

# MAJOR PROJECT

## OPEN BUG BOUNTY

STEP 1: Go to the open bug bounty, and read through the website thoroughly

The screenshot shows the Open Bug Bounty website interface. The top navigation bar includes the Open Bug Bounty logo, links for 'For Researchers', 'For Website Owners', 'About', and 'Hall of Fame', a search icon, and a 'Select Language' dropdown. The main content area is divided into two primary sections: 'Report a Vulnerability' (orange background) and 'Start a Bug Bounty' (blue background). The 'Report a Vulnerability' section includes a form for submitting a vulnerability, with fields for 'Company or Bug Bounty Name' (filled with 'mmex.in') and a 'Submit' button. The 'Start a Bug Bounty' section includes a form for launching a bug bounty program, with a 'Launch' button. Below these sections, there is a 'General' section with a 'Please carefully fill-in the form below to launch your bug bounty:' heading. The right sidebar contains a '@Enfim' section with links for 'General Functions' (Logout, Community Forum, Community Blog) and 'Website Owner Functions' (Claim a Website, My BugBounty Preview, My BugBounty Preferences, My BugBounty Notifications). At the bottom, there is a 'Latest Patched' section with a list of patched vulnerabilities, including '28.03.2025 lastafe.tas.edu.au' and '27.03.2025 marcopolo.me'.

mmex.in Bug Bounty Program

openbugbounty.org/bugbounty/Enfim/

openbugbounty

For Researchers For Website Owners About Hall of Fame

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.

1,789,675 coordinated disclosures  
1,479,089 fixed vulnerabilities  
2,108 bug bounty programs, 4,099 websites  
40,077 researchers, 1,750 honor badges

OpenBugBounty.org > Open Bug Bounty Customization

Open Bug Bounty does triage and verification of the submissions. However, we never intervene to the further process of your communication with the researchers, vulnerability remediation and disclosure. Once a vulnerability is verified and reported to you, our role in coordinated disclosure process is over.

For website owners, we provide vulnerability data export option to the following SDLC, DevOps and bug tracking systems:

Jira Software splunk mantis Bugzilla

**General**

Please carefully fill-in the form below to launch your bug bounty:

Company or Bug Bounty Name: mmex.in

Submit

openbugbounty

For Researchers For Website Owners About Hall of Fame

Select Language

OpenBugBounty.org > Claim a Website

Being a website owner you can create a personalized page for your website(s) on Open Bug Bounty to better prioritize, manage and coordinate efforts with the researchers. All you need to do is:

1. Modify or [generate a security.txt](#) on your website. The file shall contain the following line:  
OpenBugBounty: <https://openbugbounty.org/bugbounty/Enfim/>
2. Request a [verification](#) of security.txt to confirm that you are the website owner. The verification may take up to 24 hours.
3. Once verified, under your account you will be able to manage your website page.

On your website page you will be able to specify the scope of testing, required quality of submissions and other details to facilitate communications with the researchers.

**@Enfim**

**General Functions**

- Logout
- Community Forum
- Community Blog

**Website Owner Functions**

- Claim a Website
- My BugBounty Preview
- My BugBounty Preferences
- My BugBounty Notifications

**Latest Patched**

- 28.03.2025 [lastafe.tas.edu.au](#)
- 27.03.2025 [marcopolo.me](#)

Step2:log into open bug bountry so that we can report the vulnerable website

The image displays two screenshots of the OpenBugBounty website's 'Claim a Website' form. The top screenshot shows the form with placeholder text, while the bottom screenshot shows the form filled out with specific details.

