Urlbox security policy for ethical hackers, security researchers and vulnerability hunters

Introduction

Thanks for taking the time to read this document and help us triage your disclosure.

Bug Bounty

We can publicly acknowledge your contribution. We can display your name, and optionally your email, Twitter handle and a web page or other URL, like a Github or LinkedIn profile on a page on our website.

We sometimes offer a flat-fee reward of GBP £50 in the form of an Amazon (only **amazon.co.uk** or **amazon.com**) voucher sent to an email address. **This is the only form of monetary reward** and **cannot** be replaced with other Amazon country gift cards, PayPal, cryptocurrency, money transfers or any other alternative.

Scope

This policy applies to any Urlbox operated host, virtualhost or subdomain that has our `security.txt` at its root. Our `security.txt` will always have security@urlbox.com as our contact address.

We don't consider the following issues to be in scope, so please don't report them:

1. Volumetric vulnerabilities (i.e. denial-of-service or overwhelming our service with a high volume of requests)
2. ssh and ssh username enumeration
3. TLS configuration weaknesses (i.e. "weak" ciphersuite support, TLS1.0 support, etc)
4. Use of older jQuery libraries
5. Email configuration (SPF, DKIM, DMARC)
6. Gaps in common "best practice" such as missing security headers (CSP, x-frame-options, x-prevent-xss etc)
7. Non-exploitable vulnerabilities

Responsible Security Disclosure Policy

Respect our customers' and users' privacy. You must not attempt to access anyone's data, personal or otherwise. This includes, but is not limited to, usernames, passwords and other credentials. In the event that you gain access to anyone's data, personal or otherwise, you must contact us immediately by emailing security@urlbox.com. You must not save, store or transmit this information.

Act in good faith. You must report any issues found to us in good faith, with no conditions attached, by emailing security@urlbox.com.

Work with us. You must promptly report any findings by emailing security@urlbox.com. You must stop your investigations after you have found the first security issue and request permission to continue testing. You must allow us a reasonable amount of time to resolve the security issue before publicly disclosing it.

Anyone investigating security issues shall not:

Access unnecessary amounts of data. Only access the amount of data necessary to demonstrate the vulnerability;

Exfiltrate data. Use a Proof of Concept to demonstrate a vulnerability;

Share or redistribute any data retrieved from our Platforms, Systems or Services with anyone other than security@urlbox.com;

Test Platforms, Systems and Services that do not fall within the scope of this policy;

Test for security issues that do not fall within the scope of this policy;

Disable security controls for Urlbox Platforms, Systems or Services;

Alter the configuration of Urlbox Platforms, Systems or Services;

Attempt to introduce malware or malicious code or programs;

Disrupt the availability of Urlbox Platforms, Systems or Services to Users (i.e. Denial-of-Service);

Provide anyone else with access to Urlbox Platforms, Systems or Services;

Delete, destroy or modify any data on Urlbox Platforms, Systems or Services;

Perform any testing of physical security;

Perform Brute-Force or any other password attacks against Urlbox Platforms, Systems or Services;