Instructions Zerocopter App

zerocopter

Werfkade 2 | 1033 RA Amsterdam | The Netherlands
Phone: +31 20 261 67 43 | email: info@zerocopter.com
May 18th 2021, version 1.4

zerocopter

Table of Contents

zerocopter

Welcome to the Zerocopter platform!

You are here because you want to learn all about the Zerocopter platform, bug bounties, responsible disclosure and scanners. You're ready to jump right into it but want to do this right.

These instructions were created to teach you everything you need to know about bug bounties, responsible disclosure and scanner and how to use them for your company on the Zerocopter platform.

The instructions are composed of thirteen chapters:

1. Getting Started
2. Scanners
3. Responsible Disclosure
4. Researcher Programs
5. Reports
6. Dashboard
7. Notification Settings
8. Label Manager
9. Download/Export reports
10. Security
11. Badged
12. Profile
13. Some final thoughts

Starting with and executing bug bounties, responsible disclosure and scanners are no small undertaking. We are here to help you.

> **If you have any questions don't hesitate to contact our support department:**
> support@zerocopter.com
> +31 20 261 67 43

Getting started

Zerocopter is a continuous online security platform. We offer three services that you can use to improve your online security in a continuous way:

- Researcher Programs
- Responsible Disclosure Programs
- Scanner Programs

In order to use our services:

1. You need a subscription[1]
2. You need an account
3. You need to create a project

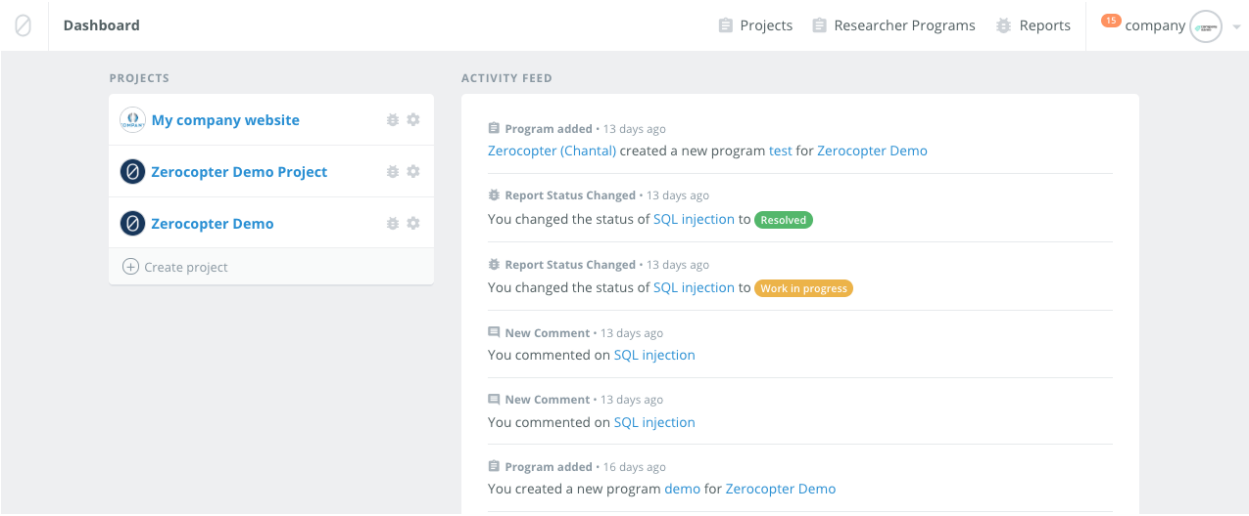
A Zerocopter account

In order to use our platform, you need an account to login. An account can be acquired by an invitation from someone who's already on the platform. This could be Zerocopter inviting you or one of your colleagues.

> **We are assuming that you are being invited. Please contact us if we are wrong:**
> support@zerocopter.com
> +31 20 261 67 43

After receiving an invitation email, click on the link and proceed with the onboarding. If you are done, you will see your dashboard. The dashboard contains the project(s) you are part of and an activity feed on the project(s). You are also able to create a new project.

[1] If somehow you are reading this document and you don't have a subscription, but you want one: please contact sales@zerocopter.com



Creating a project

The Zerocopter platform is based on projects. Within every project you can use all of our services, which we call programs. A project represents a certain scope and contains a number of team members you can manage yourself. The main reason to create multiple projects is that you have different scopes, each with different team members.

Admin or not

If you are an admin, you are able to do everything that's possible on our platform.

- Start a program (researcher program, responsible disclosure program, scanner program)
- Manage (admin) members
- Make exports
- Manage security settings (e.g. enforce 2FA)
- Manage integrations for programs
- Manage labels
- Set rewards for reports
- Assign members to reports
- Add consultants to reports
- And do the same as a normal project member

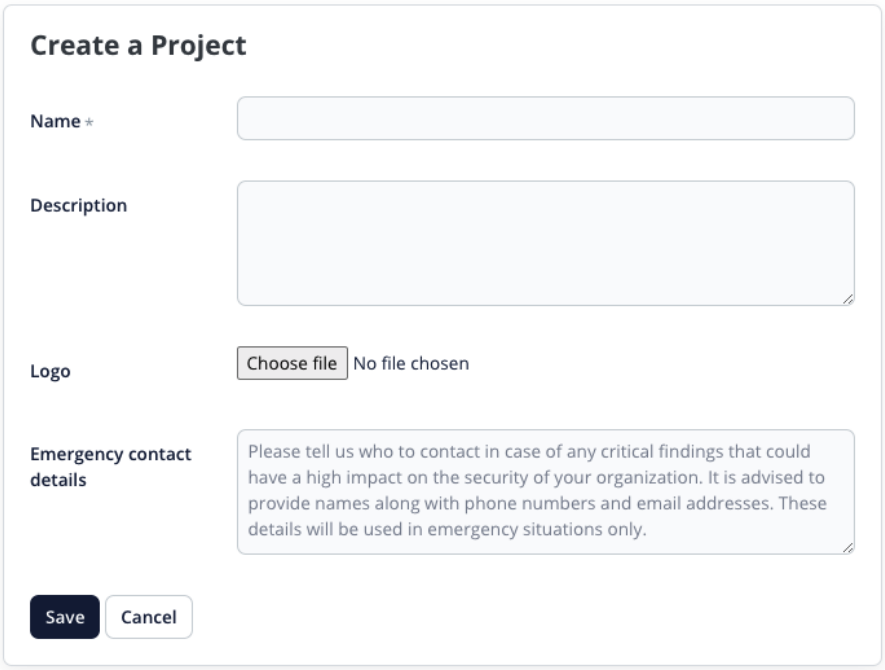
If you are a project member you are able to:

- See the programs (not manage them)

- Work with the reports (comment, set the severity, change status*)
- Manage badges

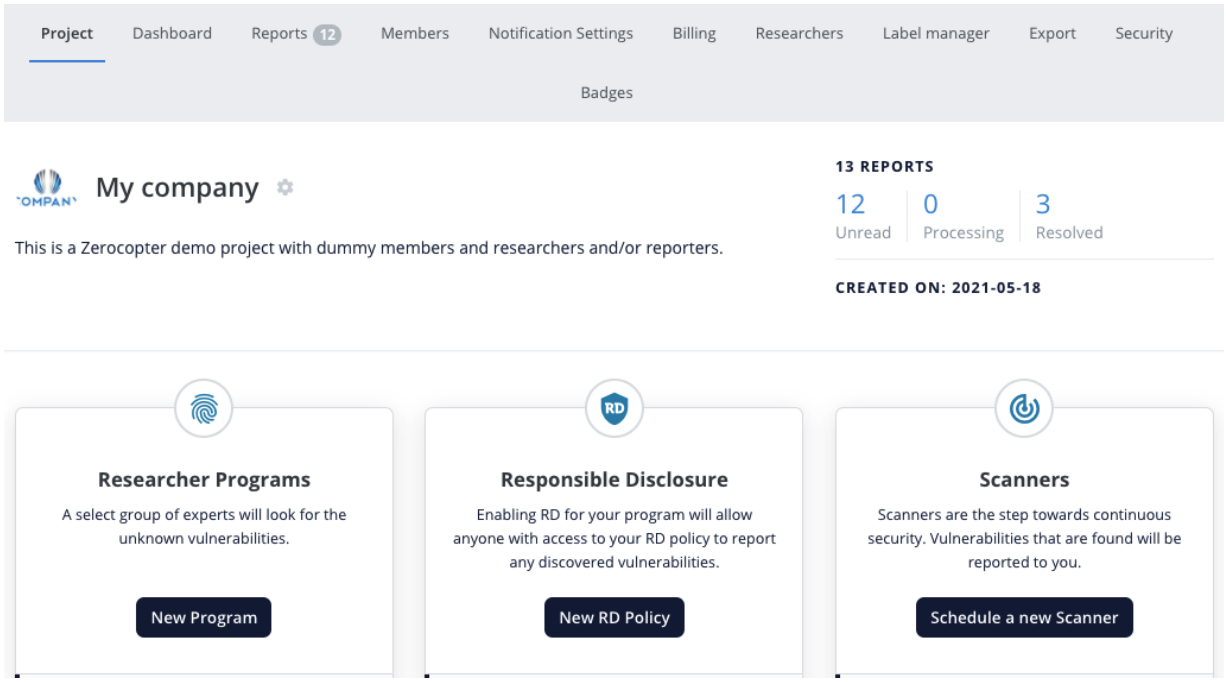
* except for “resolved” in a researcher program when the reward is not set yet.

If you want to create a new project, click on the button ‘create project’ on your dashboard and fill in a name, a description, add a logo/image and fill in your emergency contact details:



When creating a new project you will automatically be the admin of that project.

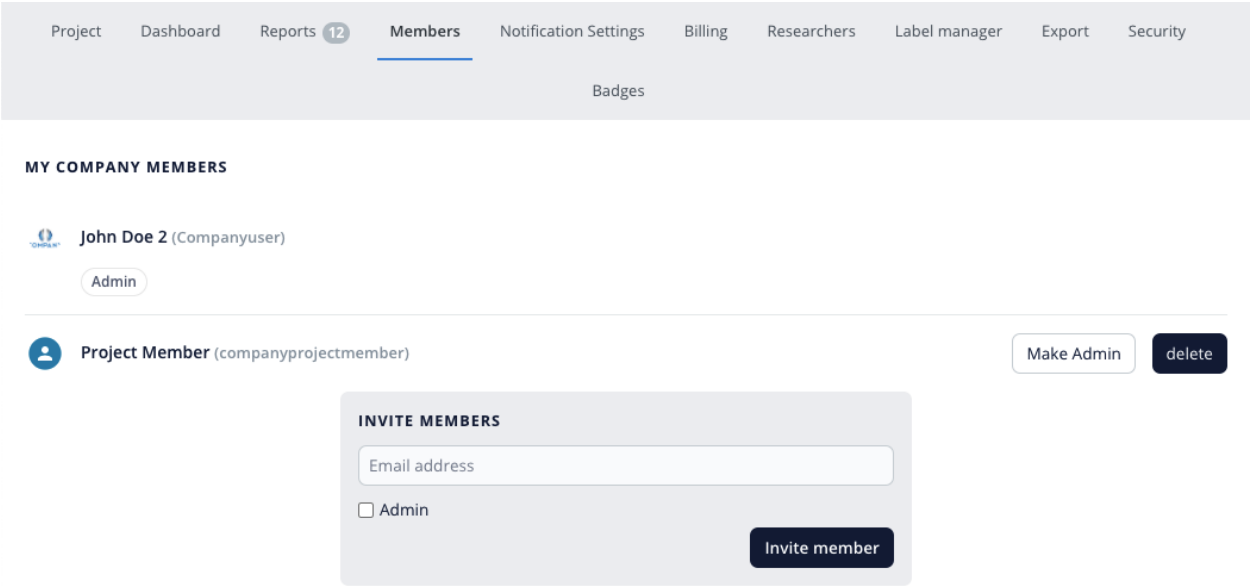
After you are done, your new project looks like this:



Adding members to a project

In most cases, the first thing you would do now is add some colleagues, team members. If you click on ‘Members’ in the top menu, you can add a member to your project by filling in email addresses. If these members already have a Zerocopter account, the project will be added to their dashboard. If these members don’t have a Zerocopter account, they will be invited by email to join our platform.

You can choose to make a member an administrator (admin). In that case, these members will be able to manage the entire project. You can also give normal project members admin rights or take them away, or remove members entirely from the project.



Scanners

Scanners is the last program in line, but in most cases the first program our clients activate. We have implemented OWASP ZAP to scan your scope for so called known vulnerabilities (e.g. missing patches, old software versions and misconfigured SSL certificates). It's always a good thing to scan your scope for known vulnerabilities on a regular basis. If at some point you need to update or fix something, our scanner will tell you.

We scan your targets using the passive version of the OWASP ZAP scanner. This is a non-invasive scanner that scans all HTTP requests and responses and then reports on any vulnerabilities.

The full list of items being scanned can be found here:
https://www.zaproxy.org/docs/desktop/addons/passive-scan-rules/

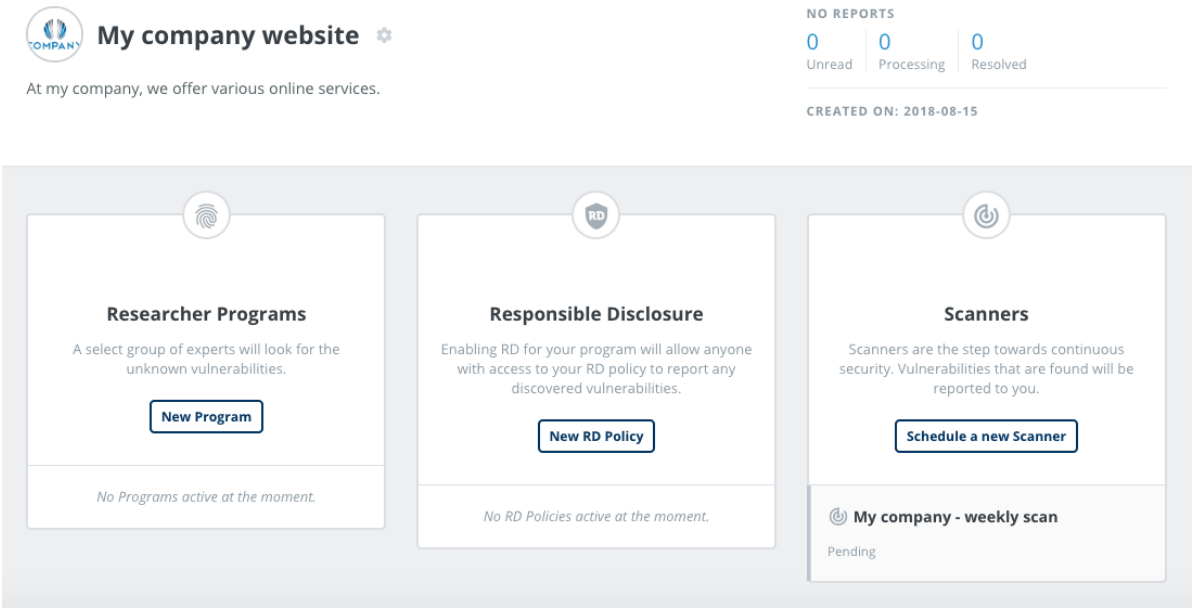
Scheduling a scanner

You can run our scanner on a monthly, weekly or daily basis. You can set the exact time the scanner should start and you can add multiple URLs the scanner should scan.

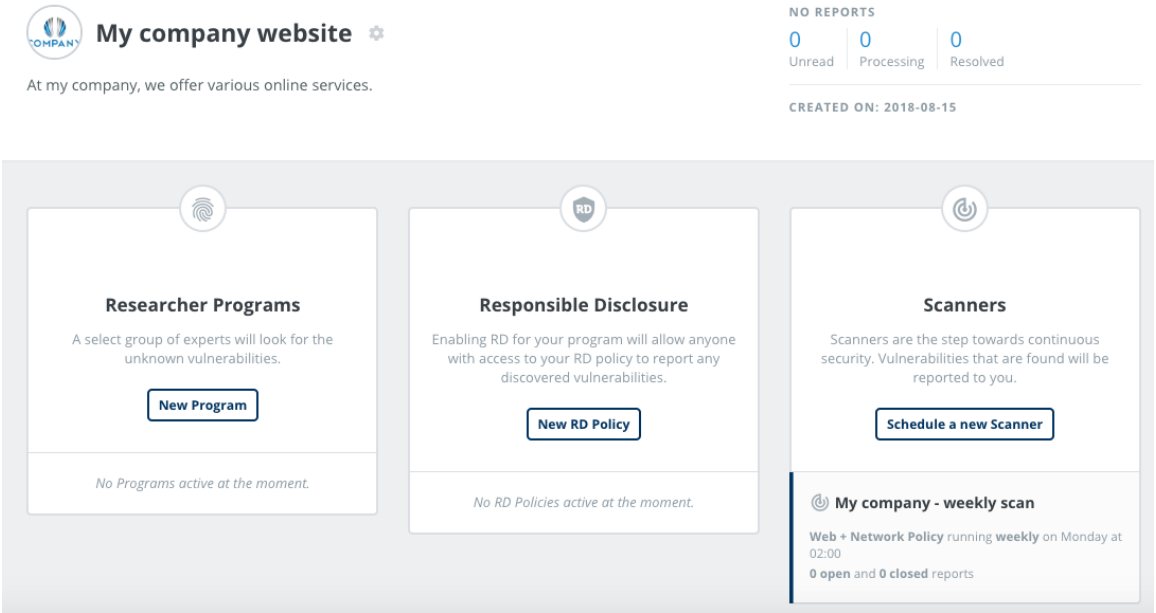
Additional options

- Policy: you are able to scan on web policy, network policy or both. Default 'web + network policy' is selected, since we advise to scan on both unless you have a good reason not to.
- Informationals: you can toggle Informationals on if you would like to receive these reports as well. Informationals are reports that might concern vulnerabilities, but need your assessment to classify them that way. For example: if a certain port is open, this might be intentional and completely safe, but it could also be a serious vulnerability. If you are not sure what to do, we advise you to do an initial scan without informationals. Later on you can toggle informationals on if you have fixed the open reports from the initial scan.
- Whitelisting: The scanner could be blocked by your firewall, since the scanner might be identified as 'undesirable behavior'. The easiest way to find out is if the scan only took 30 minutes and there are no reports. In that case you can whitelist the scanner's IP numbers: `52.29.28.253` and `3.121.187.22`

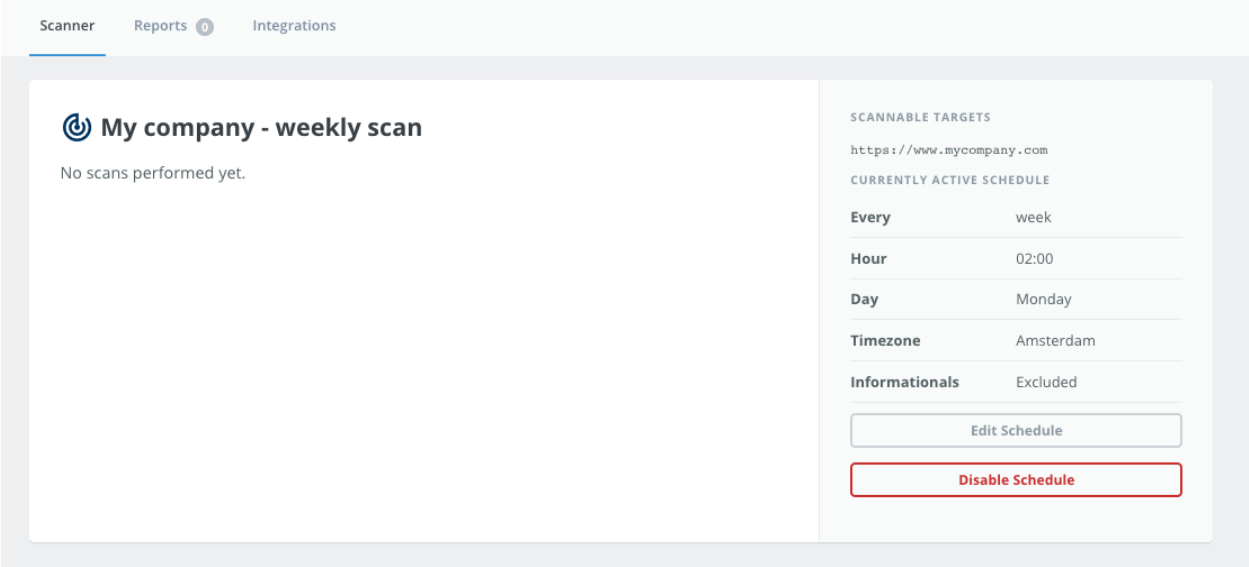
If you saved your scanner schedule, you can see in your project that you have added a scanner.



