Bug Bytes #84 – From XSS to SSRF, Chaining bugs to RCE & Automation for mass recon and exploitation

BY ANNA HAMMOND · AUGUST 19, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from 07 to 14 of August.

Our favorite 5 hacking items

1. Conference of the week

Red Team Village (DEF CON Safe Mode), especially:

- Mechanizing the Methodology: by Daniel Miessler
- Knock knock, Who's There? Identifying Assets in the Cloud by @NahamSec and StaticFlow
- Combining notebooks, datasets, and cloud for the ultimate automation factory by Ryan Elkins
- Android Application Exploitation & Material

I know I've mentioned Red Team Village last week, but these videos were just uploaded and are really worth viewing. Three of them are about advanced automation for higher efficiency. The idea is to leverage automation to free up time and be able to focus on other things that cannot be automated. @DanielMiessler, @NahamSec/_StaticFlow_ and @ryanelkins present three different solutions that will probably make you want to rework your tools!

The last talk is about Android app testing. @B3nac shares his methodology and common attack vectors, with focus on Deep links. This is the talk to wathc if you want to focus on Android bounties.

2. Writeups of the week

CVE-2020-11518: how I bruteforced my way into your Active Directory

Open Sesame: Escalating Open Redirect to RCE with Electron Code Review

These are excellent examples of bug chains that escalate impact to the max.

@honoki followed a lead for Java insecure deserialization that needed arbitrary file upload. So, he reproduced the target environment locally, found a vulnerable file upload functionality, and a bruteforeable authentication key. The combination of all these bugs resulted in RCE on an AD-connected server, which means remote access to the company's internal networks.

In the second writeup, @spaceraccoonsec explains in great details how XSS (with CSP bypass) and open redirect in an Electron app can be escalated to RCE.

3. Video of the week

Alyssa_Herrera_ Talks About Bug Bounties, Pulse Secure Research, Hacking US Dept of Defense & More!

@Alyssa_Herrera_ is known for her research on SSRF, Pulse Secure VPN, and for hacking the United Stated Department of Defense. It's nice to hear her talks about all this, and many other things like her background, testing methodology, burnout, imposter syndrome, etc.

4. Tools of the week

SQLi Query Tampering

Credential Digger

SQLi Query Tampering is a Burp Suite extension that basically ports Sqlmap's tampering functions to Burp. It helps process and generate custom payloads to manually test for SQL injection. This is really handy when you need to generate payloads that evade WAFs and filters, and prefer manual testing to Sqlmap.

Credential Digger is a Github scanner that looks for hardcoded credentials and filters false positives using machine learning models. I haven't tested it yet, but the machine learning aspect makes it worth testing. Automatically scouring Github for secrets, with less false positives, is interesting for recon.

5. Tip of the week

> **"Got an XSS? Try to 'upgrade' it to SSRF to get a bigger #BugBounty. Thanks for the #BugBountyTip, @georgeomnet!**
> **Never head of ESI Injection before? Check out this @defcon talk:**
> **https://t.co/ltXGAuP6AZ#BugBountyTips #HackWithIntigriti pic.twitter.com/0XYUgWrS0M**
> **— Intigriti (@intigriti) August 14, 2020"**

This is a great tip by @georgeomnet! The next time you find XSS and caching is used, remember to test for ESI injection. It can lead to SSRF, increasing the impact of the XSS.

Other amazing things we stumbled upon this week

Videos

- How to Stop Learning and Start Hacking!
- Interview with Th3g3nt3lman
- Perspective is everything
- Post #Defcon28 – @JHaddix

- CyberTalk ep.9-@LiveOverflow Talks About CTFs, binary exploitation, reverse engineering & bug bounty
- XSS Filter Bypass | Pseudo protocol | Part 7
- $37,500 Shopify auth bypass – Hackerone
- Real Bugs – API Information Disclosure
- Roasting Resumes & Interview with a Cybersecurity Recruiter
- Kill Chain: The Cyber War on America's Elections | Full Documentary for DEF CON | HBO
- Security Weekly BlackHat 2020

Podcasts

- Geneva – Great Firewall Of China, Black Hat/DEFCON 2020, Have I Been Pwned
- Risky Business #594 — How ESNIs will change censorship and NDR
- The InfoSec & OSINT Show 20 – Robert Baptiste (Elliot Anderson) & Mobile App Hacking
- CoalCast #17 – Rastamouse
- Security in Five Episode 805 – China Blocking TLS 1.3, Here's Why And Why You Should Want To Use It
- SWN #55 – Kr00k Vuln, Banning TikTok, & Mercedes-Benz Vulns

