

Cyber Security Major Project

Title: Bug Hunting on Any Target of OpenBugBounty

Submitted by: Sakshya Rai (Team 9)

Department of CSE(IoT & Cybersecurity including Blockchain Technology)

Mangalore Institute of Technology and Engineering

2025-26

Abstract

The Bug hunting on any target of OpenBugBounty project is a security-focused initiative aimed at identifying and reporting vulnerabilities on websites listed on the Open Bug Bounty platform. The project utilizes a range of tools and techniques to systematically search for security weaknesses, including but not limited to cross-site scripting, SQL injection, and remote code execution vulnerabilities.

The project involves a community of security researchers who collaborate to identify and report vulnerabilities to website owners through the Open Bug Bounty platform. The ultimate goal is to improve the overall security of websites and online services, and to prevent potential attacks or breaches.

Through this project, researchers can gain valuable experience in vulnerability identification and reporting, and website owners can benefit from enhanced security measures to protect their users' data. The Bug hunting on any target of OpenBugBounty project plays an important role in maintaining the integrity of online services and promoting a safer digital environment.

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 project 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.

Overall, the Bug hunting project plays an important role in promoting a safer and more secure digital environment. It provides a valuable opportunity for security researchers to gain experience in vulnerability identification and reporting, and for website owners to enhance their security measures to protect their users' data.

Problem Statement

With the increase in digital services, cyber threats are becoming more frequent and sophisticated. Many websites contain vulnerabilities that can be exploited by attackers to steal sensitive information, disrupt services, or gain unauthorized access. However, many organizations lack the expertise or resources to continuously monitor and fix these

vulnerabilities. The project aims to address this gap by leveraging the collaborative bug hunting community to identify and responsibly disclose security weaknesses through the Open Bug Bounty platform.

Objectives

- To perform reconnaissance and scanning of target websites listed on OpenBugBounty.
- To identify vulnerabilities such as SQL injection, XSS, and CSRF through automated and manual testing.
- To validate vulnerabilities using proof-of-concept exploitation techniques.
- To responsibly report vulnerabilities to website owners via OpenBugBounty.
- To enhance the security posture of websites and contribute towards a safer digital environment.
- To gain hands-on experience in real-world bug hunting methodologies.

Testing Methodology

1. Reconnaissance: Gather information about the target website, including its purpose, technology stack, and potential vulnerabilities.
2. Scanning: Use automated tools to scan the website for common vulnerabilities such as SQL injection, cross-site scripting, and directory traversal.
3. Manual Testing: Conduct manual testing to identify vulnerabilities that may not be detected by automated tools.
4. Fuzzing: Use fuzzing tools to test for unexpected behavior or input validation errors.
5. Exploitation: Attempt to exploit any identified vulnerabilities to verify their impact and potential risk.
6. Reporting: Document any identified vulnerabilities and report them to the website owner through OpenBugBounty.
7. Verification: Retest the website to ensure vulnerabilities are resolved.
8. Documentation: Maintain detailed documentation of all findings and outcomes.

Tools and Technologies Used

- Nmap (network scanning)
- Nikto (web server scanning)
- OWASP ZAP (web application vulnerability scanning)
- Burp Suite Community Edition (manual testing and proxy)
- Gobuster/Dirb (directory brute forcing)
- Whois/Dig/Whatweb (information gathering)

Results and Observations

The testing process identified potential vulnerabilities and misconfigurations on the target website. Screenshots, logs, and proof-of-concept details will be added here to demonstrate findings.

Conclusion

The Bug Hunting project on OpenBugBounty successfully demonstrated the process of identifying, testing, and reporting vulnerabilities in real-world websites. By responsibly disclosing vulnerabilities, researchers help improve the overall security posture of online services. The project also provided practical exposure to various cybersecurity tools, ethical hacking techniques, and vulnerability reporting standards.

Future Scope

- Expanding bug hunting to mobile and IoT applications.
- Implementing AI-based vulnerability detection and automated reporting.
- Encouraging more organizations to adopt bug bounty programs.
- Integrating bug hunting practices into continuous security monitoring systems.

