Bug Bytes #155 – When logout logs you in, 120 days bug hunting challenge & Testing reverse proxies with Nuclei

BY ANNA HAMMOND · JANUARY 19, 2022 · 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.

CLICK HERE TO SUBSCRIBE

This issue covers the week from January 10 to 17, 2022.

Our favorite 5 hacking items

1. Tutorials of the week

Recon Weekly #2: GitHub Code Search Preview (for Hackers)
Abusing Reverse Proxies, Part 1: Metadata & Part 2: Internal Access

Did you see hackers tweeting about GitHub's new code search and wondered what all the hype was about?
If you want a quick preview, @sshell_ goes over why this new feature was needed and how it can be leveraged for recon.

The second tutorial is about open reverse proxy misconfigurations. Did you know that Nuclei introduced templates that detect these vulnerabilities? If not, make sure to read this refresher on reverse proxy abuse and test the new templates.

2. Writeups of the week

RCE In Adobe Acrobat Reader For Android(CVE-2021-40724) (Google, Adobe, $10,000)
Pre-Auth RCE in Moodle Part II – Session Hijack in Moodle's Shibboleth
120 Days of High Frequency Hunting

The first writeup is about a clever RCE via path traversal found by @hulkvision in Acrobat Reader for Android.

The second one is about an interesting session management issue in Moodle. Basically when a user logouts out, they are logged in as a random user for a fraction of a second. Simply refreshing the page gives access to the user's session.

The third writeup is about @caffeinevulns and @kuldeepdotexe's inspiring bug bounty challenge. They found 36 vulnerabilities in 120 days and share details on some of these findings.

3. Article & Tool of the week

Dissecting NTLM EPA With Love & Building A MiTM Proxy & Prox-Ez

This is probably not something you will need everyday, but it will be very handy if you find yourself testing a Web app that uses NTLM EPA authentication.
Firefox and other browsers do not support EPA, so @b1two_ created a proxy that allows you to correctly authenticate even if your browser that does not support this mechanism.

4. Video of the week

Buffer Overflows Made Easy (2022 Edition)

If you like @thecybermentor's teaching style and want to learn about buffer overflows, this is an amazing introduction. It starts with the basic concepts, details how to detect and exploit these vulnerabilities using Python 3, then demos a walkthrough of a TryHackMe room.

5. Resource of the week

Offensive Hacking Education Landscape

You probably already know about most content creators and learning platforms in this article, but it is a really good selection for newcomers. It takes little time to check out and maybe discover valuable new resources.
Personally, I wasn't aware of the cwinfosec Youtube channel. So, now I have two dozen videos to watch to catch up on all these cool interviews and tutorials I missed.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Introduction to Fuzzing: Binary Exploitation (Spike, Boo-Fuzz, Boo-Gen, and Custom Scripts)
- Wfuzz VS ffuf – Who is the faster web fuzzer for bug bounty? Web Security #1
- Impact of log4j | Nullcon Webcast 2022
- EternalBlue – MS17-010 – Manual Exploitation
- 2022 Cybersecurity roadmap: How to get started?
- My Top Tips for using Windows Terminal like a Pro

Conferences

- Pen Test HackFest Summit 2021

- OWASP Global AppSec US 2021 Virtual, especially:
  - Request Forgery on the Web – SSRF, CSRF and Clickjacking
  - We're not in HTTP anymore: Investigating WebSocket Server Security
  - Exploiting web messaging implementations
  - Outside the box: pwning IoT devices through their applications
- OWASP 20th Anniversary, especially:
  - Common NGINX Misconfigurations That Leave Your Web Server Open To Attack
- LASCON 2021, especially:
  - Manual JavaScript Analysis is a Bug
  - JWTs – Patterns & Anti-patterns

Tutorials

- Burp Suite Pro real-life tips & tricks: Authentication engine for command-line tools
- My Perfect Bug Bounty Docker Setup
- XSS With Hoisting
- Finding unhandled errors using CodeQL

Writeups

Challenge writeups

- Source maps in React?! Solution to January '22 XSS Challenge
- Hack The Box – Intro to Reversing – You Can't C Me
- HackTheBox – Developer
- How File Upload Vulnerabilities Work! & Web Shell via Denylist Bypass!
- SSRF – Lab #6 Blind SSRF with out-of-band detection & Lab #7 Blind SSRF with Shellshock exploitation

