Bug Bytes #17 – 5 Important Bug Bounty Tips by @stokfredrik & @jhaddix, @securinti Is Just Reading The Docs & the Intigriti XSS Challenge Write-ups

BY INTIGRITI · MAY 7, 2019 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand.** Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 26 of April to 3 of May.

Our favorite 5 hacking items

1. Video of the week

> "5 super important main-app testing tips for bug bounty hunters with STOK&Haddix"

Any video by @stokfredrik & @jhaddix is a must watch! This one has 5 crucials things you want to do as a bug hunter:

- Don't limit yourself to the external attack surface. Log in as different users & try to find where the sensitive functionality is => access controls bugs & IDOR
- Find out how the site references you as a user (& what you're allowed to do) => IDOR, File upload, RCE
- Test all parameters => SSRF, LFI, RFI, Path traversal
- Content discovery => hidden paths, private data leakage => Authentication bypass, logic flaws
- Find out which business flaws the target cares about (other than technical bugs)

But this is not all. Watch the video. It's short but full-packed with information!

2. Conference of the week

> "Nullcon Goa 2019, especially:
> – Best Of Google VRP 2018
> – How To Use Bug Bounty To Start A Career In Silicon Valley
> – Automating Security Testing with Functional Testing Test Cases
> – Getting to $10,000 – the variables at play in determining bounty awards
> – Introducing the ASVS 4.0
> – Interview with Robert Baptiste aka Elliot Alderson [@fs0c131y]"

I really recommend watching the talk “How To Use Bug Bounty To Start A Career In Silicon Valley”. It has awesome advice on leveraging bug bounty hunting to build a solid resume and find a job in Silicon Valley (or anywhere else). This includes which bugs and programs to focus on, which pitfalls to avoid, etc.
“Best Of Google VRP 2018” is also a good resource for bug hunters who want to succeed with Google VRP. Some of the advice applies to other programs too (like specializing in a product/attack vector).

3. Article of the week

> “Meet the Hacker: Inti De Ceukelaire – “While everyone is looking for XSS I am just reading the docs.””

This is an excellent interview of @securinti. What I like about it most is that the interviewer, @_zulln, is also a hacker. So unlike most interviews of this sort, the questions and answers are very technical and mindblowing for anyone starting out as a bug hunter.
I highly recommend this read if you want to find out what sets apart successful bug hunters from beginners.
Here are some interesting excerpts:

- “Many hackers look for bugs, I look for attack scenarios and then for the bugs. And it works for me as I get fewer duplicates. The downside is that I spend time researching ideas that sometimes yield nothing.”
- “Scanners do not detect logical bugs, because to detect them you need context, you need to understand the application and the business logic. While everyone is looking for XSS I am just reading the docs.”

4. Resource of the week

> “Android App Reverse Engineering 101”

If you’re interested in Android app hacking, checkout this workshop. It’s about reverse engineering Android apps and includes both theory and exercises. Just awesome!

5. Non technical item of the week

> “Mental Health and Security”

So many hackers suffer from at least of the mental struggles mentioned in this article: imposter syndrome, burnout, anxiety and depression.
I hear/read more and more testimonies on this especially on Twitter, and I have similar experience myself. Hacking involves so much learning/change/stress…
So it’s nice to know that I am/we are not alone in this. And it is helpful to read a fellow hacker’s perspective on these issues, and how he deals with them.

6. Intigriti News

6.1 XSS Challenge Write-up

We’ve made a conclusive write-up about our XSS Challenge in April. More than 100k people saw the challenge, but only 90 researchers were able to solve it. Do you want to know how? Read the solution

here

6.2 Platform update coming up – longer titles (Finally)

Yes, that's right! We listened to the community and we're happy to announce that in the upcoming days the limit of 25 characters will be raised to 50 characters! Time to show us some juicy titles!

6.3 Wimigames – a new public program (registered only)

Wimigames is a company developing bingo and café games. They are mainly interested on how you can influence their gambling games. Does it sounds like a program for you? Don't hesitate and check out it out now! **Note: this is a registered only program!**

Start hunting here!