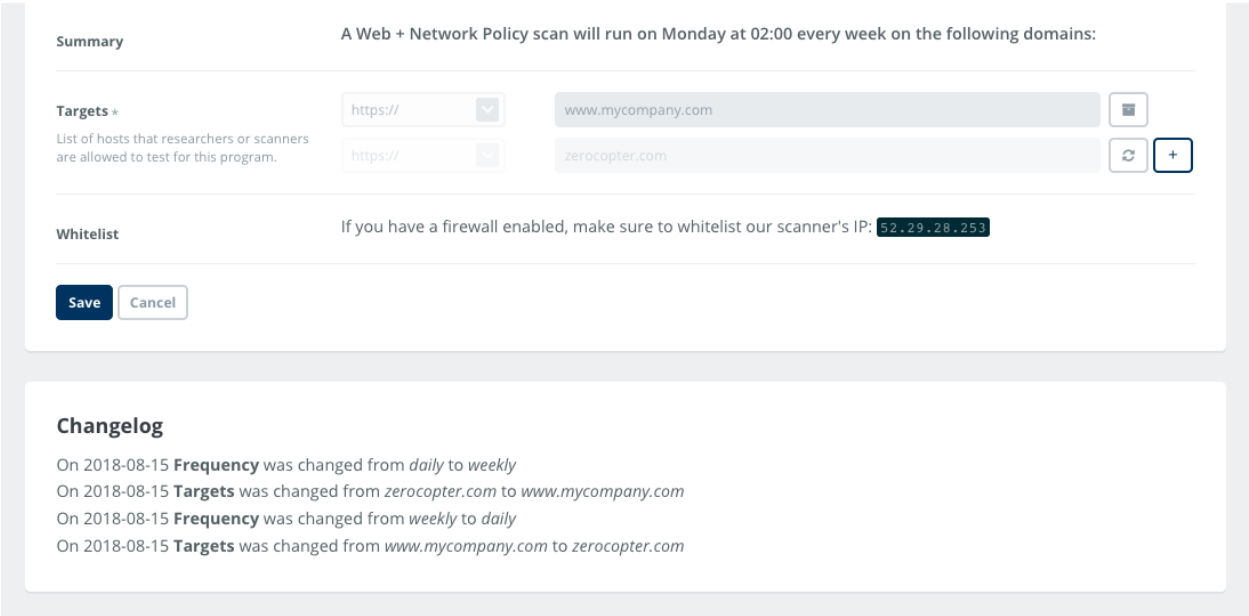
Please note the scanner is pending, Zerocopter needs to approve all new programs within a project. After approving it will look like this:



If you click on the scanner scheduler, you can see some details about the scheduler, you can edit the scheduler and you can disable the scheduler.

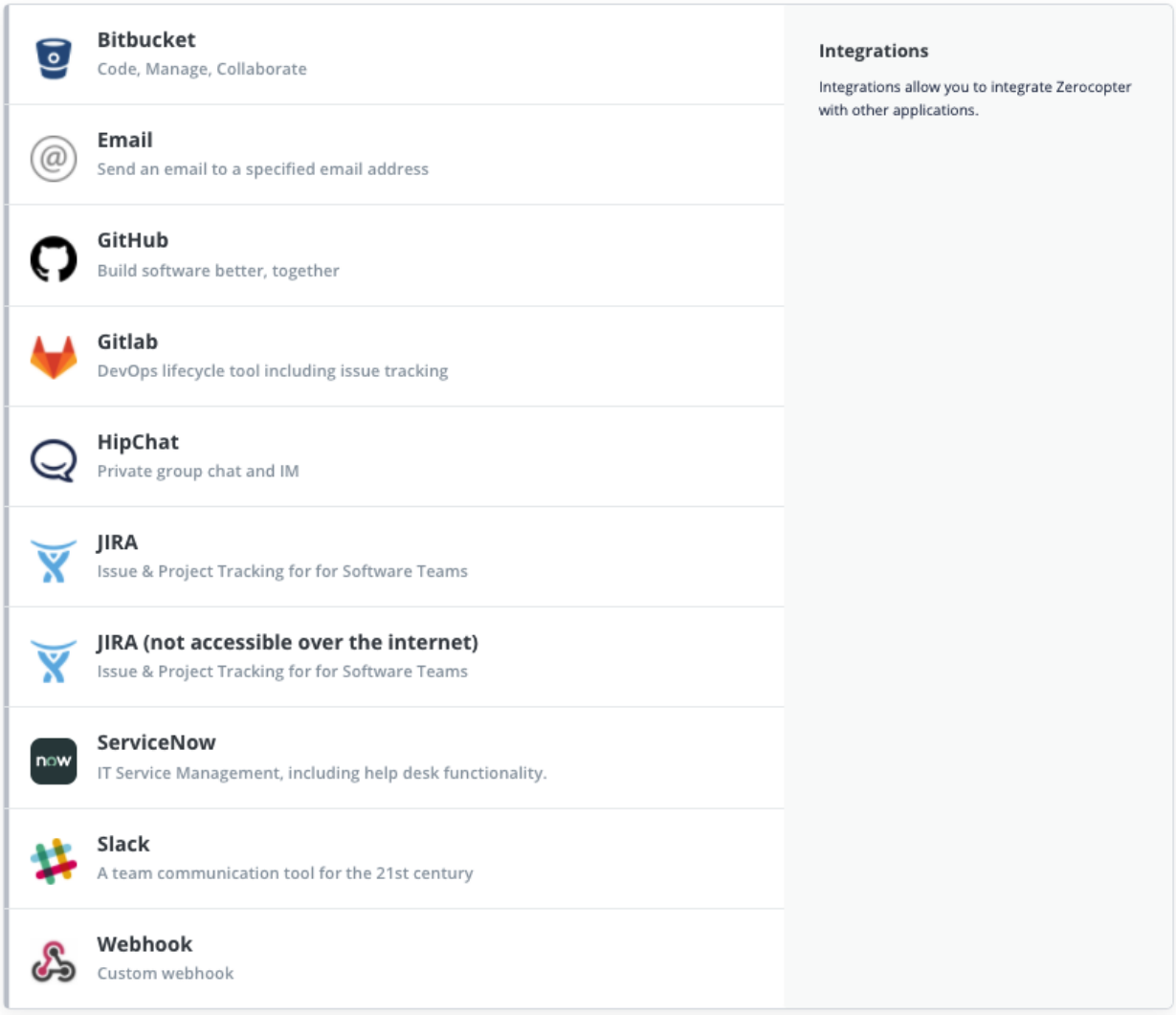


If you click on ‘edit schedule’, you can edit all options. You can also see a changelog at the bottom.



Integrations

Integrations allows you to push all scanner reports to other applications.

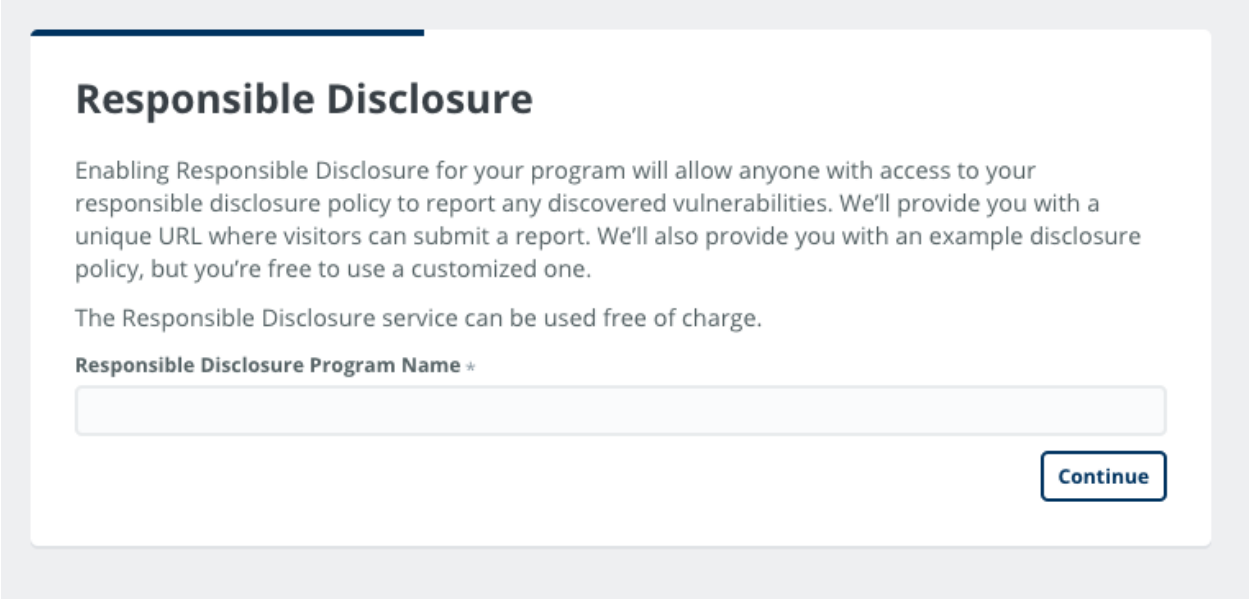


Please note only new reports will be pushed. So if you activate integrations at a later stage, be aware that old reports will not be pushed to your integration. Also: integrations are one-way traffic. Editing a report in an integrated application will not automatically edit the report in our platform.

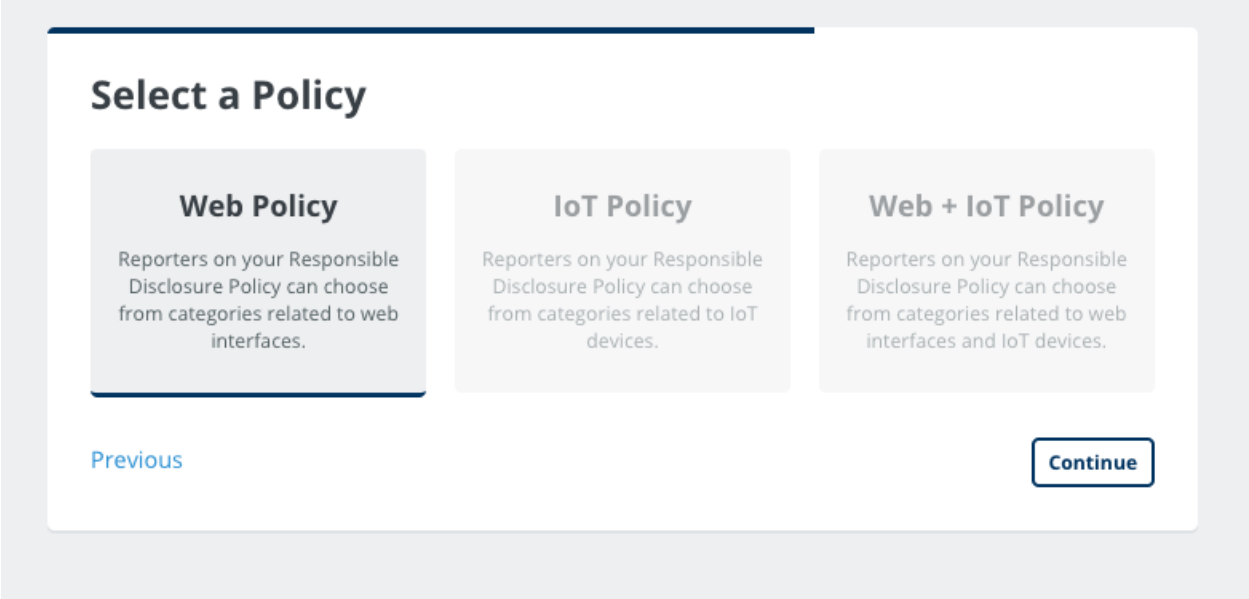
Responsible Disclosure

By creating a Responsible Disclosure policy, you can allow anyone to report discovered vulnerabilities on your online environment(s) or your IoT devices. We provide you with a default policy text and a unique link to a form where a vulnerability can be reported.

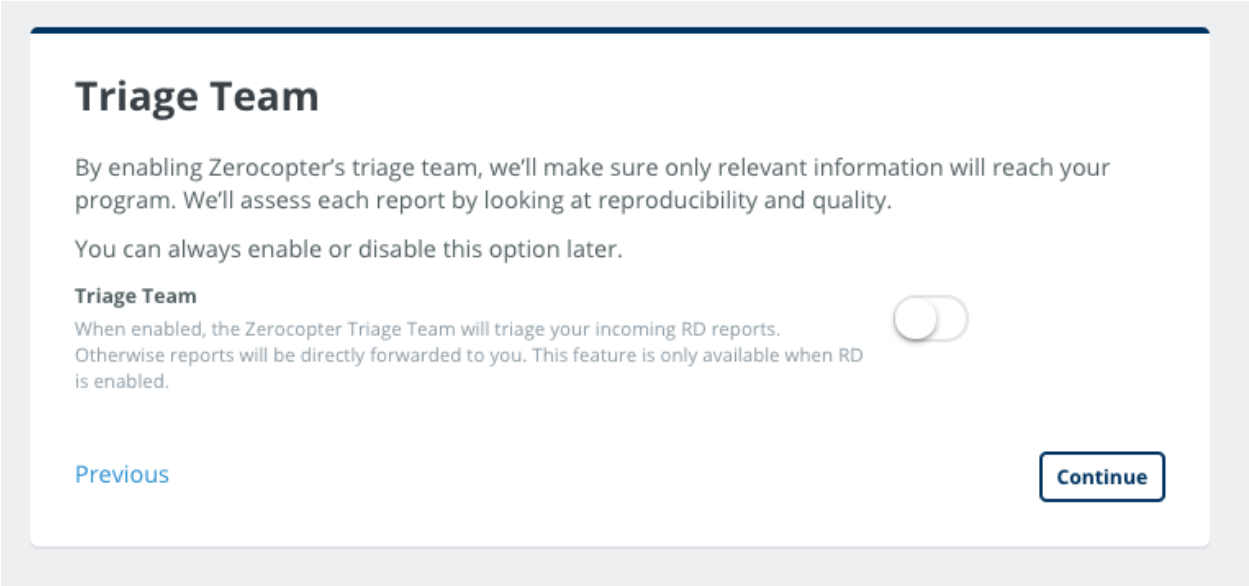
When you start creating a Responsible Disclosure policy, first give it a name.



After that, please select a policy. The policy you select here will determine the categories a reporter can choose from when reporting a vulnerability. Web policy is the default policy, but you can also select IoT or both.

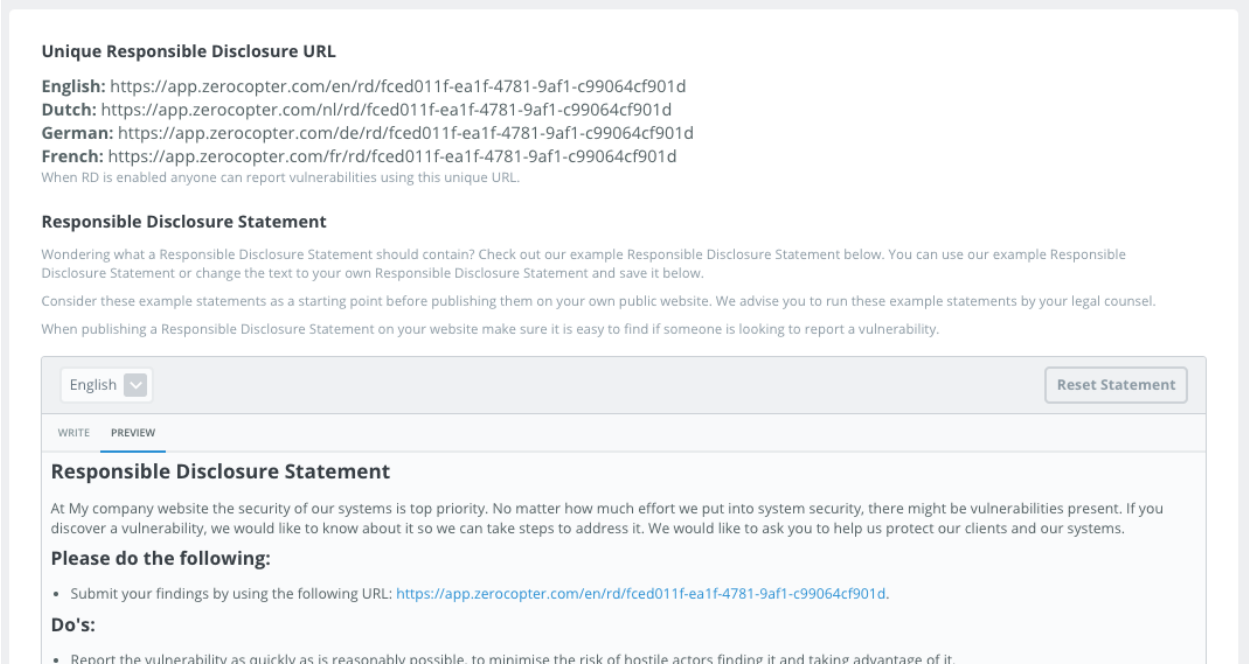


Now toggle triage team on, if you would like our triage team to check all incoming reports.



