digiteal

REINVENTING INVOICING AND PAYMENT

Bug Bounty Program Policy

Introduction

Developers of hardwares and softwares often require time and resources to address vulnerabilities. Often, it is ethical hackers who find these vulnerabilities. Hackers and computer security researchers have the opinion that it is their social responsibility to make the public aware of vulnerabilities. Hiding problems could cause a feeling of false security. To avoid this, the involved parties coordinate and negotiate a reasonable period of time for repairing the vulnerability. Depending on the potential impact of the vulnerability, the expected time needed for an emergency fix or workaround to be developed and applied and other factors, this period may vary between a few days to several months.

Coordinated vulnerability disclosure may fail to satisfy security researchers who expect to be financially compensated. At the same time, reporting vulnerabilities with the expectation of compensation is viewed by some as extortion. While a market for vulnerabilities has developed, vulnerability commercialization (or "bug bounties") remains a hotly debated topic. Independent firms financially supporting coordinated vulnerability disclosure by paying bug bounties include Facebook, Google, and Barracuda Networks.

The Digiteal Security Bug Bounty Program is designed to encourage security research in Digiteal software and to reward those who help us make the internet a safer place.

Digiteal is committed to protecting our customers and their users. As part of this commitment, we invite security researchers to help protect Digiteal and its users by proactively identifying security vulnerabilities via our bug bounty program. Our program is inclusive of all Digiteal brands and technologies and offers rewards for a wide array of vulnerabilities. We encourage security researchers looking to participate in our bug bounty program to review this policy to ensure compliance with our rules and also to help you safely verify any vulnerabilities you may uncover.

Software security researchers are increasingly engaging with Internet companies to hunt down vulnerabilities.

Security is a collaboration : Digiteal encourages security researchers to work with us to mitigate and coordinate the disclosure of potential security vulnerabilities.

Digiteal works with security experts across the globe to stay up-to-date with the latest security techniques. If you've discovered a security issue that you believe we should know about, we'd gladly work with you. Our bug bounty program provides a monetary reward for these efforts.

The Digiteal's Bug Bounty Program applies to security vulnerabilities found within Digiteal's public-facing online environment. This includes, but is not limited to,

- Digiteal's websites,
- exposed APIs,
- mobile applications.

We are continuously working to evolve our bug bounty program. We aim to respond to incoming submissions as quickly as possible and make every effort to have bugs fixed within 90 days of being triaged.

The latest version of all currently supported products and services provided by Digiteal are included in our bug bounty program. Please review the program scope before submitting a report. Private scope is accessible to invited researchers only.

For the protection of our customers, we do not disclose, discuss or confirm security matters until comprehensively investigating, diagnosing and fixing any known issues.

Testing

Web traffic to and from Digiteal and our hosting partners produces very large amounts of data every day. When testing, you can make it easier for us to identify your testing traffic against our normal data and the malicious actors out in the world. Please do the following when participating in Digiteal bug bounty programs:

- Where possible, register accounts using your primary email address used to contact Digiteal.
- Provide your IP address in the bug report. We will keep this data private and only use it to review logs related to your testing activity.
- Include a custom HTTP header in all your traffic. Burp and other proxies allow the easy automatic addition of headers to all outbound requests. Report to us what header you set so we can identify it easily.

When testing for a bug, please also keep in mind:

- Only use authorised accounts so as not to inadvertently compromise the privacy of our users
- When attempting to demonstrate root permissions with the following primitives in a vulnerable process please provide the following:
    - **Read**: The contents of the file /proc/1/maps, or any other such sensitive file that you deem demonstrates the vulnerability
    - **Write**: Create or modify the file (including metadata such as creation/modification times) /root/<your username>*or a location you can write to whilst maintaining compliance with this policy
    - **Execute**: id, hostname, pwd (or any other shell level command that you deem demonstrates a vulnerability)
- Minimise the mayhem. Adhere to program rules at all times. Do not use automated scanners/tools that include payloads that could trigger state changes or damage production systems and/or data.
- Before causing damage or potential damage: Stop, report what you've found and request additional testing permission.

Bounty Eligibility

To be eligible for a reward under this program:

You must agree and adhere to
- the Program Rules and
- Legal terms

as stated in this policy.

Rules of Engagement or Program Rules

- The security bug must be original and previously unreported.
- For issues in client applications, there is a four-day grace period that begins when the vulnerability is checked into the primary source repository. If the issue is identified internally within those four days, it is ineligible for a bounty, even if the issue is not recognized as a

security vulnerability at time of first identification. If it lasts undiscovered for more than four days, it becomes eligible for a bounty.

