NOTE:

- If multiple submissions indicate a general pattern of weakness, only the first report that clearly establish the pattern will be eligible for a full bounty
- Rewards are tier-dependent, but final amounts are based on the CVSS score and at the discretion of the Eternal Security Team
- Public disclosure of the vulnerability prior to resolution will result in disqualification from the program.

Disclosure Policy

- Let us know as soon as possible upon discovery of a potential security issue, and we'll make every effort to quickly resolve the issue.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with the explicit permission of the account holder.
- Provide us a reasonable amount of time to resolve the issue before any disclosure to the public or a third-party

Test Plan

Please include a header `WITH YOUR USERNAME OR NAME e.g Defcomm bug bounty: (username)` when you test so we can identify your requests easily

In-scope vulnerabilities

- APIs
- Web app
- Servers
- Devices

Below, you can find examples of vulnerabilities and their impacts grouped by our severity ranking. This is not an exhaustive list and it is designed to give you insight on how we rate vulnerabilities.

Critical

- Remote Code Execution (RCE) - able to execute arbitrary commands on a remote device
- SQL Injection - able to read Personally Identifiable Information (PII) or other sensitive data / full read/write access to a database
- Server-Side Request Forgery (SSRF) - able to pivot to internal application and/or access credentials (not blind)
- Information Disclosure - mass PII leaks including data such as names, emails, phone numbers and addresses (Combined)

High

- Stored Cross-Site Scripting (XSS) - stored XSS with access to non HttpOnly cookies
- Information Disclosure - leaked credentials
- Subdomain Takeover - If a proper PoC is provided that can demonstrate an attacker getting access to confidential user data and able to perform unauthorized operations without leveraging phishing attack vectors.
- Cross-Site Request Forgery (CSRF) - leading to account takeover
- Account Takeover (ATO) - with no or minimal user interaction
- Insecure Direct Object Reference (IDOR) - read or write access to sensitive data or important fields that you do not have permission to
- SQL Injection - able to perform queries with a limited access user

Medium

- CSRF - able to modify important information (authenticated)
- ATO - required user interaction
- IDOR - write access to modify objects that you do not have permission to
- XSS - reflected/DOM XSS with access to cookies

Low

- Directory listings
- XSS - Without access to cookies/Auth Data
- XSS - POST based XSS (with CSRF bypass)
- Lack of HTTPS on dynamic pages (judged on a case-by-case basis)
- Server information page (no credentials)
- Subdomain Takeover - on an unused subdomain

Informative Bugs

- Broken Link Hijacking issues are categorized as low severity and are not eligible for rewards.
- Credential leakage reports are considered informational if two-factor authentication (2FA) is in place
- SSL Pinning/Root Detection Bypass
- Able to retrieve user's public information

Out of scope vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug. The following issues are considered out of scope:

- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Google Maps API Keys Leakage
- Missing best practices in SSL/TLS configuration.
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Missing best practices in Content Security Policy.

- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Public Zero-day vulnerabilities that have had an official patch for less than 1 month will be awarded on a case by case basis.
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Any activity that could lead to the disruption of our service (DoS).
- Rate limiting or bruteforce issues on non-authentication endpoints and our external Help Desk forums
- Removing all organization owners from the organization (or demoting all users to a "basic user" role)
- Creating an organization with the same name as an existing organization