STARTING YOUR BUG HUNTING CAREER NOW

by Jay Turla
AGENDA

• Whoami

• What is a Bug Bounty or Bug Hunting?

• Some Companies with Bug Bounty Programs

• Bugcrowd Introduction and VRT

• Bug Hunter Methodology

• Sample Issues

• DEMO
WHOAMI

• Jay Turla a.k.a The Jetman

• Application Security Engineer @Bugcrowd

• Metasploit Contributor: Host Header Injection Detection, BisonWare BisonFTP Server Buffer Overflow, Zemra Botnet CnC Web Panel Remote Code Execution, etc.

• Twitter: @shipcod3

• ROOTCON Goon

• Former Senior Security Consultant at HP Fortify on Demand
BOUNTY HUNTING?

WANTED

THE NOTORIOUS PYRATE
EZKIEL BLACKHEART

A BOUNTY OF FIVE HUNDRED POUNDS
WILL BE PAID ON THE PROOF OF
CAPTURE OR DEATH BY HIS MAJESTYS
GOVERNOR IN PORT ROYAL
WHAT IS A BUG BOUNTY?
(THINK OF IT AS A COMPETITION)

Independent security researchers from all over the world are recruited → Vulnerabilities are found and reported → Rewards are exchanged for reporting vulnerabilities in company applications
SOME COMPANIES THAT HAVE BUG BOUNTY PROGRAMS <3

facebook
Microsoft
Google
Mozilla
Tesla
Cisco
Atlassian
Bugcrowd
Crowdsourced security platforms like Bugcrowd connects organizations to a curated crowd of tens of thousands of researchers from around the world to identify vulnerabilities in their applications, devices, and code—before the bad guys do.

Hack now at https://bugcrowd.com/programs
IS THIS A NEW SCAM? WAIT WHAT?
**UPCOMING PAYMENTS**

<table>
<thead>
<tr>
<th>Description</th>
<th>Due Date</th>
<th>Expected Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd Place March HoF</td>
<td>April 09, 2017</td>
<td>$1,500.00</td>
</tr>
<tr>
<td>Monthly Bugcrowd Leaderboard Bonus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Side Template Injection - RCE at</td>
<td></td>
<td>$5,000.00</td>
</tr>
<tr>
<td>Stored XSS</td>
<td></td>
<td>$900.00</td>
</tr>
<tr>
<td>Stored XSS</td>
<td></td>
<td>$900.00</td>
</tr>
<tr>
<td>XML External Entity Injection</td>
<td></td>
<td>$2,828.57</td>
</tr>
</tbody>
</table>

* Justin Kennedy @jstnkndy · Apr 7
  Who says bug bounties don’t pay? [pic.twitter.com/FoOAPPkbkU](https://twitter.com/jstnkndy)
WHO IS THIS GUY?

Justin Kennedy

Verified

“I am both a principal security consultant that leads a security team at a global consulting organization as well as a Bugcrowd researcher. Why? Because security testing is my passion.”
YOU CAN BE A HERO