After these 3 steps you enabled your Responsible Disclosure policy. Please note your Responsible Disclosure policy is pending, since Zerocopter needs to approve all new programs within a project.

You have your unique URLs (1 form in 4 languages) on which a vulnerability can be reported.



We also provide you with a template Responsible Disclosure Statement, that you can edit to suit your organisation.

Responsible Disclosure Statement

At [COMPANY] the security of our systems is top priority. No matter how much effort we put into system security, there might be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it. We would like to ask you to help us protect our clients and our systems.

Please do the following:

- Submit your findings by using the following URL: [URL]

Do's:

- Report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it.
- Report in a manner that safeguards the confidentiality of the report so that others do not gain access to the information.
- Provide sufficient information to reproduce the problem, so we will be able to resolve it. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient. But complex vulnerabilities may require further explanation.

Don'ts:

- Reveal the vulnerability or problem to others until it is resolved.
- Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks.
- Utilise a vulnerability further than necessary to establish its existence.
- Copy, modify or delete data on the system. An alternative for doing so is making a directory listing of the system.
- Make changes to the system.
- Repeatedly gain access to the system or sharing access with others.
- Use brute force attacks, attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties to gain access to the system.

What we promise:

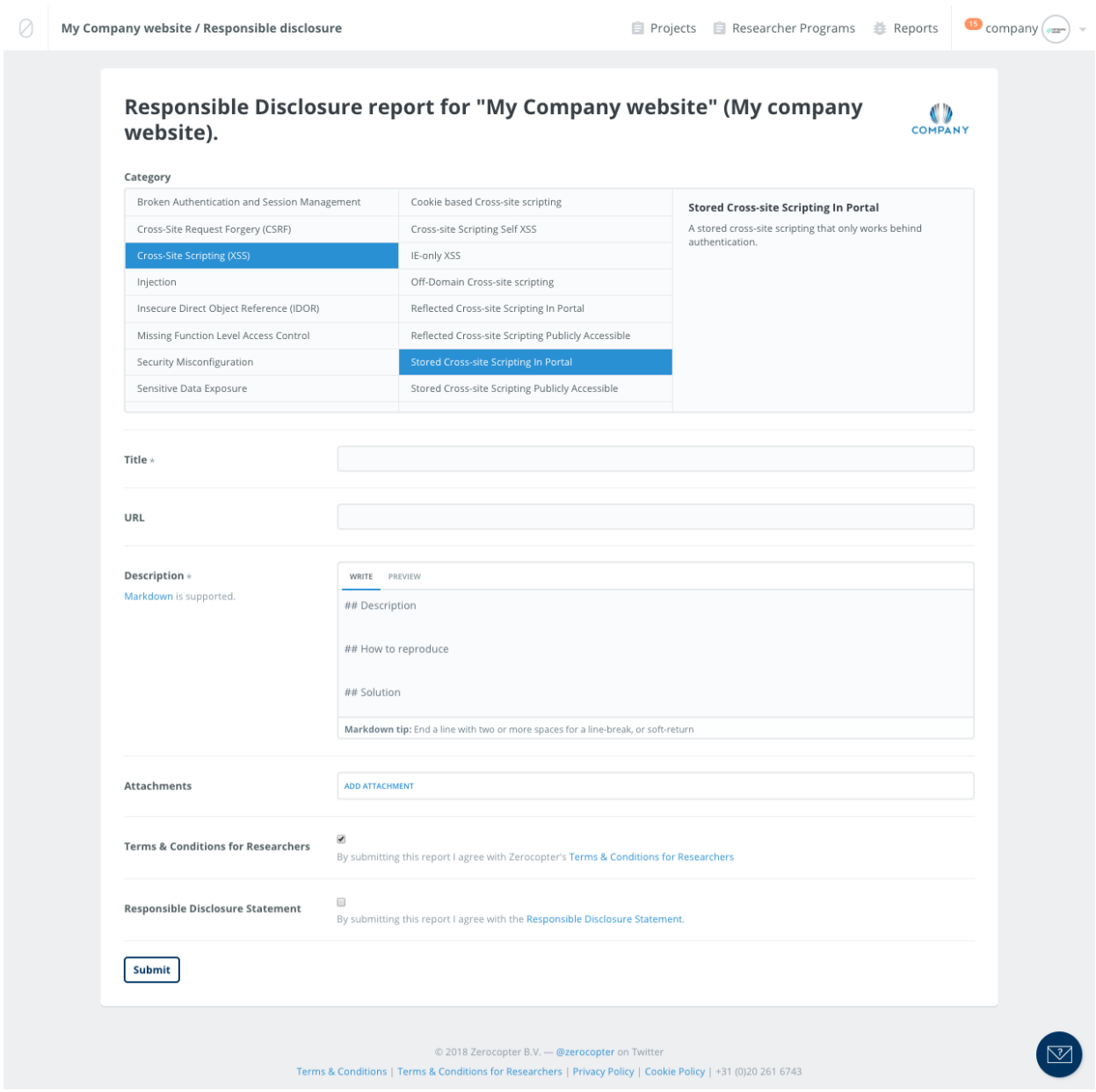
- We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.
- If you followed the instructions above, we will not take any legal action against you concerning the report.
- We will not pass on your personal details to third parties without your permission, unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible.
- We will keep you informed of the progress towards resolving the problem.
- In the public information concerning the reported problem, we will give your name as the discoverer of the problem (unless you desire otherwise).

> We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.
> This Responsible Disclosure policy is based on an example written by Floor Terra and the Responsible Disclosure Guideline of the NCSC.

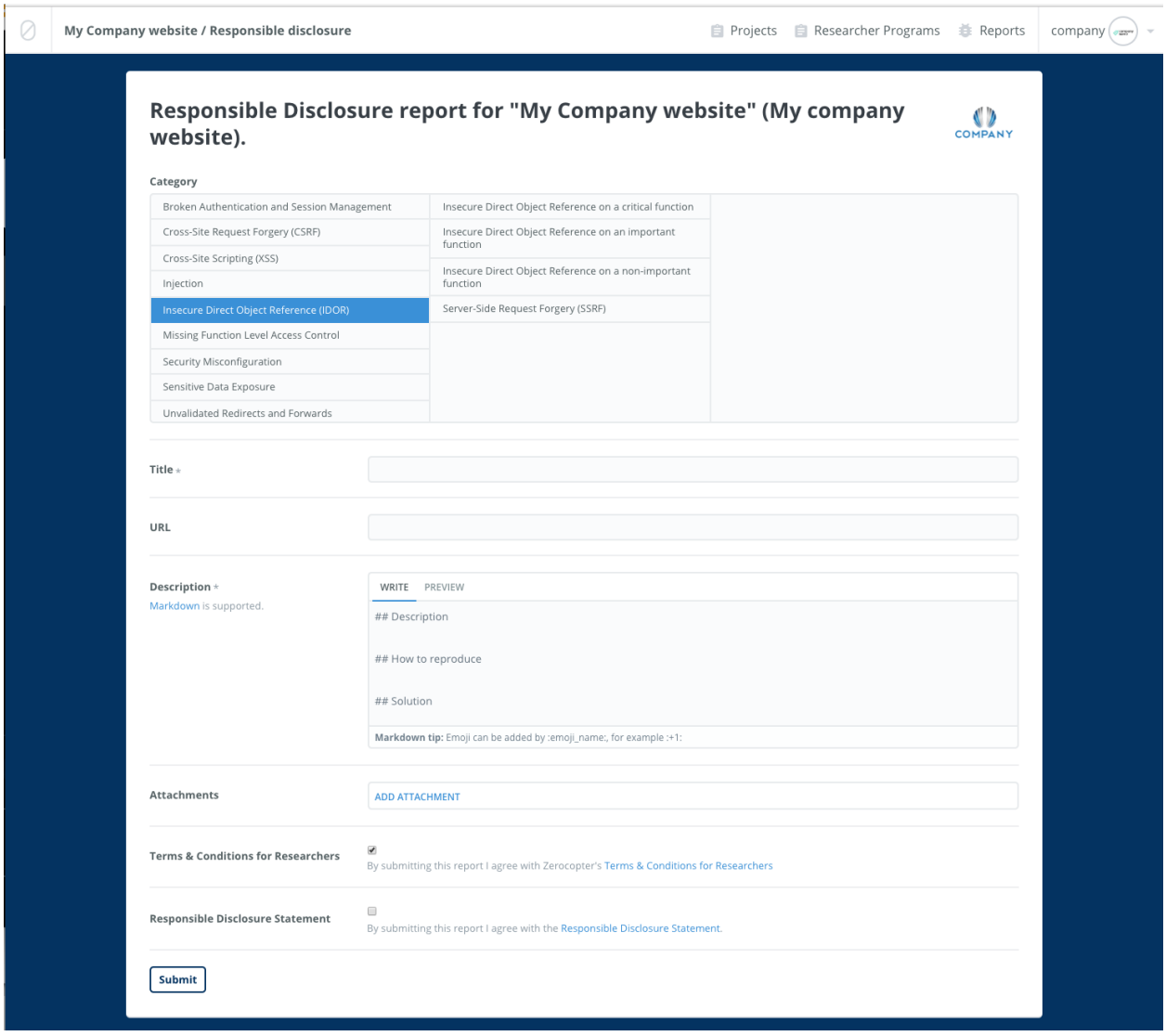
Additional options

- Add 'Request acceptance': make reporters accept your Responsible Disclosure policy before they submit a report
- Add logo: make your form more attractive by adding your company logo.
- Add background color: make your form more attractive by adding a custom background color.

Once you added a logo the form where a vulnerability can be reported looks like this:

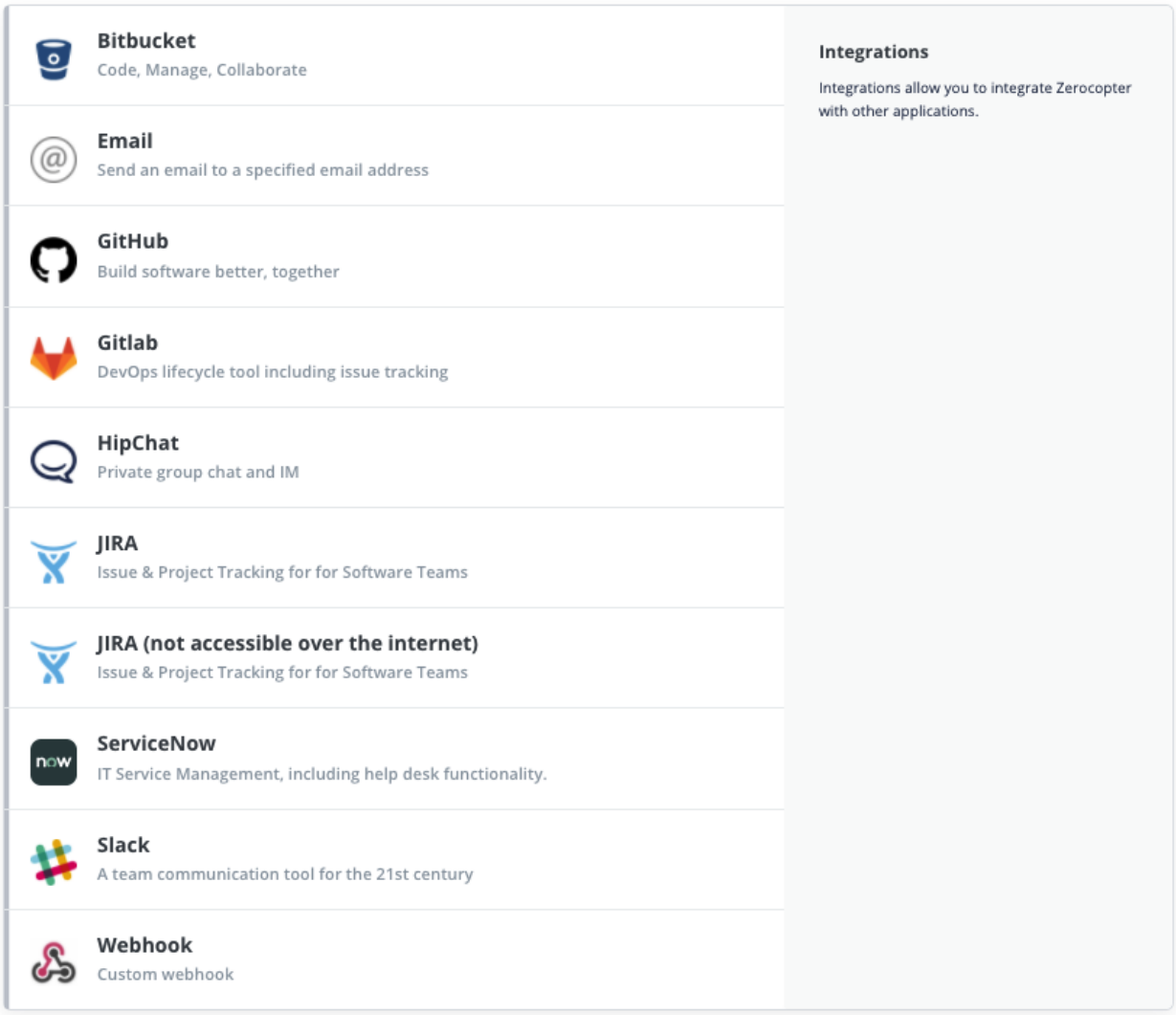


After you changed the background color the form where a vulnerability can be reported looks like this:



Integrations

Integrations allow you to push all Responsible Disclosure reports to other applications.



Please note only new reports will be pushed. So if you activate integrations at a later stage, be aware that old reports will not be pushed to your integration. Also: integrations are one-way traffic. Editing a report in an integrated application will not automatically edit the report in the Zerocopter platform.

Researcher Programs

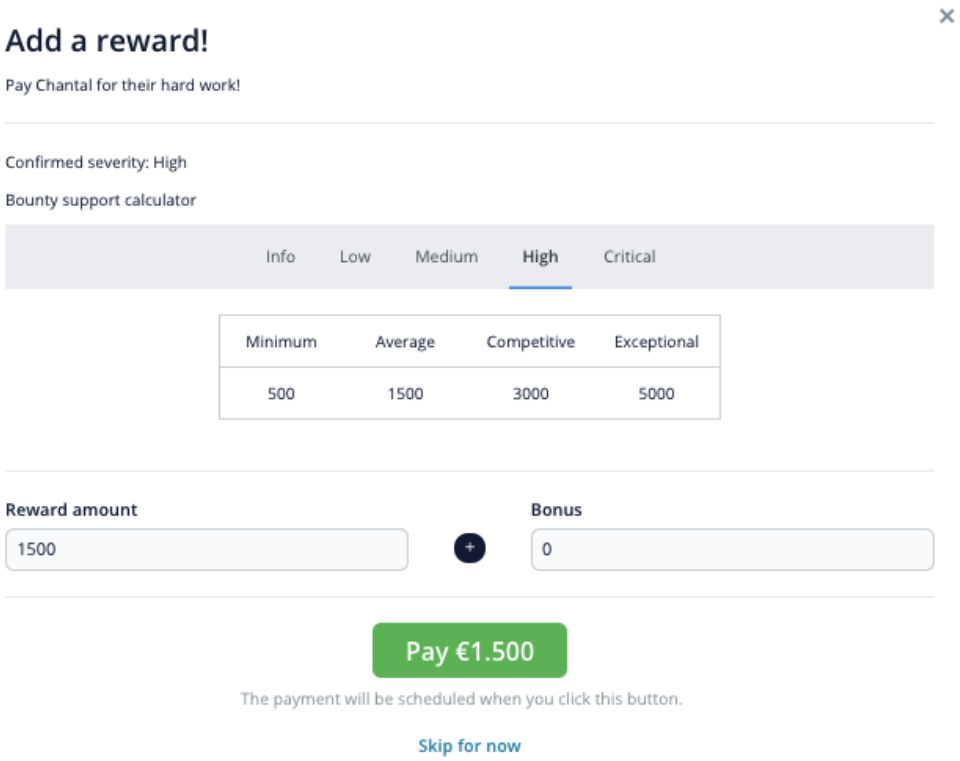
With our Researcher Programs (bug bounties) you are able to leverage the best security researchers in the world to look for unknown vulnerabilities within your scope / online environment(s). During a Researcher Program, researchers will be rewarded for discovering unknown vulnerabilities. Our triage team checks all incoming reports, we make sure you don't receive duplicates or incomplete reports.

Rewards for researcher programs are determined by the severity of the report. The severity can be determined by using a CVSS-calculator. The available severities are Informational, Low, Medium, High and Critical. Each severity has a minimum reward.

