How to launch and run a successful bug bounty program

Alexandra Ulsh
Information Security Engineer, Mapbox
A security team perspective
I want more bug bounty programs
The Bug Bounty Nightmare 😨
security@company.com
No process
Any update?

- Security Researcher
It has been 2 days since my report. If you don’t fix in 1 day I will publicly disclose!

Also, any bounty?

- Another Security Researcher
The Bug Bounty Dream
Noise → Quality
Abuse → Professionalism
Irresponsible → Responsible disclosure
No process → Incident response framework (IRF)
vs.
Noise → Quality
What’s noise?
Bug bounty reports by status

24 March 2015 - 1 December 2015

<table>
<thead>
<tr>
<th>Status</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>0.2%</td>
</tr>
<tr>
<td>N/A</td>
<td>32.2%</td>
</tr>
<tr>
<td>Duplicate</td>
<td>20.1%</td>
</tr>
<tr>
<td>Resolved</td>
<td>11.9%</td>
</tr>
<tr>
<td>Info</td>
<td>35.5%</td>
</tr>
</tbody>
</table>
Signal to noise ratio

24 March 2015 - 1 December 2015

Valid 11.9%

Noise 88.1%
First, reduce noise
- Presence of public (pk.*) access tokens in web pages or JavaScript; these are public by design.
- **Username enumeration**, including an oracle that discloses whether a given username or email address is associated with an account.
- Reports of CSRF or reports of a lack of CSRF tokens on www.mapbox.com, unless accompanied by a detailed proof of concept exploit. We have alternative CSRF mitigations in place.
- Missing HTTP security headers, unless accompanied by a detailed proof of concept exploit that leverages their absence.
- Existence of access-controlled administrative pages.
- OPTIONS HTTP method enabled
- HTTPS Mixed Content Scripts
- **Username / email enumeration**
  - via Login Page error message
  - via Forgot Password error message
- Missing HTTP security headers, specifically (https://www.owasp.org/index.php/List_of_useful_HTTP_headers), e.g.
  - Strict-Transport-Security
  - X-Frame-Options
we feel are sensitive and we do not consider the lack of HTTPOnly on other cookies to be a vulnerability.

- **Username enumeration** through login or password reset. While username enumeration can be a vulnerability in a number of web applications, Etsy is a public marketplace and as such usernames can be enumerated by design through a number of ways including listings, forum posts, shops, etc.

- CSRF issue submitted with a proof-of-concept containing a nonce.

Things to be aware of while testing
Warn before submission

Hold on...

Per our program guidelines, reports about status.mapbox.com are out of scope and are ineligible. Please instead submit your report to the bug bounty program for StatusPage.io.

Submit Report

No, don't submit
Doubled resolved reports

- First year: 11.3%
- Second year: 11.3%
- Third year: 24.8%
Better signal to noise ratio

1 March 2017 - today

Valid: 24.8%
Noise: 75.2%
Then, improve quality
Great having the @Mapbox sec team @Hacker0x01 HQ today discussing all things bug bounty our amazing hackers H1+Mapbox #togetherwehitharder
Unexpected spike in reports
We love #swag (who doesn't?!) Thanks @Mapbox for the sweet mugs.
Unexpected spike in reports

Tweets

33% resolved
Largest bounty to date

$5,000 bounty

Tweets
No process → Incident Response Framework (IRF)
Any new bug bounty report could be a past, current, or future security incident.
security@mapbox.com

March 2015

Private launch
Public launch: Incident response framework

March 2016 - January 2017
On call contract
Average first response time (hours)

24 March 2015 - present

IRF
Decrease in first response time

Before IRF

After IRF

4 days

20 hours
Abuse → Professionalism
Empathy
Growth
Responsiveness
24 hours
first response time
17 days
time to bounty
Award before fix
Report timeline

1. Acknowledge  
   10 minutes

2. Classify  
   60 minutes

3. First response  
   12 hours
4. Triage/close
   4 days

5. Accepted by engineering
   10 days

6. Award bounty
   15 days
7. Deploy fix
   \textit{30 days}

8. Public disclosure
   \textit{45 days}
Irresponsible → Responsible disclosure
Mapbox Security Bulletins

Millions of people touch Mapbox every month. That's why we are committed to creating the most secure and privacy-minded mapping and location platform in the world.

Check this page for security announcements related to Mapbox software and our platform. You can also subscribe to our security bulletins RSS feed.

Need to report a security issue? Check out our bug bounty program on HackerOne or email us at security@mapbox.com.
692+ public GitHub repos
Interactive, thoroughly customizable maps in native Android, iOS, macOS, Node.js, and Qt applications, powered by vector tiles and OpenGL  https://mapbox.com/mobile

Contributors

friedbunny [ios] Update podssecs for v3.7.0-alpha.1

Latest commit 366a697 10 hours ago

- .tx
  [ios] Configured stringsdict from Transifex

- benchmark
  Add {Source,CompositeCamera}Function benchmarks (#9838)

- bin
  [node, tests] Consolidate headless rendering logic in HeadlessFrontend

- cloudformation
  Combine AWS keys (#9679)

- cmake
  [core] remove map update update enum
Security fix for L.mapbox.shareControl. See detailed commit messages for technical discussion.

Advisory to Node Security submitted and will be published as soon as possible after latest version has been deployed to all public release channels.

@ianshward - ☀️ and final approval for merge with mb-pages?

/cc @tmcw @jfirebaugh @scothis @mapbox/devops
Content Injection via TileJSON Name

Module: mapbox.js

Published: January 12th, 2016

Reported by: Alexandra Ulsh, Abdullah Ahmet Erdem

CVE-NONE

Vulnerable: <1.6.6 || < 2.2.4 > 2.0.0
Patched: >=1.6.6 <2.0.0 || >= 2.2.4

CVSS 4.9
Medium
Noise → Quality
Abuse → Professionalism
Irresponsible → Responsible disclosure
No process → Incident response framework (IRF)
Why?
I want more bug bounty programs
I want people to report security issues
The Bug Bounty Dream
Questions?

ulsh@mapbox.com

@AlexUlsh