DOO FINANCIAL

GLOBAL PARTNER

Kebijakan Pengungkapan Kerentanan
Vulnerability Disclosure Policy

PT. Doo Financial Futures

1.	**Perkenalan**	***1.***	***Introduction***
1.1	PT Doo Financial Futures (selanjutnya disebut " **Doo Financial** ") menyadari perlunya mendekati komunitas keamanan siber untuk melindungi data pelanggan dan bekerja sama untuk menciptakan solusi dan aplikasi yang lebih aman. Kebijakan ini dimaksudkan untuk memberikan pedoman yang jelas kepada peneliti keamanan untuk melakukan aktivitas penemuan kerentanan dan untuk menyampaikan preferensi kami dalam cara menyampaikan kerentanan yang ditemukan kepada kami .	*1.1*	*PT Doo Financial Futures (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	Peneliti dipersilakan untuk melaporkan secara sukarela kerentanan yang mereka temukan terkait dengan sistem Doo Financial . Kebijakan ini menjelaskan sistem dan jenis penelitian apa saja yang tercakup dalam kebijakan ini dan cara mengirimkan laporan kerentanan kepada kami .	*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	Pengiriman laporan kerentanan tunduk pada syarat dan ketentuan yang ditetapkan di halaman ini, dan dengan mengirimkan laporan kerentanan kepada Doo Financial, peneliti mengakui bahwa mereka telah membaca dan menyetujui syarat dan ketentuan ini.	*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.	**Syarat dan Ketentuan**	***2.***	***Terms and Conditions***
2.1	**Safe Harbor / Otorisasi**	***2.1***	***Safe Harbor / Authorisation***
2.1.1	Untuk menjaga integritas dan keamanan layanan Doo Financial , otorisasi tertulis **sebelumnya dari Doo Financial harus diperoleh terlebih dahulu** sebelum melakukan aktivitas penelitian kerentanan dan/atau pengujian keamanan.	*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	Saat melakukan penelitian kerentanan, menunjukkan upaya itikad baik untuk mematuhi kebijakan ini, kami menganggap penelitian Anda: • Diotorisasi terkait dengan undang-undang antiperetasan yang berlaku dan kami tidak akan	*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*

merekomendasikan atau melakukan tindakan hukum terhadap Anda atas penelitian Anda. • Diotorisasi berkenaan dengan undang-undang anti-penghindaran yang relevan dan kami tidak akan mengajukan tuntutan terhadap Anda atas penghindaran kontrol teknologi. • Sah, membantu keamanan Internet secara keseluruhan, dan dilakukan dengan itikad baik.	*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 Anda diharapkan untuk mematuhi semua hukum yang berlaku. Jika tindakan hukum dilakukan oleh pihak ketiga terhadap Anda atas aktivitas yang Anda lakukan dengan itikad baik sesuai dengan kebijakan ini, kami akan memberitahukan otorisasi ini .	*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 Jika sewaktu-waktu Anda memiliki kekhawatiran atau tidak yakin apakah penelitian keamanan Anda konsisten dengan kebijakan ini, silakan kirimkan laporan melalui salah satu Saluran Resmi kami (sebagaimana ditentukan di bawah ini) sebelum melangkah lebih jauh.	*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 Perhatikan bahwa Safe Harbor hanya berlaku untuk klaim hukum di bawah kendali organisasi yang berpartisipasi dalam kebijakan ini, dan bahwa kebijakan tersebut tidak mengikat pihak ketiga yang independen.	*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 Pedoman	***2.2 Guidelines***
2.2.1 Berdasarkan kebijakan ini, “penelitian” berarti aktivitas di mana Anda: • Beritahu kami sesegera mungkin setelah Anda menemukan masalah keamanan nyata atau potensial. • Lakukan segala upaya untuk menghindari pelanggaran privasi, penurunan pengalaman pengguna, gangguan pada sistem produksi, dan penghancuran atau manipulasi data. • Gunakan eksploitasi hanya sejauh yang diperlukan untuk mengonfirmasi keberadaan	*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*

