DOO FINANCIAL

GLOBAL PARTNER

Vulnerability Disclosure Policy

Doo Financial Australia Limited

1. Introduction

1.1 Doo Financial Australia Limited (hereinafter "**Doo Financial**") recognizes the need to approach the cybersecurity community to protect customer data and work together to create more secure solutions and applications. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

1.2 Researchers are welcome to voluntarily report vulnerabilities they can find connected to Doo Financial's systems. This policy describes what systems and types of research are covered under this policy and how to submit vulnerability reports to us.

1.3 The submission of vulnerability reports is subject to the terms and conditions set forth on this page, and by submitting a vulnerability report to Doo Financial the researchers acknowledge that they have read and agreed to these terms and conditions.

2. Terms and Conditions

2.1 Safe Harbor / Authorisation

2.1.1 In order to maintain the integrity and security of Doo Financial's services, **prior written authorization from Doo Financial must first have been obtained** before conducting any vulnerability research and/or security testing activities.

2.1.2 When conducting vulnerability research, showing good faith effort to comply with this policy, we consider your research to be:

- Authorised concerning any applicable anti-hacking laws and we will not recommend or pursue legal action against you for your research.
- Authorised concerning any relevant anti-circumvention laws and we will not bring a claim against you for circumvention of technology controls.
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

2.1.3 You are expected to comply with all applicable laws. If legal action is initiated by a third party against you for activities that you have conducted in good faith in accordance with this policy, we will make this authorisation known.

2.1.4 If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels (as determined herein below) before going any further.

2.1.5 Note that the Safe Harbor applies only to legal claims under the control of the organisation participating in this policy, and that the policy does not bind independent third parties.

2.2 Guidelines

2.2.1 Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.

2.2.2 You are also requested to:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail.
- Only interact with your own test accounts.
- Limit account creation to two (2) accounts total for any testing.
- Use only the Official Channels to disclose and/or discuss vulnerability information with us.
- Submit one vulnerability per report, unless you need to chain vulnerabilities to demonstrate the impact.
- Securely delete all data retrieved during research once the report is submitted.
- Perform testing only on in-scope systems, and respect systems and activities which are out of scope.
- Avoid using high-intensity invasive or automated scanning tools to find vulnerabilities.
- Do not publicly disclose any vulnerability without Doo Financial's prior written consent.
- Do not perform any "Denial of Service" attack.
- Do not perform social engineering and/or physical security attacks against Doo Financial's offices, users, and/or employees.
- Do not perform automated/scripted testing of web forms, especially "Contact Us" forms that are designed for customers to contact our support team.

2.2.3 Once you've established that a vulnerability exists or you unintendedly encounter any sensitive data (including personally identifiable information ("PII"), financial information, proprietary information, or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**. You should also limit your access to the minimum data required for effectively demonstrating proof of concept.

2.3 Obtaining Authorization / Reporting a Vulnerability / Official Channels

2.3.1 Please obtain the prior written authorization from Doo Financial before conducting any vulnerability research and/or security testing activities via security.cloud@doo.com, providing all relevant information including but not limited to:

- Systems or components you intend to test
- Testing methodologies
- Proposed timeline
- Contact information

Doo Financial will review your request and respond accordingly.

2.3.2 Please report security issues / actual or potential vulnerability findings via security.cloud@doo.com, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

2.3.3 To help us triage and prioritise submissions, we recommend that your reports:

- Describe the location or application path where the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof-of-concept scripts or screenshots are helpful).
- Include as many details as possible.
- Include the IP address that you were testing from, the email address, user-agent and username(s) used in the trading platform (if any).
- Be in English, if possible.

2.4 Scope

2.4.1 This policy applies to:

- Public-facing systems and services owned or operated by Doo Financial
- Web applications, APIs, and mobile applications developed by Doo Financial
- Infrastructure and cloud assets under our control

2.4.2 Out-of-Scope Systems / Services

- Denial of Service (DoS) vulnerabilities
- Social engineering or phishing attacks
- Physical security vulnerabilities
- Spam or content-related issues
- **Any service (such as connected services), system, or domain not expressly listed in Clause 2.4.1 above, are excluded from scope** and are not authorised for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you are not sure whether a system is in scope or not, contact us at security.cloud@doo.com.

2.4.3 In-Scope Vulnerabilities

- SQL Injection
- Cross-Site Scripting (XSS)
- Remote code execution (RCE)
- Server-Side Request Forgery (SSRF)
- Broken authentication and session management
- Insecure Direct Object Reference (IDOR)
- Sensitive data exposure
- Directory/Path traversal
- Local/Remote File Inclusion
- Cross-Site Request Forgery (CSRF) with demonstrable high impact
- Open redirect on sensitive parameters
- Subdomain takeover (for subdomain takeover add a friendly message like: "We are working on it and we will be back soon.")

2.4.4 Our-of-Scope Vulnerabilities: Certain vulnerabilities are considered out-of-scope for the Vulnerability Disclosure Program. Those out-of-scope vulnerabilities include, but are not limited to:

- Mail configuration issues including SPF, DKIM, DMARC settings
- Clickjacking vulnerabilities that do not lead to sensitive actions, such as account modification
- Self-XSS (i.e., where a user would need to be tricked into pasting code into their web browser)
- Content spoofing where the resulting impact is minimal (e.g., non-HTML text injection)
- Cross-Site Request Forgery (CSRF) where the resulting impact is minimal (e.g., CSRF in login or logout forms)
- Open redirect - unless an additional security impact can be demonstrated
- CRLF attacks where the resulting impact is minimal
- Host header injection where the resulting impact is minimal
- Missing HttpOnly or Secure flags on non-sensitive cookies
- Missing best practices in SSL/TLS configuration and ciphers
- Missing or misconfigured HTTP security headers (e.g., CSP, HSTS)
- Forms missing Captcha controls

- Username/email enumeration via Login Page error message
- Username/email enumeration via Forgot Password error message
- Issues that require unlikely user interaction
- Password complexity or any other issue related to account or password policies
- Lack of session timeout
- Brute-force attacks
- Rate limit issues for non-critical actions
- WordPress vulnerabilities without proof of exploitability
- Vulnerable software version disclosure without proof of exploitability
- Any activity that could lead to the disruption of our service (DoS)
- Lack of Root protection / Bypass of Root protection (mobile applications)
- Lack of SSL certificate pinning / Bypass of SSL certificate pinning (mobile applications)
- Lack of code obfuscation (mobile applications)

2.5 Response Time

2.5.1 Doo Financial is committed to coordinating with you as openly and as quickly as possible and will make best efforts to meet the following response targets for researchers participating in our program:

- Time to first response (from day of submission of the report) is five (5) days. Within five business days, we will acknowledge that your report has been received.
- Time to triage (from report submission) is five (5) days.

2.5.2 To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, as well as issues or challenges that may delay resolution. We'll try to keep you informed about our progress throughout the process.

3. Feedback

3.1 If you wish to provide feedback or suggestions on this policy, please contact us at security.cloud@doo.com.

(The rest of this page has been intentionally left blank.)