Qualifio

Information Security Management System

Bug Bounty Program

Code :	DOC-010
Version:	1.1
Date of version:	06/09/2022
Created by:	Patrick Nollet
Approved by:	Quentin Paquot
Approval date:	23/09/2022
Confidentiality level:	Public

Change history

Date	Version	Created by	Description of change
14/01/2021	1.0	Patrick Nollet	Initial version
06/09/2022	1.1	Patrick Nollet	Annual review

Table of content

Bug Bounty Program **1**

Change history **2**

Table of content **3**

Qualifio Bug Bounty Program **4**

- **Scope** **4**
- **Non-qualifying vulnerabilities** **4**
- Social Engineering 5
- Disclosure Policy 5
- Bounty 5

Qualifio Bug Bounty Program

Keeping Qualifio application and end-user information safe and secure is a top priority and a core value for us as a company.

As such, We welcome the contribution of external security researchers and look forward to awarding them for their invaluable contribution to the security of all Qualifio users.

No technology is perfect, and Qualifio believes that working with skilled security researchers across the globe is crucial in identifying weaknesses in any technology.

If you believe you've found a security issue in our product or service, we encourage you to notify us. We welcome working with you to resolve the issue promptly.

Reported bugs will be assessed by our security team to determine if they qualify for a reward. Qualifio will consider the impact to the company and to our users, and will calculate the reward accordingly. Bug submissions will be reviewed within 30 days.

Scope

Our Bug Bounty program is limited to security vulnerabilities in the Qualifio web application.

Are strictly out of scope:

- Social Engineering attacks: such as (but not limited to) phishing against our staff and end-users
- Attacks that result in the unavailability of our services to all users: such as DoS attacks, spam people, or do other similarly questionable things.
- Vulnerability testing tools that automatically generate significant volumes of traffic are strictly prohibited.

The following sites and applications are in scope for this program:

- *.qualifio.com

Vulnerabilities reported on other Qualifio properties or applications, such as blog.qualifio.com or commercial website (www.qualifio.com or qualifio.com) are currently not eligible for rewards

Non-qualifying vulnerabilities

The following bugs are unlikely to be eligible for a reward:

- Issues found through automated testing
- Scanner output or scanner-generated reports
- CVE Vulnerabilities released within the last 60 days
- Missing http security headers
- Logout and other instances of low-severity Cross-Site Request Forgery
- SSL/TLS best practices
- Denial of Service attacks or Rate limiting issues

- Brute Force attacks
- Lack of Captcha
- Lack of Secure/HTTPOnly flags on non-sensitive Cookies
- Spam including:
- DMARC, SPF and DKIM issues
- Content injection
- Hyperlink injection in emails
- Content Spoofing / text injection
- Issues relating password and account recovery policies, such as reset link
- expiration or password complexity
- Full-Path Disclosure on any property
- Clickjacking/UI redressing with no practical security impact
- CSRF-able actions that do not require authentication (or a session) to exploit
- Reports related to the following security-related headers:
    - Strict Transport Security (HSTS)
    - XSS mitigation headers (X-Content-Type and X-XSS-Protection)
    - X-Content-Type-Options
    - Content Security Policy (CSP) settings (excluding nosniff in an exploitable scenario)
- Bugs that do not represent any security risk
- Security bugs related to third-party applications and services used by Qualifio
- Email signup and verification methods

Social Engineering

Social engineering attacks against our staff and end-users are strictly prohibited. This will most likely result in your account being blacklisted and no bounty will be awarded.

Disclosure Policy

- Let us know as soon as possible via security@qualifio.com upon discovery of a potential security issue, and we'll make every effort to quickly resolve the issue. More information can be found under https://qualifio.com/security.txt

- Provide us a reasonable amount of time to resolve the issue before any disclosure to the public or a third-party.

- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service.

Bounty

Qualifio will reward security researchers based on the CVSS score, assessing amongst others :

- The impact to the company and to our users
- The complexity of the attack

Rewards provided by Qualifio will be under the format of e-vouchers to redeem on main online services (Netflix,...) or webshops (Amazon). No monetary bounty will be provided by the company.

Thank you for helping keep Qualifio and our users safe and secure!