	kerentanan. Jangan gunakan eksploitasi untuk membahayakan atau mencuri data, membuat akses baris perintah yang persisten, atau menggunakan eksploitasi untuk beralih ke sistem lain.		*exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.*
2.2.2	Anda juga diminta untuk: • Patuhi aturan, termasuk mengikuti kebijakan ini dan perjanjian terkait lainnya. Jika terdapat ketidakkonsistenan antara kebijakan ini dan ketentuan lain yang berlaku, ketentuan kebijakan ini akan berlaku. • Hanya berinteraksi dengan akun pengujian Anda sendiri. • Batasi pembuatan akun hingga dua (2) akun total untuk pengujian apa pun. • Gunakan hanya Saluran Resmi untuk mengungkapkan dan/atau mendiskusikan informasi kerentanan dengan kami. • Kirimkan satu kerentanan per laporan, kecuali jika Anda perlu merantai kerentanan untuk menunjukkan dampaknya. • Hapus semua data yang diambil selama penelitian dengan aman setelah laporan diserahkan. • Lakukan pengujian hanya pada sistem yang masuk dalam cakupan, dan hormati sistem dan aktivitas yang berada di luar cakupan. • Hindari penggunaan alat pemindaian invasif atau otomatis berintensitas tinggi untuk menemukan kerentanan. • Jangan mengungkapkan kerentanan apa pun kepada publik tanpa izin Doo Financial persetujuan tertulis sebelumnya. • Jangan melakukan serangan "Penolakan Layanan" apa pun. • Jangan melakukan rekayasa sosial dan/atau serangan keamanan fisik terhadap kantor , pengguna, dan/ atau karyawan Doo Financial . • Jangan melakukan pengujian otomatis/berskrip pada formulir	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.*

web, terutama formulir "Hubungi Kami" yang dirancang bagi pelanggan untuk menghubungi tim dukungan kami .	
2.2.3 Setelah Anda memastikan bahwa kerentanan itu ada atau Anda secara tidak sengaja menemukan data sensitif apa pun (termasuk informasi identitas pribadi (“PII”) , informasi keuangan, informasi kepemilikan, atau rahasia dagang pihak mana pun), **Anda harus menghentikan pengujian, segera memberi tahu kami, dan tidak mengungkapkan data ini kepada siapa pun** . Anda juga harus membatasi akses Anda ke data minimum yang diperlukan untuk menunjukkan bukti konsep secara efektif.	*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 Memperoleh Otorisasi / Melaporkan Kerentanan / Saluran Resmi	***2.3 Obtaining Authorization / Reporting a Vulnerability / Official Channels***
2.3.1 Harap dapatkan otorisasi tertulis sebelumnya dari Doo Financial sebelum melakukan penelitian kerentanan dan/atau aktivitas pengujian keamanan melalui security.cloud@doo.com , dengan memberikan semua informasi relevan termasuk namun tidak terbatas pada: • Sistem atau komponen yang ingin Anda uji • Metodologi pengujian • Garis waktu yang diusulkan • Informasi kontak Doo Financial akan meninjau permintaan Anda dan menanggapinya sebagaimana mestinya.	*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 Harap laporkan masalah keamanan/temuan kerentanan aktual atau potensial melalui security.cloud@doo.com , dengan memberikan semua informasi yang relevan. Semakin banyak detail yang Anda berikan, semakin mudah bagi kami untuk memilah dan memperbaiki masalah.	*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 Untuk membantu kami memilah dan memprioritaskan kiriman, kami sarankan agar laporan Anda: • Jelaskan lokasi atau jalur aplikasi tempat kerentanan ditemukan dan dampak potensial eksploitasi. • Berikan deskripsi terperinci mengenai langkah-langkah yang diperlukan untuk mereproduksi kerentanan (skrip bukti konsep atau tangkapan layar akan sangat membantu). • Sertakan rincian sebanyak mungkin. • Sertakan alamat IP yang Anda uji, alamat email, agen pengguna, dan nama pengguna yang digunakan pada platform perdagangan (jika ada). • Jika memungkinkan, gunakan bahasa Inggris.	*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 Cakupan	***2.4 Scope***
2.4.1 Kebijakan ini berlaku untuk: • Sistem dan layanan yang menghadap publik yang dimiliki atau dioperasikan oleh Doo Financial • Aplikasi web, API, dan aplikasi seluler yang dikembangkan oleh Doo Financial • Infrastruktur dan aset cloud di bawah kendali kami	*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 Sistem / Layanan di Luar Cakupan • Kerentanan Penolakan Layanan (DoS) • Rekayasa sosial atau serangan phishing • Kerentanan keamanan fisik • Spam atau masalah terkait konten • **Layanan apa pun (seperti layanan terhubung), sistem, atau domain yang tidak secara tegas tercantum dalam Klausul 2.4.1 di atas, dikecualikan dari cakupan** dan tidak diizinkan untuk pengujian. Selain itu, kerentanan yang ditemukan dalam sistem dari vendor kami berada di luar cakupan kebijakan	*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*

