Bug Bytes #42 – XML to RCE, GitHub for Recon & Cloud Hacking Heaven

BY INTIGRITI · OCTOBER 29, 2019 · LAST UPDATED ON JULY 30, 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.

This issue covers the week from 18 to 25 of October.

intigriti news

- Introducing our new platform: what to expect
    - Don't forget to save your drafts securely, as they will not be migrated!

Our favorite 5 hacking items

1. Tools of the week

> "– Github-subdomains.py
> – Erlenc"

Github-subdomains.py is one of many Github scripts shared lately by @gwendallecoguic for Github recon. It takes a domain as input and returns its subdomains found on Github.
Sometimes, this is just what you need for recon or OSINT!
Erlenc also does one thing: It is a command line tool for URL-encoding and URL-decoding data streams. It can be useful for scripting, or if you find yourself playing with URL encoding all the time during tests.

2. Writeup of the week

> "Don't open that XML: XXE to RCE in XML plugins for VS Code, Eclipse, Theia, ..."

Exploiting an XXE during a pentest unexpectedly triggered two DNS interactions instead of one. This led the authors to investigate, and discover that opening the XXE payload in their text editor was triggering the second interaction.
What could have been neglected by others became the subject of very interesting research. From weaponizing the XXE to get RCE, to testing other products that share the same underlying vulnerable library... There are many lessons in this writeup, both technical and about mindset and tenacity.

3. Conference of the week

> "Kawaiicon 2019 – Liar, Liar: a first-timer "red-teaming" under unusual restrictions"

This is the story of an unusual red teaming mission. I don't want to spoil it by saying to much. So, let's just that it is captivating, witty, and perfect for those times when you want to relax while still doing something hacking-related.

4. Resource of the week

> "Cloud Security Wiki"

This is a collection of links for cloud security (from both offensive and defensive aspects). They are organized by topic: AWS/Google/Azure Cloud, vulnerable apps, Kubernetes and Docker.
It is nice to have all these resources at the same place. It should help if you're interested in Cloud security and don't know where to start.
I am also realizing there are some tools and presentations listed that I haven't checked out yet.

5. Article of the week

> "Attempting EC2 Subdomain Takeover"

Subdomain takeover get harder to find on bug bounty programs. This article breaks down a more subtle form of the attack which affects some subdomains pointing to EC2 instances.
Who knows, it might help you get some of those juicy bounties!

Other amazing things we stumbled upon this week

Videos

- Live Bug Bounty Recon Session and Creating a Recon Database for Yahoo W/ @0xpatrik
- HackerOne Hacker Interviews: Katie (InsiderPhD)
- Solving XSS Challenges from PortSwigger's Web Academy
- Cybertalk – EP1 – Secure Coding, HackTheBox & Web App Penetration Testing

Podcasts

- Security Now 737 – Biometric Mess
- Risky Business #559 — Maybe it was the Israelis hacking the Russians to masquerade as Iranians?
- Hackable? 33 – Who's Watching
- The Hacker Next Door – Black Hat Hacker Skylar Rampersaud
- Hack Naked News #238
- Paul's Security Weekly #624

Webinars & Webcasts

- Modern Web Application Penetration Testing Part 1, XSS and XSRF Together
- Successful Infosec Consulting 101

Conferences

- GrrCON 2019 Videos, especially:
  - Hashes; Smothered and Scattered: Modern Password Cracking as a Methodology
  - Beginner's Guide to Mobile Applications Penetration Testing
- BSidesLV 2019

Slides only

- What's wrong with WebSocket APIs? Unveiling vulnerabilities in WebSocket APIs
- Side-Channels on the Web: Attacks and Defenses
- Postscript Pat and His Black and White Hat
- Additional slides and paper of SSO Wars from @BlackHatUSA
- The Path Less Traveled: Abusing Kubernetes Defaults
- Bash & Recon

Tutorials

Medium to advanced

- Exploiting the Java Deserialization Vulnerability
- Reverse Proxies Setup for Malicious Purposes
- Bypassing LLMNR/NBT-NS honeypot
- Red Team Diary, Entry #2: Stealthily Backdooring CMS Through Redis' Memory Space
- Persistence – Security Support Provider & Time Providers
- Red Team Tactics: Active Directory Recon using ADSI and Reflective DLLs

Beginners corner

- JWT (JSON Web Token) (in)security & jwt-pwn (Security Testing Scripts for JWT)
- Deep Dive into .NET ViewState deserialization and its exploitation
- XSS Filter Evasion

- Reddit OSINT Techniques
- Windows Privilege Escalation via DLL Hijacking

Writeups

Challenge writeups

- TreesForFuture – hack.lu CTF 2019
- [SECCON 2019] — Writeup
- AWAE/OSWE PREP (Code analysis to gaining rce and automating everything with Python)

