Bug Bytes #31 – HTTP Desync Attacks by @albinowax, Exploiting Out Of Band XXE by @Zombiehelp54, GitHub Recon and Sensitive Data Exposure

BY INTIGRITI · AUGUST 13, 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.

This issue covers the week from 02 to 09 of August.

Our favorite 5 hacking items

1. Slides of the week

> "Black Hat USA 2019 Slides & presentation materials"

It feels like Hacker Summer Camp (Black Hat, Defcon, BSides Las Vegas...) has dominated the news this week. A huge chunk of new vulnerabilities, tools, slides, and whitepapers published were shared during these events.
So I am not going to share with you all the links because there are way too many. But you can find slides and whitepapers on the Black Hat website. You can start going through that while waiting for the video recordings to come out.
Also here is what I do to find materials on a topic I'm interested in: I check out the talk's title and author in the presentations schedule or in the workshops page. Then I search for it on Twitter/Google/Github.
For example, I found these using this method:

- Material from @ithilgore's segment at the medical device hacking workshop
- Serverless Workshop

Also, don't forget to check out the arsenal section. You won't necessarily see links to the tools there, but you can find them on Github/Google (e.g. Eyeballer & JSShell).

2. Writeup of the week

> "Exploiting Out Of Band XXE using internal network and php wrappers"

A few days ago, @Zombiehelp54 tweeted about having exploited an XXE despite a firewall blocking all outgoing requests including DNS lookups. That was suspenseful! Here is how he did it:

- The app had an "xml" parameter that was encrypted

- The encryption function was readable in JavaScript, but it was hard to read. So he used breakpoints to modify the XML data just before encryption. This allowed him to inject his own encrypted payloads
- It was possible to inject external entities. The XXE was proved but a firewall blocked all outgoing requests. Only requests to the internal network were allowed and Mahmoud couldn't fetch external DTD files from his server
- Using *data://* didn't work. But the firewall could be bypassed by using *php://* to fetch a resource from a *data://* URI
- Of course, this work because the app is in PHP!
- The payload was: *php://filter//resource=data://text/plain;base64,PCFFTlRJVFkgJSBkYXRhIFNZU1R...*

Note that this is just a summary. Check out the writeup, it's full of awesome advanced XXE exploitation techniques.

3. Article / Tool of the week

> "HTTP Desync Attacks: Request Smuggling Reborn
> – Whitepaper
> – HTTP Request Smuggler
> – Web Security Academy (course & challenges)"

To be honest, I haven't had the time to properly read this article. But judging from @albinowax's previous research, I know for sure that it's good. He earned over $70k bug bounties while doing this research!
The attack is based on a forgotten technique called "HTTP request smuggling". It can lead to bypassing security controls or accessing unauthorized sensitive data, and can be chained with Web cache poisoning and XSS.
The awesome part is that, since James works at PortSwigger, a Burp extension to scan for Request Smuggling bugs is already available. A new scan check was also added to the Burp scanner. And a new lesson was added to the Web Security Academy (with 12 labs).
Also, he only tested approx 5% of bug bounty sites, so there's still room for us mortals to play with this bug.

4. Podcast of the week

> " 404 Podcast Not Found #4 /w PwnFunction"

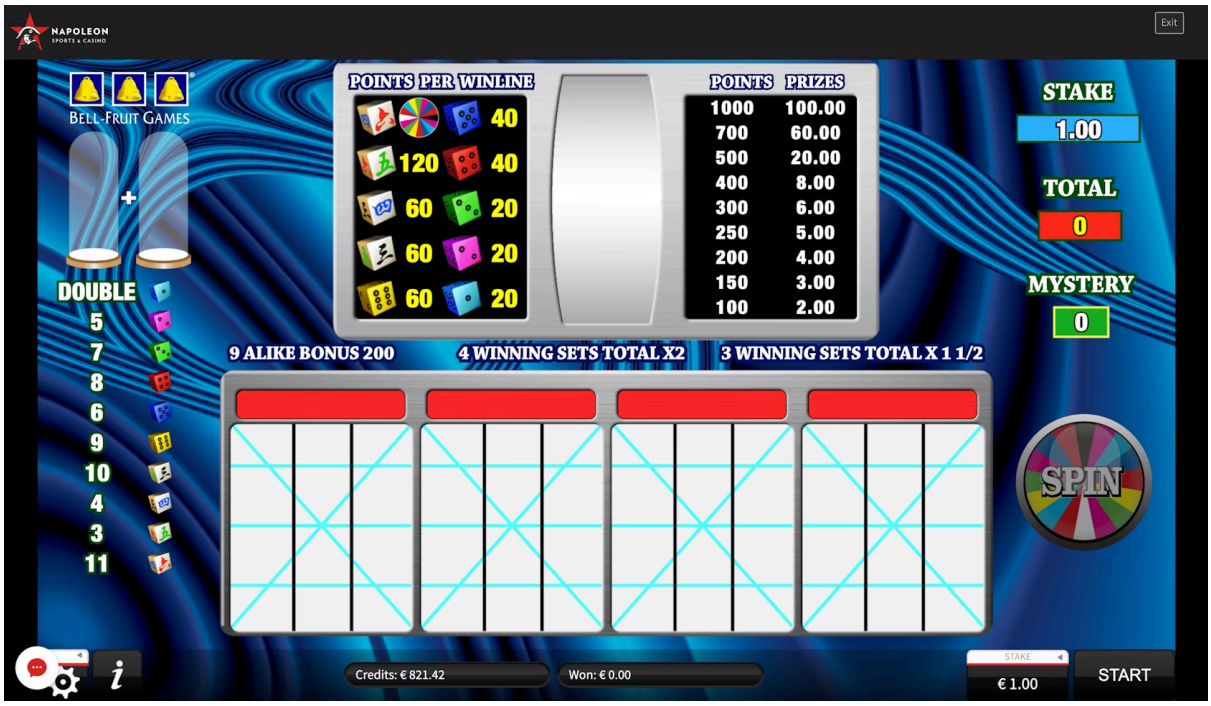
This is a cool podcast episode if you're looking for something to pass the time while commuting, walking or exercising.
It's not technical at all, it's more in the entertainment category. But it's nice getting to know the mysterious @PwnFunction. Also I love the trivia quizz, wish it was longer!