Webinars & Webcasts

- Cisco and Pentester Academy Attacking Active Directory Class
- Easing into Consulting, COVID edition: 10 Qs and As

Conferences

- Out of Hand :: Attacks Against PHP Environments – Powerful PHP Pwn Primitives & Slides
- USENIX '20

Tutorials

Medium to advanced

- Modern PHP Security Part 1: bug classes
- How to Create Unlimited Rotating IP Addresses with AWS
- Semgrep A Practical Introduction

- Hunting for Skeleton Key Implants #BlueTeam
- Debugging into .NET
- IoT Security – Part 11 (Introduction To CoAP Protocol And Security)

Beginners corner

- Practical GraphQL attack vectors
- Tips and Tricks for Pen-testing iOS Apps with jailbreak detection
- Apple iPhone Activation, Asymmetric Encryption & (un)tethering.
- Take Dorking to the next level with this tool
- Gain access to an internal machine using Port forwarding — Setup experiment environment & Penetration testing
- Offense and Defense – A Tale of Two Sides: Group Policy and Logon Scripts

Writeups

Challenge writeups

- Arbitrary Parentheses-less XSS
- Pwn2Own -> Xxe2Rce
- Bugcrowd & Vullnerability XSS Challenge 2020

Pentest writeups

- Data Exfiltration | Bypassing a misconfigured DLP to exfiltrate sensitive data.
- Chaining multiple vulnerabilities to exfiltrate over 250GB of PIA

Responsible(ish) disclosure writeups

- Exploiting vBulletin: "A Tale of a Patch Fail" & vBulldozer #Web #CodeReview
- Newsletter Plugin Vulnerabilities Affect Over 300,000 Sites #Web
- Don't be silly – it's only a lightbulb #IoT #ZigBee
- Keeping the gate locked on your IoT devices: Vulnerabilities found on Amazon's Alexa #IoT
- Just another Null Byte Poison via Unicode variant (MuPDF mutool RCE) #RCE
- Hunting for SQL injections (SQLis) and Cross-Site Request Forgeries (CSRFs) in WordPress Plugins #Web

- Path Traversal Vulnerability in SecurEnvoy impacts on remote command execution through file upload #Web #CodeReview
- SSD Advisory – TerraMaster OS exportUser.php Remote Code Execution #Web
- Follow the Data: A Hidden Directory Traversal Vulnerability in QNX Slinger #Web
- Cisco Unified IP Conference Station 7937G #Web
- Critical Vulnerabilities Patched in Quiz and Survey Master Plugin #Web #CodeReview

Bug bounty writeups

- Hacking Zoom: Uncovering Tales of Security Vulnerabilities in Zoom (Zoom)
- CSP Bypass Vulnerability in Google Chrome Discovered – Almost Every Website In The World Was At Risk (Google, $3,000)
- Leaking AWS Metadata – The Unusual Way
- Bug Hunting with Param Miner: Cache poisoning with XSS, a peculiar case
- Denial of Service(DoS) By Regex
- Smear phishing: a new Android vulnerability (Google)
- Pre-auth Denial-of-Service in Dovecot RPA implementation (Open-Xchange, $550)
- Denial-of- service By Cache Poisoning The Cross-Origin Resource Sharing Misconfiguration Allow Origin Header (Automattic, $200)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- CertEagle & Intro: Asset monitoring utility using real time CT log feeds
- gl-redteam/gitrob: Gitrob fork that adds several features to gitrob including GitLab support, commit content searching, in-memory repository cloning, and more
- ardse: Extracts subdomains of a specified domain using https://api.recon.de

More tools, if you have time

- Whoxyrm: A reverse whois tool based on Whoxy API
- Vailyn: A phased, evasive Path Traversal scanning & exploitation tool in Python
- pmg: Extract parameters/paths from urls
- 403fuzzer: Fuzz 403/401ing endpoints for bypasses

