iSignthis®

# iSignthis Security Bug Bounty Program

## PURPOSE OF PROGRAM

The purpose of this program is to discover any vulnerabilities that may exist in the iSignthis payment and/or identity services and provide End Users the most secure service possible.

## ELIGIBILITY

Vulnerabilities are limited to those discovered in the following domains:

www.verify.iSignthis.com or
www.dashboard.isignthis.com or
our embedded iFrames in our merchant's websites

Program participants may not perform the following actions:

(a) Using a discovered vulnerability to view, delete, alter, or publish user data;
(b) Using an automated vulnerability scanner to launch attacks against iSignthis systems.

Participants who perform any of these actions will be disqualified from receiving reward money.

## CONDITIONS FOR PARTICIPATION

To be eligible for participating into the Bug Bounty Program, a participant must not:

a. be less than 18 years of age;
b. be an employee of the Company or an affiliated company, or of any of our merchants or partners;
c. be an immediate family member of a person employed by iSignthis or its affiliates;
d. be an entity or part of an entity that had carried out or is carrying out a project that is being advanced with the Company;
e. be able to communicate in standard English;
f. not reside in a country subject to Australian or EU economic sanctions at the time of reward payment for the Program.

If iSignthis discovers that you meet any of the above conditions, iSignthis will remove you immediately from the Bug Bounty Program and disqualify you from receiving any bounty payments.

## REWARDS

| Vulnerability | Description | Example |
|---|---|---|
| SQL Injection | Ability to access private information through an SQL injection attack | AUD$ 3,000 |
| Cross-Site Scripting (XSS) | Ability to hijack a session or execute scripts through an XSS attack | AUD$ 500 |
| Cross-Site Request Forgery (CSRF) | Ability to force a iSignthis user to perform an undesired process through a CSRF attack | AUD$ 500 |
| Remote Code Execution | Ability to send packets containing arbitrary code to the client or server side | AUD$ 10,000 |
| Authentication Bypass | Ability to masquerade as another person by bypassing authentication procedures | AUD$ 5,000 |
| Purchase Bypass | Ability to obtain items while bypassing in-app payment procedures | AUD$ 5,000 |
| Encryption Break | Ability to obtain another person's authentication information or personal information by cracking encrypted data | AUD$ 10,000 |
| Other | Other vulnerabilities | AUD$ 500 |

## VULNERABILITIES NOT ELIGIBLE FOR REWARDS

In general, the following are not considered eligible for rewards:

- Logout CSRF
- Our policies on presence/absence of SPF/DMARC records
- Missing autocomplete attributes
- Self-XSS (we require evidence on how the XSS can be used to attack another End user)
- Use of a known-vulnerable library (without evidence of exploitability)
- Social engineering
- Missing cookie flags on non-sensitive cookies
- Reports from automated tools or scans
- HTML Injection
- Hosting malware/arbitrary content on iSignthis sites
- Issues located within third party components
- Denial of service attacks

Further examples of vulnerabilities not eligible for cash rewards are listed below.

(1) Reporting a vulnerability as-is after detection using an automated scanner

(2) Reporting hypothetical or theoretical vulnerabilities without actual verification code
(3) Reporting susceptibility to a denial-of-service attack
(4) Reporting susceptibility to brute force attacks aimed at retrieving passwords or tokens
(5) Reporting the ability to spam iSignthis End Users arbitrarily with spam messages
(6) Reporting email verification deficiencies, expiration of password reset links, and password complexity policies
(7) Reporting on the absence of CRSF tokens
(8) Reporting login/logout CSRF
(9) Reporting the susceptibility to an attack via physical access to a user's device
(10) Reporting on missing security headers
(11) Reporting on script executions that do not affect iSignthis End Users
(12) Reporting vulnerabilities found in areas other than the iSignthis verify websites:

> Ex 1: Reporting vulnerabilities found in domains other than those nominated above.
> Ex 2: Reporting vulnerabilities found on platforms other than Windows, MacOS, iOS or Android
> Ex 3: Reporting vulnerabilities found in iSignthis related apps or websites, including those of our partners or merchants

