Bug Bytes #95 – Spooky NAT Slipstreaming, WebLogic RCE in one GET request & Server-side vulnerabilities demystified

BY ANNA HAMMOND · NOVEMBER 4, 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 25 of October to 01 of November.

Intigriti News

Intigriti's November XSS Challenge

Security Snacks #4 – Psychotherapy patients blackmail, Trump vs Hackers & How not to use Microsoft 365

Our favorite 5 hacking items

1. Conference of the week

#Eko2020 Workshops | Rajanish Pathak, Rahul Maini & Harsh Jaiswal: Demystifying the Server Side & Slides

This is a great workshop on server-side vulnerabilities. It includes concise introductions to SSRF, XXE, Remote Code Execution and Reverse Proxy attacks. The case studies especially are very interesting.

2. Writeups of the week

Weblogic RCE by only one GET request — CVE-2020–14882 Analysis (in Vietnamese), Exploit, Bypass & AttackerKB analysis
Ability To Backdoor Facebook For Android

CVE-2020-14882 is a pre-authentication Remode Code Execution in Oracle WebLogic. It was patched but a bypass was released a week after. So, now it is being exploited in the wild. For pentesters and bug hunters, it is interesting to add to testing workflows as it has a 9.8/10 CVSSv3 score and takes only one GET request to exploit.

The second writeup is about an insecure development deeplink that could've allowed backdooring Facebook for Android. It provides great insight into deeplinks abuse, an excellent read on Android hacking!

3. Article of the week

NAT Slipstreaming

Samy Kamkar (@samykamkar) updated an old attack that tricks firewalls and NAT devices to give access to machines not normally reachable from the Internet. After first reading about this incredible impact, I thought it was some kind of Halloween joke but the attack is real. The lenghty writeup goes into all technical details and prerequisites (Application Level Gateway support and that the victim visits a malicious site). If you just want the gist of it, here is a high-level TL;DR.

4. Tool of the week

Copy Request Response & Intro

Reporting, whether in bug bounty or pentest, can be tedious. This Burp extension will help as it makes copying HTTP requests, responses and response headers quicker and easier. A fantastic ideas since copy/pasting these elements is always needed for reporting vulnerabilities.

5. Video of the week

How I made 1k in a day with IDORs! (10 Tips!)

Katie Paxton-Fear (@InsiderPhD) already has a couple of introductory videos on IDOR. With this new one, she digs deeper into the topic with 10 hunting tips and a recent bug she found. If you understand IDORs but struggle to find them on bug bounty programs, this might just be the video you need.

Other amazing things we stumbled upon this week

Videos

- Honoki Talks About Recon, Bug Bounty Reconnaissance Framework, Hacking on Intigriti, and more!
- Leaking COVID risk group via XS-Leaks & Demo
- RIP.. MY 40TB QNAP NAS DIED.. (this weeks bug bounty news)
- What is a File Format?
- Bypassing Restrictions | Website Unblocking | ft. UserAgent | Medium, ETPrime
- Most Popular BurpSuite Pro extensions

Podcasts

- The InfoSec & OSINT Show 31 – Chris Rock & Cyber Mercenaries
- Darknet Diaries EP 77: OLYMPIC DESTROYER
- Security Now: Top 25 Vulnerabilities – Chrome 0-Day, Edge for Linux, WordPress Loginizer
- Risky Business #603 — YOU get sanctions, and YOU get sanctions

Webinars & Webcasts

- Live API Demo with OWASP Santa Barbara
- HTTP Request Smuggling In 2020

Conferences

- SECARMY Village @ GrayHat 2020 & Red Team Village, especially:
  - Application Testing Methodology and Scope-based Recon by Harsh Bothra & Slides
  - How to Get Into Bug Bounty by Katie Paxton-Fear @InsiderPhD
  - Offensive Docker for CTF, Pentesting and Bug Bounty by Arsenio Aguirre
  - The Dark Side of Cloud Configuration – Vulnerability or Feature? by Vladi Sandler
- YASCON 2020 Livestream & Schedule

Tutorials

Medium to advanced

- A Beginners Guide to Gathering Azure Passwords
- ffuf filters
- Writing Semgrep rules: a methodology
- The Tale Of The Lost, But Not Forgotten, Undocumented Netsync: Part 1 & Part 2
- Remote Desktop Services Shadowing – Beyond the Shadowed Session