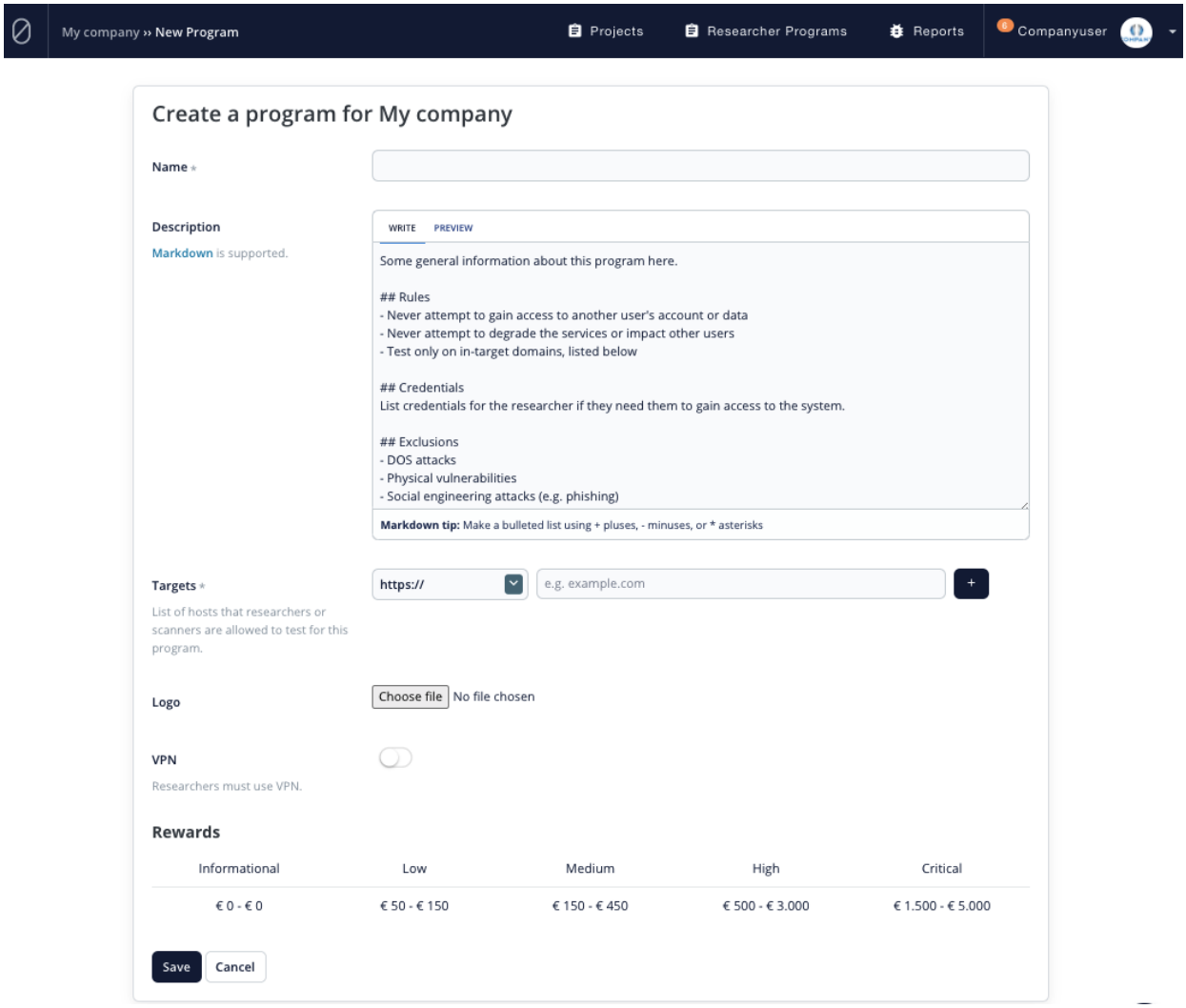
Informational	Low	Medium	High	Critical
€ 0 - € 0	€ 50 - € 150	€ 150 - € 450	€ 500 - € 3.000	€ 1.500 - € 5.000

We subtract the average reward amount from your researcher program budget per validated vulnerability, once you set the actual reward this amount will be subtracted from the researcher program budget.

We provide guidance on the reward amount based on the severity of report:



Creating a Researcher Program



Most important thing is a proper description of your scope: what needs to be investigated? We use the following template for you to describe the scope:

> # Title of the Researcher Program
>
> Some general information about this program here and an introduction to the company/scope.

Rules

- Never attempt to gain access to another user's account or data
- Never attempt to degrade the services or impact other users
- Test only on in-target domains, listed below

Credentials

List credentials for the researcher if they need them to gain access to the system.

Exclusions

- DOS attacks
- Physical vulnerabilities
- Social engineering attacks (e.g. phishing)

Technical details

For example the programming language, CMS, webserver, operating system or other relevant technical details.

Known security issues

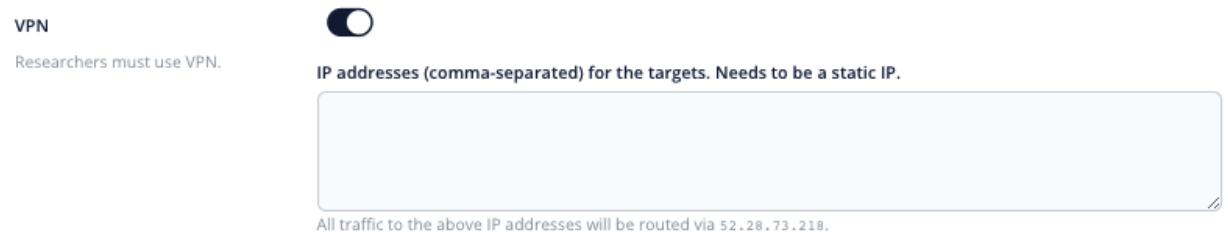
List known security issues which the researcher does not have to report.

After filling in the description you need to fill in the target URLs on which the scope can be found. Zerocopter will always double check a Researcher Program before we get started. Depending on your subscription plan, we can also support you during the process of defining your scope.

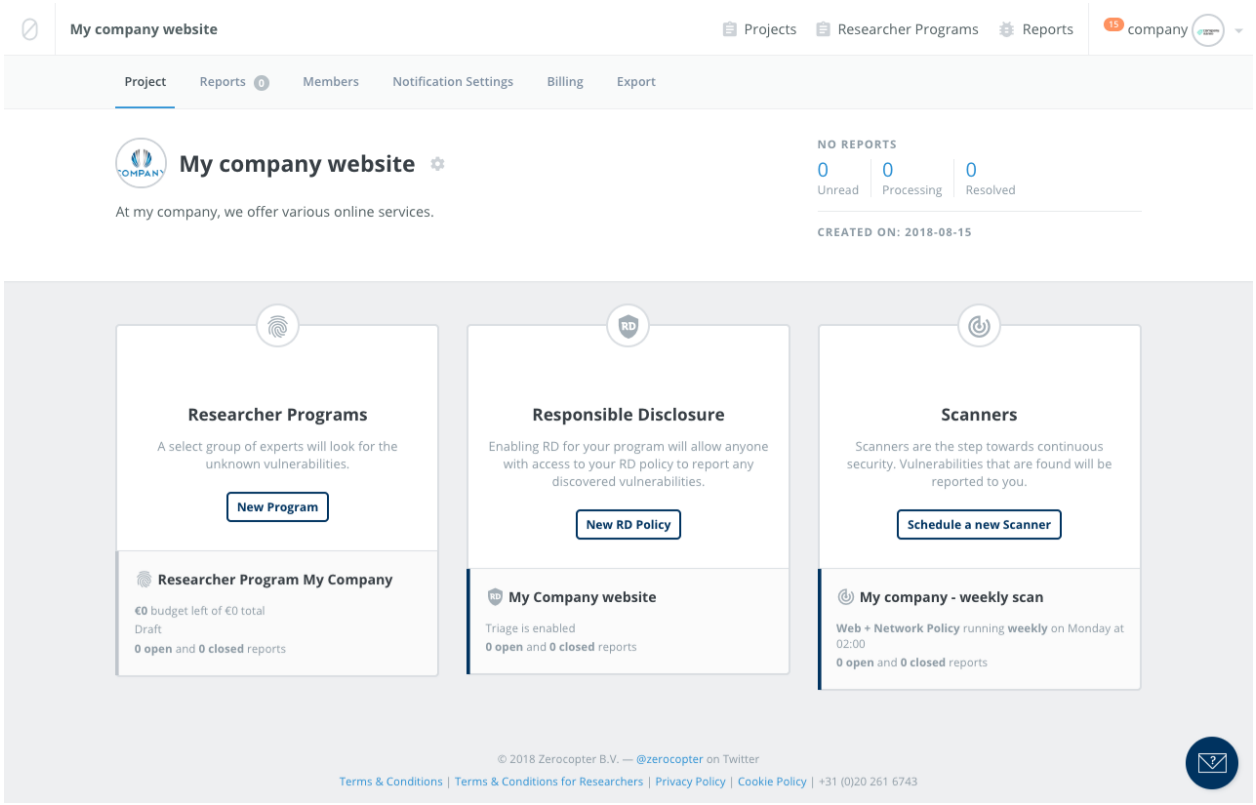
VPN

We offer the possibility to use our VPN service. Enabling our VPN, we provide all researchers with a VPN config file, so they will be investigating your scope from one IP-number. This makes it easier to investigate, for example, a scope that is not publicly accessible and whitelisting is needed.

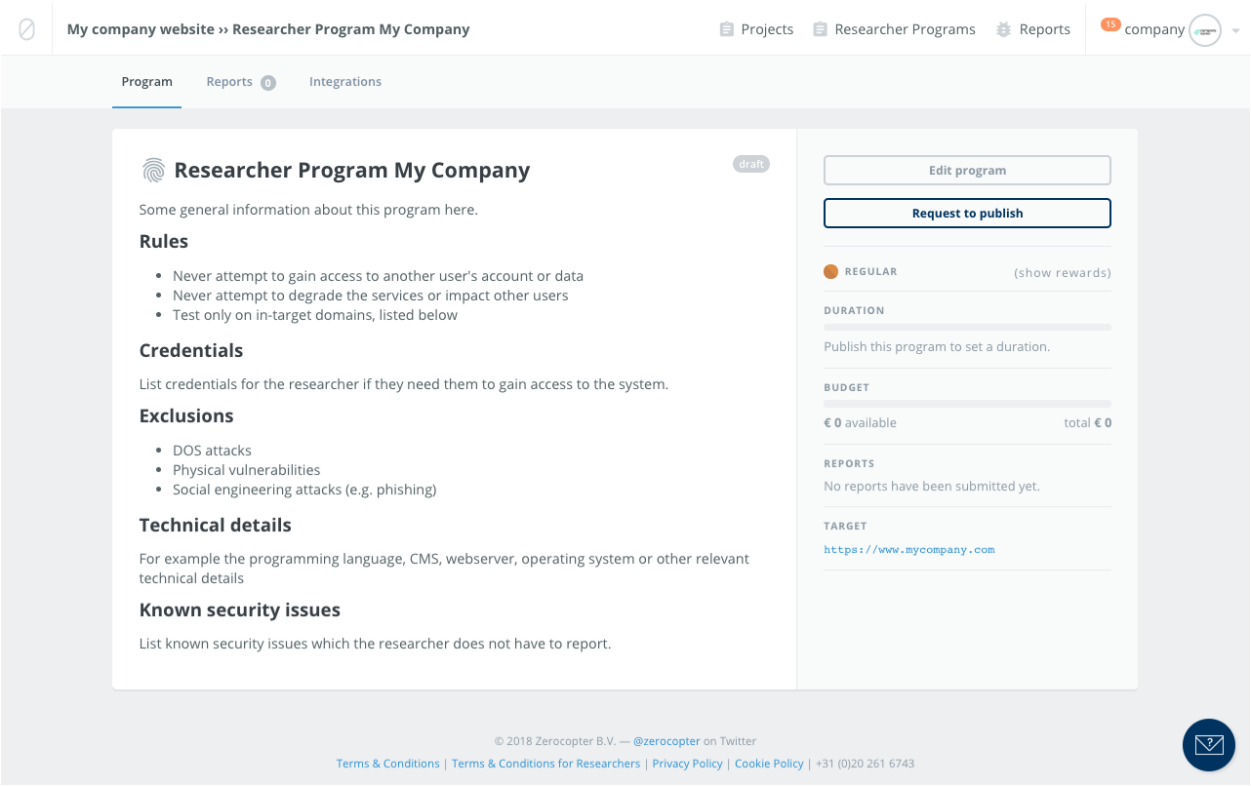
In order to set up the VPN service, we ask you to add all IP addresses that are needed to investigate the scope. Only traffic to those IP addresses will be tunneled through the VPN. When using our VPN service, ensure that the scope is accessible through a static IP number. The traffic will come from the following ip address: `52.28.73.218`



When you save your program, you can see a Researcher Program has been added to your project.

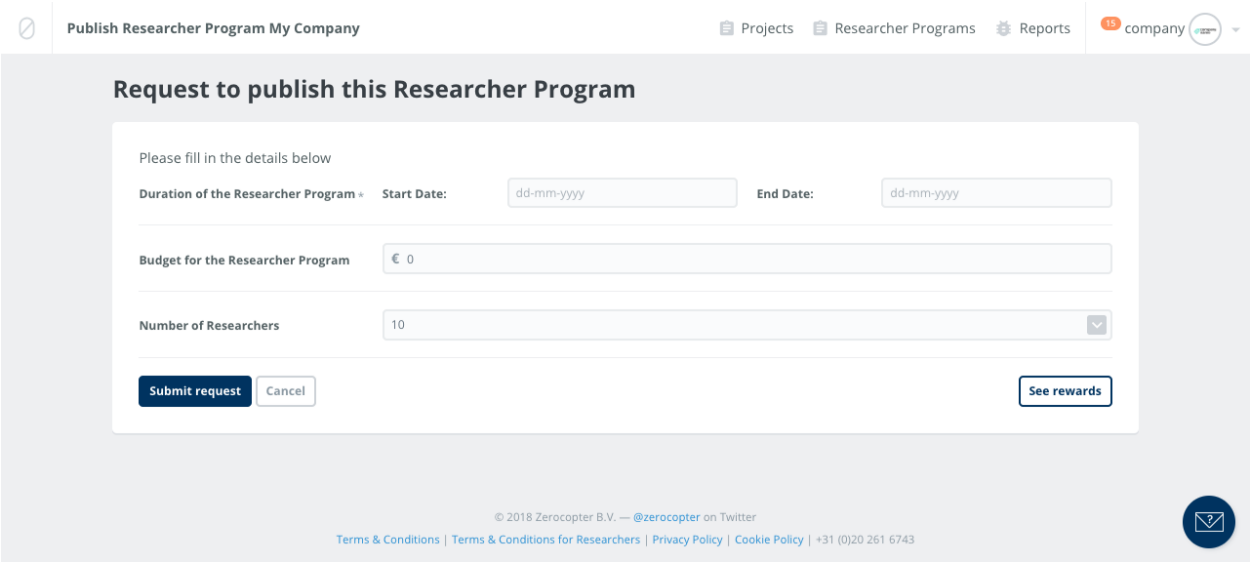


When you click on your program, you can click the blue button ‘Request to publish’.



At this point you need to provide us with some extra information:

- The duration of the Researcher Program (start and end date)
- The available budget for the Researcher Programs. Please note this budget is the budget for the Researchers. We charge a 30% handling fee on all paid bounties, keep in mind that, for example, spending 10.000 euros on budget will result in 13.000 euros costs.
- The number of researchers you would like to invite to your Researcher Program, if you have a preference.



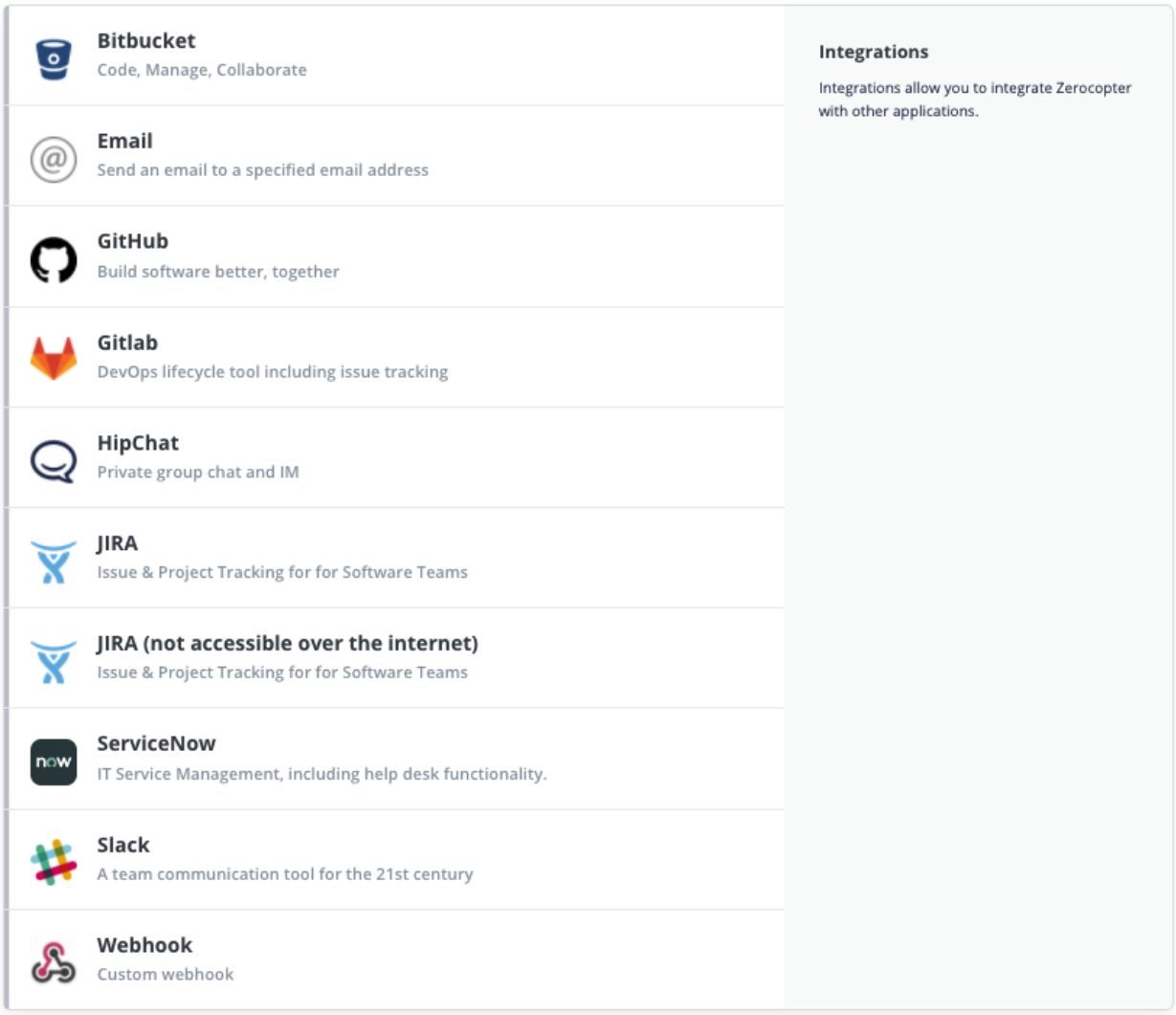
After filling in these fields, you are done. Please, note your Researcher Program is pending, since Zerocopter needs to approve all new programs within a project and double check all Researcher Programs.

