Security Vulnerability Responsible Disclosure Policy

Prepared by: Geof Birchall
June 30th, 2015

Table of Contents

Revision History

Date	Version	Individual	Details
5/26/2015	1.0	Geof Birchall	Initial draft
5/26/2015	1.01	Geof Birchall	Edits for clarity around Abuse
6/30/2015	1.02	Geof Birchall	Edits for final urls

Summary of Purpose

Web.com supports the safety of its customer's assets and data, the environment we provide them, as well as the health of our partners, peers and the Internet broadly.

To assist that greater good Web.com encourages security researchers, white hat hackers and our users to report security flaws that they may discover through our **Security Vulnerability Responsible Disclosure Policy**.

This document describes what to report and how to do it in a way that protects our customers, Web.com and the reporting individual from negative consequences.

The public disclosure of security flaws on Web.com systems or products puts other users at risk. Therefore we ask that you give us a reasonable timeframe in which to mitigate or remediate the problem before releasing any details to the security community or the public at large. This timeframe may vary according to the complexity of the issue however it will usually not exceed 30 days.

If you follow this process in good faith and especially avoid the behaviors listed in What Not to DoWhat Not to Do we will not bring any lawsuit against you nor report your activity to law enforcement.

What to Report?

Any issue that is serious in nature and presents tangible risk to Web.com and its customers should be reported through this mechanism.

The types of issues that should be reported are as follows:

1. Cross-Site Scripting (XSS)
2. Cross-Site Request Forgery (CSRF/XSRF)
3. Authentication or authorization defects
4. Circumvention of any platform or privacy permissions
5. Remote Code Execution (RCE)
6. Privilege escalation
7. Provisioning errors resulting in serious information disclosure

Do not report any of the following types of issues through this process:

1. Spam
2. Content injection
3. The public availability of content stored on our CDN (this is by design)
4. Social engineering techniques
5. Bugs originating from versions of browsers or third-party plugins
6. Suspected malicious traffic originating from our network (these should be reported to our Abuse Team at http://abuse.web.com

What Not to Do

Please avoid any of the following activities during your investigation of the vulnerability.

1. Do not remove, copy, transfer or edit/destroy any data that you may discover during your investigation.
2. Do not interact with any other persons account without the written permission of that user.
3. Do not use automated testing scripts or software during your investigation that are overly broad in scope or unqualified in their targeting.
4. Do not engage in any activity that could result in a degraded service to our other customers, denial of service or damage to data.

How to Report?

The preferred method of reporting possible security vulnerabilities is by completing the web form found at http://disclosure.web.com.

Firstly it's important that we have a good way to communicate with you. Please provide us with your email address and real name. Your Twitter handle or website url would be appreciated so that when this report is completed we are able to credit you effectively.

Please provide as much detail as possible especially around steps to reproduce.

If you are unable to use the web form or prefer to submit the report as a document please send an email to security@web.com with the report attached.

At a minimum include the following information

1. Your email
2. The bug type
3. The url or location of the defect
4. Who is affected
5. A detailed description of the vulnerability
6. Steps to reproduce
7. Any trace dump/WGET/http request information
8. Any information about parameters affected, cookies etc.

What Happens Next?

If you have identified a verified security vulnerability in our systems and have abided by this policy we commit to providing you with:

1. A prompt response to your vulnerability report
2. An estimated timetable for resolution of the vulnerability
3. A notification of when the vulnerability has been corrected
4. A public (through the Web.com website) acknowledgement of your contribution
5. A heartfelt thanks!