Mahmoud Saber (facebook.com/admin msm)
Teofil Cojocariu (Cyber Security Research Center from net-sq.com)
Savan Gadhiya (about.me/gadhiyasa)
Narendra Bhati (@NarendraBhatiB)
Muhammad Talha Khan
Shahee Mirza (@shaheemirza)
Ahmed El-Mahalawy (facebook.com/A7medELMa7ala)
Jay Turla
Edis Konstantini - (facebook.com/edis.konstantini)
Deepanker Chawla (www.deepanker.in)
BTopi (@qckstil)
Mazin Ahmed - (https://mazinahmed.net)
Olivier Beg & Yasser Ali from lanaru.com
Michael Weissbacher
Ebrahim Hegazy (www.sec-down.com - @Zigoo0)
Hardik Tailor (https://twitter.com/hardiktai1or, https://shankhnaad.net, sanatan.org, narendra modi.in, bjp.org)
Shritam Bhowmick and Paulos Yibelo (defencely.com)
Ashesh Kumar (facebook.com/ashesh1708 , www.cat)
Deba Akrem Fares (akram4.com)
P.B.Surya.Subhash (fb.com/pbssubhash22), Yogesh
<table>
<thead>
<tr>
<th>Priority</th>
<th>OWASP Top Ten + Bugcrowd Extras</th>
<th>Specific Vulnerability Name</th>
<th>Variant or Affected Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>A1 - Injection</td>
<td>File Inclusion</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>A2 - Injection</td>
<td>Remote Code Execution (RCE)</td>
<td>Error-Based</td>
</tr>
<tr>
<td></td>
<td>A3 - Injection</td>
<td>SQL Injection</td>
<td>Blind</td>
</tr>
<tr>
<td></td>
<td>A4 - Injection</td>
<td>XML External Entity Injection (XXE)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A2 - Broken Authentication and Session Management</td>
<td>Authentication Bypass</td>
<td>Vertical</td>
</tr>
<tr>
<td></td>
<td>A4 - Insecure Direct Object References (IDOR)</td>
<td>Insecure Direct Object Reference (IDOR)</td>
<td>Critical Function</td>
</tr>
<tr>
<td></td>
<td>A5 - Security Misconfiguration</td>
<td>Insufficient Cross-Origin Resource Sharing</td>
<td>Critical Impact</td>
</tr>
<tr>
<td></td>
<td>A5 - Security Misconfiguration</td>
<td>Using Default Credentials</td>
<td>Production Server</td>
</tr>
<tr>
<td></td>
<td>A6 - Sensitive Data Exposure</td>
<td>Sensitive Data</td>
<td>Password Disclosure</td>
</tr>
<tr>
<td></td>
<td>A6 - Sensitive Data Exposure</td>
<td>Sensitive Data</td>
<td>Private API Keys</td>
</tr>
<tr>
<td></td>
<td>A7 - Insufficient Authentication/Authorization</td>
<td>Cryptographic Flaw</td>
<td>Incorrect Usage</td>
</tr>
<tr>
<td></td>
<td>A8 - Insecure Cloud Interface</td>
<td>Insecure Direct Object Reference (IDOR)</td>
<td>Critical API Function</td>
</tr>
<tr>
<td></td>
<td>A9 - Insecure Software/Firmware</td>
<td>Command Injection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A9 - Insecure Software/Firmware</td>
<td>Handcuffed Password</td>
<td>Privileged User</td>
</tr>
<tr>
<td>P2</td>
<td>A2 - Broken Authentication and Session Management</td>
<td>Authentication Bypass</td>
<td>Horizontal</td>
</tr>
<tr>
<td></td>
<td>A3 - Cross-Site Scripting (CSS)</td>
<td>Stored</td>
<td>Non-Admin to Anyone</td>
</tr>
<tr>
<td></td>
<td>A4 - Insecure Direct Object References (IDOR)</td>
<td>Insecure Direct Object Reference (IDOR)</td>
<td>Important Function</td>
</tr>
<tr>
<td></td>
<td>A4 - Insecure Direct Object References (IDOR)</td>
<td>Server-Side Request Forgery (SSRF)</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>A5 - Security Misconfiguration</td>
<td>Insufficient Cross-Origin Resource Sharing</td>
<td>High Impact</td>
</tr>
<tr>
<td></td>
<td>A5 - Security Misconfiguration</td>
<td>Misconfigured DNS</td>
<td>Subdomain Takeover</td>
</tr>
<tr>
<td></td>
<td>A5 - Security Misconfiguration</td>
<td>Using Default Credentials</td>
<td>Staging/Development Server</td>
</tr>
<tr>
<td></td>
<td>A8 - Cross-Site Request Forgery (CSRF)</td>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>Critical Function</td>
</tr>
<tr>
<td></td>
<td>B1 - Application-Level Denial-of-Service (DoS)</td>
<td>Critical Impact and/or Easy Difficulty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B1 - Application-Level Denial-of-Service (DoS)</td>
<td>Insecure Data Storage</td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>A9 - Insecure Software/Firmware</td>
<td>Insecure Direct Object Reference (IDOR)</td>
<td>Important API Function</td>
</tr>
<tr>
<td></td>
<td>A9 - Insecure Software/Firmware</td>
<td>Handcuffed Password</td>
<td>Non-Privileged User</td>
</tr>
<tr>
<td>P3</td>
<td>A1 - Injection</td>
<td>HTTP Response Manipulation</td>
<td>Response Splitting (CRLF)</td>
</tr>
<tr>
<td></td>
<td>A1 - Injection</td>
<td>Content Spoofing</td>
<td>iFrame Injection</td>
</tr>
<tr>
<td></td>
<td>A10 - Unvalidated Redirects and Forwards</td>
<td>Open Redirect</td>
<td>GET-Based (Unauthenticated)</td>
</tr>
</tbody>
</table>
In 2016, a critical issue was reported every... 13 HRS
EASY SIGNUP
BUG HUNTER METHODOLOGIES
METHODOLOGY FOR BUG HUNTING
JASON HADDIX

- https://github.com/jhaddix/tbhm
- Video & Slides
- https://bugcrowd.com/resources/how-to-shot-web-by-jason-haddix
METHODOLOGY FOR BUG HUNTING ON NEW BOUNTIES
BRET BÜERHAUS