If you click on the Researcher Program again, you can see your budget and the duration on the right of the program. Once the program starts, you can see how many days the program runs and how long it takes until the program ends. You can also see how much of your budget has been spent on bounties and what's left of your budget.

Please note that the budget spent includes reports that are in triage. For example: you have a budget of 10.000 euros and someone submits a report with a value of 1.000 euros. At that point you have 9.000 euros left. If triage approves the report, this will remain 9.000 euros. If triage doesn't approve the report, the budget will be 10.000 euros again.

Integrations

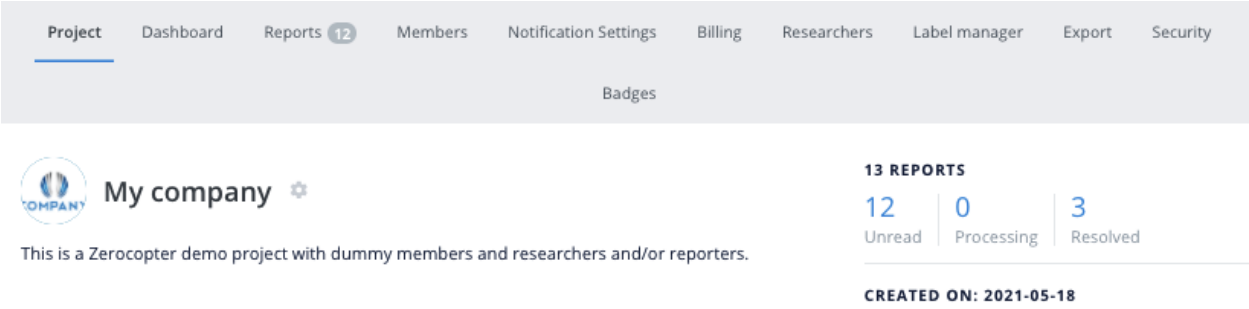
Integrations allows you to push all Researcher Program reports to other applications.



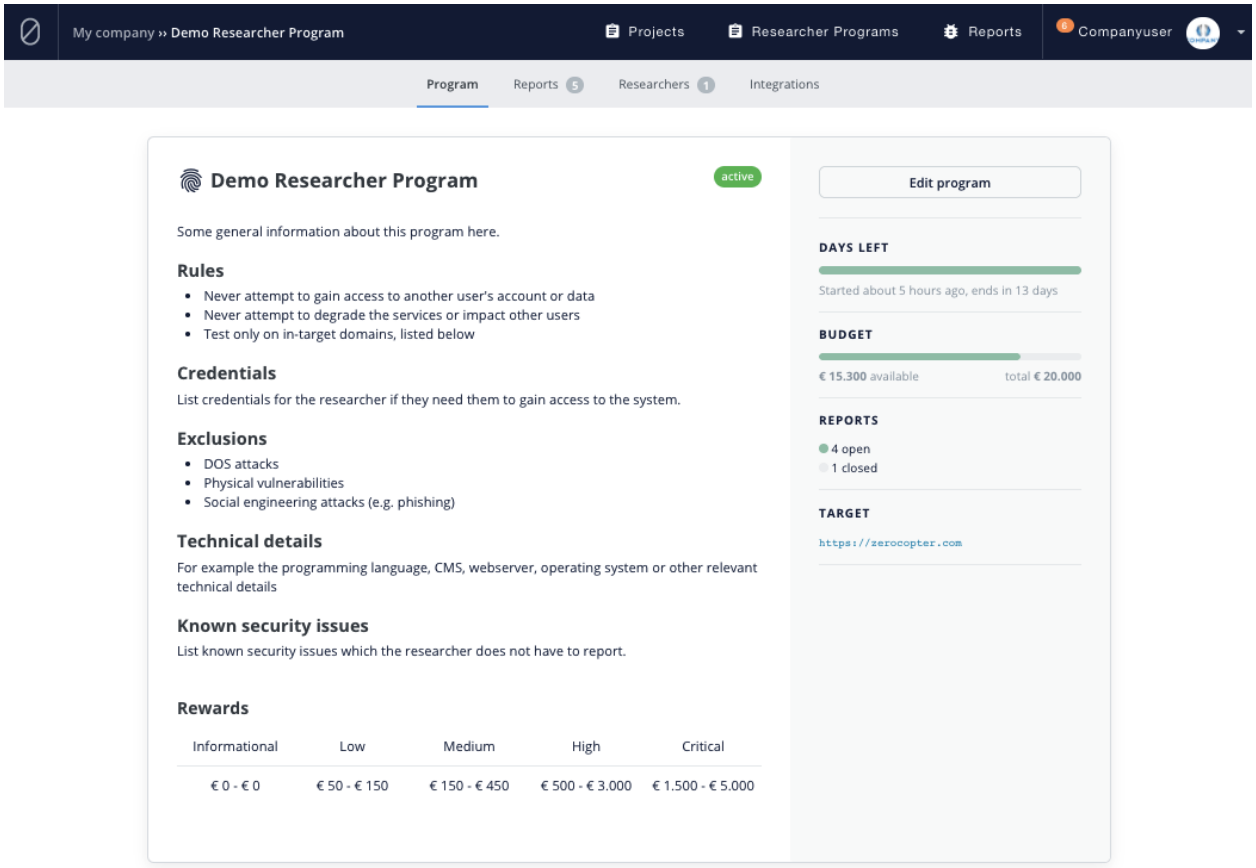
Please note only new reports will be pushed. So if you activate integrations at a later stage, be aware that old reports will not be pushed to your integration. Also: integrations are one-way traffic. Editing a report in an integrated application will not automatically edit the report in our platform.

Reports

All our services result in vulnerability reports, which you can access by clicking on Reports in the top menu. The number behind ‘reports’ in the top menu shows how many reports are open. On the right of your project page you can see the total number of reports, divided by ‘Unread’, ‘Processing’ and ‘Resolved’.



Clicking on Reports gives you access to all reports in our platform. If you prefer to see reports from a particular program (for example a Researcher program), click on the program first and then click on reports. In this case, the number behind ‘Reports’ shows all available reports within the particular program, including closed reports.


My company ›› Demo Researcher Program
Projects
Researcher Programs
Reports
Companyuser
Program
Reports 5
Researchers 1
Integrations
Demo Researcher Program
active
Some general information about this program here.
Rules
Never attempt to gain access to another user's account or data
Never attempt to degrade the services or impact other users
Test only on in-target domains, listed below
Credentials
List credentials for the researcher if they need them to gain access to the system.
Exclusions
DOS attacks
Physical vulnerabilities
Social engineering attacks (e.g. phishing)
Technical details
For example the programming language, CMS, webserver, operating system or other relevant technical details
Known security issues
List known security issues which the researcher does not have to report.
Rewards
Informational
Low
Medium
High
Critical
€ 0 - € 0
€ 50 - € 150
€ 150 - € 450
€ 500 - € 3.000
€ 1.500 - € 5.000
Edit program
DAYS LEFT
Started about 5 hours ago, ends in 13 days
BUDGET
€ 15.300 available
total € 20.000
REPORTS
4 open
1 closed
TARGET
https://zerocopter.com

Report statuses

When you click on Reports in the top menu, you see all open reports, based on their status. The following statuses show a regular flow from a vulnerability report:

- New. New reports need to be checked by our triage team first, you don't see new reports in your overview. Please note that scan reports don't have a new-status, since they are automatically accepted.
- Accepted by Zerocopter. These reports have been validated by our triage team, Zerocopter is responsible for adding this status to a report. Scan reports automatically get this status.
- Work in progress. If you start working on a vulnerability report, you should change the status from 'Accepted by Zerocopter' to 'Work in Progress'. This way you keep an overview on the reports you decided to work on. In case this concerns a report from a Researcher within a Researcher Program or Responsible Disclosure, the Researcher can actually see that you changed the status from the report. So it's also a sign to the Researcher that you started working on his report!
- Retest requested. If you fixed the vulnerability, you can change the status of the report to Retest requested. If the report has been filed by a Researcher (within a Researcher program) or a Reporter (within a Responsible disclosure program), this person will check if the vulnerability has actually been fixed. Please note that this status doesn't apply to scanner reports.
- Resolved. If the vulnerability has been resolved, please change the status to Resolved. In case of a Researcher program, you will need to set the reward and after that the Researcher will receive his reward!

We consider a report to be open, if the report has one of the following statuses: Accepted by Zerocopter, Work in progress or Retest requested.

Other statuses

- Rejected by Zerocopter. Our triage team rejected this report because it's not a valid vulnerability or it's out of scope.
- False positive. Mostly used for scanner reports but sometimes a report from a researcher or reporter can also be a false positive.
- Duplicate. Our triage team rejected this report because the vulnerability has already been submitted by another reporter and it has not been resolved yet.
- Won't fix. You are able to use this status if you decide not to fix a report. This status is usually being used for scanner reports. This requires an expiration date for ISO 127001 standards, you will be notified when the won't fix status expires via mail.

Report severity levels

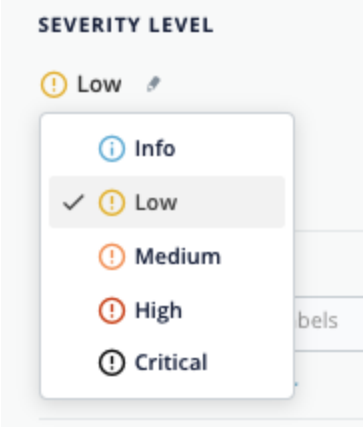
We use the following severity levels for reports:

- Informational (this might or might not actually concern a vulnerability, but we feel you should read and investigate it)
- Low
- Medium
- High
- Critical (needs immediate attention, we will use the emergency contact details in the project to notify you as soon as possible)

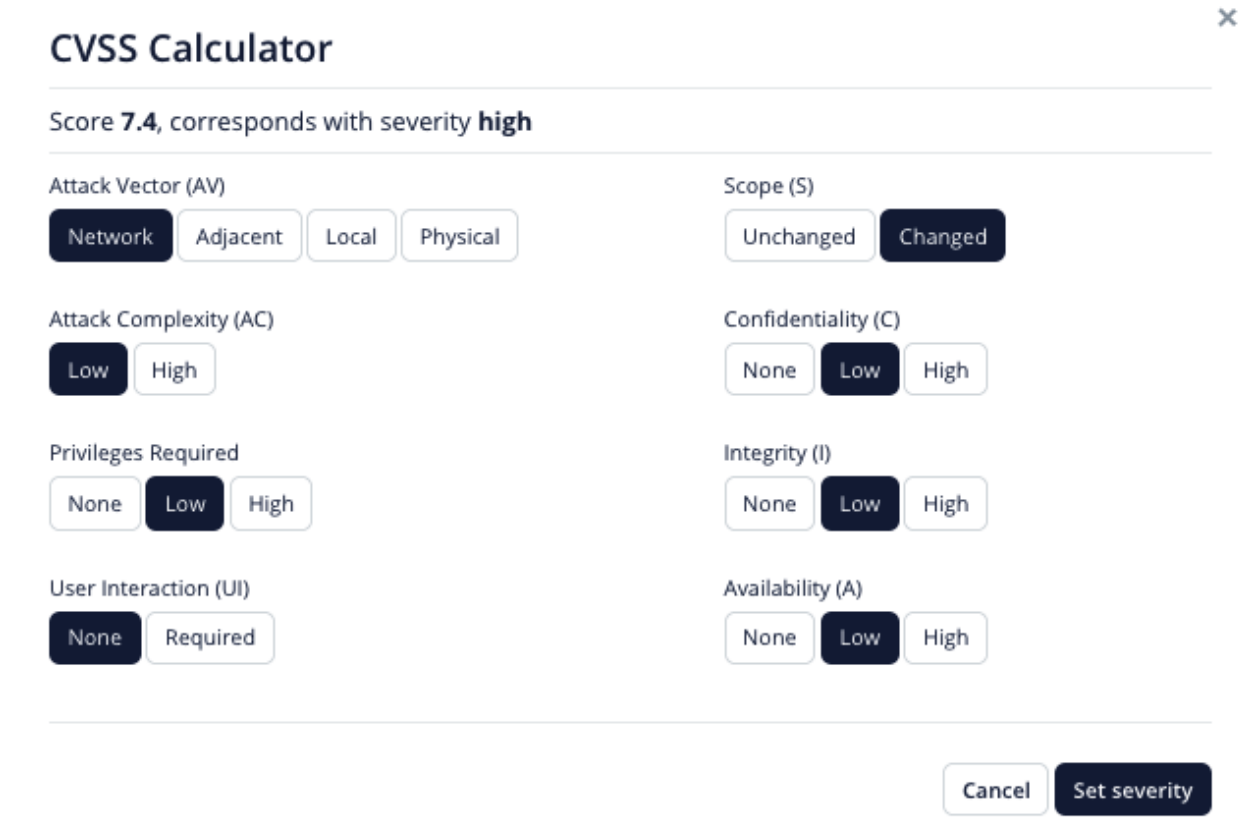
You are always able to change the severity level from a report, since scanners and researchers are not always able to estimate the impact of a vulnerability.

There are two ways to change the severity of a report.

Severity level dropdown:



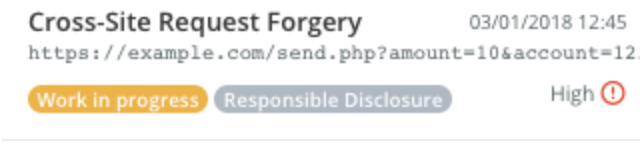
CVSS Calculator:



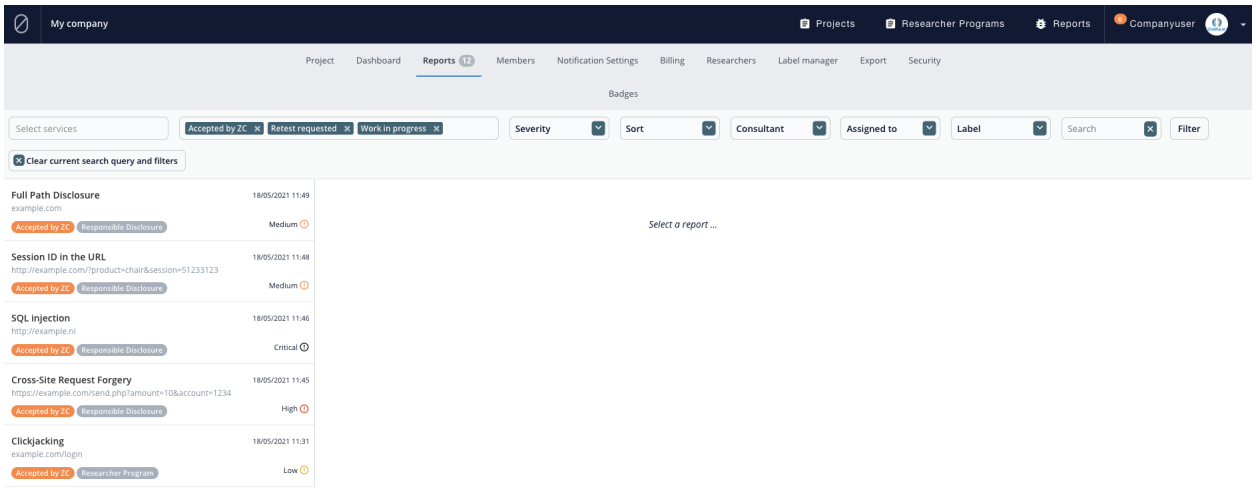
Researchers, reporters and triage can also set the severity using the severity level dropdown or by using the CVSS calculator. CVSS calculator scores will be saved.

Reports overview

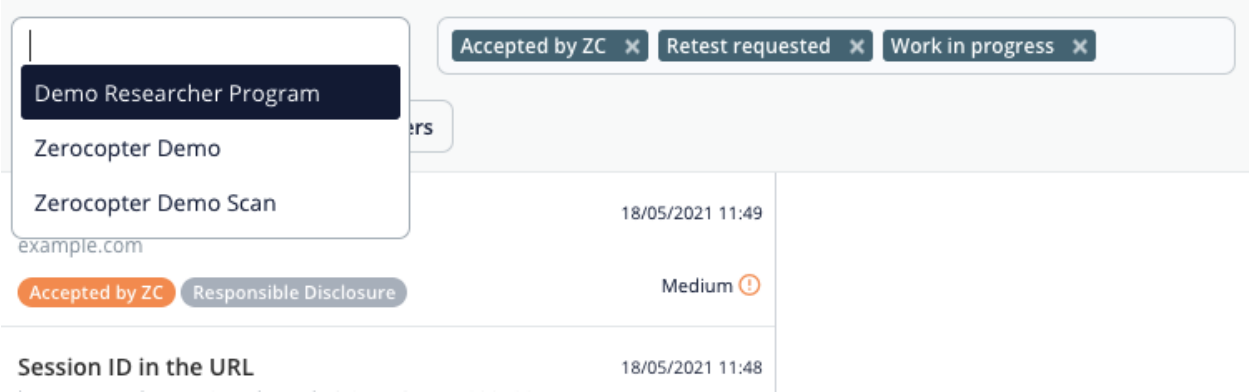
When you click on Reports from the top menu, you see an overview of all open reports. A report snippet contains the title and the URL of the report, the date and time it was submitted, the type of program it was reported within, the status of the report and the severity level.



