Bug Bounty Operations

An Inside Look

Thursday, September 21, 2017

bugcrowd

- 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: ryancblack

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/

FINANCIAL SERVICES

WESTERN UNION

mastercard.

DISCOVER

CONSUMER TECH

fitbit

Pinterest

MOTOROLA

RETAIL & ECOMMERCE

indeed

jet

AUTOMOTIVE

FCA
FIAT CHRYSLER AUTOMOBILES

TESLA

INFRASTRUCTURE TECH

heroku

Barracuda

aruba

twilio

SECURITY TECHNOLOGY

LastPass•••|

okta

1Password

OTHER

(ISC)²®

NETGEAR®

OWASP

ZEPHYR HEALTH

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

bugcrowd

+2

Jason Haddix

Head of Trust and Security

Jay Turla

Application Security Engineer

The ROOTCON Bug Bounty Track

9:45 - 10:45	Bug Bounty Operations - An Inside Look	CTF Setup	Ryan Black
10:45 - 11:45	Starting Your Bug Hunting Career Now		Jay Turla
16:00 - 17:00	The Bug Hunters Methodology 2.0		Jason Haddix
Day 2			
9:00 - 10:00	Discovery: Expanding Your Scope Like A Boss	CTF Setup	Jason Haddix
10:00 - 16:00	Bugcrowd CTF		Team