**Top Screenshot (Placeholder Text):**

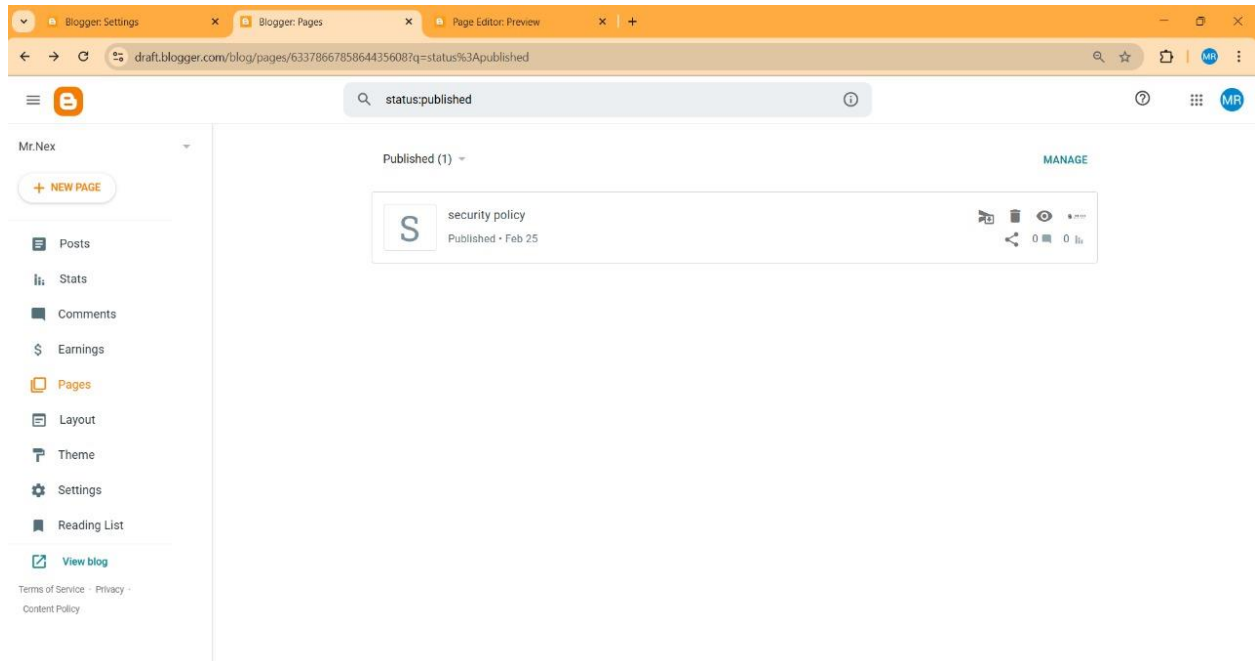
- Contact:** [description]  
mailto:security@example.com
- Encryption:** [description]  
https://example.com/pgp-key.txt
- Acknowledgements:** [description]  
https://example.com/acknowledgements.html
- Policy:** [description]  
https://example.com/security-policy.html
- Signature:** [description]  
https://example.com/well-known/security.txt.sig
- Hiring:** [description]  
https://example.com/jobs.html
- OpenBugBounty:**  
https://openbugbounty.org/bugbounty/Enfirm/