Other amazing things we stumbled upon this week

Videos

- Zero to Hero Pentesting: Episode 7 – Exploitation, Shells, and Some Credential Stuffing

Podcasts

- Security Now 712: Credential Stuffing Attacks
- Darknet Diaries Ep 37: LVS
- Security In Five Episode 480 – Tools, Tips and Tricks – Spring Clean Your Windows by Taproot Security
- Secure Digital Life #108 – Spy Cameras
- Paul's Security Weekly #601 – The Canary Tool, Thinkst
- Hack Naked News #216 – April 30, 2019

Webinars & Webcasts

- BHIS Webcast: Weaponizing Corporate Intel. This Time, It's Personal! & Slides
- Webcast: Attack Tactics 5 – Zero to Hero Attack
- CSIAC Webinars – OWASP Amass: Discovering Your Exposure on the Internet

- Safe Harbor for Hackers & Slides
- Building a Small and Flexible Wireless Exfiltration Box with SDR & Demo: Wireless Exfil Box w/ SDR (Paul Clark)

Conferences

- Code and Command Infection flaws in Web Apps & Slides
- BSidesCharm 2019
- BSides Edinburgh 2019

Slides only

- Injection attacks in apps with NoSQL Backends
- Github security bug bounty hunting
- Exploit development for penetration testers

Tutorials

Medium to advanced

- Fun with Burp Suite Session Handling, Extensions, and SQLMap
- AWS IAM Exploitation
- Unauthenticated Session Fixation Attacks
- Attacking RMI based JMX services
- Android Application Diffing: CVE-2019-10875 Inspection
- Frida Android libbinder
- Running Fuchsia on the Android Emulator
- Cronjob Backdoors
- Automating Red Team Homelabs: Part 2 – Build, Pentest, Destroy, and Repeat
- How to Weaponize the Yubikey
- Manually Enumerating Active Directory
- Exploiting Unconstrained Delegation

Beginners corner

- Using Google groups for OSINT

- Google groups misconfiguration
- Burp Suite Tips – Volume 1 & Volume 2
- Apache Server-Status
- Crawl a web page, extract all domains and resolve them to IP addresses
- Swagger API
- Finding your WiFi password using netsh on Windows 10
- Windows Privilege Escalation using sudo su?
- Windows PrivEsc: Weak Service Permission
- USB Password Stealer Turorial

Writeups

Challenge writeups

- Intigriti XSS challenge solutions
  - by @karouf
  - by @dee__see
  - by @dPhoeniixx
  - by @terjanq
  - by daudmalik06
  - by _zulln
- BountyCon CTF 2019
- The Butcher challenge by @0xGiraffe

Pentest writeups

- Analysis-Report Chinese Police App "IJOP" 12.2018: Not exactly a pentest report, but interesting if you're into mobile app security. Cure53 tested IJOP, an Android app used by Chinese law enforcement, to find out if it violates human rights
- Komodosec| Through the cloud—remote debugging to crack MQ
- Serverless Security & The Weakest Link (Avoiding App DoS)

Responsible disclosure writeups

- How I hacked 50+ Companies in 6 hrs
- Put.io API design issues – "I can haz your files"
- Story of a Hundred Vulnerable Jenkins Plugins

- Why you shouldn't do client-sided checks only; unlimited data via EE gifting system
- Remote Code Execution (RCE) in CGI Servlet – Apache Tomcat on Windows – CVE-2019-0232
- WebLogic RCE (CVE-2019-2725) Debug Diary
- OEM Presentation Platform Vulnerabilities
- Remote Code Execution on most Dell computers & PoC
- Synacktiv advisories regarding a bunch of pre-authenticated issues in GLPI

Bug bounty writeups

- XSS & Cache poisoning on Twitter ($2,520)
- XSS on Twitter ($2,940)
- Local file theft/JS injection/open redirect on Twitter ($1,120)
- 2FA bypass on private program
- Cookie bombing on private program ($350)
- Account takeover due to password autofill on Linode & Reddit discussion
- Logic flaw on Google
- SSRF on private program
- Facebook IDOR bug in GraphQL (video)

See more writeups on The list of bug bounty writeups.