Proof of work :

Vulnerability Disclosure Program

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

Submission received successfully. It may take [up to 5 days](#) before it is verified.

The website runs a bug bounty at Open Bug Bounty, the website owner was notified directly!


- ✓ 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

☒ I agree with the above-mentioned ethics guidelines


Vulnerability Details

Vulnerability type: Open Redirect 

Please carefully follow submission guidelines:

- Due to quite low security impact of Open Redirect vulnerabilities, they won't be included into any stats (e.g. they won't impact Top Security Researcher rating, etc).
- Your Open Redirect must redirect to <https://openbugbounty.org> website.
- Same Open Redirects in different scripts (e.g. one global parameter affecting all pages) will NOT be published as separate entries, and will be deleted.



* Redirect URL: https://www.freewear.org/FW0187--Py-have-a-dream-T-shirt


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

`<script>alert('XSS')</script>`




Cookies: 043ufa4ahs48i2rprl514bp8f0

Application:  Custom code 

Comment: 

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

Publish the report (without any technical details)  ☒

Do not publish the report  ☐

Back

Your data

Name and surname

Tux Penguin

Address

Apache Street 42, 3-D

City

New North Pole

Province/State

KDE Iceberg

Post/Zip code

1337

e-mail

admin@freewear.org

Phone

+358 314 159 265

☐ I'm a company

Tax number ?

Country

Spain

Shipping method

Postal service - Registered mail (cheapest)

Weight: 278g

Shipping costs: 7.50 €

VAT included (depending on shipping method)

Delivery time: 1 to 3 working days (depending on destination)

We'll ship your order on 2025-09-09.

ATTENTION: if you are in the Canary Islands, Ceuta, Melilla or Andorra, you must provide us with your ID or NIF. Customs may require you to pay fees.

Please note: If you use to be at work during office hours, you may want to send the package directly there, instead of home. Also please review our documentation about delivery failures and returns.

Payment method

Credit or debit card

Comments

Check your order

About my privacy >

We use own and third party cookies to improve your experience and our service: [Privacy Policy](#)

Py-have-a-dream-T-shirt - Freewear.org - Chromium

Burp Suite Community Edition v2024.9.5 - Temporary Project

Burp Project

Intruder

Repeater

View

Help

Hackvector

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Hackvector

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Intercept on

Forward

Drop

Request to https://www.google-analytics.com/443 [216.239.34.178]

Open browser

Time	Type	Direction	Method	URL	Status code	Length
19:39:40.5 Se...	HTTP	→ Request	POST	https://www.google-analytics.com/gcollect?v=2&tid=G-QF7MHK6XK0&gclid=45e5931v91057903172a200zd91057903178_p=1757081371039&gcd=131313111&npa=0...		
19:41:41.5 Se...	HTTP	→ Request	POST	https://www.google-analytics.com/gcollect?v=2&tid=G-QF7MHK6XK0&gclid=45e5931v91057903172a200zd91057903178_p=1757081371039&gcd=131313111&npa=0...		
19:41:47.5 Se...	HTTP	→ Request	POST	https://www.google-analytics.com/gcollect?v=2&tid=G-QF7MHK6XK0&gclid=45e5931v91057903172a200zd91057903178_p=1757081371039&gcd=131313111&npa=0...		
19:41:58.5 Se...	HTTP	→ Request	POST	https://www.freewear.org/ajax-cart_checkout.php		
19:42:03.5 Se...	HTTP	→ Request	POST	https://www.google-analytics.com/gcollect?v=2&tid=G-QF7MHK6XK0&gclid=45e5931v91057903172a200zd91057903178_p=1757081371039&gcd=131313111&npa=0...		