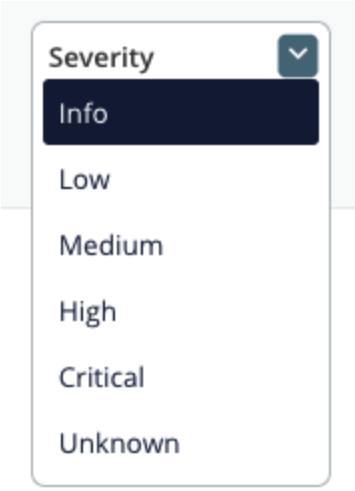
In the overview page you can see that 3 reports statuses have been selected by default so all open reports are displayed. You can change this by adding statuses or deleting statuses. If you delete all statuses, you can see all reports.



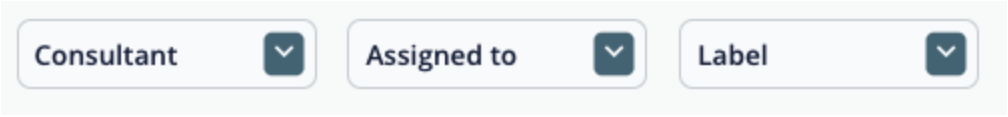
You can filter by selecting a specific program. You can combine this with one or more programs.



You can filter the reports by selecting a severity level. You can combine this with one or more report statuses.

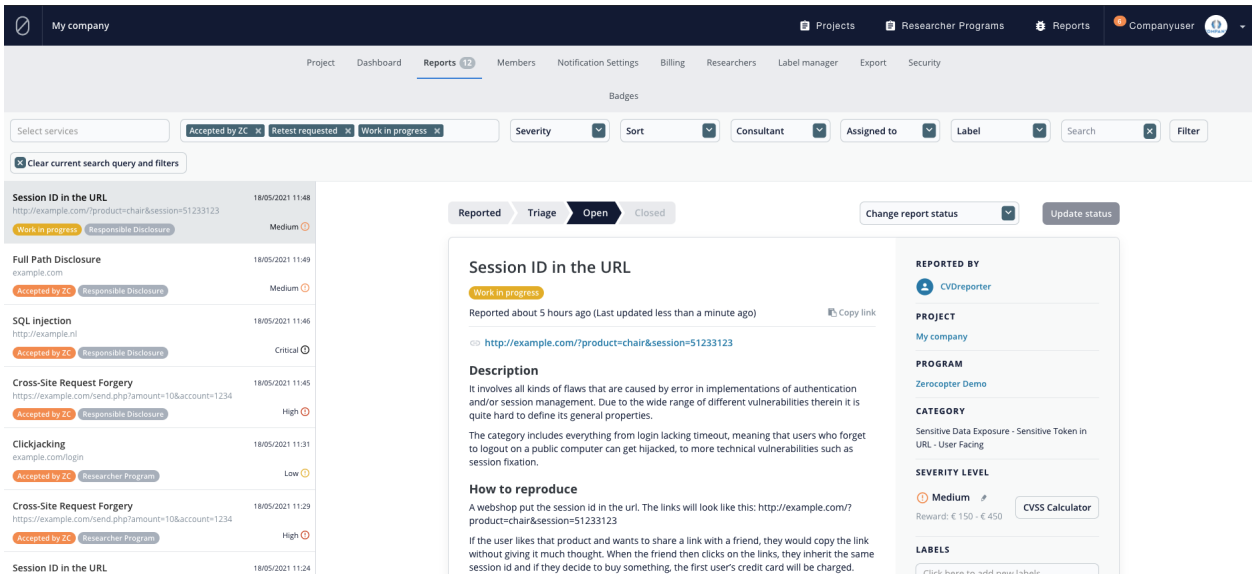


You can filter the reports by selecting an assigned consultant, project member or label. You can combine these as well.



Finally you can search within reports to filter your overview and sort on activity or creation date.

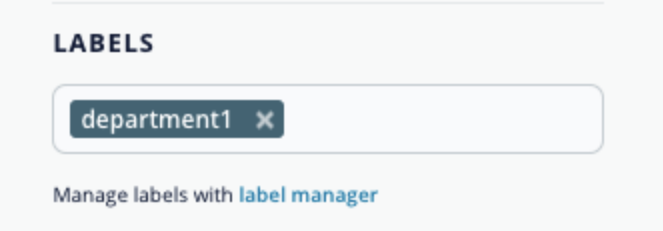
Report details



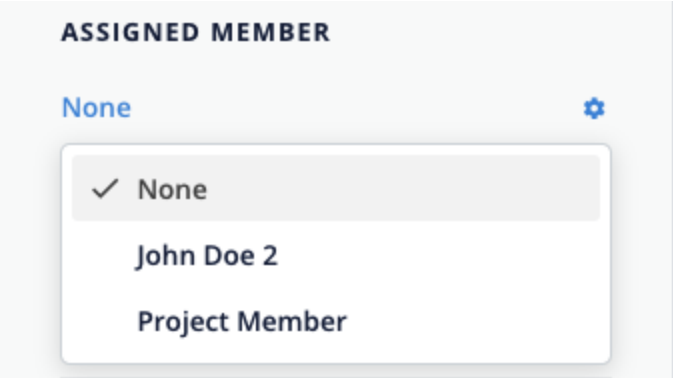
When you click on a snippet you get to see the full report. Above the title you can see it's an open report and on the right you can change the status of the report. In the middle of your screen you can see the full report. On the right you can see some additional data:

- Reported by. The username of the Researcher or 'Scanner' if the report has been submitted by our scanner. In some cases there is no name, this means someone has anonymously submitted a report to your Responsible Disclosure program. We are not able to contact reporters of an anonymously submitted report, we inform reporters before they submit the report that we are not able to contact them if they submit a report anonymously.
- Project. The name of the project in which the report has been submitted.
- Program. The name of the program in which the report has been submitted.
- Category. When a report is submitted by a Researcher or a Reporter, they have to select a category and a sub category regarding the type of vulnerability they want to report. In this particular example: Sensitive Data Exposure - Sensitive Token in URL - User Facing. Note that the category of a scanner report doesn't contain these categories (the category here is always 'Scanner - ZC-ZAP').
- Severity level. The severity level of the reported vulnerability. You can edit the severity level by clicking on the pencil or using the CVSS calculator.

- Labels. Labels can be created and added to reports.



- Assigned member. You can assign members in the project to a report. They will be notified when they are assigned to a report via mail.

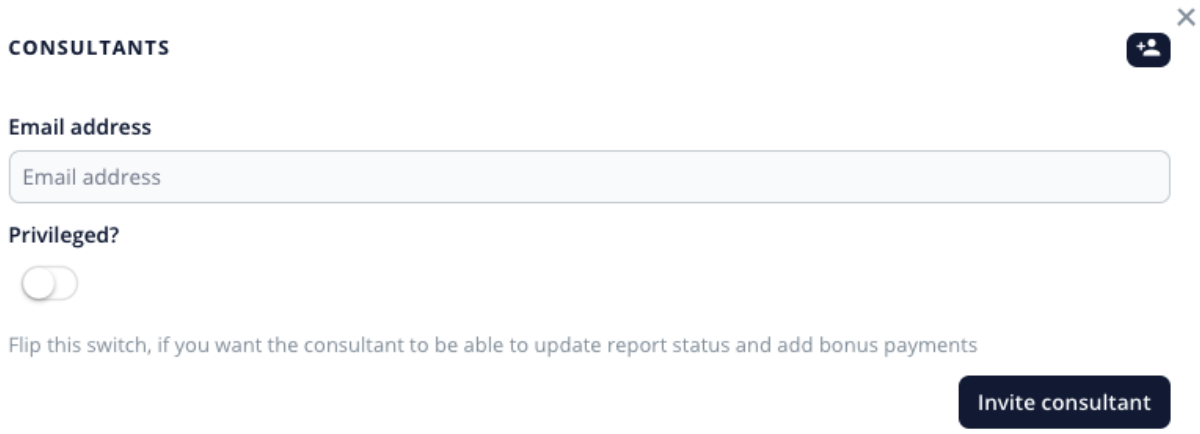


- Reward amount. By clicking on “Pay your researcher” you can set the reward amount.
- Payment status. Here you can see the status of a payment. Of course this is not available within a scanner report. There are 4 statuses available:
    - Not paid
    - Payment scheduled
    - Paid
    - Not applicable (rewards total is 0)

Additional functionalities

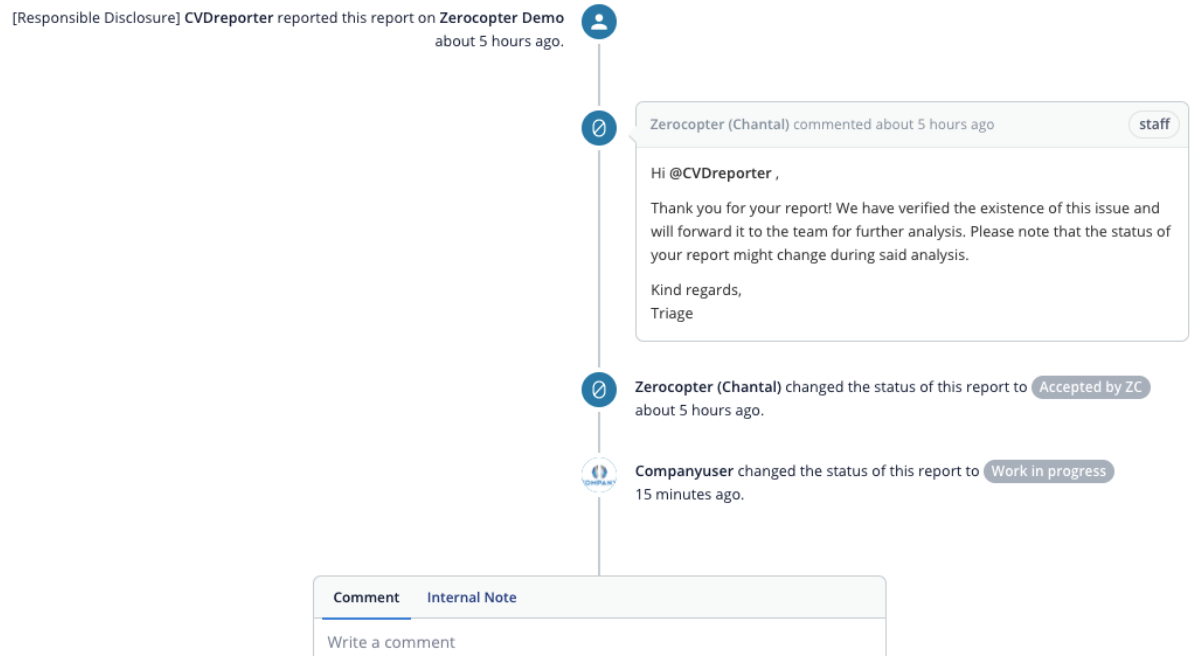
- Add bonus. You can add a bonus to a report. Within a Researcher Program or Responsible disclosure, a bonus is added to the reward. So if the reward amount is 500 euros and you add a 100 euros bonus, we will pay the Researcher 600 euros in total. For Responsible Disclosure the reward and the bonus are optional.
- Consultants. You can add one or more consultants to a single report. These consultants can help you fix the vulnerability and will only be able to see the report you’ve added them to. You can simply add one or more email addresses to invite people to assist you on the report by clicking on

the button. You can make a consultant privileged or not (default). Privileged consultants are able to also update report statuses and add bonuses.



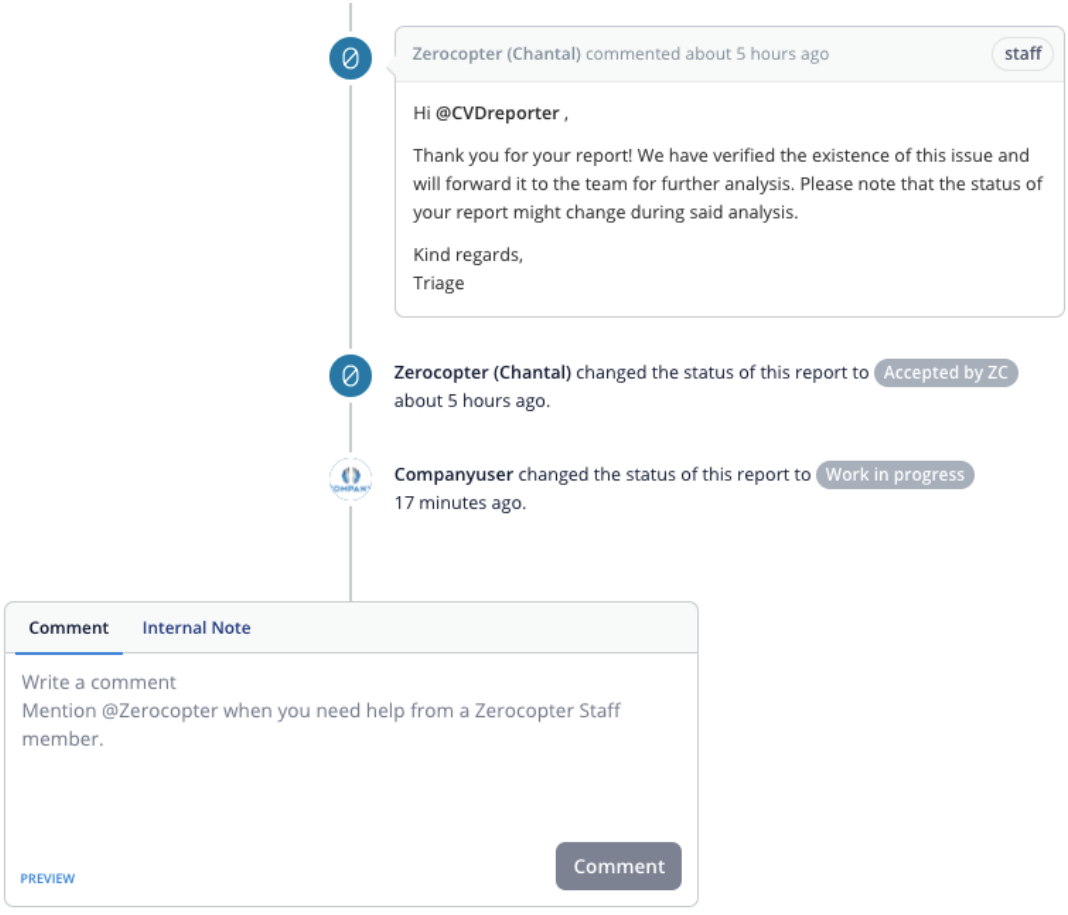
Updates and additions

Below a report you can see the status updates from the report.



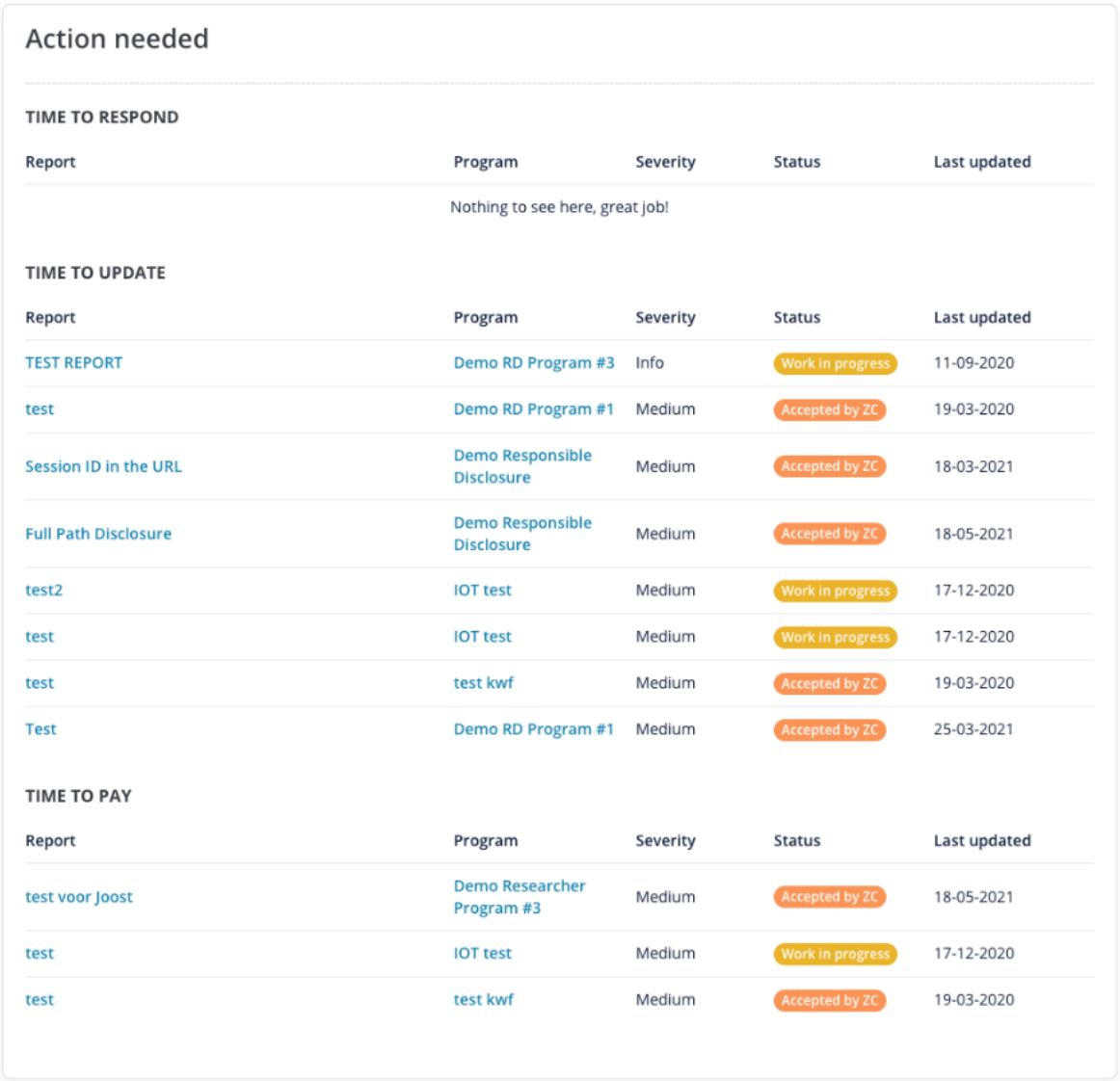
You can also add comments or internal notes to a report. There are several reasons to add comments or internal notes. Internal notes could be for internal use, for example adding a JIRA ticket ID or discussing a fix with your colleague. You can also communicate with Zerocopter support and/or our triage team, as well as with the Researcher (in case the report has been submitted during a Researcher Program), by mentioning someone (for example @zerocopter or @researcher). You could be mentioned as well! There are 2 ways you can add a comment:

- Comment. In this case everyone involved can read your comment.
- Internal note. Everyone except the Researcher can read your comment.



