YogOsha

Vulnerability Disclosure Program Policies

September 2022

Description :

The Client encourages hunters to work with us on potential issues in their services or their website. This policy outlines how the Client will coordinate the management of the potential discovered vulnerabilities using Yogosha's services and platform, vulnerabilities that if exploited may have an impact on the confidentiality, integrity or availability of their services, servers, applications or data.

Non-Qualifying Vulnerabilities (a.k.a Out of Scope) :

Any domain not contained within the Client is out of scope for the purposes of the Vulnerability Disclosure Program.

The following actions do not qualify for disclosure and should not be tested by hunters participating in the Program:

- DoS or DDoS attacks
- Physical Attacks against the Client properties or data centers
- Phishing and Social Engineering Attacks
- Missing http security headers which do not lead to a vulnerability (you must deliver a proof of concept that leverages their absence)
- Vulnerabilities in third-party applications or services which use or integrate with the Client services and applications.
- Reports from automated tools or scans without an exploitation proof of concept
- Missing cookie flags on non-sensitive cookies
- Reports of SSL best practices or insecure ciphers (unless you have a working proof of concept -- and not just a report from a scanner)

The Client will not accept reports from automated vulnerability scanners hence aggressive scans are not tolerated to avoid services disturbance.

Qualifying Vulnerabilities :

The Client will accept a report of any vulnerability that substantially affects the confidentiality, integrity or availability of any eligible Client service. Eligible vulnerabilities include, but are not limited to:

- Cross Site Scripting (XSS)

- Authentication and Authorization Flaws
- Cross Site Request Forgery (CSRF)
- Remote Code Execution
- SQL Injection
- Directory Traversal
- Privilege Escalation

Best Practises When Reporting :

1. The more detailed your steps for reproducing the bug, the better. This should include any pages that you visited, user IDs, links clicked, etc.
2. Images are always useful
3. Exploit POC code that consistently works can allow us to verify your vulnerability more quickly.
4. Remember – details, details, details! which permits us and you to gain time by triaging the vulnerability quicker.

Rewards :

According to the finding report, if the vulnerability is valid and has an impact on the Client’s assets, the Client may be willing to show their appreciation by rewarding the hunter. Rewards, at their own discretion, can vary from goodies, hall of fame and to monetary rewards according to the vulnerability severity and exploitability.

Confidentiality :

Any information that you collect about the Client, the Client employees, or the Client customers (“Confidential Information”) through the Vulnerability Disclosure Program must be kept confidential and may only be used in connection with the Program. You may disclose vulnerabilities only after proper remediation has occurred and you may not disclose Confidential Information without the Client’s prior written consent. Any disclosure of Confidential Information outside of this requirement will result in immediate legal proceedings.

Legal :

By participating in the Client‘s Vulnerability Disclosure Program, you acknowledge that you have read and agree to Yogosha’s Terms and Conditions.

Your testing must not violate any law, disrupt services, or compromise any data that is not your own.

You commit to abide by the applicable regulations in terms of personal data protection, in particular the Regulation (EU) 2016/679 from the 27th April 2016 (General regulations on data protection) (the “GDPR”) as well as the Law n°78-17 from the 6th January 1978 relative to data, files and liberties, such as it has been successively modified.

<u>Disclaimer :</u>

Yogosha acts only as an intermediary between the bug hunter and the Client.

Therefore we are not responsible for any direct or indirect damage to the vulnerability hunter, the client or any third party involved in the process. Also Yogosha does not take part in estimating the rewards nor pre-triaging or triaging the vulnerability reports.