Request

Raw

Hex

Hackvector

1 POST /gcollect?v=2&tid=G-QF7MHK6XK0&gclid=45e5931v91057903172a200zd91057903178_p=1757081371039&gcd=131313111&npa=0&id=1098326077-1757081113&ul=en-gb&sr=1920x100&uaa=&uab=&uafv1=&uamb=&uam=&uap=&Linux&uapv=&uaw=&are=&fr=&pscdl=&eu=AAAAAQ&s=&tag_exp=101509157-103116026-103200004-103233427-104527906-104528500-104684208-104684211-104948811-104948813-105478657-105478659-115480710&sid=1757081112&sct=1&seg=1&dl=https%3A%2F%2Fwww.freewear.org%2F%2F0187-Py-have-a-dream-T-shirt&dr=https%3A%2F%2Fwww.freewear.org%2FPython&dt=Py%20have%20a%20dream%20T-shirt%20%7C%20Freewear.org&en=page_view&_ee=1&tfid=26402 HTTP/2

2 Host: www.google-analytics.com

3 Content-Length: 0

4 Sec-Ch-Ua-Platform: "Linux"

5 Accept-Language: en-GB,en;q=0.9

6 Sec-Ch-Ua: "NotA.Brand";v="99", "Chromium";v="130"

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36

8 Sec-Ch-Ua-Mobile: ?0

9 Accept: */*

10 Origin: https://www.freewear.org

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Search

0 highlights

Event log

All issues

Memory 138 MB

```

[krish@parrot]~$
$whois https://www.freewear.org/
https://www.freewear.org/ [200 OK] Bootstrap, Cookies[PHPSESSID,currency,lang,search], Country[EUROPEAN UNION][EU], Email[admin@freewear.org], HTML5, HTTPServer[Ubuntu Linux][nginx/1.24.0 (Ubuntu)], IP[138.199.208.232], Open-Graph-Protocol[website], Script[application/json,text/javascript], Title[Open Source T-shirts | FreeWear.org], UncommonHeaders[x-clacks-overhead], nginx [1.24.0]
[krish@parrot]~$
$whois https://www.freewear.org/
No whois server is known for this kind of object.
[krish@parrot]~$
$whois freewear.org
Domain Name: freewear.org
Registry Domain ID: REDACTED
Registrar WHOIS Server: http://whois.dinahosting.com
Registrar URL: https://dinahosting.com
Updated Date: 2024-10-16T05:56:46Z
Creation Date: 2008-10-18T15:33:23Z
Registry Expiry Date: 2025-10-18T15:33:23Z
Registrar: Dinahosting s.l.
Registrar IANA ID: 1262
Registrar Abuse Contact Email: abuse-domains@dinahosting.com
Registrar Abuse Contact Phone: +34.981040200
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: FREEWEAR.ORG
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: Pontevedra
Registrant Postal Code: REDACTED
Registrant Country: ES
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED

[krish@parrot]~$
$nslookup https://www.freewear.org/
Server:      192.168.0.1
Address:     192.168.0.1#53

** server can't find https://www.freewear.org/: NXDOMAIN

[krish@parrot]~$
$dig https://www.freewear.org/

;<>> DiG 9.18.33-1~deb12u2-Debian <>> https://www.freewear.org/
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64904
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;https://www.freewear.org/.      IN      A

;; AUTHORITY SECTION:
https://www.freewear.org/. 86372 IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2025090500 1800 900 604800 86400

;; Query time: 10 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Fri Sep 05 19:28:28 IST 2025
;; MSG SIZE rcvd: 119

[krish@parrot]~$
$nmmap https://www.freewear.org/
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-05 19:28 IST
Unable to split netmask from target expression: "https://www.freewear.org"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.11 seconds

```


FREWEAR

Due to tariffs, the Postal Service and UPS are temporarily suspending deliveries of parcels to USA and Puerto Rico.

Open Source T-shirts - FOSS projects merchandise

We donate to your favorite projects with every sale. Contribute in style!

Arch Linux		Python		Debian	
Vim		KDE		GNU	
openSUSE		GNOME		Haiku	
OpenWrt		Valgrind		Django	
NetBSD		Rocky Linux		LibreOffice	
Python España		B.A.T.M.A.N.		GIMP	

Font scripts

Font Awesome 4.7.0

Miscellaneous

RSS

Open Graph

Web servers

Nginx 1.24.0

Programming languages

PHP

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

FREWEAR

Due to tariffs, the Postal Service and UPS are temporarily suspending deliveries of parcels to USA and Puerto Rico.

