Program Details

At Sheryians Coding Schools we take security very seriously. If you believe that you have found a security vulnerability on Sheryians Coding Schools, we encourage you to let us know straight away. We will investigate all legitimate reports and do our best to quickly fix the problem.

We give out rewards for reported bugs and vulnerabilities but these are discretionary and provided on a case by case basis.

Responsible Disclosure Guideline

- You will not publicly disclose a bug before it has been fixed.
- You will protect our users' privacy and data. You will not access or modify data without our permission.
- You will ensure no disruption to our production systems and no destruction of data during security testing.
- You do not violate any other applicable laws or regulations. Sheryians Coding Schools will not be responsible for non-adherence of laws from your end.
- If any privacy violation is inadvertently caused by you while testing, you are liable to disclose it immediately to us.
- You do not exploit a security issue you discover for any reason other than for testing purposes, and you do not conduct testing outside of your own account, a test account, or another account

for which you have the explicit written consent of the account owner to test.
- You will not attempt phishing or security attacks.
- Due to a high number of submissions, we may take a reasonable time to fix the vulnerability reported by you. You have to allow us time to respond to you.
- You must be the first person to report the issue to us. We will review duplicate bugs to see if they provide additional information, but otherwise only reward the first reporter.
- You will provide necessary assistance to us, if required, in resolving the security issue

Please send all reports to: support@sheryians.com

Rewards

We award rewards in cash, goodies,etc. Rewards are evaluated on a case to case basis depending on the severity of the vulnerability.
It is entirely at Sheryians Coding Schools discretion to decide whether a bug is significant enough to be eligible for a reward. Bounty rewards are not negotiable.

Certificates and Hall Of Fame are work in progress, and will be announced here when available.

What's in scope?

sheryians.com

Not in scope

- Issues related to software/application not under Sheryians Coding Schools control
- Spam or social engineering techniques.
- Denial-of-service attacks.
- Self-type Cross Site Scripting / Self-XSS
- CSRF issues on actions with minimal impact
- Reports indicating a lack of DMARC, DKIm, missing SPF records.
- Presence of banner, server version information, EXIF information on images.
- CSRF issues on actions with minimal impact
- Brute force attacks
- Standard user enumeration attacks
- Reports indicating a lack of rate-limiting on certain APIs
- Click Jacking
- Lack of security headers, httponly flags, etc
- Scanner output or scanner-generated reports, including any automated or active exploit tool
- Any internal or development services.
- Content injection (also "content spoofing" or "HTML injection") is out of scope unless you can clearly demonstrate a significant risk.

Breach of our program's terms

You are expected to respect all the terms and conditions of the Bug Bounty Program. Non-adherence or non-compliance will automatically disqualify you. A serious breach may also lead to suspension of your account.

Changes to Program Terms

Sheryians Coding School Bug Bounty Program, and its policies, are subject to change or cancellation at any time, without notice. Also, we may amend the terms and/or policies of the program at any time. In case of any change, a revised version will be posted here.