# MAJOR PROJECT

## TITLE: **Bug Hunting on any target of Openbugbounty**

## GROUP NUMBER**:** 6

## TEAM MEMBER:

SALMAN DUDEKULA

Lashkar Varunesh

Deepak Mohanty

G Preetam Kumar

Gorla Bhargav Reddy

Devarasetti Kalyan

C.sudheer Kumar Reddy

**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.

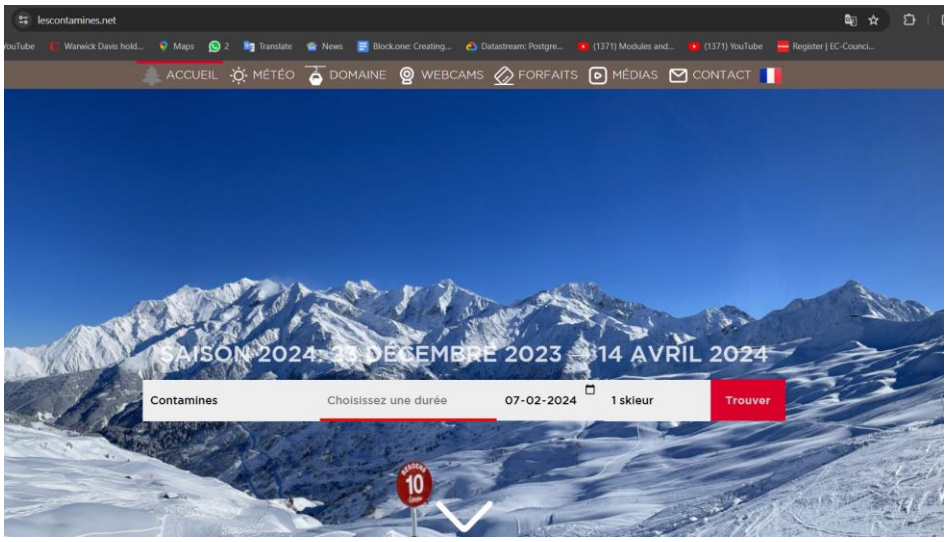
The Bug hunting on any target of openbugbounty involves a community of security researchers who use a range of tools and techniques to systematically search for security weaknesses on websites. By identifying and reporting vulnerabilities, the project helps website owners to improve their website's security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

Testing Methodology:

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

## Choose a target from OpenbugBounty platform:

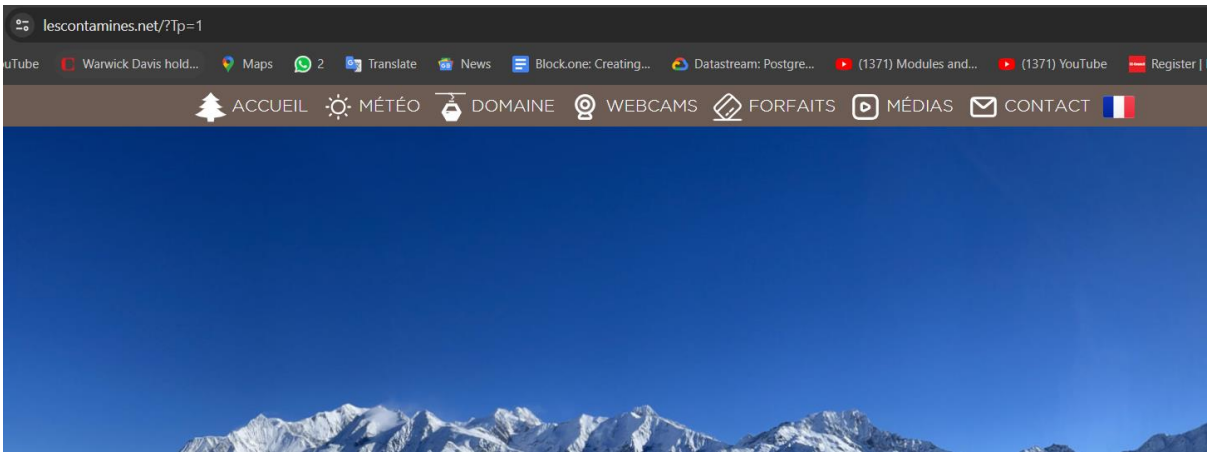
1. First create an account on openbugbounty in order to participate in their bug bounty program.
2. Now, here we are choosing [https://lescontamines.net/](https://lescontamines.net/) that was listed on OpenBugBounty as a target for our bug hunting.