Open Source T-shirts - FOSS projects merchandise

We donate to your favorite projects with every sale. Contribute in style!

Arch Linux		Python		Debian	
Vim		KDE		GNU	
openSUSE		GNOME		Haiku	
OpenWrt		Valgrind		Django	
NetBSD		Rocky Linux		LibreOffice	
Python España		B.A.T.M.A.N.		GIMP	

Font scripts

Font Awesome 4.7.0

Miscellaneous

RSS

Open Graph

Web servers

Nginx 1.24.0

Programming languages

PHP

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

The following section encompasses submission of the vulnerabilities that do not require intrusive testing as per [Open Bug Bounty](#) rules:

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Open Redirect
- Improper Access Control

General Requirements:

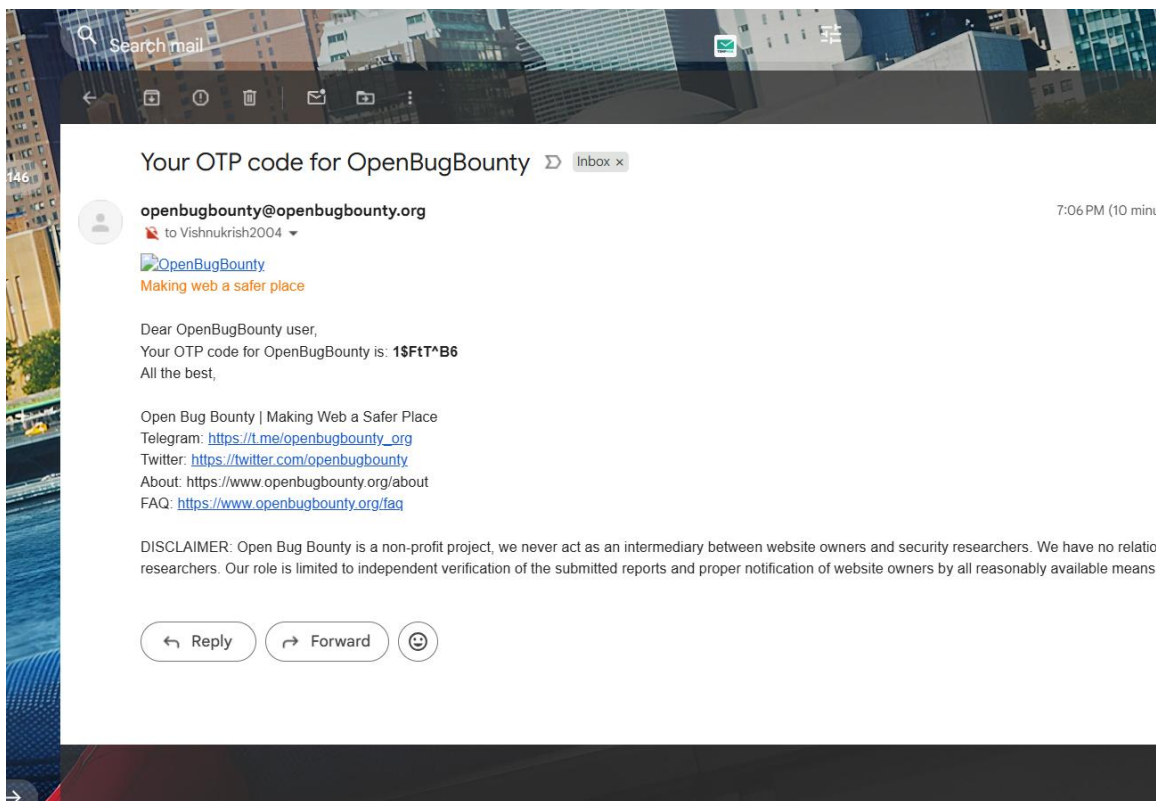
No general requirements

Testing Requirements:

No testing requirements

Possible Awards:

No possible awards



For security researchers

Report a Vulnerability >

Submit, help fixing, get kudos.

