Issio Solutions Vulnerability Disclosure Policy v1.0

This Vulnerability Disclosure Policy applies to any vulnerabilities that are reported using the security.txt file found at **https://www.issio.net/.well-known/security.txt**

Please read the this policy before reporting vulnerabilities and proceed in full compliance.

Reporting

Please compile and submit as much technical information as possible, including steps to reproduce and validate the issue.

Please allow up to 5 business days for confirmation of the reported issue.

Please wait until notified that the vulnerability has been resolved before disclosing it to others. We take the security of our customers very seriously, however some vulnerabilities take longer than others to resolve.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Guidelines for Responsible Disclosure Program

Please do NOT:

- Cause potential or actual damage to Issio Information System users, systems or applications.
- Use an exploit to view unauthorized data or corrupt data.
- Test third party services
- Engage in disruptive testing like DoS or any action that could impact the confidentiality, integrity or availability of information and systems
- Engage in social engineering or phishing of customers or employees
- Request for compensation for time and materials or vulnerabilities discovered

Out of Scope Vulnerabilities:

- Account/e-mail enumeration using brute-force attacks
    - Valid user account/email enumeration not requiring brute-force will be considered
- Any low impact issues related to session management (i.e. concurrent sessions, session expiration, password reset/change log out, etc.)
- Bypassing content restrictions in uploading a file without proving the file was received

- Clickjacking/UI redressing
- Client-side application/browser autocomplete or saved password/credentials
- Descriptive or verbose error pages without proof of exploitability or obtaining sensitive information
- Directory structure enumeration (unless the fact reveals exceptionally useful information)
- Incomplete or missing SPF/DMARC/DKIM records
- Issues related to password/credential strength, length, lockouts, or lack of brute-force/rate limiting protections
  - Account compromises (especially admin) as a result of these issues will likely be considered VALID
- Lack of SSL or Mixed content
  - Leaking Session Cookies, User Credentials, or other sensitive data will be reviewed on a case by case basis
  - If leaking of sensitive data requires MiTM positioning to exploit, it will be considered out of scope
- Login/Logout/Unauthenticated/Low-impact CSRF
  - CSRF Vulnerabilities may be acceptable if they are of higher impact. Examples of low impact CSRF include: Add/Delete from Cart, Add/remove wishlist/favorites, Nonsevere preference options, etc.
- Low impact Information disclosures (including Software version disclosure)
- Missing Cookie flags
- Missing/Enabled HTTP Headers/Methods which do not lead directly to a security vulnerability
- Reflected file download attacks (RFD)
- Self-exploitation (i.e. password reset links or cookie reuse)
- SSL/TLS best practices that do not contain a fully functional proof of concept
- URL/Open Redirection
- Use of a known-vulnerable library which leads to a low-impact vulnerability (i.e. jQuery outdated version leads to low impact XSS)
- Valid bugs or best practice issues that are not directly related to the security posture of the client
- Vulnerabilities affecting users of outdated browsers, plugins or platforms

- Vulnerabilities that allow for the injection of arbitrary text without allowing for hyperlinks, HTML, or JavaScript code to be injected
- Vulnerabilities that require the user/victim to perform extremely unlikely actions (i.e. Self-XSS)
    - Self-XSS for a Persistent/Stored XSS will be considered. Please review the Self-XSS article for more information.
    - Any type of XSS that requires a victim to press an unlikely key combination is NOT in scope (i.e. alt+shift+x for payload execution)
- Additional specific vulnerability types considered out of scope due to low impact:
    - IIS Tilde File and Directory Disclosure
    - SSH Username Enumeration
    - Wordpress Username Enumeration
    - SSL Weak Ciphers/ POODLE
    - CSV Injection
    - PHP Info
    - Server-Status if it does not reveal sensitive information
    - Snoop Info Disclosures

Accepted Web Vulnerabilities:

- OWASP Top 10 vulnerability categories
- Other vulnerabilities with demonstrated impact