- The security bug must be a part of Digiteal's code, not the code of a third party. We will pay bounties for vulnerabilities in third-party libraries incorporated into shipped client code or third-party websites utilised by Digiteal.
- You must not have written the buggy code or otherwise been involved in contributing the buggy code to the Digiteal project.
- You must be old enough to be eligible to participate in and receive payment from this program in your jurisdiction, or otherwise qualify to receive payment, whether through consent from your parent or guardian or some other way.
- Digiteal employees (including former employees that separated from Digiteal within the prior 12 months), contingent workers, contractors and their personnel, and consultants, or otherwise have a business relationship with Digiteal or any of its subsidiaries, as well as their immediate family members and persons living in the same household, are not eligible to receive bounties or rewards of any kind under any Digiteal programs, whether hosted by Digiteal or any third party.
- You should use your best effort not to access, modify, delete, or store user data or Digiteal's data. Instead, use your own accounts or test accounts for security research purposes.
- If you inadvertently access, modify, delete, or store user data, we ask that you notify Digiteal immediately at security@digiteal.eu and delete any stored data after notifying us.
- You should also use your best effort not to harm the availability or stability of our services, for example, by running aggressive scanning of those services. Instead, use manual testing or restrict your tests to the test environment of Digiteal and only try to confirm the vulnerability in the production environment.
- Whenever it is explicitly stated in our program scope, you are expected to test on the provided instances (e.g. test) instead of production.
- You must not be on an EU or belgian sanctions list or in a country on the EU or belgian sanctions list.
- You are not a resident of a EU Commission embargoed country.
- You must not exploit the security vulnerability for your own gain.
- All submissions will grant us permission to make use of all submissions.

- You must be available to supply additional information, as needed by our team, to reproduce and triage the issue.
- Do not intentionally harm the experience or usefulness of the service to others, including degradation of services and denial of service attacks.
- Do not attempt to view, modify, or damage data belonging to others.
- Do not disclose the reported vulnerability to others until we've had reasonable time to address it.
- Do not attempt to gain access to another user's account or data.
- Do not use scanners or automated tools to find vulnerabilities. They're noisy and we may ban your IP address.
- Do not attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.
- Researchers may not, and are not authorised to engage in any activity that would be disruptive, damaging or harmful to Digiteal, its brands or its users. This includes: social engineering, phishing, physical security and denial of service attacks against users, employees, or Digiteal as a whole.
- Test vulnerabilities only against accounts that you own or accounts that you have permission from the account holder to test against.
- Never use a finding to compromise/exfiltrate data or pivot to other systems. Use a proof of concept only to demonstrate an issue.
- If sensitive information, such as personal information, credentials, etc., is accessed as part of a vulnerability, it must not be saved, stored, transferred, accessed, or otherwise processed after initial discovery. All copies of sensitive information must be deleted and must not be retained.
- Abide by the program scope. Only reports submitted to this program and against assets in scope will be eligible for monetary award.
- Researchers may not publicly disclose vulnerabilities (sharing any details whatsoever with anyone other than authorized Digiteal employees), or otherwise share vulnerabilities with a third party, without Digiteal's express written permission.

- You are reporting in your individual capacity or, if you are employed by a company or other entity and are reporting on behalf of your employer, you have your employer's written approval to submit a report to the Digiteal Bug Bounty Program.
- You agree to participate in testing mitigation effectiveness and coordinating disclosure/release/publication of your findings with Digiteal.
- You did not and will not access any personal information that is not your own, including by exploiting the vulnerability.
- You did not and will not violate any applicable law or regulation, including laws prohibiting unauthorized access to information. To clarify, Digiteal does not view testing that is done in compliance with the terms and conditions of this bug bounty program as unauthorized.
- There may be additional restrictions on your eligibility to participate in the bug bounty depending upon your local laws.
- The parties to this agreement are you and Digiteal.
- You must abide by the law.
- By submitting the vulnerability, you affirm that you have not disclosed and agree that you will not disclose the bug or your submission to anyone other than Digiteal via our Bug Bounty Program.
- Submissions selected for rewards, and the individuals who submitted the vulnerabilities will receive appropriate recognition at the discretion of Digiteal.
- By submitting information about a potential vulnerability, you are agreeing to these terms and conditions and granting Digiteal a worldwide, royalty-free, non-exclusive license to use your submission for the purpose of addressing vulnerabilities. Only the first report of a given issue that Digiteal had not yet identified is eligible.
- Eligibility for rewards and determination of the recipients and amount of reward is left up to the discretion of Digiteal.
- The Program is focused predominantly on: Internet-facing Digiteal websites executing on internet domains that provide significant business value to Digiteal, and are supported directly by Digiteal and its suppliers; Digiteal-branded mobile applications; and the Digiteal API. Vulnerabilities submitted outside this scope are generally less likely to receive recognition or rewards under this Program.