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

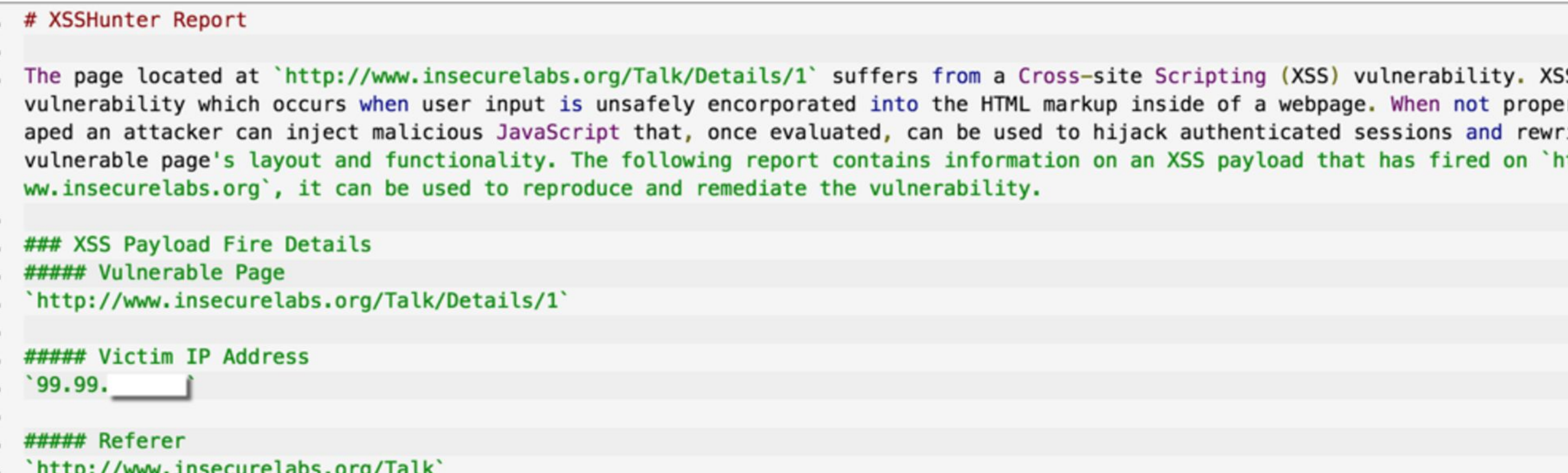
Don’t

- 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



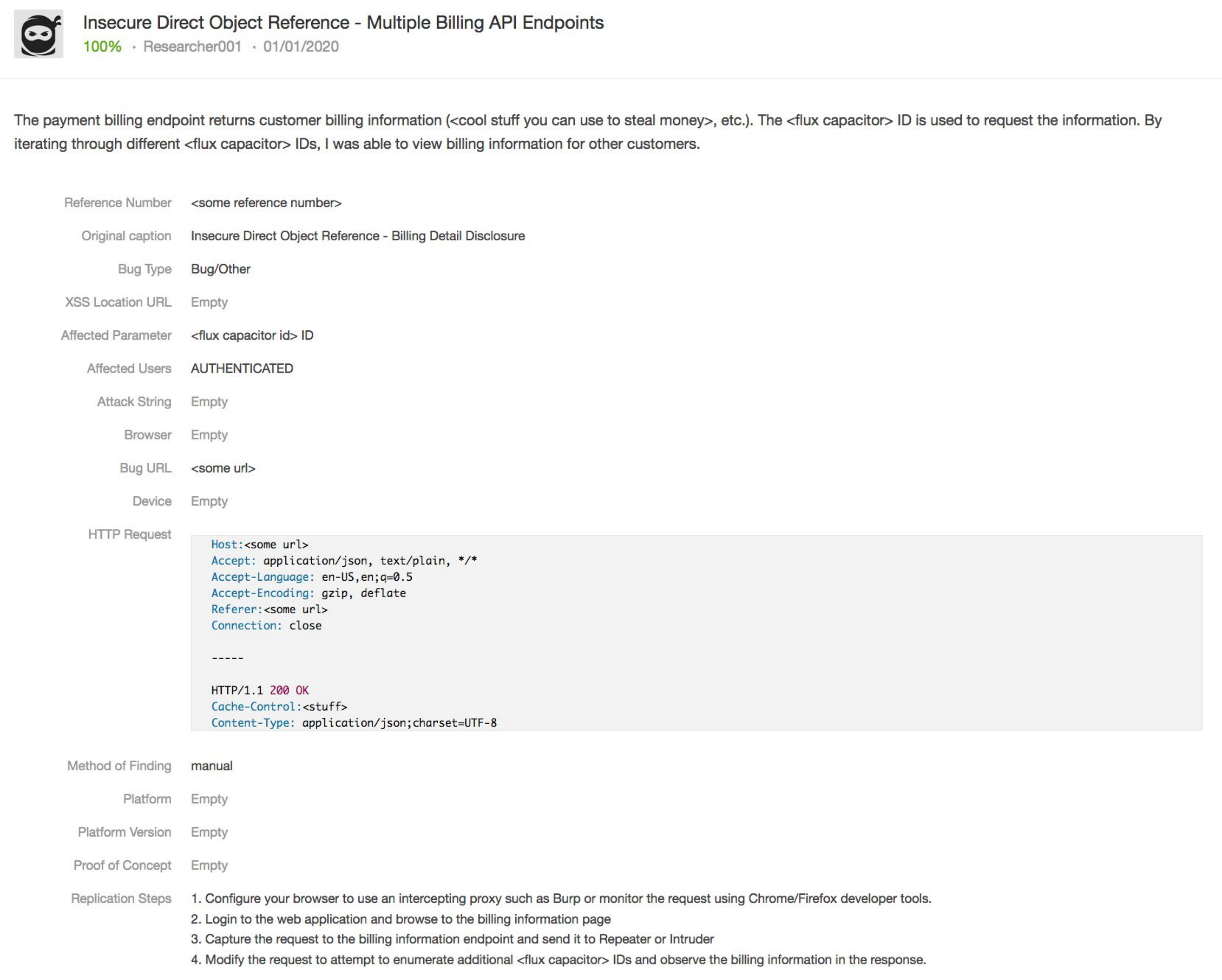
```
# XSSHunter Report

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

##### Referer
`http://www.insecurelabs.org/Talk`
```



Insecure Direct Object Reference - Multiple Billing API Endpoints

100% · Researcher001 · 01/01/2020

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.

Reference Number	<some reference number>
Original caption	Insecure Direct Object Reference - Billing Detail Disclosure
Bug Type	Bug/Other
XSS Location URL	Empty
Affected Parameter	<flux capacitor id> ID
Affected Users	AUTHENTICATED
Attack String	Empty
Browser	Empty
Bug URL	<some url>
Device	Empty

HTTP Request

```
Host:<some url>
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
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:

1. Visit: http://bugcrowd.com/rootcon2017
2. Create an account
3. Accept the invitation to the private program rootcon2017ctf

Questions?