GUVI

Security Testing Policy

This policy outlines when and how one may conduct security testing on any Product of GUVI, including vulnerability and penetration testing.

We will engage with you as external security researchers (The Researcher) when the vulnerabilities are reported to us in accordance with this “Security Policy”.

If a Researcher follows the rules set out in this Security Testing Policy when reporting a security vulnerability to us, unless prescribed otherwise by law or the payment scheme rules, we commit to:

- promptly acknowledging receipt of your vulnerability report and work with the researcher to understand and attempt to resolve the issue quickly.
- validating, responding and fixing such vulnerability in accordance with our commitment to security and privacy. We will notify you when the issue is fixed.
- not suspend or terminate access to our platform if you are a Student/Learner.

Purpose

The goals of the policy such as ensuring web application vulnerabilities are analyzed on a periodic and consistent basis in order to reduce the security threat to our customers.

Rules of Engagement

The following rules apply to the penetration and vulnerability testing:

1. Your testing must not target any of the customers or learners of our platform.
2. You are strictly prohibited from using automated tools and any POC submitted to us should have a proper step-by-step guide to reproduce the issue.
3. Abuse or Sharing of any of the vulnerabilities found shall be liable for legal actions.
4. You are strictly prohibited for the usage of the tools such as Denial of Service Attacks (DOS) or Simulation of such, or any “Load Testing”.

SCOPE

Any POC submitted to us should have a step by step guide to reproduce the same issue,

1. Able to bypass the login flow.
2. SQL injections.
3. Remote Code Execution Vulnerabilities.
4. Shell Upload Vulnerabilities. (Use the script to just print some string But anything more that is not permitted).
5. Stored XSS.
6. Bulk Sensitive user data leak.

DOMAINS

- https://www.guvi.in/
- https://www.guvi.io/
- *.guvi.in
- *.guvi.io
- And any subdomains of GUVI.

OUT OF SCOPE

Login and Session Related,

1. Login page bruteforce not enforced.
2. Lack of Captcha.
3. Sessions Related vulnerability.

System Related,

1. Network Issues.
2. Password complexity.
3. Email Related such as, Email Bombs, Unsubscribing from marketing emails.
4. Information Leakage such as HTTP pages with 404 and any Directory known to the public.

General,

1. Any services hosted by 3rd party providers and services not provided by GUVI.
2. Any service that is not mentioned in the In Scope domains section.
3. Duplicate submissions in any of the pages.
4. Known issues.
5. Rate limiting (Unless it implies severe threat to data and user).
6. Clickjacking and issues only exploitable through clickjacking.
7. Issues without clearly identified security impact such as missing security headers.
8. Open redirects.
9. Multiple reports for the same vulnerability type with minor differences (only one will be rewarded).

TESTING

A Researcher can test only against a student account if they are an account owner to conduct such testing.

As a Researcher, in no event are you permitted to access, download or modify data residing in any other account or that does not belong to you or attempt to do any such activities.

The following test types are expressly excluded from scope and testing: any findings from physical testing (office access, tailgating, open doors) or DOS or DDOS vulnerabilities. A responsible disclosure also does not include identifying any spelling mistakes, or any UI and UX bugs.

RULES

We require that all Researchers must:

- Make every effort to avoid privacy violations, degradation of user or merchant experience, disruption to production systems, and destruction of data during security testing.
- Not attempt to gain access to any other persons account, data or personal information.

- Use their real email address to signup and report any vulnerability information to us.
- Keep information about any vulnerabilities you've discovered confidential between yourself and GUVI. Respected Team will take a reasonable time to remedy such vulnerability (approximately 1 month as a minimum but this is dependent on the nature of the security vulnerability and regulatory compliance by GUVI). The Researcher shall not publicly disclose the bug or vulnerability on any online or physical platform before it is fixed and prior written approval to publicly disclose from GUVI.
- Not perform any attack that could harm the reliability, integrity and capacity of our Services. DDoS/spam attacks are STRICTLY not allowed.
- **Remember that you must never attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.**

Please include the following information with your report:

- Detailed description of the steps required to help us reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us)
- Your email address.

Report Template:

The identified bug shall have to be reported to our security team by sending us a mail from their registered email address to reach@guvi.in (SUBJECT: SUSPECTED VULNERABILITY ON {Domain}) (without changing the subject line else the mail shall be ignored and not eligible for bounty). The mail should strictly follow the format below:

Tester's Detail :

Name :

Mobile Number:

Any Publicly Identifiable profile(LinkedIn):

Bug Details:

Name of Vulnerability:

Areas Affected :

Impact of Vulnerability:

Detailed steps to reproduce (With Documentation):

RECOGNITION

- By helping GUVI continuously keep our data secure, once the vulnerability is verified and fixed as a result of a report, we would provide monetary compensation or we would like to put your name in the Hall of Fame page.
- Please Note that the monetary compensation we provide will be based on our decision, and any request or demand will be ignored.
- And any vulnerability that doesn't affect our users or learners or branding of GUVI wont be considered for monetary compensation.

PUBLIC DISCLOSURE POLICY:

By default, this program is in "*PUBLIC NONDISCLOSURE*" mode which means:

"THIS PROGRAM DOES NOT ALLOW PUBLIC DISCLOSURE. ONE SHOULD NOT RELEASE THE INFORMATION ABOUT VULNERABILITIES FOUND IN THIS PROGRAM TO PUBLIC, FAILING WHICH SHALL BE LIABLE FOR LEGAL PENALTIES!"

NOTE:

We may modify the terms of this program or terminate this program at any time. GUVI employees and their family members are not eligible for bounties.