**Bottom Screenshot (Filled Form):**

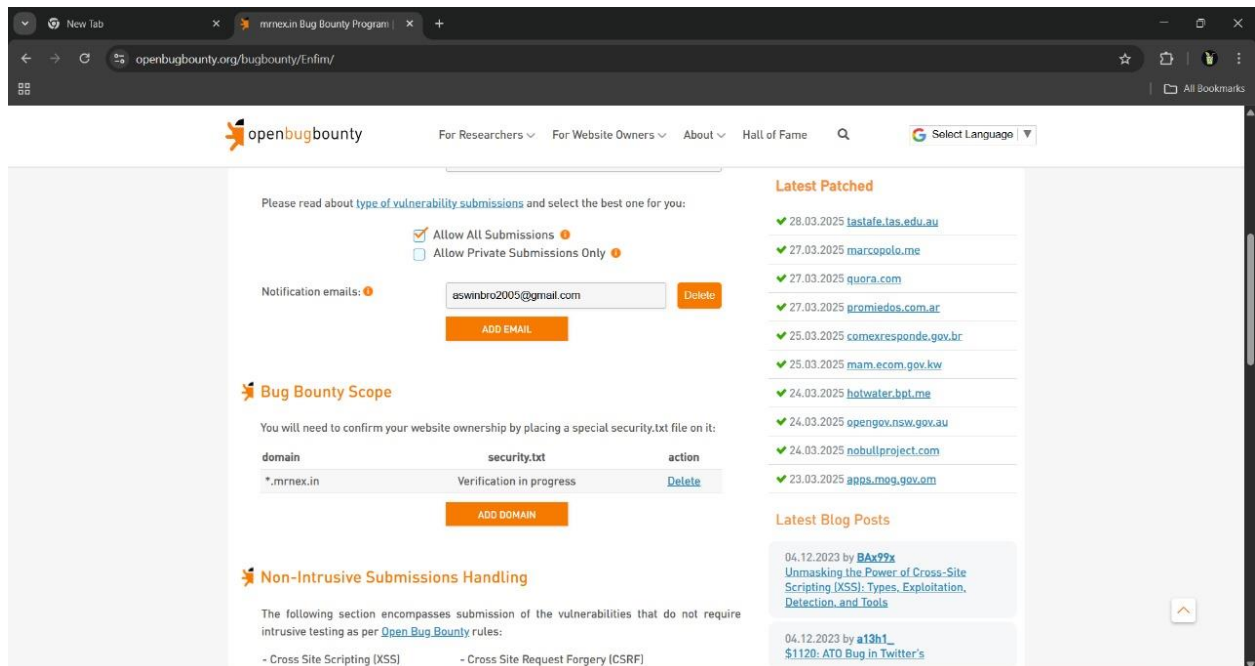
- Contact:** [description]  
ioetshortz2005@gmail.com
- Encryption:** [description]  
no pgp key available. Send the reports via email privately
- Acknowledgements:** [description]  
will be acknowledged publically on the website
- Policy:** [description]  
anything is good just avoid any harm causing elements ddos or data leaks
- Signature:** [description]  
Mr.Nex
- Hiring:** [description]  
na
- OpenBugBounty:**  
https://openbugbounty.org/bugbounty/Enfirm/

The bottom screenshot also shows a Windows taskbar at the bottom with the date 3/29/2025 and time 7:09 PM. A McAfee WebAdvisor notification is visible in the bottom right corner of the browser window.

Step3:I have found vulnerable in mrnex.in website which has some security.txt file problem



STEP 4: NOW WE NEED TO REPORT THE VULNERABILITY.



## STEP 5: NOW THE ABOVE VULNERABLE WILL BE PROCESSES AND IT SHOWS AS SUCCEED

The screenshot displays the Open Bug Bounty website interface. The browser's address bar shows the URL `openbugbounty.org/reports/4040355/`. The page features a navigation bar with links for 'For Researchers', 'For Website Owners', 'About', and 'Hall of Fame', along with a search icon and a language selector.

### Coordinated Disclosure Timeline

Vulnerability Reported:	26 March, 2025 13:35 GMT
Vulnerability Verified:	26 March, 2025 13:42 GMT
Website Operator Notified:	26 March, 2025 13:42 GMT
<ul style="list-style-type: none"><li>a. Using the ISO 29147 guidelines ✓</li><li>b. Using publicly available security contacts ✓</li><li>c. Using Open Bug Bounty notification framework ✓</li><li>d. Using security contacts provided by the researcher ✓</li><li>x. Using Twitter notification ✓</li></ul>	
Public Report Published [without technical details]:	26 March, 2025 13:42 GMT
Vulnerability Fixed:	27 March, 2025 19:54 GMT
Scheduled Public Disclosure:	25 April, 2025 13:35 GMT

### For Website Operators and Owners

Please read how Open Bug Bounty [helps make your websites secure](#) and then [contact the researcher](#) directly to get the vulnerability details. The researcher may also help you fix the vulnerability and advice on how to prevent similar issues:

SECURITY RESEARCHER

OPEN BUG BOUNTY

OPEN BUG BOUNTY

WEBSITE OWNER

SECURITY RESEARCHER

SECURITY RESEARCHER

Recent Recommendations

- 28 March, 2025**  
**marcop:**  
yoksuz assisted us in finding a XSS vulnerability on one of our search pages that wasn't picked up by our automated tooling. He was professional over email and was able to demonstrate the issue for us. Thanks yoksuz!
- 25 March, 2025**  
**BugFixer:**  
Hatim did great job on reporting an XSS bug. His security report was very thorough. Big thanks and recommending!

T.HARIVISHALINI