(13) Reporting vulnerabilities attributable to out-of-date browsers or platforms
(14) Reporting vulnerabilities related to auto fill web forms
(15) Reporting the absence of secure flag attributes for non-critical cookies
(16) Reports related to unsafe SSL/TLS cipher suites or protocol version
(17) Reporting the accessibility of user data via a rooting device
(18) Reporting the accessibility of profile photos, Timeline photos, and other information by anyone via URL
(19) Reporting vulnerabilities attributable to a virtual phone number
(20) Reporting vulnerabilities of which ISIGNTHIS has already received a report, ISIGNTHIS is already aware, or which has already been made public
(21) Reporting vulnerabilities related to server banner information
(22) Reporting vulnerabilities related to information contained within error messages (stack trace, application, or server errors)
(23) Reporting vulnerabilities related to unset values for SPF record, DMARC, and DKIM
(24) Reporting vulnerabilities which enable the use of an illegal HTTP method
(25) Reporting vulnerabilities related to clickjacking

However, iSignthis may deem additional cases eligible for the cash reward at its own discretion.

## REPORTING AND REVIEW

Please describe the bug or vulnerability, and the circumstances under which it arises.

a) Your full name and contact details, including email and phone.
b) Please provide a detailed technical description of the vulnerability.
c) Please describe the steps to reproduce. If a special environment is required, please also describe the procedure to build the environment.
d) Please describe the attack scenarios. When exploiting the vulnerability, please describe the vulnerability and its impact to our services or End Users.
e) Please advise any countermeasures.
f) Other details that may be helpful in our assessing the vulnerability.

Please submit to info@isignthis.com
The participant should not publicly disclose the findings or the contents of the submitted report in any way.

Failure to follow the above described procedure of report and/or the above terms, will result in immediate disqualification from the Bug Bounty Program and ineligibility for receiving any bounty payment.

## NOTES REGARDING REPORTING AND REVIEWS

Vulnerability reviews are conducted according to standards established by iSignthis.

a) If the vulnerability is recognized, the submitter will be contacted by e-mail. We will require that you identify yourself fully via our identity process.
b) Vulnerabilities of which the company is already aware shall not be eligible for review.
c) If a report on a vulnerability is received while we are already in the process of reviewing a separate report on the same vulnerability, we will recognize the first report submitted.
d) Furthermore, multiple vulnerabilities will be treated as a single vulnerability when:
e) the same vulnerability can be exploited under multiple parameters through a single method,
f) the same vulnerability exists for a method that runs across multiple domains.
g) After a vulnerability is recognized, in addition to receiving a cash reward, the submitter will, with their permission, have their name (or nickname) posted along with the discovered vulnerability to the Hall of Fame to be published soon.

## BOUNTY PAYMENTS

Provided that the participant is (i) the first person to submit a vulnerability eligible for reward, (ii) the vulnerability has been recognized as such by iSignthis's team and (iii) the participant has complied with all the above Program Terms, then the participant may be eligible to receive a monetary reward, or 'bounty'.

Bounty payments, if any, will be determined by iSignthis, in iSignthis's sole discretion. In no event shall iSignthis be obligated to pay you a bounty for merely submitting a report.

In the event iSignthis team has confirmed that a participant is eligible for a bounty, ISignthis may proceed with the payment. The format and timing of all bounty payments shall be determined in iSignthis's sole discretion.

All bounty payments will be made in Australian dollars (AUD). The participant will be responsible for any tax implications related to bounty payments that receive, as determined by the laws of participant's jurisdiction of residence or citizenship.

All determinations as to the amount of a bounty made by iSignthis team are final.

## CHANGES TO iSignthis SECURITY BUG BOUNTY PROGRAM

The Bug Bounty Program, may be subject to change or cancellation by iSignthis at any time, without notice. iSignthis may amend any of the above Terms and/or Conditions at any time by posting a revised version on its website. By continuing to participate in the Bug Bounty Program after iSignthis posts any such changes, participants accept the Program Terms and/or Conditions, as modified.