## Manual Testing:

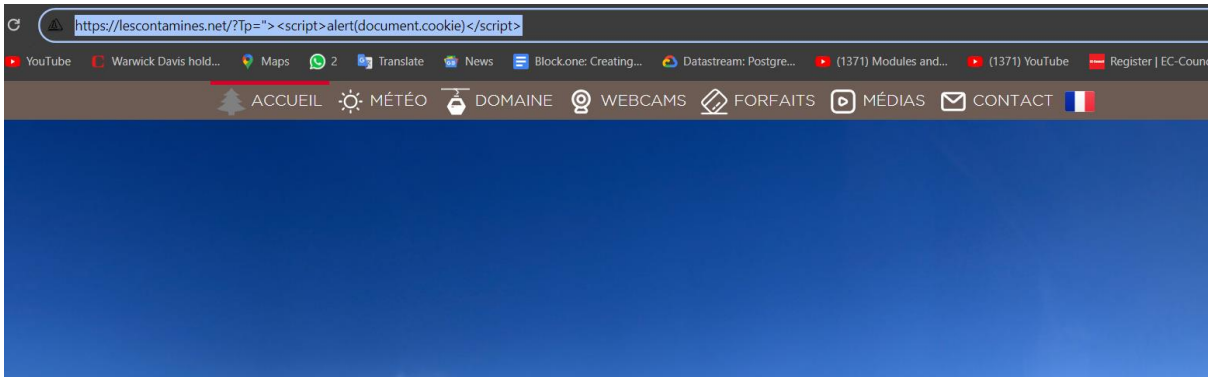
3. Next, conduct manual testing to identify vulnerabilities.
   Vulnerable found: CWE-79: Cross-site scripting (XSS)
   Type: Critical

   XSS:

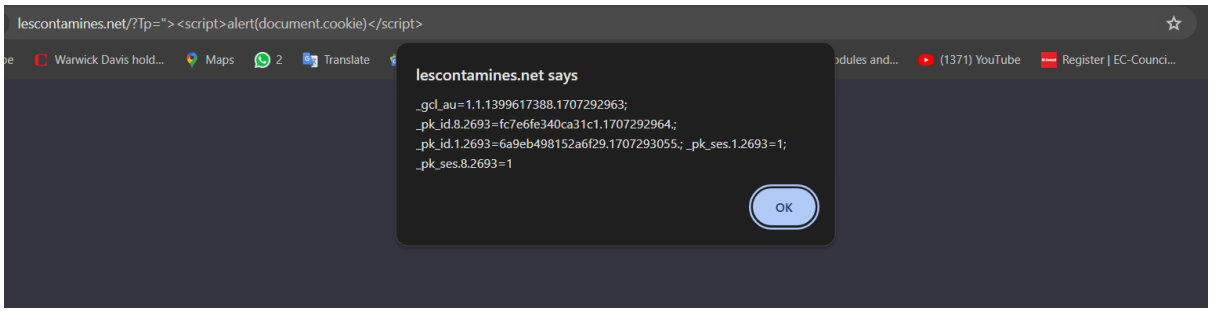


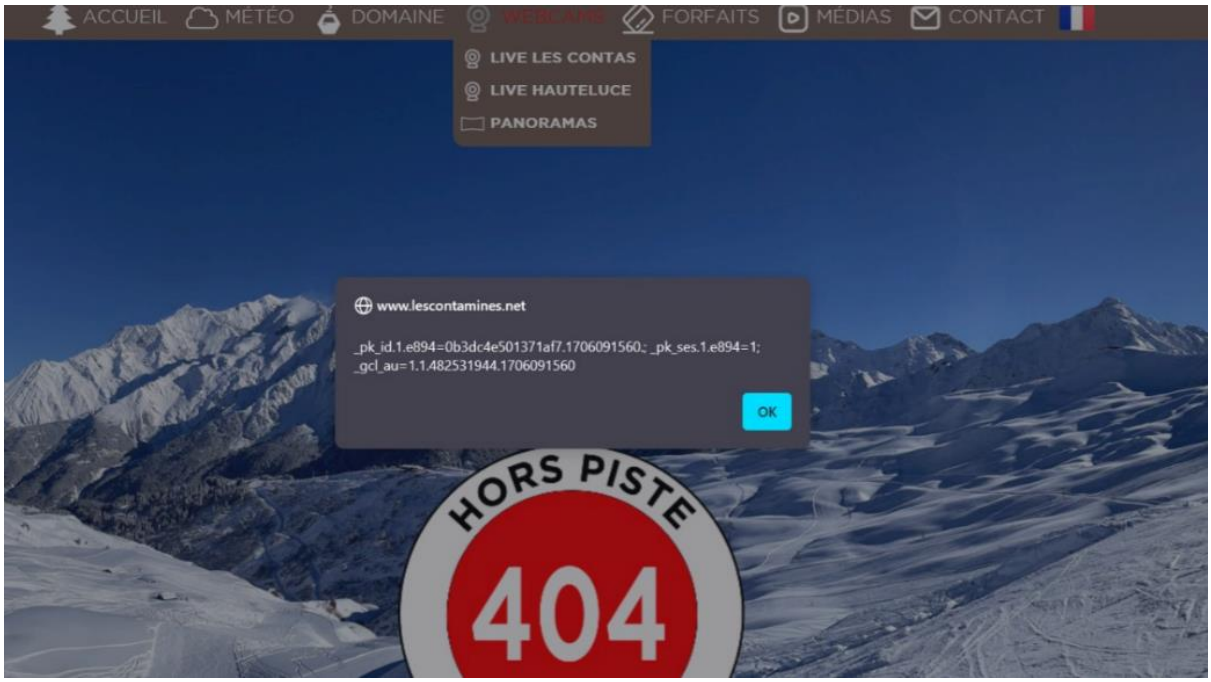
## Exploitation:

