

MAJOR PROJECT

**Bug hunting on any target of
openbugbounty**

TEAM MEMBER:

Deepak Mohanty

G Preetam Kumar

SALMAN DUDEKULA

Gorla Bhargav Reddy

Lashkar Varunesh

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.

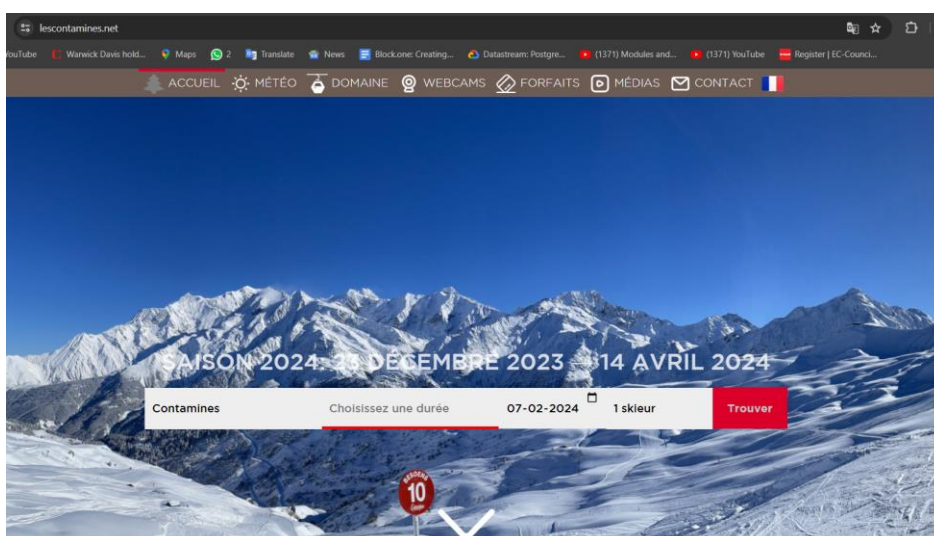
The Bug hunting on any target of openbugbounty involves a community of security researchers who use a range of tools and techniques to systematically search for security weaknesses on websites. By identifying and reporting vulnerabilities, the project helps website owners to improve their website's security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

Testing Methodology:

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



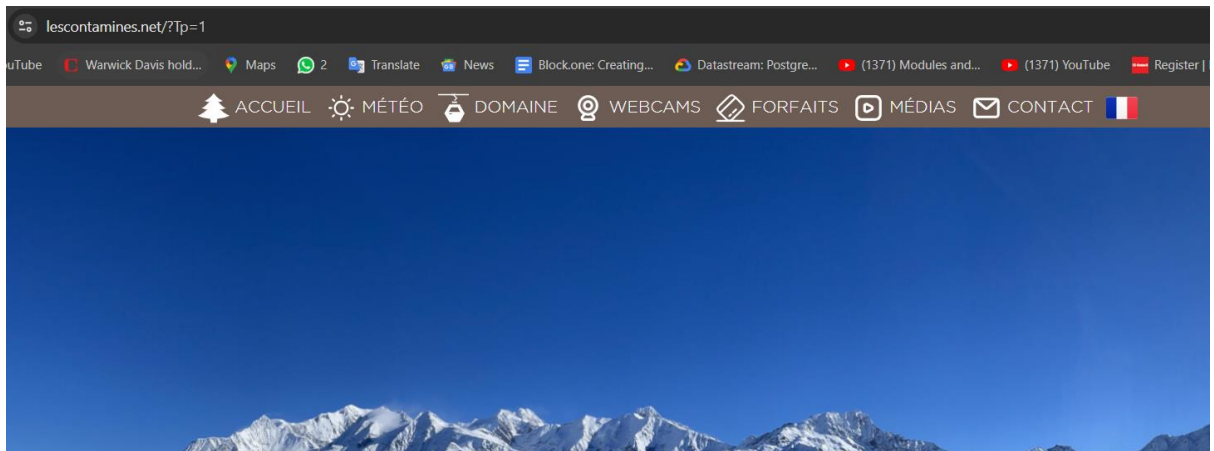
Manual Testing:

3. Next, conduct manual testing to identify vulnerabilities.

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

Type: Critical

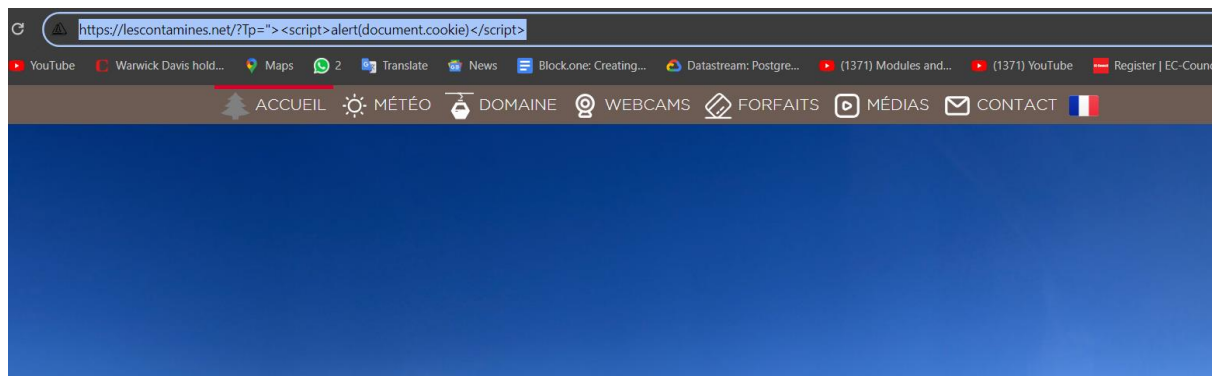
XSS:



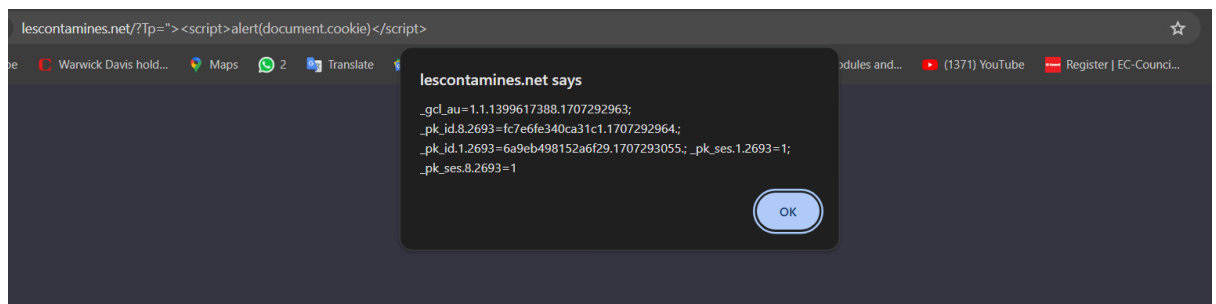
Exploitation:

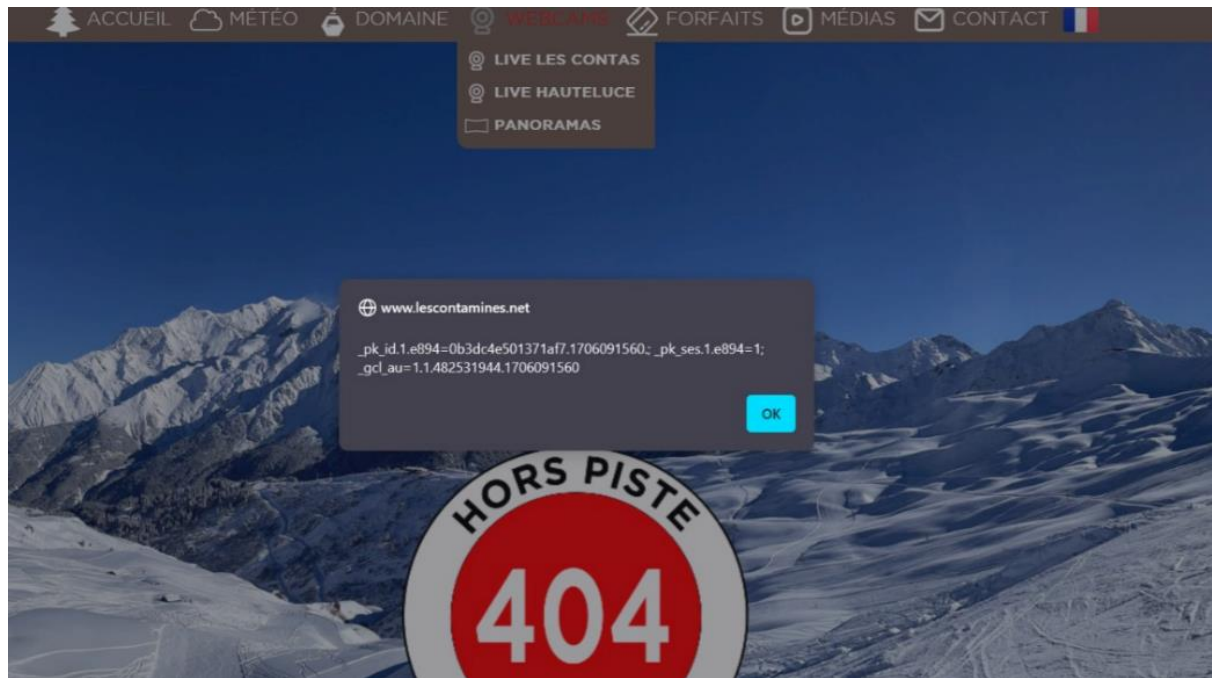
4. Exploit the vulnerability by injecting the following script into the URL:

"><script>alert(document.cookie)</script>".



5. Observe the page triggered with on XSS.





Reporting:

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

openbugbounty

For Researchers ▾ For Website Owners ▾ About ▾ Hall of Fame Forum 🔍 [Select Language](#) ▼

For security researchers
Report a Vulnerability >
Submit, help fixing, get kudos.

For website owners
Start a Bug Bounty >
Run your bounty program for free.

1,682,755 coordinated disclosures
1,347,620 fixed vulnerabilities
1,944 bug bounty programs, 3,843 websites
44,187 researchers, 1,632 honor badges

[OpenBugBounty.org](#) > [Report Vulnerability](#)

🚩 Vulnerability Disclosure Program

Here you can submit a vulnerability via the [Open Bug Bounty](#) following coordinated and responsible disclosure:

- ✓ Use **only non-intrusive testing techniques that will not affect confidentiality, integrity or availability** of the website, any related data or infrastructure.
- ✓ Notify website owner in a prompt and reliable manner to help fixing the vulnerability, follow ISO 29147 guidelines of responsible disclosure.
- ✓ Avoid reporting any vulnerabilities that will unlikely be fixed by the website owner.
- ✓ Follow technical submission guidelines, otherwise submission may be declined.

☒ I agree with the above-mentioned ethics guidelines

🚩 Vulnerability Details

@DeepakMohanty

General Functions

- [Logout](#)
- [Community Forum](#)
- [Community Blog](#)

Researcher Functions

- [My Profile](#)
- [Pending Submissions](#)
- [Rejected Submissions](#)
- [On Hold Vulnerabilities](#)
- [Researcher Account Settings](#)

Latest Patched

✓ 06.02.2024 [robiz.synology.me](#)

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>`
 - ``
 - `<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)

Latest Patched

- 06.02.2024 [robiz.synology.me](#)
- 06.02.2024 [katalog.us.edu.pl](#)
- 06.02.2024 [orange-ct.gov](#)
- 06.02.2024 [meteorologia...civil.gov.co](#)
- 06.02.2024 [cancer.net](#)
- 06.02.2024 [elearning070...rsoft.edu.vn](#)
- 05.02.2024 [7cups.com](#)
- 05.02.2024 [dexa.ai](#)
- 05.02.2024 [publichealth.unn.edu.ng](#)
- 05.02.2024 [asi.edu.au](#)

Latest Blog Posts

04.12.2023 by [BAx99x](#)
[Unmasking the Power of Cross-Site Scripting \(XSS\): Types, Exploitation, Detection, and Tools](#)