Tools

- Argument Injection Hammer & Introduction: Burp extension for detecting argument injection and manipulation vulnerabilities
- Docker_burp & Introduction: Burp as a Docker Container
- Dirmap & Introduction: "An advanced web directory scanning tool that will be more powerful than DirBuster, Dirsearch, cansina, and Yu Jian."
- HostHunter: A recon tool for discovering hostnames using OSINT techniques
- DumpTheGit: Searches through public repositories to find sensitive information uploaded to the Github repositories
- pentest.sh: Installs pentesting tools, then symlinks them to be ran seamlessly
- WhatBreach: OSINT tool to find breached emails and databases
- PwnedOrNot: OSINT Tool to Find Passwords for Compromised Email Addresses

- Coerchck: PowerShell Script For Listing Local Admins
- EvilClippy: A cross-platform assistant for creating malicious MS Office documents. Can hide VBA macros, stomp VBA code (via P-Code) and confuse macro analysis tools. Runs on Linux, OSX and Windows
- SSL Kill Switch 2: Blackbox tool to disable SSL certificate validation – including certificate pinning – within iOS and OS X Apps

Misc. pentest & bug bounty resources

- What_is_this_c2: For quick visual fingerprinting of login panels
- XSS Tricks
- Android Security Monthly Recap #4 | April 2019
- APIsecurity.io Issue 29: OAuth2 attacks, car GPS vulnerabilities, and honeypot stats
- Nginx Admin's Handbook
- @nullenc0de's password cracking dictionary
- Yes We Hack IRC chan
- PwnSec Discord server

Challenges

- Google CTF 2019 is here: "Qualification round will take place online Sat/Sun June 22 and 23 2019"

Articles

- ESI Injection Part 2: Abusing specific implementations & Edge Side Includes abused to enable RCE
- My Recon Process—DNS Enumeration
- Bypassing SOP Using the Browser Cache
- The Difference Between URLs, URIs, and URNs (updated)
- How to do application security on a budget
- 59 Hosts to Glory—Passing the OSCP
- Port Scanning, Spoofing & Blacklists
- An inside look at how credential stuffing operations work
- How did I break a captcha with Puppeteer and Google Vision ?
- The inception bar: a new phishing method

News

Bug bounty / Pentest news

- Google Chrome's XSS Auditor goes back to filter mode
- 2019 Buggy Award Winners
- Amazon S3 will no longer support path-style API requests starting September 30th, 2020: S3 will only accept paths in the form `https://<bucketname>.s3.amazonaws.com/key`, not `https://s3.amazonaws.com/<bucketname>/key`
- AWS changes its PenTesting permission requirement, Appsecco found out exactly what is allowed and what is not

Vulnerabilities

- Remote root access on all Cisco Nexus 9000 Series devices due to a default SSH key pair: Accident or backdoor?
- Hundreds of Orpak gas station systems can be easily hacked thanks to hardcoded passwords
- Millions of consumer smart devices exposed by serious security flaw: A software feature called iLnkP2P, identified in at least two million devices made by several companies, is vulnerable to MiTM attacks.
- More than half of popular email clients are vulnerable to signature spoofing

Breaches & Attacks

- A hacker is wiping Git repositories and asking for a ransom: "all evidence suggests that the hacker has scanned the entire internet for Git config files, extracted credentials, and then used these logins to access and ransom accounts at Git hosting services"
- Report: Unknown Data Breach Exposes 80 Million US Households
- Microsoft Outlook Email Breach Targeted Cryptocurrency Users: "a hacker getting hold of a Microsoft customer support worker's login credentials; from there, the hacker could dive into the content of any non-corporate Outlook, Hotmail, or MSN account"
- Latest WebLogic vulnerability exploited for Cryptomining and DDoS Attacks & Ransomware
- Hackers Steal and Ransom Financial Data Related to Some of the World's Largest Companies: A hacker blackmailed and leaked financial data stolen from Citycomp. It's an internet infrastructure firm that provides services to many large companies like Oracle, Volkswagen & Airbus
- Recent Confluence vulnerability exploited in the wild by AESDDoS, a botnet that performs RCE, DDoS & Cryptocurrency mining

Other news

- Hacker takes over 29 IoT botnets: “Hacker “Subby” brute-forces the backends of 29 IoT botnets that were using weak or default credentials.”
- Security experts weigh in on EU biometrics database plan
- Firefox Addons Being Disabled Due to an Expired Certificate: All Firefox addons disabled because of an expired intermediary certificate used to sign Mozilla addons.
- Is a sticky label the answer to the IoT’s security problems?

Non technical

- What I Learned After a Year as a Cybersecurity Mentor
- Learn to code in less than a week
- OSINT Recon Great? – Unique Usernames Are Better Than Unique Passwords

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You’re welcome to read them directly on Twitter: Tweets from 04/26/2019 to 05/03/2019.

*Curated by Pentester Land & Sponsored by Intigriti*Subscribe to the newsletter here!*Disclaimer: The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.*