5. Intigriti News

5.1 Exclusive game at Wimigames

Wimigames allows you to test their new Dice spinner. This game is not publicly available and exclusively for intigriti users. You need to be a registered intigriti user to see the program Be the first one to test it!

Start hunting here!



6. Videos of the week

> "GitHub Recon and Sensitive Data Exposure, Advanced Burp Suite, Recon & Discovery XML External Entity Injection & Server Side Forgery Request"

Wow, that's a lot to watch! My hacker watchlist keeps alarmingly growing these days.
Bugcrowd University just dropped 5 new videos on recon, Github, Burp, XXE and SSRF. They look really interesting. And judging from their length, there is probably something new to learn here for everyone.

Other amazing things we stumbled upon this week

Videos

- Live Bug Bounty Recon Session on Yahoo (Part 3 – 7/28/2019)
- Live chat with zseano from Bug Bounty Notes
- XSS Polyglot
- Pentesting for n00bs: Episode 1 – Legacy

- Teaching my Wife Buffer Overflows
- Burp Suite 2 tutorials

Podcasts

- Security Now 726 – Steve's File Sync Journey
- Risky Business #550 — CapitalOne owned, Hutchins sentenced, VxWorks horror-show and more!
- Darknet Diaries EP 44: Zain
- Attacking and Defending Kubernetes, with Ian Coldwater
- 7MS #375: Tales of Pentest Fail #3
- Security In Five Episode 555 – Tools, Tips and Tricks – Random.Org
- Cyber – Why The FBI Arrested the Hacker Who Saved the World From WannaCry

Conferences

- Security patterns for keeping secrets in the browser

Slides & Material

- Active Directory Security: 8 (very) low hanging fruits and how to smash those attack paths
- TLS 1.3 for Penetration Testers (and the talk that came with it)
- Lessons from 3 years of crypto and blockchain security audits

Tutorials

Medium to advanced

- Blind Xss (A new way)
- Debugging Cordova Applications
- Kubernetes Pentest Methodology Part 1
- Tools and Methods for Auditing Kubernetes RBAC Policies
- How to Build Your Own Penetration Testing Dropbox Using a Raspberry Pi 4
- MacOS Red Teaming 207: Remote Apple Events (RAE)
- How to Start IoT device Firmware Reverse Engineering?

Beginners corner

- A NoSQL Injection Primer (with Mongo)
- How To Attack Kerberos 101
- Python 2.7 input? /bin/bash !! & Python – Hacking with style – input (Security issues fixed in Python 3)
- Linux for Pentester: scp Privilege Escalation
- Linux For Pentester: tmux Privilege Escalation
- A Beginner's Guide to OSINT Investigation with Maltego
- Mr. Robot Hacks, Part 7: How Elliot Hacks Everyone's Password

Writeups

Challenge writeups

Pentest writeups

- Three (And A Half) Vulns For The Price of One!
- Audit-kubernetes: Kubernetes pentest report, plus notes used by Trail of Bits for the audit
- Meteor Blind NoSQL Injection

Responsible(ish) disclosure writeups

- Attacking SSL VPN – Part 2: Breaking the Fortigate SSL VPN #VPN
- CVE-2019-12103 – Analysis of a Pre-Auth RCE on the TP-Link M7350, with Ghidra! #RCE #Reverse
- Group sex app leaks locations, pics and personal details. Identifies users in White House and Supreme Court #Mobile
- FB50 Smart Lock Vulnerability Disclosure (CVE-2019-13143) #IoT
- Steam Windows Client Local Privilege Escalation 0day & PoC #PrivilegeEscalation