- Review the scope
- Perform reconnaissance to find valid targets
- Scan against discovered targets to gather additional information
- Review all of the services and applications
- Fuzz for errors and to expose vulnerabilities
- Attack vulnerabilities to build proof-of-concepts
OTHER GOOD RESOURCES

- Awesome Hacking: https://github.com/Hack-with-Github/Awesome-Hacking
- The Web Application Hacker’s Handbook
- OWASP: https://www.owasp.org/index.php/Main_Page
- HPE Security Fortify Taxonomy: https://vulncat.hpefod.com/en
- ROOTCON Archives: https://www.rootcon.org/xml/archives/events
- SecLists Project: https://github.com/danielmiessler/SecLists
PRACTICING YOUR SKILLS
VIRTUAL MACHINES AND VULNERABLE WEB APPS
- EASY TO SETUP

- **vulnhub.com** - materials (mostly VMs you can play with) that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration.

- Damn Vulnerable Web Application - [http://www.dvwa.co.uk/](http://www.dvwa.co.uk/)

- OWASP Mutillidae - [https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project](https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project)


- OWASP Broken Web Applications Project - [https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project](https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)
ONLINE PLAYGROUND
-NO NEED TO SET IT UP

• [http://flaws.cloud/](http://flaws.cloud/) - series of levels you'll learn about common mistakes and gotchas when using Amazon Web Services (AWS)

• n00bs CTF Labs - [http://ctf.infosecinstitute.com/index.php](http://ctf.infosecinstitute.com/index.php)

• Google XSS Challenge- [https://xss-game.appspot.com/](https://xss-game.appspot.com/)


• CTF365 - [https://ctf365.com/](https://ctf365.com/)

• Demo Testfire - [http://demo.testfire.net/](http://demo.testfire.net/)
SOME ISSUES YOU CAN REPORT NOW

things to ponder about security issues that are easy to spot
SESSION NOT INVALIDATED AFTER LOGOUT, PASSWORD RESET, PASSWORD CHANGE
TELNET ENABLED (CREDENTIALS REQUIRED)

```bash
frodo@shire ~ $ telnet Mordor
Trying 192.168.1.15...
Connected to mordor.nixiepixel.com.
Escape character is '^]'.
One does not simply telnet into Mordor
Connection closed by foreign host.
frodo@shire ~ $ ssh frodo@mordor
The authenticity of host 'mordor (192.168.1.15)' can't be established.
ECDSA key fingerprint is d5:9e:60:5a:00:d1:82:cf:7e:2a:f6:fc:9
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mordor,192.168.1.15' (ECDSA) to known hosts.
frodo@mordor's password: 
```
MISCONFIGURED S3 BUCKETS

```bash
+ ~ s3cmd ls s3://flaws.cloud
2017-03-14 03:00 2575 s3://flaws.cloud/hint1.html
2017-03-03 04:05 1707 s3://flaws.cloud/hint2.html
2017-03-03 04:05 1101 s3://flaws.cloud/hint3.html
2017-03-25 20:58 2877 s3://flaws.cloud/index.html
2017-02-27 01:59 46 s3://flaws.cloud/robots.txt
2017-02-27 01:59 1051 s3://flaws.cloud/secret-dd02c7c.html
+ ~ s3cmd get s3://flaws.cloud/secret-dd02c7c.html
download: 's3://flaws.cloud/secret-dd02c7c.html' -> './secret-dd02c7c.html' [1 of 1]
download: 's3://flaws.cloud/secret-dd02c7c.html' -> './secret-dd02c7c.html' [1 of 1]
1051 of 1051 100% in 0s 1074.38 B/s done
+ ~ cat secret-dd02c7c.html

<html>
<head>
    <title>FLAWS</title>
    <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
    <style>
      body { font-family: Andale Mono, monospace; }
      :not(center) > pre { background-color: #202020; padding: 4px; border-radius: 5px; border-color:#000000; border-width: 1px; border-style: solid; }
    </style>
</head>
<body text="#00d000" bgcolor="#000000" style="max-width:800px; margin-left:auto; margin-right:auto"
      vlink="#00ff00" link="#00ff00">

<center>
<pre>
FLAWS
</pre>
</center>

<h1>Congrats! You found the secret file!</h1>
</body>
</html>
```
XSS (CROSS-SITE SCRIPTING)

Demo application 1:

URL: https://xss-doc.appspot.com/demo/2
SQL INJECTION

Why We Should Party

Coz according to Jolly Mongrel, the most important thing in life is to celebrate it while you are still an air-breathing creature roaming on Mother Earth with fervor, humor and without hesitation.!

5.7.17-0ubuntu0.16.04.1

3
LET’S HAVE SOME DEMO
QUESTIONS?

THAT IS AN EXCELLENT QUESTION