Pentest writeups

- 10 real-world stories of how we've compromised CI/CD pipelines
- Creating an Exploit: SolarWinds Vulnerability CVE-2021-35211 & Serv-U CVE-2021-35211 Exploit

Responsible(ish) disclosure writeups

- CVE-2021-45468: Imperva WAF bypass #Web

- Log4jHorizon & Crossing the Log4j Horizon – A Vulnerability With No Return #Web
- Microsoft HTTP protocol stack RCE (CVE-2022-21907) & PoC #Windows
- CVE-2021-20038..42: SonicWall SMA 100 Multiple Vulnerabilities (FIXED), Rapid7 analysis of CVE-2021-20039 & CVE-2021-20038 #MemoryCorruption #Web
- WordPress 5.8.2 Stored XSS Vulnerability #Web #CodeReview

Bug bounty writeups

- Searching for Deserialization Protection Bypasses in Microsoft Exchange (CVE-2022–21969) (Microsoft)
- Attacking RDP from Inside: How we abused named pipes for smart-card hijacking, unauthorized file system access to client machines and more (Microsoft)
- Stealing administrative JWT's through post auth SSRF (CVE-2021-22056) (VMWare)
- Exploiting IndexedDB API information leaks in Safari 15 (Apple)
- Mixed Messages: Busting Box's MFA Methods (Box)

See more writeups on The list of bug bounty writeups.

Tools

- Response Overview & Intro: Burp extension that groups all response bodies by similarity and shows a summary, one request/response per group
- Authz0: Automated authorization testing tool
- rustpad: Multi-threaded Padding Oracle attacks against any service. Successor to padbuster, written in Rust.
- membuddy: Early demo of a memory visualiser tool for iOS security researchers
- Ivy & Defeating EDRs with Office Products: A payload creation framework for the execution of arbitrary VBA (macro) source code directly in memory

Tips & Tweets

- @hacker_'s oneliners to generate target-based wordlists
- @Ahmad*Halabi*'s pentest story: from APK to pwning the entire company
- New Chrome feature, new XSS vector!
- Replace your Dated Linux Command Line Utilities with These Modern Alternatives.
- A story of $750 Open Redirect with multiple fix bypasses

- To ensure maximum coverage, always perform a Port scan followed by an HTTP probe before providing the input list to Nuclei.

Misc. pentest & bug bounty resources

- open-source-web-scanners
- NCC Group's 2021 Annual Research Report
- Advanced SQL Injection Cheatsheet
- FREE reverse engineering course covering x86, x64, 32-bit ARM & 64-bit ARM architectures by @mytechnotalent

Articles

- MS-FSRVP abuse (ShadowCoerce), PoC & Tutorial
- Pass the Cloud with a Cookie
- Persistence with Azure Policy Guest Configuration

Challenges

- New CloudGoat scenario & Walkthrough

Bug bounty & Pentest news

- Bug bounty
  - BreakingFormation: Orca Security Research Team Discovers AWS CloudFormation Vulnerability & Superglue: Orca Security Research Team Discovers AWS Glue Vulnerability
- Cybersecurity
  - Top 10 web hacking techniques of 2021 (vote before January 24)
  - MASVS-CRYPTO is open for comments until Januray 31
- Upcoming events
  - Pwn2Own Vancouver Returns For The 15th Anniversary Of The Contest
  - Cybersecurity conferences 2022: A rundown of online, in person, and 'hybrid' events
- Tool updates
  - Burp Suite roadmap for 2022 & Professional / Community 2021.12.1
  - Chrome to bolster CSRF protections with CORS preflight checks on private network requests
  - Why I broke your subdomain recon pipeline last night (or why tls.bufferover.run is moving from free to free*)
  - Nuclei v2.5.8

- httpx v1.1.15

Non technical

- bug-bounty-standards
- A Detailed Guide to Crack the OSWE Certification
- What to Expect From the New OSCP Exam
- Zero-Point Security's Certified Red Team Operator (CRTO) Review
- Lessons learned from my 10 year open source project