Bug bounty writeups

- SQL injection on Starbucks ($4,000)
- Information disclosure on Automattic ($100)
- Information disclosure on HackerOne ($500)
- XSS & Privilege escalation
- Race condition & Logic flaw
- Lack of rate limiting

- Account takeover via Stored XSS
- Privilege Escalation

Tools

If you don't have time

- Cloudflare-origin-ip.py: A script to perform automatic Cloudflare bypass test through Censys
- XFFenum: X-Forwarded-For [403 forbidden] enumeration
- Timeinator: Burp extension that can be used to perform timing attacks over an unreliable network such as the internet

More tools, if you have time

- Confluence_searcher.py: Python3 script to help search Confluence for different key words & output the results to a csv. Change the URL api path based on your installation
- Orca: Targeted OSINT Framework
- Irule-detector: Burp extension that detects F5 BigIP vulnerable to an RCE affecting the iRule feature
- SMTPTester: Small python3 tool to check common vulnerabilities in SMTP servers
- AttackSurfaceMapper: A tool that aims to automate the reconnaissance process
- PyDNSRecon / Runbooks: Subdomain enumeration tool that uses Censys.io, Amass & Sonar FDNS data
- Marzavec/run.js: Browser-based subdomain bruteforcing using DNS over HTTP(s) (DoH)
- LittleBrother: Information gathering (OSINT) on a person (EU). No API key or login needed

Misc. pentest & bug bounty resources

- Attacking Kubernetes: A Guide for Administrators and Penetration Testers
- Penetration Testing & Hacking Tools List for Hackers
- Metasploit Cheatsheet
- Pentestwiki.org

Challenges

- DEFCON 27 – Cloud Village CTF
- New CloudGoat scenario: "cloud_breach_s3" : Inspired by the Capital One breach
- Vulhub: Pre-Built Vulnerable Environments Based on Docker-Compose

Articles

- Don’t Underestimate Grep Based Code Scanning
- GitHub: The red-teamer’s cheat-sheet
- Is Your Serverless Application Secure?
- Attacking Unmarshallers :: JNDI Injection using Getter Based Deserialization Gadgets
- “I see ZigBees Everywhere”
- DCMS Practical Guidelines. Actionable information
- From The Depths Of Counterfeit Smartphones
- Preventing The Capital One Breach

News

Bug bounty & Pentest news

- Apple Upgrades Bug Bounty Program: Adds Macs, $1M Reward
- Google: “we’ll give out 100k USD in Grants for Google Cloud vulnerability research and we’ll pay the best report we get in 2019 another 100k”
- Microsoft launches Azure Security Lab, doubles top bug bounty to $40,000
- Commando VM 2.0: Customization, Containers, and Kali, Oh My!: “we’ve also included VcXsrv, an X Server that allows us to display the entire Linux GUI on the Windows Desktop”
- The pwnie awards winners & nominations

Reports

- LARES Continuous Defensive Improvement Through Adversarial Simulation and Collaboration
- Report: Thin Red Line – Penetration Testing Practices Examined
- We tested 21 Android antivirus apps and found these serious vulnerabilities
- Data Breaches Statistics (All You Need to Know!)
- 246 Findings From our Smart Contract Audits: An Executive Summary

Vulnerabilities

- Researcher uses GDPR data transparency clause to obtain users’ sensitive information
- Steam Zero-Day Vulnerability Affects Over 100 Million Users
- Microsoft Confirms New Windows CPU Attack Vulnerability, Advises All Users To Update Now

- Millions of Android Smartphones Vulnerable to Trio of Qualcomm Bugs
- Visa vulnerability
- Security of popular kids' tablet 'quite concerning', researchers find
- Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials

Breaches & Attacks

- More than 2m AT&T phones illegally unlocked by bribed insiders
- Clever Amazon Phishing Scam Creates Login Prompts in PDF Docs
- With warshipping, hackers ship their exploits directly to their target's mail room
- [Banking PINs exposed in Monzo secure storage slip-up(https://nakedsecurity.sophos.com/2019/08/07/monzo-sticks-a-pin-in-cybersecurity-slip-up/)
- Microsoft catches Russian state hackers using IoT devices to breach networks

Other news

- Twitter may have shared your data with its ad partners without your permission
- Eavesdropping Warning Issued To Millions of Skype And Cortana Users
- North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report
- A Multimillionaire Surveillance Dealer Steps Out Of The Shadows . . . And His $9 Million WhatsApp Hacking Van
- A design firm is hosting a contest to encourage people to reimagine cybersecurity stock images
- Half of all Google Chrome extensions have fewer than 16 installs

Non technical

- Dive into reconnaissance and PRE-ATT&CK: Introduction to MITRE ATT&CK, PRE-ATT&CK & TIBER frameworks
- Election Security: Electronic and Online Voting
- The Ultimate Guide to Strong Passwords in 2019
- Turning a MacBook into a Touchscreen with $1 of Hardware
- Learning to Forget: Infosec's Unfortunate Departure from Spaced Learning

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 08/02/2019 to 08/09/2019

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