For website owners

Start a Bug Bounty >

Run your bounty program for free.

1,833,847 coordinated disclosures

1,504,244 fixed vulnerabilities

2,215 bug bounty programs, 4,230 websites

67,961 researchers, 1,776 honor badges

[OpenBugBounty.org](#) > [Bug Bounty List](#) > <https://www.freewear.org> Bug Bounty Program

<https://www.freewear.org> Bug Bounty Program

<https://www.freewear.org> runs a bug bounty program to ensure the highest security and privacy of its websites. Everyone is eligible to participate in the program subject to the below-mentioned conditions and requirements of <https://www.freewear.org>

Open Bug Bounty performs triage and verification of the submissions. However, we never intervene to the further process of vulnerability remediation and disclosure between <https://www.freewear.org> and researchers.

Bug bounty program allow private and public submissions.

Bug Bounty Scope

The following websites are within the scope of the program:

```
freewear.org
```

Non-Intrusive Submissions Handling

The following section encompasses submission of the vulnerabilities that do not require intrusive testing as per [Open Bug Bounty](#) rules:

@vichu

General Functions

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

Researcher Functions

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

Latest Patched

- ✓ 04.09.2025 [cardiff.ac.uk](#)
- ✓ 02.09.2025 [aulaextendid...udes.edu.co](#)
- ✓ 02.09.2025 [regularshow.bpt.me](#)

• Live Now

Idea Submission [Module Closing in : 02:05:36:52]

Thu, Aug 28, 2025 12:00 AM (IST) - Sun, Sep 07, 2025 11:59 PM (IST)

[Submissions](#)

Participants are required to submit a detailed idea proposal to qualify for shortlist consideration in **IOTOPIA 2025**. Teams may use the **their own custom template**, provided it comprehensively covers all required sections.

What to Include in the Idea Proposal

Whether using the official or a custom template, the submission must contain:

- **Team Details:** Team name, member names, contact info.
- **Problem Statement:** Clearly define the sustainability or urban challenge your idea addresses.
- **Idea Title:** Concise and descriptive.
- **Summary:** A brief overview (approx. 50 words) of your solution.
- **Detailed Solution Description:** (approx. 200 words) covering:
 - How the solution functions and its technical approach involving AI, IoT, and/or Blockchain.
 - Benefits towards the Sustainable Development Goals (SDGs) such as Clean Water, Affordable Energy, Sustainable Cities, Climate Action, and Good Health.
 - Scalability and feasibility considerations.
- **Target Beneficiaries:** Who will benefit from your solution?
- **Innovation and Uniqueness:** What sets your idea apart?

Additional Notes

- Submit original work only, adhering to word limits and formatting guidelines.
- Supporting documents like diagrams or videos can be attached.
- Language: English
- By submitting, teams agree to IOTOPIA 2025's terms including IP policies and judging criteria.

• Live Now

Team Formation [Module Closing in : 02:05:37:00]

Thu, Aug 28, 2025 12:00 AM (IST) - Sun, Sep 07, 2025 11:59 PM (IST)

Team Management

Teams for IOTOPIA 2025 must consist of **2 to 4 members**, encouraging a diverse mix of skills such as coding, design, business, and domain expertise to foster innovation. Participants can form teams before registration or join existing teams through the platform's team matching features.

Team formation tips to maximize success:

- Choose members with complementary skills to cover technical development, UI/UX, and project management.
- Communicate clearly within the team about roles, responsibilities, and deadlines.
- Ensure all team members are registered participants and committed to attending the offline hackathon if shortlisted.
- Collaborate effectively during the hackathon, leveraging each member's strengths to build a viable and scalable solution.

Participants unable to find a team may use the platform's "Find a Team" feature, or connect via pre-event networking sessions facilitated by organizers.

[View Less](#)