04.12.2023 by [a13h1](#)
[\\$1120: ATO Bug in Twitter's](#)

04.12.2023 by [ClumsyLulz](#)
[How I found a Zero Day in W3 Schools](#)



[For Researchers](#) [For Website Owners](#) [About](#) [Hall of Fame](#) [Forum](#) [Select Language](#)

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

POST data: ☒ x-www-form-urlencoded ☐ multipart/form-data

key1=value1&key2=value2

Cookies: _gcl_a=1.1.1399617388.1707292963; _pk_id.8.2693=fc7e6fe340ca31

Application: Custom code

Comment: 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

Publish the report (without any technical details) ☒

Do not publish the report ☐

Notifications

ISO 29147 Recommend Notification: ☒

Open Bug Bounty Notification Framework: ☒

Notify specific security contact:

Send notification via twitter: ☒

Automatic Disclosure: ☒

SUBMIT

04.12.2023 by [ClumsyLulz](#)
[How I found a Zero Day in W3 Schools](#)

04.12.2023 by [24bkdoor](#)
[Hack the Web like a Pirate: Identifying Vulnerabilities with Style](#)

04.12.2023 by [24bkdoor](#)
[Navigating the Bounty Seas with Open Bug Bounty](#)

Recent Recommendations

30 January, 2024
[UVicInformationSecurityOffice:](#)
Thank you for letting us know about the open redirect vulnerability you found!

25 January, 2024
[CERT_rtp:](#)
The team of CERT-rtp would like to thank outofscopexd for the responsible and coordinated disclosure of XSS vulnerabilities

24 January, 2024
[rebootl:](#)
The researcher reported an XSS vulnerability on our website.
+ responsive and straightforward communication

22 January, 2024
[sourceweb:](#)
Pooja found a bug on our website that would have allowed an XSS attack. We are happy that we could fix it in minutes and we also took the opportunity to fundamentally revise our security concept

Verification :

lescontamines.net

Website Overview and Rating

The website lescontamines.net is part of a [bug bounty](#) program run by SECMH:

SSL/TLS Server Test:	A View Results
Web Server Security Test:	A View Results
Malware Test:	Click here
Domain Health Report:	Click here

[OpenBugBounty.org](#) > [OBB-3849918](#)

[Send Notification](#)[Make Featured](#)[Delete](#)

lescontamines.net Cross Site Scripting Vulnerability Report ID: OBB-3849918

Security Researcher [DeepakMohanty](#), found Cross Site Scripting security vulnerability affecting [lescontamines.net](#) website and its users.

Following the coordinated and responsible vulnerability disclosure guidelines of the [ISO 29147](#) standard, Open Bug Bounty has:

- verified the vulnerability and confirmed its existence;
- notified the website operator about its existence.

Technical details of the vulnerability are currently hidden ("On Hold") to give the website operator/owner sufficient time to patch the vulnerability without putting any of its systems or users at risk. Once patched, vulnerability details can be publicly disclosed by the researcher in at least 30 days since the submission. If for a reason the vulnerability remains unpatched, the researcher may disclose vulnerability details only after 90 days since the submission.

Affected Website:	lescontamines.net
Open Bug Bounty Program:	View Open Bug Bounty Program
Vulnerable Application:	Custom Code
Vulnerability Type:	XSS [Cross Site Scripting] / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Disclosure Standard:	Coordinated Disclosure based on ISO 29147 guidelines
Discovered and Reported by:	DeepakMohanty
Remediation Guide:	OWASP XSS Prevention Cheat Sheet

Vulnerable URL:

```
https://lescontamines.net/?Tp=""><script>alert(document.cookie)</script>
```

Cookies:

```
_gc_l_au=1.1.1399617388.1707292963;  
_pk_id.8.2693=fc7e6fe340ca31c1.1707292964.;  
_pk_id.1.2693=6a9eb498152a5f29.1707293055.; _pk_ses.1.2693=1
```

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,

Deepak Mohanty

G Preetam Kumar

SALMAN DUDEKULA

Gorla Bhargav Reddy

Lashkar Varunesh

Devarasetti Kalyan

C.sudheer Kumar Reddy

Verification:

On Hold Vulnerabilities



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.