Beginners corner

- A Pentester's Guide to Cross-Site Scripting (XSS)
- Web Cache Entanglement – Novel Pathways to Poisoning
- Identifying & Escalating HTTP Host Header Injection attacks
- A Brief Introduction to Semgrep & Part 2
- Not-So-Random: Using LD_PRELOAD to Hijack the rand() Function
- Social Media Search Strategies
- Detecting Kerberoasting

Writeups

Challenge writeups

- Flare-On 2020: TKApp

Pentest writeups

- Pentest Tales #001: You Spent How Much On Security? & Video version
- Using A C# Shellcode Runner And Confuserex To Bypass UAC While Evading AV

Responsible(ish) disclosure writeups

- Winston Privacy Version 1.5.4 #Web
- Loginizer before 1.6.4 SQLi injection #Web
- Reversing Pulse Secure Client Credentials Store #VPN
- pulse-secure-vpn-mitm-research (CVE-2020-8241 & CVE-2020-8239) #VPN
- Hunting the Hunters – RCE in Covenant C2 #Web
- Remote Command Execution in Ruckus IoT Controller (CVE-2020-26878 & CVE-2020-26879) #RCE #IoT

- Technical Advisory: Pulse Connect Secure – RCE via Uncontrolled Gzip Extraction (CVE-2020-8260) #Web
- When a stupid oplock leads you to SYSTEM #LPE #Windows
- CVE-2020-16939: WINDOWS GROUP POLICY DACL OVERWRITE PRIVILEGE ESCALATION #LPE #Windows
- F5 Advanced WAF / ASM Signature Bypass #Web
- Hörmann – Opening Doors For Everyone... #IoT

Bug bounty writeups

- Link Previews: How a Simple Feature Can Have Privacy and Security Risks
- An often overlooked Oauth misconfiguration.
- Story of an interesting bug.
- Wormable remote code execution in Alien Swarm (Valve)
- How i got 7000$ in Bug-Bounty for my Critical Finding.
- Half-Blind SSRF found in kube/cloud-controller-manager can be upgraded to complete SSRF (fully crafted HTTP requests) in vendor managed k8s service. (Kubernetes, $5,000)
- CSRF on launchpad.37signals.com OAuth2 authorization endpoint (Basecamp, $2,000)
- HEY.com email stored XSS (Basecamp, $5,000)

See more writeups on The list of bug bounty writeups.

Tools

- NetblockTool & Intro: Python script that finds netblocks owned by a company
- tld_detection.py: TLD matcher for any domain
- Scrying: A tool for collecting RDP, web and VNC screenshots all in one place
- iSH: Linux shell for iOS
- Grype: A vulnerability scanner for container images and filesystems
- Serval: A Netcat-style backdoor for pentesting and pentest exercises
- Hot Manchego & Intro: Macro-Enabled Excel File Generator (.xlsm) using the EPPlus Library
- CQOffensiveSecurity Toolkit: The Extreme Windows Offensive Security Toolkit for advanced Windows Infrastructure Penetration Testing

Misc. pentest & bug bounty resources

- Scary Strings!
- PowerShell Commands for Pentesters
- waf-comminity-bypasses
- Awesome-Android-Security
- Ultimate WDAC Bypass List
- PowerShell-Red-Team-Enum

Challenges

- Intigriti Novembre XSS challenge
- Flare-On 7 Challenge Solutions

Articles

- Repo Jacking: Exploiting the Dependency Supply Chain
- Hiding in Plain Site: Detecting JavaScript Obfuscation through Concealed Browser API Usage
- Abusing Teams client protocol to bypass Teams security policies
- Citrix ADC (Netscaler ADC) Multi-Factor Bypass
- Trick or Treat! What We Can Learn from the Spookiest Vulnerabilities of the Year
- Machine-in-the-Middle (MitM) BLE Attack
- Hacking in an epistolary way: implementing kerberoast in pure VBA
- Process Herpaderping

Bug bounty & Pentest news

- The Hackerone Top 10 Most Impactful And Rewarded Vulnerability Types – 2020 Edition
- MITRE ATT&CK Updates – October 2020 & New Network Matrix
- Coming through with Firefox 82

Non technical

- A Researcher's Guide to Some Legal Risks of Security Research
- About Cybersecurity Management and Expectations

- Humans are Bad at URLs and Fonts Don't Matter
- Collaborative bug hunting 'could be very lucrative' – security pro Alex Chapman on the future of ethical hacking
- Hacker Spotlight: Interview With Yassineaboukir
- Pentester Spotlight: Nikhil Srivastava
- You Should Be Running Your Own VPN Server
- How to Write Well: What I've learned over two decades of writing online

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 10/25/2020 to 11/01/2020.