- You are responsible for notifying Digiteal of any changes to your contact information, including but not limited to your email address. Failure to do so may lead to the forfeiture of Bounty Awards.
- Your testing activities must not negatively impact Digiteal or Digiteal's online environment availability or performance.
- Digiteal reserves the right to discontinue the Program at any time without notice.

Bounties can be donated to charity, please indicate this in the bug when filing or by contacting security@digiteal.eu.

Do not threaten or attempt to extort Digiteal. We will not award a bounty if you threaten to withhold the security issue from us or if you threaten to release the vulnerability or any exposed data to the public.

Violation of any of these rules can result in ineligibility for a bounty and/or removal from the program. Three strikes will earn you a temporary ban. Four strikes will give you a permanent ban.

Legal Terms

- In connection with your participation in this program you agree to comply with Digiteal Terms of Service, Digiteal's Privacy Policy (both available for viewing and download here, and all applicable laws and regulations, including any laws or regulations governing privacy or the lawful processing of data.
- Digiteal reserves the right to change, modify or discontinue the terms of this program at any time.
- Digiteal does not give permission/authorisation (either implied or explicit) to an individual or group of individuals to :
    - (1) extract personal information or content of Digiteal customers and/or their users or to publish this information on the open, public-facing internet without user consent or
    - (2) modify or corrupt programs or data belonging to Digiteal in order to extract and publicly disclose data belonging to Digiteal.

Safe Harbour

Digiteal strongly supports security research into our products and wants to encourage that research :

- Digiteal will not initiate a lawsuit or law enforcement investigation against a researcher in response to reporting a vulnerability unless the researcher is not fully complying with this Policy.
- Please understand that if your security research involves the networks, systems, information, applications, products, or services of another party (which is not us), that third party may determine whether to pursue legal action. We cannot and do not authorise security research in the name of other entities. If legal action is initiated by a third party against you and you have complied with this Policy, we will take reasonable steps to make it known that your actions were conducted in compliance with this Policy.
- You are expected, as always, to comply with all applicable laws and regulations.
- Please submit a report to Digiteal before engaging in conduct that may be inconsistent with or unaddressed by this Policy.

If you're not sure whether your conduct complies with this policy, please contact us first at security@digiteal.eu and we will do our best to clarify.

Program Scope

Vulnerabilities on a specific website or services should be reported if it is listed as "in scope". Please see our detailed scope list below for a full list of assets that are in scope of this program. This list is subject to change without notice.

If you've found a vulnerability that affects an asset belonging to Digiteal, but is not included as in scope on any of the Digiteal programs, please report it to security@digiteal.eu.

Valued Vulnerabilities or In-Scope

All reports will be awarded based on the **Common Weakness Enumeration classification**.

This table provides the CWEs that we will accept, the severity ranges we will classify reports within for the CWE, and some examples of common vulnerability and attack names that we classify within each CWE that we will accept.

This table serves only as a guide and the severity classification of a particular vulnerability will be determined by Digiteal in its sole discretion.

Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

At this time, the scope of this program is limited to security vulnerabilities found in following targets:

- www.digiteal.eu
- dev.digiteal.eu
- app.digiteal.eu
- auth.digiteal.eu
- api.digiteal.eu
- test.digiteal.eu
- int.digiteal.eu
- peppol-smp-prod
- peppol-smp-test
- peppol-ap-prod
- peppol-ap-test

All Digiteal code shipped with its product, both source and binaries (in binary form) as supplied.

Only the latest versions of the currently shipped and supported products are in scope.

All Digiteal Hosted services, both public and private cloud installations.

All Digiteal supplied customer service portals, third-party components excluded.

Borderline Out-of-Scope, No Bounty

These issues are eligible for submission, but not eligible for bounty or any award. Once triaged, they will be closed as Informative only if found to be valid or Spam if found to be not valid. When reporting vulnerabilities, please consider

(1) attack scenario/exploitability and

(2) security impact of the bug.