ini dan harus dilaporkan langsung ke vendor sesuai dengan kebijakan pengungkapan mereka (jika ada). Jika Anda tidak yakin apakah suatu sistem berada dalam cakupan atau tidak, hubungi kami di security.cloud@doo.com .	*are not sure whether a system is in scope or not, contact us at security.cloud@doo.com.*
2.4.3 Kerentanan Dalam Cakupan • Injeksi SQL • Skrip Lintas Situs (XSS) • Eksekusi kode jarak jauh (RCE) • Pemalsuan Permintaan Sisi Server (SSRF) • Otentikasi dan manajemen sesi rusak • Referensi Objek Langsung yang Tidak Aman (IDOR) • Paparan data sensitif • Penelusuran Direktori/Jalur • Penyertaan File Lokal/Jarak Jauh • Pemalsuan Permintaan Lintas Situs (CSRF) dengan dampak tinggi yang dapat dibuktikan • Pengalihan terbuka pada parameter sensitif • Pengambilalihan subdomain (untuk pengambilalihan subdomain tambahkan pesan ramah seperti: "Kami sedang mengerjakannya dan kami akan segera kembali.")	*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 Luar Cakupan : Kerentanan tertentu dianggap berada di luar cakupan Program Pengungkapan Kerentanan. Kerentanan di luar cakupan tersebut meliputi, tetapi tidak terbatas pada: • Masalah konfigurasi email termasuk pengaturan SPF, DKIM, DMARC • Kerentanan clickjacking yang tidak mengarah pada tindakan sensitif, seperti modifikasi akun • Self-XSS (misalnya, di mana pengguna perlu ditipu agar menempelkan kode ke browser web mereka) • Pemalsuan konten yang dampaknya minimal (misalnya, injeksi teks non-HTML)	*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)*

• Pemalsuan Permintaan Lintas Situs (CSRF) yang dampaknya minimal (misalnya, CSRF dalam formulir masuk atau keluar) • Pengalihan terbuka - kecuali dampak keamanan tambahan dapat ditunjukkan • Serangan CRLF yang dampaknya minimal • Penyuntikan header host yang dampaknya minimal • HttpOnly atau Secure hilang pada cookie yang tidak sensitif • Hilangnya praktik terbaik dalam konfigurasi dan cipher SSL/TLS • Header keamanan HTTP hilang atau salah konfigurasi (misalnya, CSP, HSTS) • Formulir tidak memiliki kontrol Captcha • Pesan kesalahan pencacahan nama pengguna/email melalui Halaman Login • Enumerasi nama pengguna/email melalui pesan kesalahan Lupa Kata Sandi • Masalah yang memerlukan interaksi pengguna yang tidak mungkin • Kompleksitas kata sandi atau masalah lain yang terkait dengan kebijakan akun atau kata sandi • Kurangnya batas waktu sesi • Serangan brute-force • Masalah batas kecepatan untuk tindakan non-kritis • Kerentanan WordPress tanpa bukti eksploitasi • Pengungkapan versi perangkat lunak yang rentan tanpa bukti eksploitasi • Segala aktivitas yang dapat menyebabkan gangguan pada layanan kami (DoS) • Kurangnya perlindungan Root / Bypass perlindungan Root (aplikasi seluler) • Kurangnya penyematan sertifikat SSL / Bypass penyematan sertifikat SSL (aplikasi seluler) • Kurangnya pengaburan kode (aplikasi seluler)	• *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	**Waktu Respon**	***2.5***	***Response Time***
2.5.1	Doo Financial berkomitmen untuk berkoordinasi dengan Anda seterbuka dan secepat mungkin dan akan berupaya sebaik mungkin untuk memenuhi target respons berikut bagi para peneliti yang berpartisipasi dalam program kami: • Jangka waktu tanggapan pertama (sejak tanggal penyerahan laporan) adalah lima (5) hari. Dalam waktu lima hari kerja, kami akan memberi tahu bahwa laporan Anda telah diterima. • Waktu untuk triase (sejak penyerahan laporan) adalah lima (5) hari.	*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	Sebisa mungkin, kami akan mengonfirmasi keberadaan kerentanan tersebut kepada Anda dan bersikap setransparan mungkin tentang langkah-langkah yang kami ambil selama proses perbaikan, serta masalah atau tantangan yang dapat menunda penyelesaian. Kami akan berusaha terus memberi tahu Anda tentang kemajuan kami selama proses berlangsung.	*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.	**Masukan**	***3.***	***Feedback***
3.1	Jika Anda ingin memberikan umpan balik atau saran tentang kebijakan ini, silakan hubungi kami di security.cloud@doo.com .	*3.1*	*If you wish to provide feedback or suggestions on this policy, please contact us at security.cloud@doo.com.*

(Sisa halaman ini sengaja dikosongkan.)
(The rest of this page has been intentionally left blank.)