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



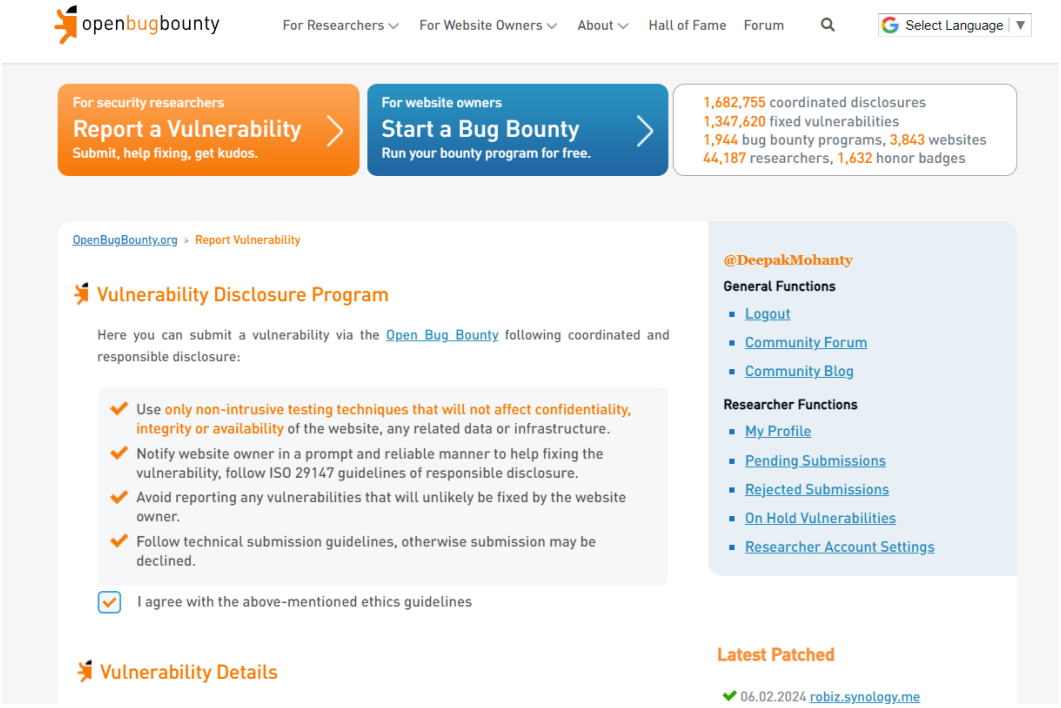

5. Observe the page triggered with on XSS.

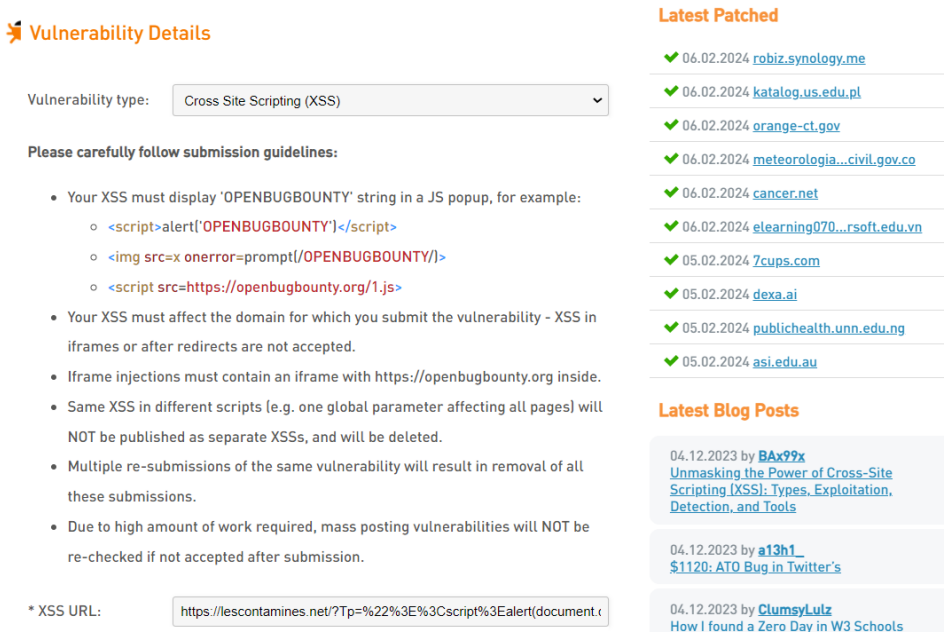


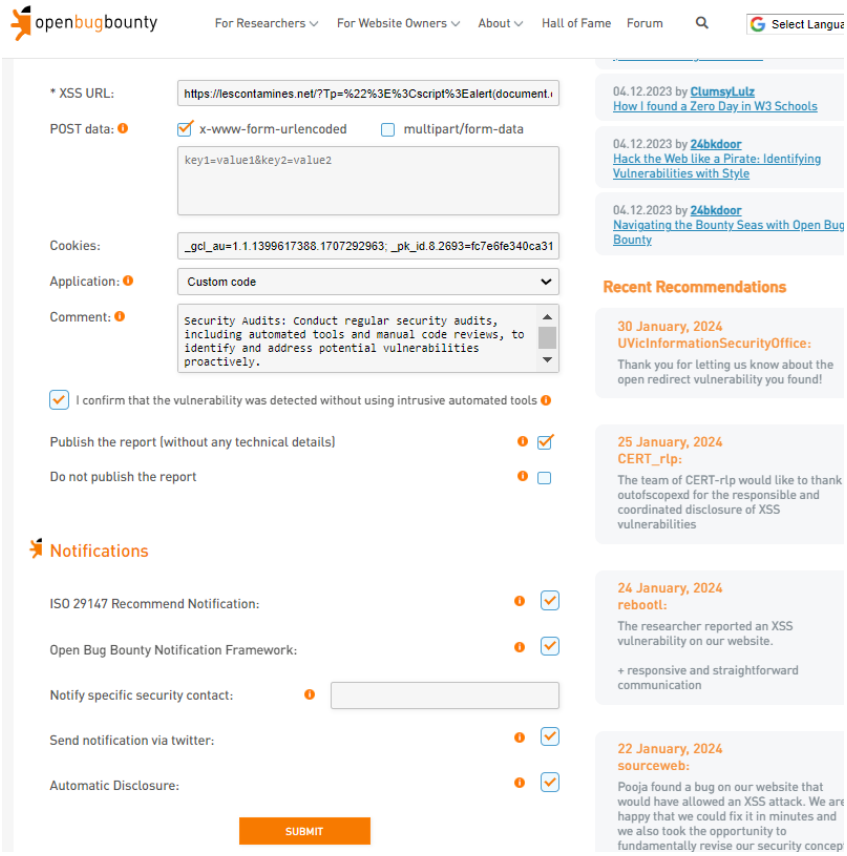



## Reporting:

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






