Who

The ROOTCON Bug Bounty Track
  - What / Why

Bug Bounties?
  - What / Why

Who Runs Bug Bounty Programs

Fun and profit - optimize for success!

CTF Details

Q&A
● **Director, Security Operations at Bugcrowd**
  ○ Triage and Validation
  ○ Services Strategy
  ○ Technical Researcher Community Liaison

● **Former HPE Fortify**
  ○ Led Static Analysis and Code Review
  ○ Infrastructure
  ○ DevOps Tooling

● **Avid open source enthusiast and gamer**

**Twitter:** @digitalwoot
**GitHub:** ryanblack
Bugcrowd

- #1 Managed Bug Bounty Platform
- Headquartered in San Francisco, CA
  - Boston, MA
  - London, UK
  - Sydney, AU
  - International Team
- Over 600 programs and 60k researchers
- Growing team!

https://www.bugcrowd.com/
<table>
<thead>
<tr>
<th>FINANCIAL SERVICES</th>
<th>CONSUMER TECH</th>
<th>RETAIL &amp; ECOMMERCE</th>
<th>AUTOMOTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Western Union</td>
<td>fitbit</td>
<td>indeed</td>
<td>FCA</td>
</tr>
<tr>
<td>Discover</td>
<td>Pinterest</td>
<td>jet</td>
<td>Tesla</td>
</tr>
<tr>
<td></td>
<td>mastercard</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Motorola</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFRASTRUCTURE TECH</td>
<td>SECURITY TECHNOLOGY</td>
<td>OTHER</td>
<td></td>
</tr>
<tr>
<td>heroku</td>
<td>Barracuda</td>
<td>LastPass</td>
<td>okta</td>
</tr>
<tr>
<td>aruba</td>
<td>Twilio</td>
<td>1Password</td>
<td>(ISC)²</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Netgear</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OWASP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zephyr Health</td>
</tr>
</tbody>
</table>

2/3rd of Programs are Private
The **ROOTCON** Bug Bounty Track

- Investing in the community
  - LevelUp
  - Conference presence
  - Tools: HUNT
  - Bugcrowd Vulnerability Rating Taxonomy
  - CTFs and Training
Jason Haddix
Head of Trust and Security

Jay Turla
Application Security Engineer
### The Bug Bounty Track

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:45 - 10:45</td>
<td>Bug Bounty Operations - An Inside Look</td>
<td>Ryan Black</td>
</tr>
<tr>
<td>10:45 - 11:45</td>
<td>Starting Your Bug Hunting Career Now</td>
<td>Jay Turla</td>
</tr>
<tr>
<td>16:00 - 17:00</td>
<td>The Bug Hunters Methodology 2.0</td>
<td>Jason Haddix</td>
</tr>
</tbody>
</table>

**Day 2**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 - 10:00</td>
<td>Discovery: Expanding Your Scope Like A Boss</td>
<td>Jason Haddix</td>
</tr>
<tr>
<td>10:00 - 16:00</td>
<td>Bugcrowd CTF</td>
<td>Team</td>
</tr>
</tbody>
</table>
Bug Bounties - What

• Platform managed or customer managed
• Public or private
• Limited duration or ongoing
• Before or after traditional testing
• Pay-for-results
Bug Bounties - Why

• Results-driven
• Cost Effectiveness
• Specialized Testing
  – IoT / Reverse Engineering
  – Thick clients
  – Mobile
  – Automotive
Bug Bounties - Who’s Running Them?

- Nearly half of companies > 500 employees, a quarter under 50
- Information Security, AppSec Teams, or Engineering
- Security Generalist, SME, or Developers
- Vulnerability feedback process varies
Fun and Profit - Optimize Your Success

• First, understand how reports are reviewed
  – Scope
  – Clarity
  – Risk and Impact
Do

- Be professional
- Communicate impact
- Facilitate understanding
- Self advocate

Don’t

- Threaten disclosure
- Confuse category/reward
- Mishandle data
- Lack patience

Providing value and building a rapport pays off!
Example - XSS Hunter (https://xsshunter.com)

Detailed notes with reproduction information and remediation advice

---

# XSSHunter Report

The page located at `http://www.insecurelabs.org/Talk/Details/1` suffers from a Cross-site Scripting (XSS) vulnerability. XSS vulnerability which occurs when user input is unsafely incorporated into the HTML markup inside of a webpage. When not properly aped an attacker can inject malicious JavaScript that, once evaluated, can be used to hijack authenticated sessions and rewire the vulnerable page's layout and functionality. The following report contains information on an XSS payload that has fired on `http://www.insecurelabs.org`, it can be used to reproduce and remediate the vulnerability.

### XSS Payload Fire Details

#### Vulnerable Page

`http://www.insecurelabs.org/Talk/Details/1`

#### Victim IP Address

`99.99.____.____`

#### Referer

`http://www.insecurelabs.org/Talk/`
The payment billing endpoint returns customer billing information (cool stuff you can use to steal money), etc.). The flux capacitor ID is used to request the information. By iterating through different flux capacitor IDs, I was able to view billing information for other customers.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>&lt;some reference number&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original caption</td>
<td>Insecure Direct Object Reference - Billing Detail Disclosure</td>
</tr>
<tr>
<td>Bug Type</td>
<td>Bug/Other</td>
</tr>
<tr>
<td>XSS Location URL</td>
<td>Empty</td>
</tr>
<tr>
<td>Affected Parameter</td>
<td>&lt;flux capacitor id&gt; ID</td>
</tr>
<tr>
<td>Affected Users</td>
<td>AUTHENTICATED</td>
</tr>
<tr>
<td>Attack String</td>
<td>Empty</td>
</tr>
<tr>
<td>Browser</td>
<td>Empty</td>
</tr>
<tr>
<td>Bug URL</td>
<td>&lt;some url&gt;</td>
</tr>
<tr>
<td>Device</td>
<td>Empty</td>
</tr>
</tbody>
</table>

**HTTP Request**

```
Host:<some url>
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;en-8.5
Accept-Encoding: gzip, deflate
Referer:<some url>
Connection: Close

-----

HTTP/1.1 200 OK
Cache-Control:<stuff>
Content-Type: application/json;charset=UTF-8
```

**Method of Finding**

manual

**Platform**

Empty

**Platform Version**

Empty

**Proof of Concept**

Empty

**Replication Steps**

1. Configure your browser to use an intercepting proxy such as Burp or monitor the request using Chrome/Firefox developer tools.
2. Login to the web application and browse to the billing information page.
3. Capture the request to the billing information endpoint and send it to Repeater or Intruder.
4. Modify the request to attempt to enumerate additional <flux capacitor> IDs and observe the billing information in the response.
CTF Details

Our Bugcrowd Bug Bounty CTF offers the following prizes:

- First: $1,500
- Second: $1,000
- Third: $500
- Fourth: $250

Invitations to private programs will also be awarded based on performance!
CTF Setup

If you already have a researcher account on Bugcrowd:

1. Visit: http://bgcd.co/rootconsignup
2. Provide your researcher username and associated email address
3. Accept the invitation to the private program rootcon2017ctf

If you do not:

2. Create an account
3. Accept the invitation to the private program rootcon2017ctf
Questions?