Dashboard

The dashboard provides a summary of the project's reports and statistics. Firstly, you will clearly see the reports that require your action (respond/update/pay). Secondly, you will be able to filter the reports per time, see the exact amount of reports per status and per severity. Thirdly, you will have the information about the rewards (paid, scheduled, unpaid).



Action needed

TIME TO RESPOND

Report	Program	Severity	Status	Last updated
Nothing to see here, great job!				

TIME TO UPDATE

Report	Program	Severity	Status	Last updated
TEST REPORT	Demo RD Program #3	Info	Work in progress	11-09-2020
test	Demo RD Program #1	Medium	Accepted by ZC	19-03-2020
Session ID in the URL	Demo Responsible Disclosure	Medium	Accepted by ZC	18-03-2021
Full Path Disclosure	Demo Responsible Disclosure	Medium	Accepted by ZC	18-05-2021
test2	IOT test	Medium	Work in progress	17-12-2020
test	IOT test	Medium	Work in progress	17-12-2020
test	test kwf	Medium	Accepted by ZC	19-03-2020
Test	Demo RD Program #1	Medium	Accepted by ZC	25-03-2021

TIME TO PAY

Report	Program	Severity	Status	Last updated
test voor Joost	Demo Researcher Program #3	Medium	Accepted by ZC	18-05-2021
test	IOT test	Medium	Work in progress	17-12-2020
test	test kwf	Medium	Accepted by ZC	19-03-2020

zerocopter

Statistics

Date range

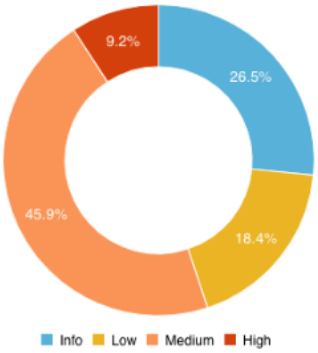
Adjust the dates to see the statistics in that period of time.

From 13/12/2017 to 18/05/2021

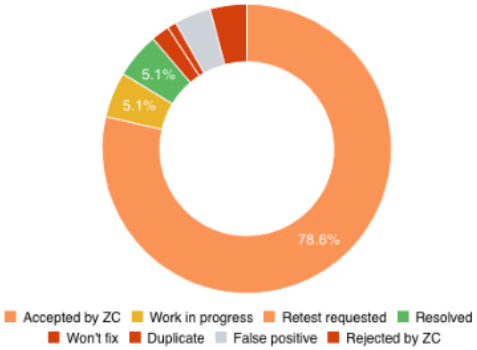
Filters: All | Last year | Last month | Last week | Last 24h

Total	Open	Per status	Status
98	82	77	Accepted by ZC
		5	Work in progress
		0	Retest requested
		5	Resolved
		2	Won't fix
		1	Duplicate
		4	False positive
		4	Rejected by ZC

Severities



Statuses

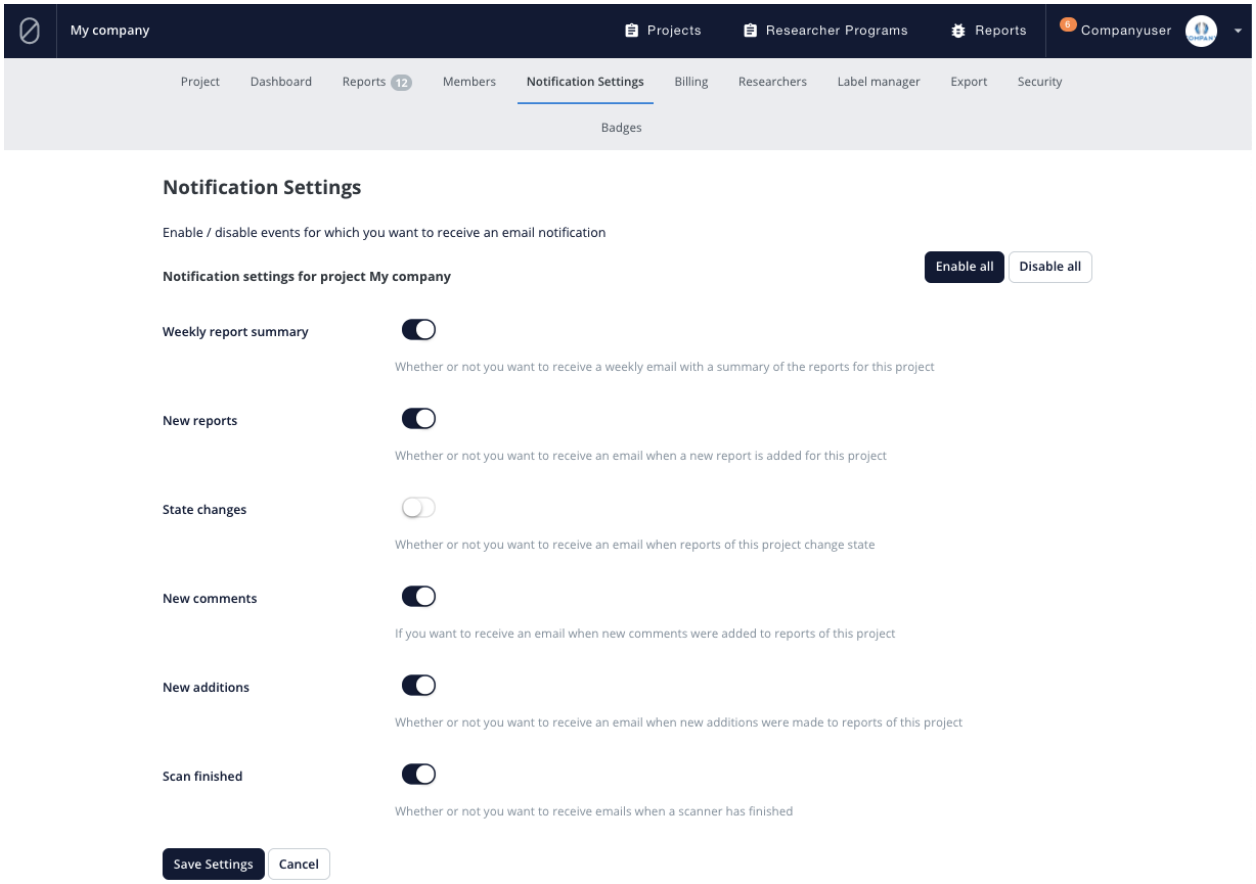


Rewards

Paid	Scheduled	Unpaid
€ 50	€ 0	€ 5.409

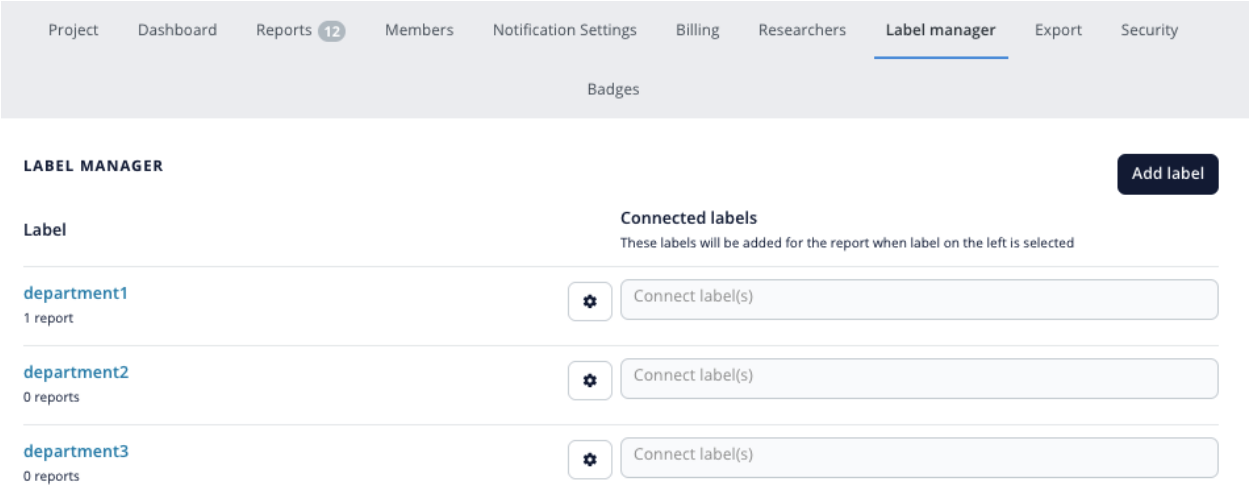
Notification settings

We notify you via email when something happens on our platform, for example, a new report has been added or someone placed a comment below a report. These notifications don't contain any sensitive information like the content of a report, but only a notification that there is a new report or comment. You can manage your notification settings by clicking on it in our top menu.



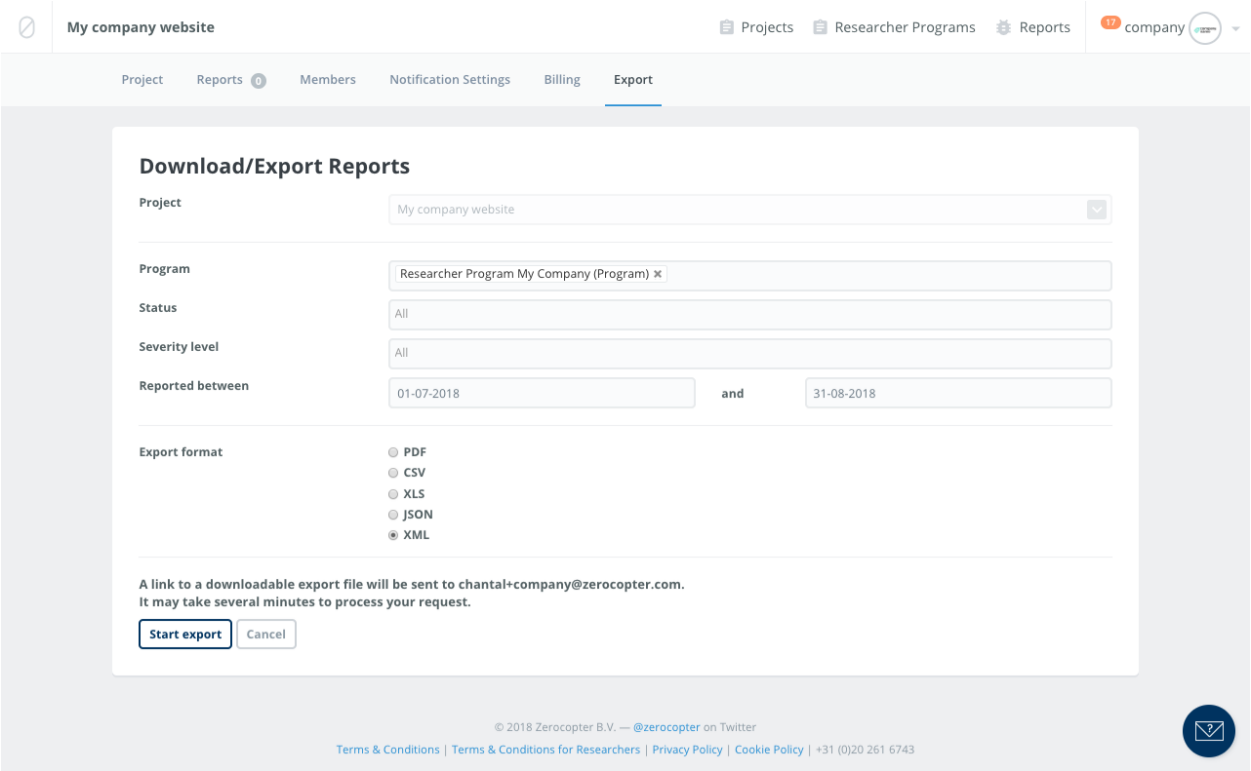
Label manager

In the label manager you can create/edit/remove labels and link labels to each other. Labels can be used in the reports. In report overviews you can sort reports by label. The labels are not seen by researchers or reporters.



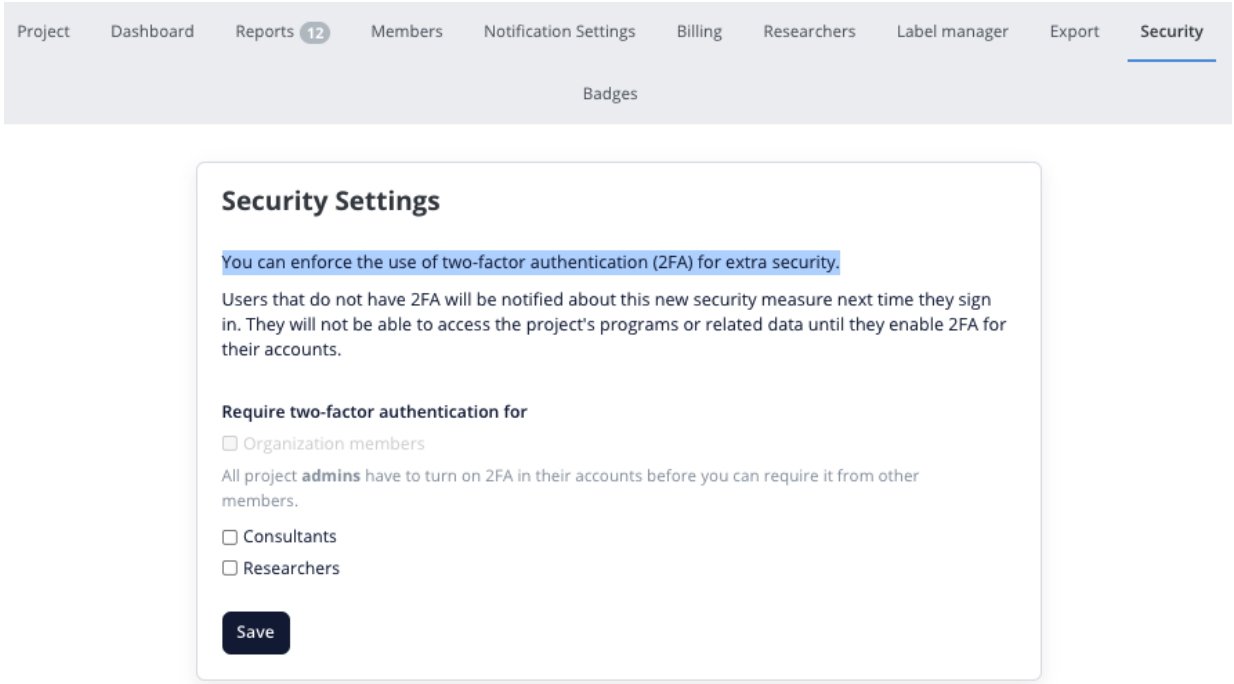
Download / export reports

You can download (a selection of) reports by clicking on ‘Export’ in the top menu. You can use several filters and we offer multiple export formats.



Security

In security settings you can enforce the use of two-factor authentication (2FA) for extra security.

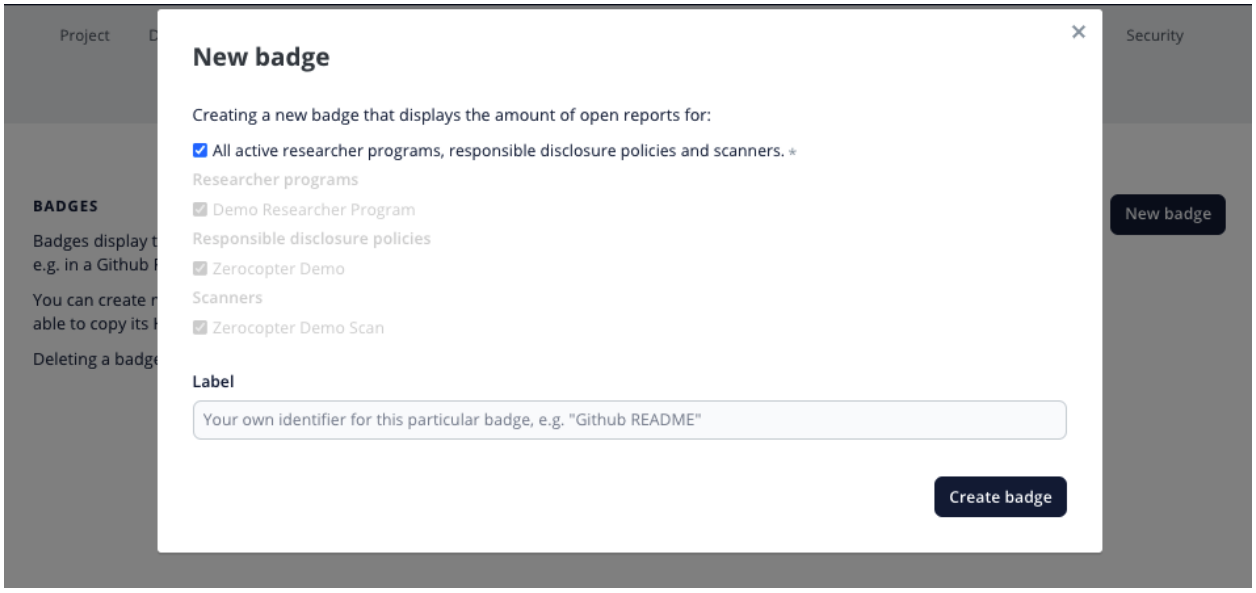


Badges

Badges display the amount of open reports within this project and can be embedded on any third-party website, e.g. in a Github README. Clicking on the badge will take you to the list of the open reports.