**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,

SALMAN DUDEKULA

Lashkar Varunesh

Deepak Mohanty

G Preetam Kumar

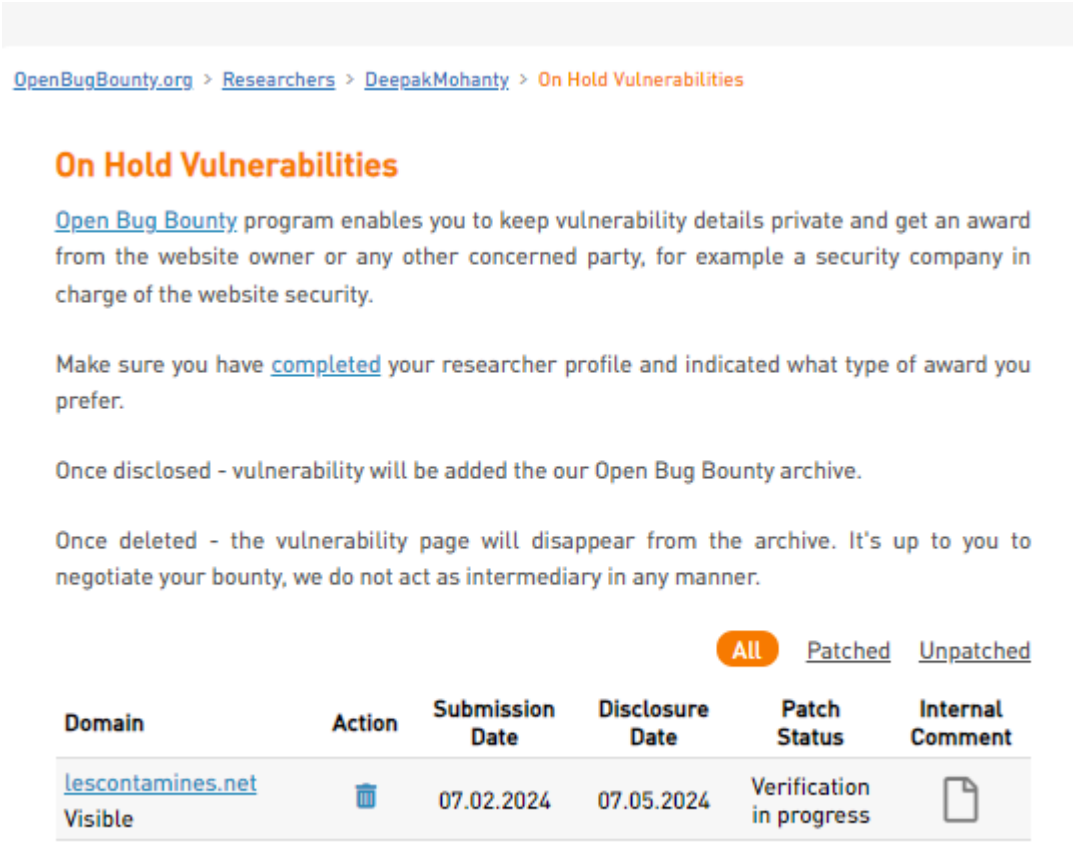
Gorla Bhargav Reddy

Devarasetti Kalyan

C.sudheer Kumar Reddy

Verification:

On Hold Vulnerabilities




## Conclusion:

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.