Pentest writeups

Responsible(ish) disclosure writeups

- Hacking a Banksy with Bash and Varanid #Web
- PHP Remote Code Execution 0-Day Discovered in Real World CTF Exercise #Web #RCE
- CVE-2019-16278 – Unauthenticated Remote Code Execution in Nostromo web server #Web #RCE #CodeReview
- CVE-2019-12643: Cisco IOS XE Authentication Bypass Vulnerability #Web
- OneDrive/SharePoint File Picker Access Token Hijacking #Web #OAuth

Bug bounty writeups

- Privilege escalation on Semmle ($2,000)
- Information disclosure on HackerOne ($2,500) => IDOR
- DoS on Moneybird ($100)
- Privilege escalation using Autorize
- NFC Beaming Bypasses Security Controls in Android
- RTLO on Opera
- Session expiration bypass on Facebook ($1,5000)
- RCE, XSS, Logic flaw & Information disclosure on AntiHack.me

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Stepper: A Burp extension designed to be a natural evolution of Burp Suite's Repeater tool, providing the ability to create sequences of steps and define regular expressions to extract values from responses which can then be used in subsequent steps
- GitHunter: A tool for searching a Git repository for interesting content
- Jsfuzz: Coverage-guided fuzzer for testing JavaScript/NodeJS packages

More tools, if you have time

- Domain-finder: Quick script to find domains who belong to a company through http://whoxy.com (key required but free)
- Apk-mitm: A CLI application that prepares Android APK files for HTTPS inspection
- Ntlmscan: Scan for NTLM directories
- Dirstalk: Modern alternative to dirbuster/dirb
- RAS-Fuzzer: RAndom Subdomain Fuzzer
- SUID3NUM: Python script to enumerate SUID binaries, separate default binaries from custom binaries, cross-match those with bins in GTFO Bin's repository & auto-exploit those
- BabooSSH: Python script that allows you, from a simple SSH connection to a compromised host, to quickly gather info on other SSH endpoints to pivot and compromise them.
- Lava: Microsoft Azure exploitation framework
- HomePWN: Swiss Army Knife for Pentesting of IoT Devices
- OneLogicalMyth_Shell: A HTA shell to assist with breakout assessments
- PHuiP-FPizdaM: Exploit for a bug in php-fpm (CVE-2019-11043)

Misc. pentest & bug bounty resources

- APIsecurity.io Issue 54: API vulnerabilities in eRosary, Kubernetes, Harbor
- Quick and Dirty Penetration Testing Notes
- Lateral Movement
- Awesome Bloodhound
- Red team Slack channel by @netbiosX
- How to check for CVE-2019-11253 on your Kubernetes Clusters

Challenges

- ED 105: Server Side Template Injection (SSTI): SSTI lab & walkthough

- XSS challenge by @terjanq
- Bypass-sql-inj-waf lab (9 levels)

Articles

- Responsible denial of service with web cache poisoning
- CPDoS: Cache Poisoned Denial of Service
- Tracking down the developer of Android adware affecting millions of users #OSINT
- CSS Injection Primitives
- Bypassing Authentication on SSH Bastion Hosts & SSHession
- Bypassing Low Type Filter in .NET Remoting
- Breach Scenario – Retail Industry
- Abusing Windows 10 Narrator 'Feedback-Hub' for Fileless Persistence
- Discovering the Anti-Virus Signature and Bypassing It

News

Bug bounty & Pentest news

- You can now exec Python/JS in Hackvertor!
- Chrome 79 Dev Tools now includes a new tab "Initiator" to investigate why a network resource was requested. This will be hugely helpful in debugging JS applications.
- We are launching our new platform soon! What you can expect... (Intigriti)
- Check out @Hacker0x01's new badges for Live Hacking Events! I don't think @fransrosen needs any more badges though !

Reports

- 2019 Cyberthreat Defense Report by Imperva

Vulnerabilities

- Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping
- Vulnerability in content distribution networks found by researchers
- ATTK of the Pwns: Trend Micro's antivirus tools 'will run malware – if its filename is cmd.exe'
- Unpatched Linux bug may open devices to serious attacks over Wi-Fi
- New Amazon Echo Warning As Wi-Fi Cyberattack Risk Confirmed

- Equifax used ‘admin’ as username and password for sensitive data: lawsuit

Breaches & Attacks

- Researchers find stealthy MSSQL server backdoor developed by Chinese cyberspies
- Hacker breached servers used by NordVPN
- Russian cybercrooks co-opted Iranian hacking tools to attack dozens of countries
- A Brief History of Russian Hackers’ Evolving False Flags

Malicious apps/sites

Other news

- 15 Years Later, Metasploit Still Manages to be a Menace
- Air Force finally retires 8-inch floppies from missile launch control system
- Weaponizing and Gamifying AI for WiFi Hacking: Presenting Pwnagotchi 1.0.0

Non technical

- Through a Hacker’s Eyes: Recapping h1-604
- How to Start a Bug Bounty Program
- Build An InfoSec Lab ‘The Right Way’

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 10/18/2019 to 10/25/2019.

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