Examples:

- Any non-Digiteal Applications
- Missing Security Best Practices
- Use of known-vulnerable library (without proof of exploitability)
- Missing cookie flags
- SSL/TLS Best Practices

- Physical attacks
- Results of automated scanners
- Autocomplete attribute on web forms
- “Self” exploitation
- Flash-based XSS
- Verbose error pages (without proof of exploitability)
- Digiteal software that is End of Life or no longer supported
- Missing Security HTTP Headers (without proof of exploitability)

Note: 0-day vulnerabilities may be reported 30 days after initial publication.

Do Not Report or Out-of-Scope

The following issues are considered out of scope:

- Vulnerabilities in pre-release product versions (e.g., Beta, Release Candidate).
- Vulnerabilities in product versions are no longer under active support.
- Vulnerabilities already known to Digiteal.
- Vulnerabilities present in any component of an Digiteal product where the root-cause vulnerability in the component has already been identified for another Digiteal product.
- Vulnerabilities in products and technologies that are not listed as eligible Digiteal branded products and technologies, including vulnerabilities considered out of scope as defined above.
- Those that resolve to third-party services
- Issues that we are already aware of or have been previously reported
- Issues that require unlikely user interaction
- Disclosure of information that does not present a significant risk
- Cross-site Request Forgery with minimal security impact
- CSV injection
- General best practice concerns
- All Flash-related bugs

Special Situations

Same Bug, Different Host

For each report, please allow Digiteal sufficient time to patch other host instances. If you find the same bug on a different (unique) host, prior to the report reaching a triaged state, file it within the

existing report to receive an additional 5% bonus (per host, not domain). Any reports filed separately, while we are actively working to resolve the issue, will be treated as a duplicate.

Same Payload, Different Parameter

In some cases, rewards may be consolidated into a single payout. For example, multiple reports of the same vulnerability across different parameters of a resource, or demonstrations of multiple attack vectors against a fundamental framework issue. We kindly ask you to consolidate reports rather than separate them.

Submit Your Report

To be eligible for bounty award consideration, your report must meet the following requirements:

1. The report and any accompanying material has been filed on https://support.digiteal.eu or to security@digiteal.eu
2. The Digiteal products in your report correspond to an item explicitly listed below as eligible Digiteal branded products and technologies.
3. The vulnerability you identify must be original, not previously reported to Digiteal, and not publicly disclosed.
4. The report must show that the potential vulnerability has been demonstrated against the most recent publicly available version of the affected product or technology.

If our security team cannot reproduce and verify an issue, a bounty cannot be awarded. To help streamline our intake process, and In order to help us triage and prioritise submissions, we recommend that your reports:

Mandatory:

- Description of the vulnerability
- Steps to reproduce the reported vulnerability
- Proof of exploitability (e.g. screenshot, video)

Recommended:

- Perceived impact to another user or the organization
- Proposed CVSSv3 Vector & Score (without environmental and temporal modifiers)
- List of URLs and affected parameters
- Other vulnerable URLs, additional payloads, Proof-of-Concept code
- Browser, OS and/or app version used during testing

- Describe the location 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).
- The name(s) of the Digiteal product or technology and the respective version information.
- Detailed description of the potential security vulnerability.
- Recommendation to resolve the issue

The more details provided in the initial report, the easier it will be for Digiteal to evaluate your report.

Note: Failure to adhere to these minimum requirements may result in the loss of a reward.

If you are having trouble reporting your vulnerability report or have any questions about the process send a message to Digiteal's Product Security Incident Response Team (PSIRT) (security@digiteal.eu).

All supporting evidence and other attachments must be stored only within the report you submit. Do not host any files on external services.

It's important to include at least the following information in the service desk ticket / email in English:

- Organisation and contact name
- Disclosure plans, if any
- If you want public recognition

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. A well written report will allow us to more quickly and accurately triage your submission.

Digiteal, at its sole discretion, may reject any submission that we determine does not meet these criteria above or that are deemed as ineligible as set forth below.

Rewards

You may be eligible to receive a monetary reward if:

- You are the first person to submit a site or product vulnerability
- That vulnerability is determined to be a valid security issue by Digiteal's security team
- You have complied with all Program Terms

All bounty amounts will be determined at the discretion of Digiteal PSIRT who will evaluate each report for severity, impact and quality. Rewards amounts vary depending upon the severity of the vulnerability reported. There could be submissions that we determine have an acceptable level of risk such that we do not make changes.