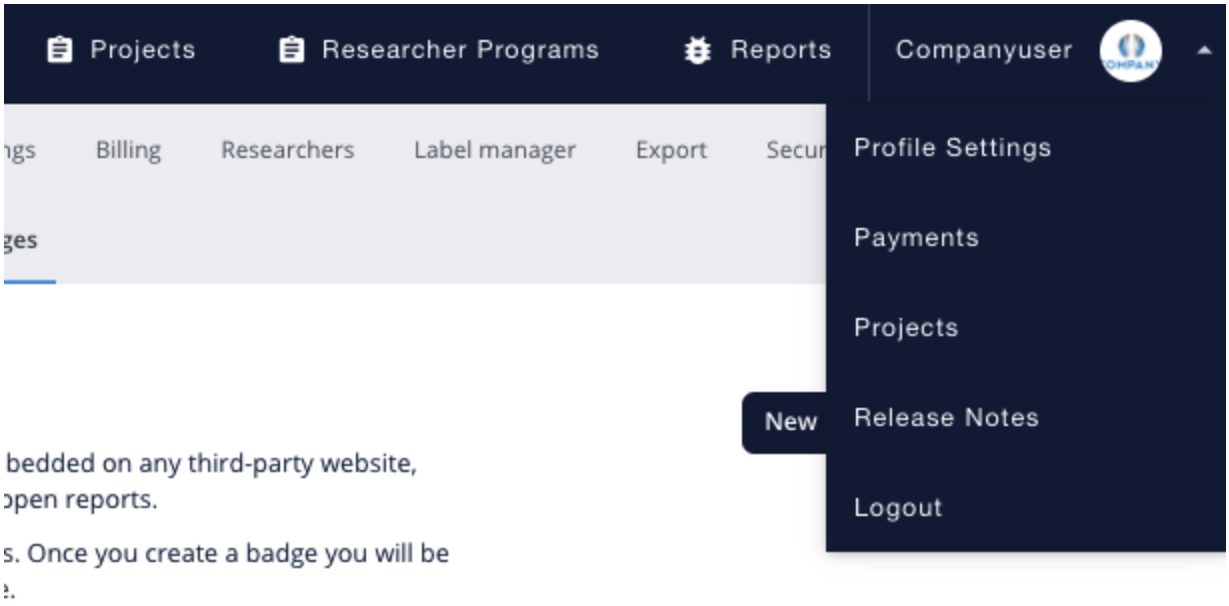
You can create multiple badges per project and use them in different contexts. Once you create a badge you will be able to copy its HTML or Markdown code to the web document of your choice.

Deleting a badge will deactivate its link and remove the image from the web documents it was used in.



Profile

In the top right you can see your profile. If you click on it, you have five options.



We will not discuss payments in this document because this is only applicable to users that receive payments for bounty hunting.

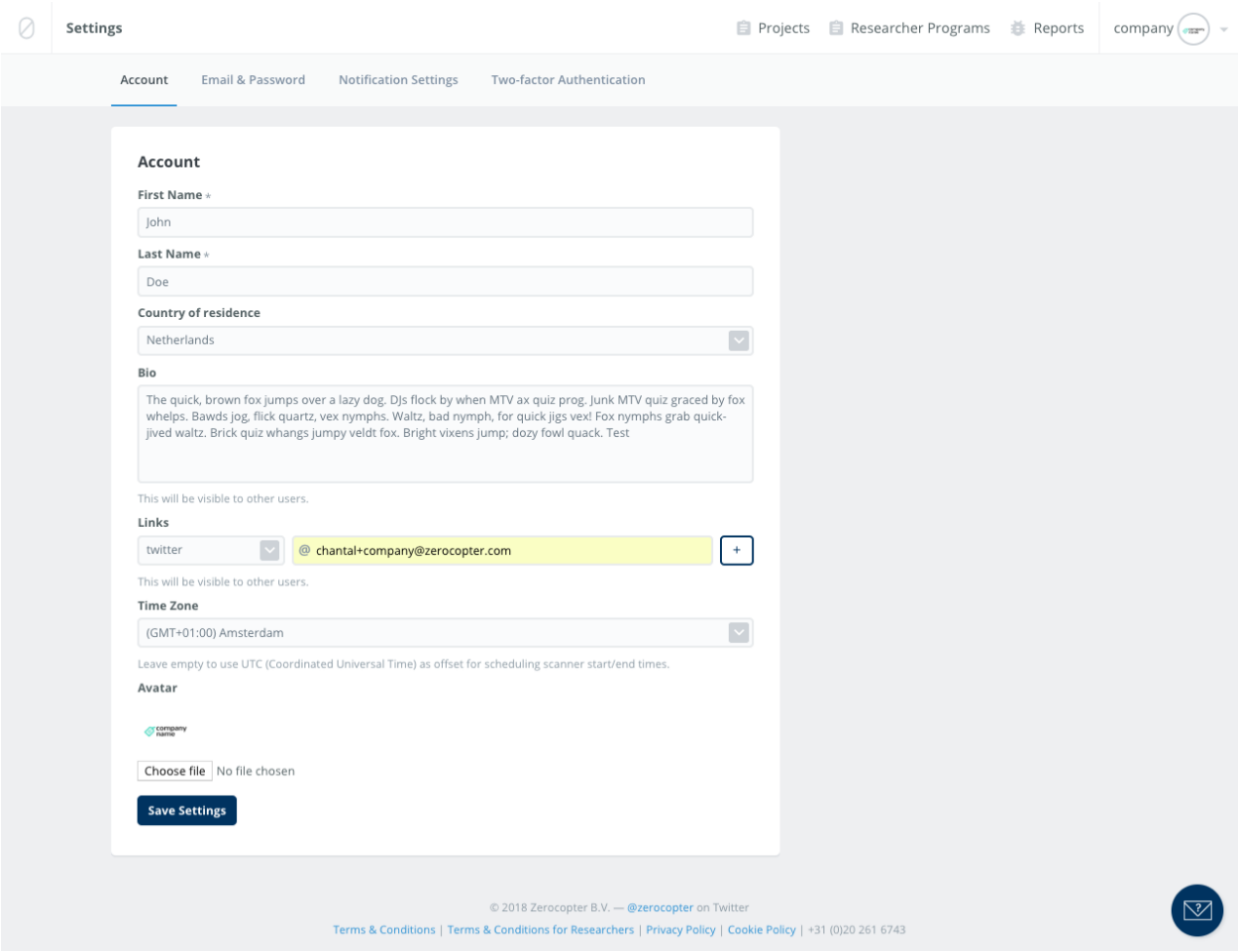
Profile Settings

Here you can see and edit your profile. You have six submenu items here:

- Account
- Email & Password
- Notification settings (only usable for people who also submit reports, so we don't mention this option in these instructions)
- Two-factor Authentication
- Payment settings (applicable to users that do bounty hunting, so we don't mention this option in these instructions)
- Delete account

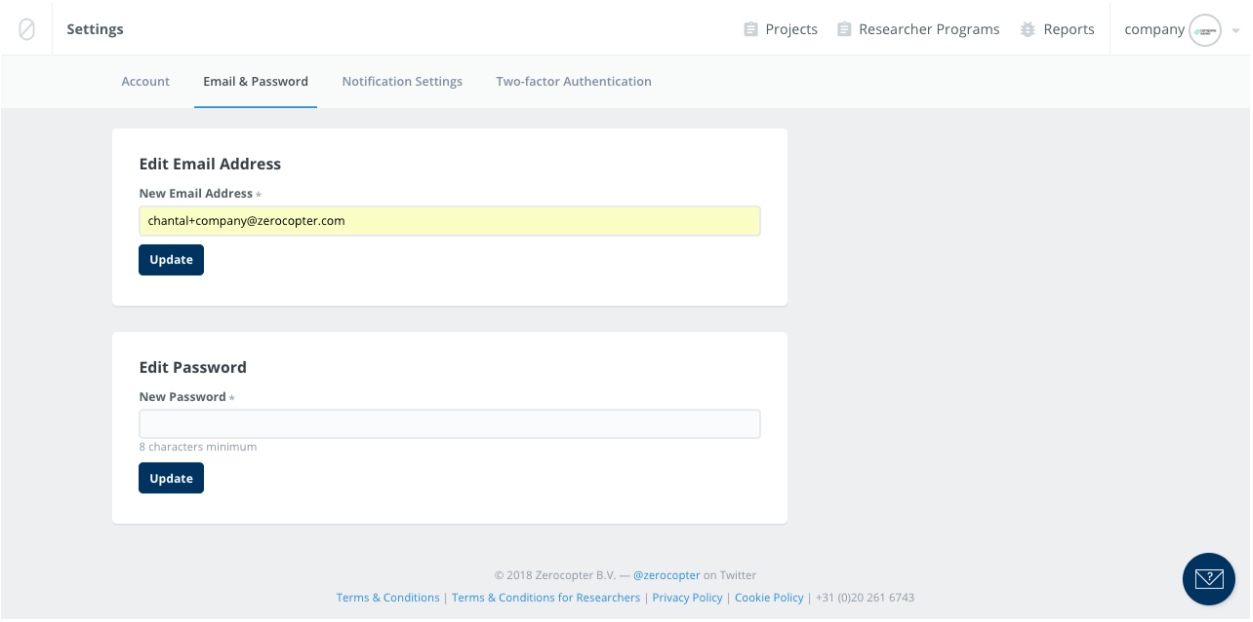
Account

In this section you can manage and change your default account settings, like your name, timezone and avatar.



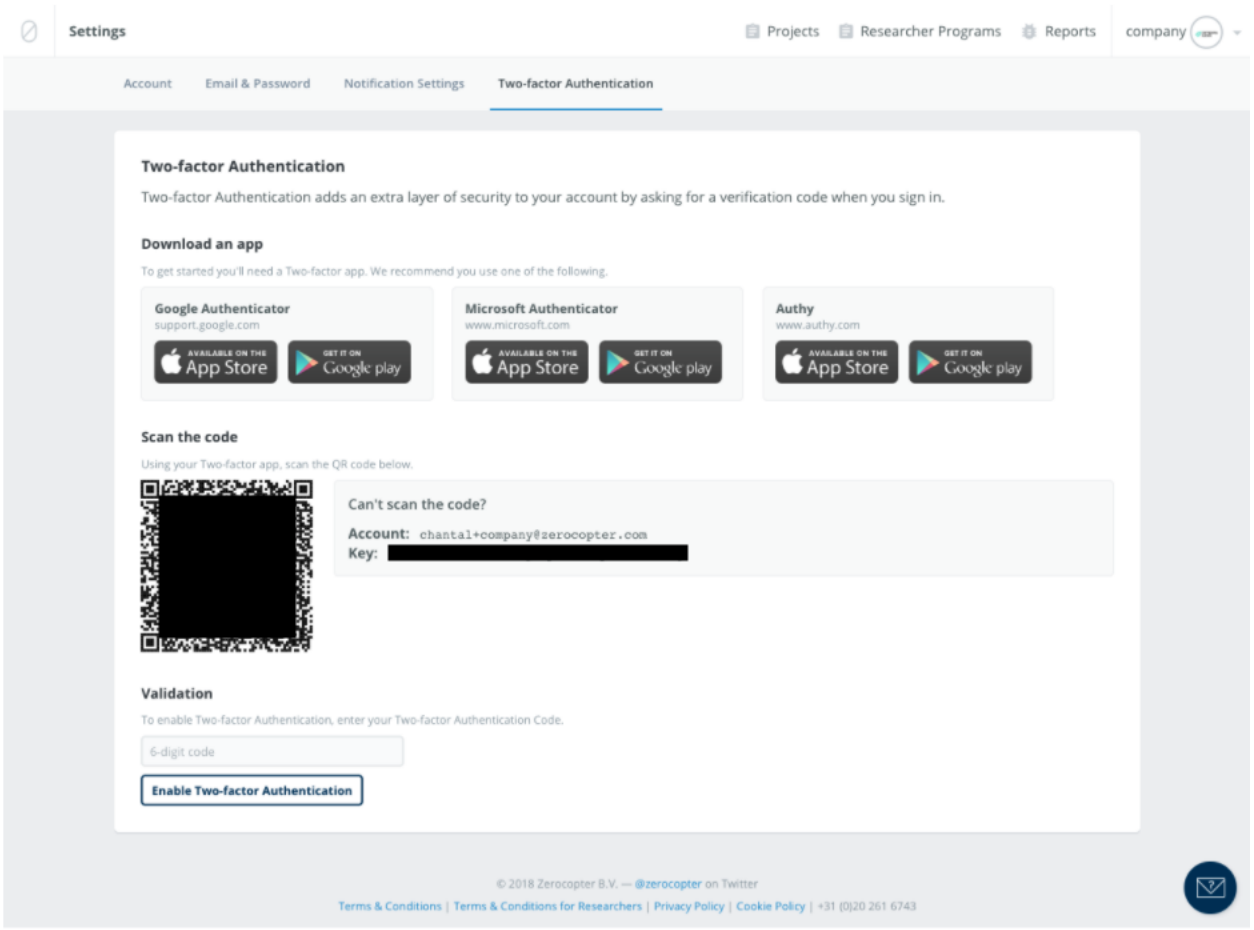
Email & Password

In this section you can manage your email address and change your password.



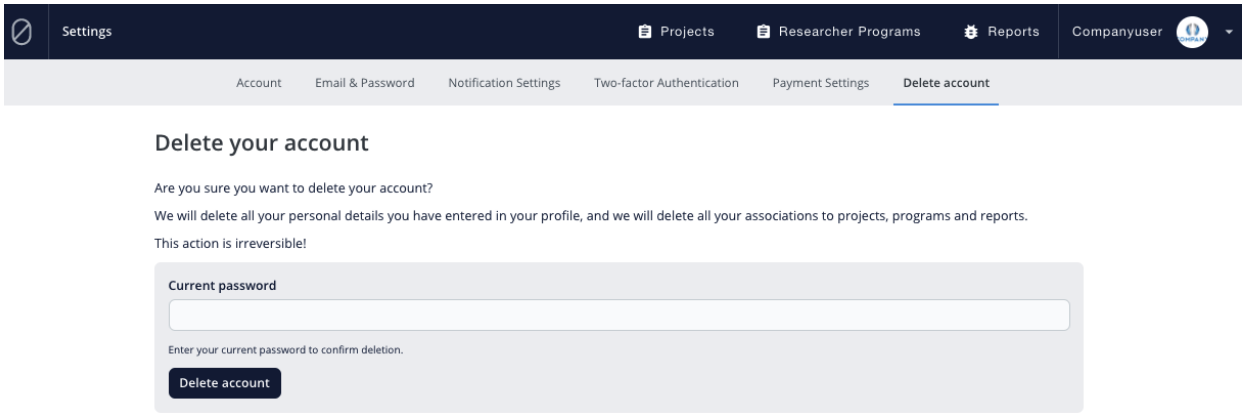
Two-factor Authentication

We strongly advise you to enable two-factor Authentication, by following the steps on this page. Make sure you save the recovery codes in a safe place!



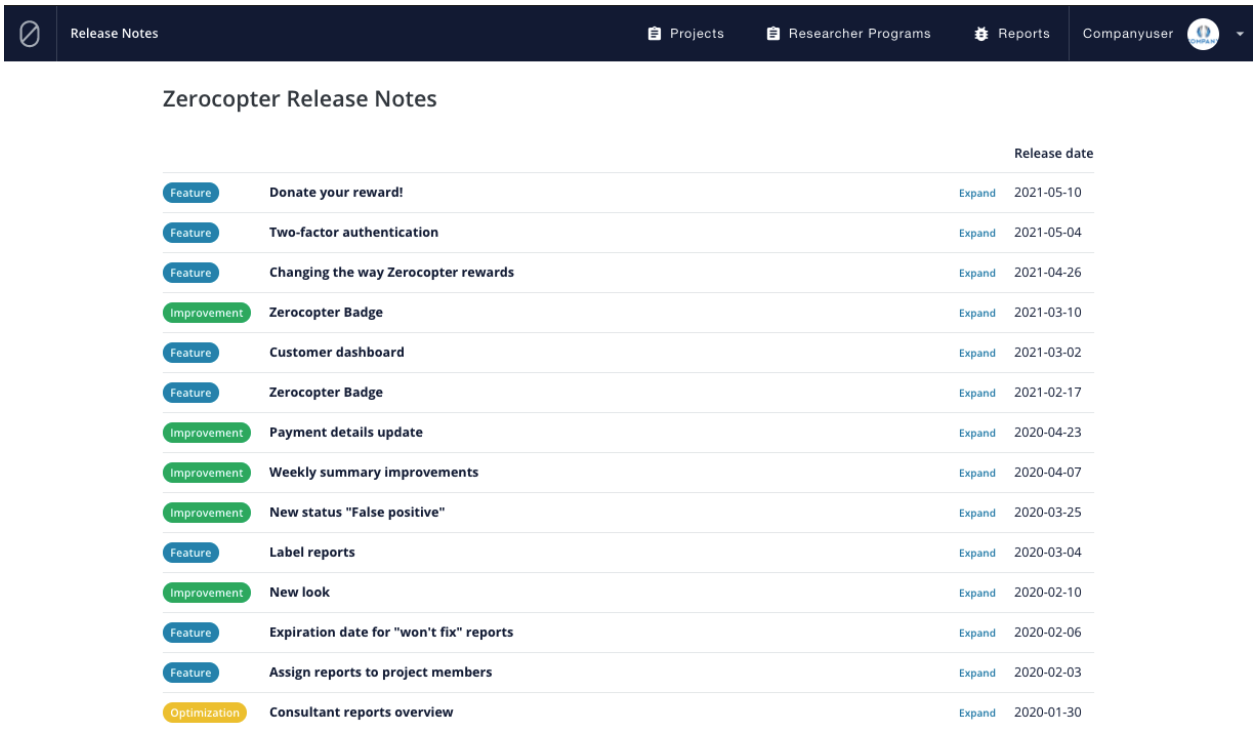
Delete your account

We will delete all your personal details you have entered in your profile, and we will delete all your associations to projects, programs and reports. Be careful: this action is irreversible!



Release Notes

Here you can see all changes we make to our platform. In case we add a release note, you will see an icon popping up in your profile menu.



Some final thoughts

- Run a scanner before running a Researcher Program. If the scanner finds a vulnerability and a Researcher does as well, the report from the Researcher will be marked as a duplicate.
- If credentials are needed to run a Researcher Program, please provide us with at least 5 to 10 credentials, ideally 100 credentials in a txt file. And please also provide us with 2 credentials for our triage team.
- Don’t change the scope of a Researcher Program 2 weeks before, 2 weeks after and during the program.
- When you decide to use our VPN service, make sure the scope is accessible with static IP numbers.
- When starting a Researcher Program, please inform colleagues and other people who are involved in the program, so they can schedule some time to work on reports.
- Researchers are being paid if the vulnerability is resolved. Please take this into account.
- If you don’t agree on the category of a report, please explain this to the Researcher.
- Once a report is closed, you can’t re-open it.
- Please inform the Researchers about development / progress concerning the reports. They really appreciate an update from time to time!