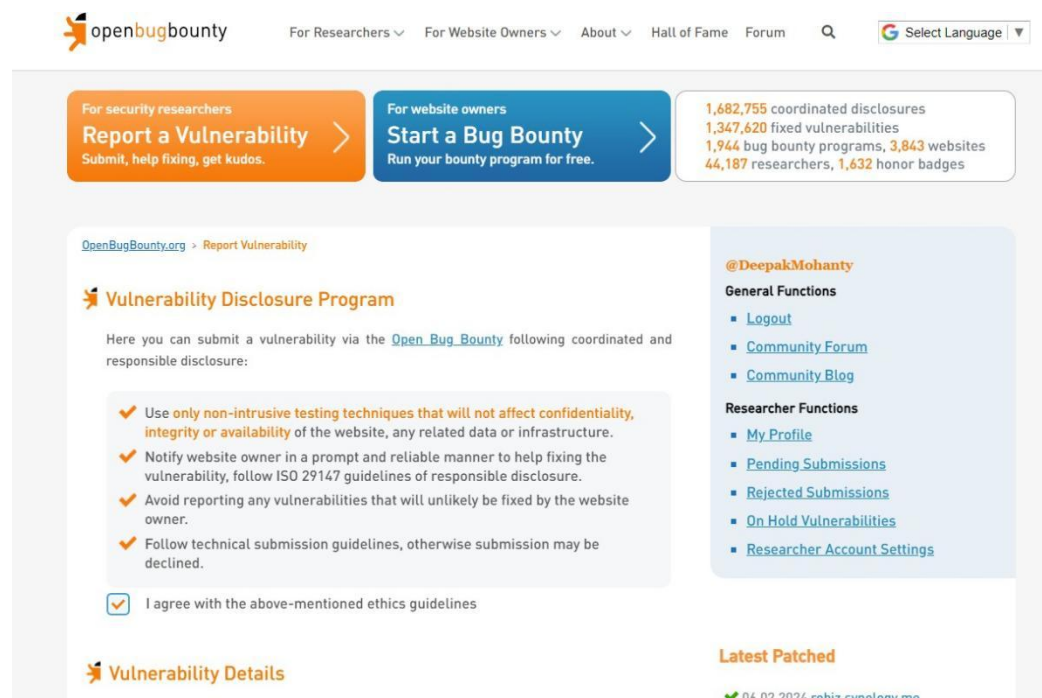   "><script>alert(document.cookie)</script>.

5. Observe the page triggered with on XSS.

Reporting:

6. Next, Reporting identified vulnerability to the website owner through the OpenBugBounty platform.

🏹 Vulnerability Details

Vulnerability type: [Cross Site Scripting (XSS) ▼]

Please carefully follow submission guidelines:

- Your XSS must display 'OPENBUGBOUNTY' string in a JS popup, for example:
  - ○ <script>alert('OPENBUGBOUNTY')</script>
  - ○ <img src=x onerror=prompt(/OPENBUGBOUNTY/)>
  - ○ <script src=https://openbugbounty.org/1.js>
- Your XSS must affect the domain for which you submit the vulnerability - XSS in iframes or after redirects are not accepted.
- Iframe injections must contain an iframe with https://openbugbounty.org inside.
- Same XSS in different scripts (e.g. one global parameter affecting all pages) will NOT be published as separate XSSs, and will be deleted.
- Multiple re-submissions of the same vulnerability will result in removal of all these submissions.
- Due to high amount of work required, mass posting vulnerabilities will NOT be re-checked if not accepted after submission.

* XSS URL: [https://lescontamines.net/?Tp=%22%3E%3Cscript%3Ealert(document.( ]

🏹 open**bug**bounty   For Researchers ⌄   For Website Owners ⌄   About ⌄   Hall of Fame   Forum   🔍   G Select Langua

* XSS URL:	https://lescontamines.net/?Tp=%22%3E%3Cscript%3Ealert(document.(
POST data: ❶	☑ x-www-form-urlencoded ☐ multipart/form-data
	key1=value1&key2=value2
Cookies:	_gcl_au=1.1.1399617388.1707292963; _pk_id.8.2693=fc7e6fe340ca31
Application: ❶	Custom code ▼
Comment: ❶	Security Audits: Conduct regular security audits, including automated tools and manual code reviews, to identify and address potential vulnerabilities proactively.

☑ I confirm that the vulnerability was detected without using intrusive automated tools ❶

Publish the report (without any technical details)   ❶ ☑

Do not publish the report   ❶ ☐

🏹 Notifications

ISO 29147 Recommend Notification: ❶ ☑

Open Bug Bounty Notification Framework: ❶ ☑

Notify specific security contact: ❶ [   ]

Send notification via twitter: ❶ ☑

Automatic Disclosure: ❶ ☑

[**SUBMIT**]

Verification :

Proper Report is:

Dear lescontamines Security Team,

We are writing to report a critical security vulnerability on website, https://lescontamines.net/, specifically related to CWE-79: Cross-Site Scripting (XSS). This vulnerability exposes users to the risk of having their private information, including session cookies, compromised by malicious actors.

Vulnerability Details:

Vulnerability Type: CWE-79: Cross-Site Scripting (XSS)

Affected URL: https://lescontamines.net/

Steps to Reproduce:

Navigate to the website https://lescontamines.net/.

Exploit the vulnerability by injecting the following script into the URL: "><script>alert(document.cookie)</script>.

Observe the triggered XSS on the page.

Impact:

The identified XSS vulnerability allows an attacker to:

Impersonate or Masquerade as the Victim User: The attacker can assume the identity of a legitimate user.

Read Any Data Accessible to the User: Access sensitive user information.

Capture User Login Credentials: Obtain login credentials, compromising user accounts.

Perform Unauthorized Actions: Execute actions on behalf of the user, potentially causing harm.

Recommendations (Mitigation):

Input Validation: Implement thorough input validation mechanisms to sanitize and validate user inputs, preventing the injection of malicious scripts.

Output Encoding: Apply proper output encoding to all user-generated content before rendering it on web pages to prevent script execution.

Content Security Policy (CSP): Utilize a Content Security Policy to restrict the types of content that can be loaded on your web pages, mitigating the impact of XSS attacks.

Security Audits: Conduct regular security audits, including automated tools and manual code reviews, to identify and address potential vulnerabilities proactively.

 Thank You..! Sincerely,

Yogaraj.S

SURUTHILAYA D V

Prajit k

MARK JOHN MHANDO

Nanda Kishore E S

DURGA NANTHINI DEVI.S

Harson Dasou

Yogaraj.S

SURUTHILAYA D V

Prajit k

MARK JOHN MHANDO

Nanda Kishore E S

DURGA NANTHINI DEVI.S

Harson Dasouni

On Hold Vulnerabilities

Open Bug Bounty program enables you to keep vulnerability details private and get an award from the website owner or any other concerned party, for example a security company in charge of the website security.

Make sure you have completed your researcher profile and indicated what type of award you prefer.

Once disclosed - vulnerability will be added the our Open Bug Bounty archive.

Once deleted - the vulnerability page will disappear from the archive. It's up to you to negotiate your bounty, we do not act as intermediary in any manner.

All Patched Unpatched

Domain	Action	Submission Date	Disclosure Date	Patch Status	Internal Comment
lescontamines.net Visible	🗑	07.02.2024	07.05.2024	Verification in progress	📄

Conclusion:

The Bug hunting on any target of openbugbounty project can help to ensure that vulnerabilities are identified and reported accurately, and that website owners can take necessary measures to improve their website's security.