The minimum bounty amount for a validated bug submission is 50€ and the maximum bounty for a validated bug submission is 2.000€ (see Payout Table). Digiteal's Bug Bounty team retains the right to determine if the bug submitted to the Bug Bounty Program is eligible. All determinations as to the amount of a bounty made by the Digiteal Bug Bounty team are final.

Eligibility for any bug bounty award and award amount determinations are made at Digiteal's sole discretion. These are some general guidelines that may vary from published documentation (case-by-case basis):

- Awards may be greater:
    - based on the potential impact of the security vulnerability
    - for well-written reports with complete reproduction instructions / proof-of-concept (PoC) material. See the eligible report requirements above.
    - if a functional mitigation or fix is proposed along with the reported vulnerability.
- Digiteal will award a bounty award for the first eligible report of a security vulnerability.
- Awards are limited to one (1) bounty award per eligible root-cause vulnerability.
- Digiteal will publicly recognize awarded security researchers via Digiteal Security Advisories at or after the time of public disclosure of the vulnerability, in coordination with the security researcher who reported the vulnerability.
- Award amounts may change with time. Past rewards do not necessarily guarantee the same reward in the future.

Bounty Award Schedule

Each bug bounty report is individually evaluated based on the technical details provided in the report. Digiteal generally follows the processes below to evaluate and determine the severity of a reported potential security vulnerability.

- Vulnerability Assessment – Digiteal PSIRT ensures that all requested information has been provided for Triage. See the Bug Bounty Reporting section above for a list of required information.
- Triage - A team of Digiteal product engineers and security experts will determine if a vulnerability is valid and an eligible Digiteal product or technology is impacted.

- Vulnerability severity determination – Digiteal PSIRT works with the Digiteal product security engineers and Digiteal security experts to determine the severity and impact of a vulnerability.

Payout table

Vulnerability Severity	Reward
Critical	Up to 2.000€
High	Up to 1.000€
Medium	Up to 500€
Low	Up to 50€
Informative	0€

Digiteal makes no representations regarding the tax consequences of the payments Digiteal makes under this program. Participants in this program are responsible for any tax liability associated with bounty award payments.

Possibly, you will also be eligible to be honored in our “Hall of Fame“ if you agree.

The Digiteal Hall of Fame honors researchers who have made, or are making, significant contributions to the advancement of the security of our company.

Our Hall of Fame is displayed on our website www.digiteal.eu (pending first accepted security finding).

Payment

You'll need to submit an invoice in order to receive payment. The invoice has to meet all legal requirements. The reference on the invoice must be “Bug Bounty”.

Payments will be paid within 30-days after Digiteal awards the bounty to the researcher.

Digiteal accepts the following payment method:

Payment method	Data necessary for payment
Wire transfer	• First and last name • Address • Bank name • SWIFT • IBAN • Sort code

Confidentiality

Intellectual Property

By submitting your content to Digiteal (your “Submission”), you agree that Digiteal may take all steps needed to validate, mitigate, and disclose the vulnerability, and that you grant Digiteal any and all rights to your Submission needed to do so.

In Scope eligible products and technologies are listed above, if you are unsure whether a product or technology is eligible, contact Digiteal PSIRT at security@digiteal.eu .

Digiteal encourages the reporting of all potential vulnerabilities.

Digiteal reserves the right to alter the terms and conditions of this program at its sole discretion.

Sensitive and Personal Information

Never attempt to access anyone else's data or personal information including by exploiting a vulnerability. Such activity is unauthorised. If during your testing you interacted with or obtained access to data or personal information of others, you must:

- Stop your testing immediately and cease any activity that involves the data or personal information or the vulnerability.
- Do not save, copy, store, transfer, disclose, or otherwise retain the data or personal information.
- Alert Digiteal immediately and support our investigation and mitigation efforts.

Failure to comply with any of the above will immediately disqualify any report from bounty award eligibility.

Any information you receive or collect about Digiteal through the Bug Bounty Program must be kept confidential and only used in connection with the Bug Bounty Program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your Submission and information you obtain when researching the Digiteal sites, without Digiteal's prior written consent.

Response SLA

Response efficiency metrics are tracked and reported in business days - Monday to Friday from 8 AM to 5 PM CET.

Time to respond to private bug bounty participation request.	
First response time	1 business day
Triage time	5 business days
Bounty time	30 business days

Questions

Any questions about Digiteal's Bug Bounty Program can be directed to security@digiteal.eu.