- Evine: Interactive CLI Web Crawler
- paraglider: Python tool to check source-code for (hidden) parameters
- Mística: An open source swiss army knife for arbitrary communication over application protocols
- SkyArk: Helps to discover, assess and secure the most privileged entities in Azure and AWS
- Manuka: A modular OSINT honeypot for blue teamers
- Overlord: Red Teaming Infrastructure Automation
- Cotopaxi: Set of tools for security testing of Internet of Things devices using specific network IoT protocols
- Carnivore: A username enumeration and password spraying tool for Microsoft services (Skype for Business, ADFS, RDWeb, Exchange and O365)
- DeepSea Phishing Gear: Aims to help RTOs and pentesters with the delivery of opsec-tight, flexible email phishing campaigns carried out on the outside as well as on the inside of a perimeter
- AutoGadgetFS: Open source framework that allows users to assess USB devices and their associated hosts/drivers/software without an in-depth knowledge of the USB protocol
- Mythic & Intro: Apfell C2 framework is re-branded as Mythic with new features

Misc. pentest & bug bounty resources

- Attack flow for an oauth CSRF
- Attack Detection Fundamentals
- Hacking sites
- cve-search public api
- Short alert() XSS payloads
- Mozilla Observatory

Challenges

- BugPoc's Buggy Calculator XSS Challenge
- LEVELUP0X07 CTF Challenge
- @filedescriptor 6 years old XSS challenges

Articles

- When alert fails: exploiting transient events
- How I Got Access to Other People's Medium Accounts

- Excel Sheet to Word Report by PowerShell
- ACE to RCE #ActiveDirectory
- Type-awareness in semantic grep
- Geolocating Mobile Phones With An IP
- Unbricking a $2,000 Bike With a $10 Raspberry Pi
- Fun with Creating a VBS Payload to Bypass Endpoint Security

News

Bug bounty & Pentest news

- What's new in Covenant v0.6

Reports

- Positive Technologies research shows hackers only need 30 minutes to penetrate an organization's local network
- Cybersecurity Skills Gap Worsens, Fueled by Lack of Career Development
- Upstream attacks on open source ecosystem up 400% as criminals seek to compromise applications at scale
- Coronavirus: Fall in healthcare data breaches could be due to 'pandemic distraction'

Vulnerabilities

- vBulletin zero-day vulnerability revealed, failed patch to blame
- CVE-2019-0230: Apache Struts Potential Remote Code Execution Vulnerability
- Patch Tuesday – August 2020
- TeamViewer fixes bug that lets attackers access your PC
- ReVoLTE attack can decrypt 4G (LTE) calls to eavesdrop on conversations
- Intel, ARM, IBM, AMD Processors Vulnerable to New Side-Channel Attacks
- Citrix warns of patch-ASAP-grade bugs in its working-from-home products, just as we're all working from home
- Remote code execution vulnerability exposed in popular JavaScript serialization package
- Beyond KrØØk: Even more Wi Fi chips vulnerable to eavesdropping
- Nearly 50% of all smartphones affected by Qualcomm Snapdragon bugs

Breaches & Attacks

- A mysterious group has hijacked Tor exit nodes to perform SSL stripping attacks
- Newly discovered APT group RedCurl offering hack-for-hire services, report warns
- SANS shares details on attack that led to their data breach
- CREST: We are investigating NCC Group certification cheat sheet scandal – and not with NCC personnel
- This NSA, FBI security advisory has four words you never want to see together: Fancy Bear Linux rootkit
- Windows, IE11 zero-day vulnerabilities chained in targeted attack
- Mac malware spreads through Xcode projects, abuses WebKit, Data Vault vulnerabilities

Other news

- Mozilla is laying off 250 people and planning a 'new focus' on making money
- Google Rolls Out Samesite Cookie Changes To Chrome
- Google: We'll test hiding the full URL in Chrome 86 to combat phishing
- Firefox 79: Latest browser release enables Enhanced Tracking Protection 2.0 by default
- Rite Aid deployed facial recognition systems in hundreds of U.S. stores
- For six months, security researchers have secretly distributed an Emotet vaccine across the world
- Instagram Retained Deleted User Data Despite GDPR Rules

Non technical

- Bug Business #8 – Get to know Intigriti's Top Hackers in Q2: kuromatae
- Security Engineers By Day, Hackers By Night – An Interview With Two Of Singapore's Top Ethical Hackers
- Hacker Spotlight: Interview With Ziot
- How to Defend Against Pegasus, NSO Group's Sophisticated Spyware
- How to document your knowledge (in a CV/resume)
- Doing Cloud in China
- The Bug Bounty Game song

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 08/07/2020 to 08/14/2020.