Bug Bytes #172 – Pre-hijacking accounts, CSP bypass using WordPress & Unusual SSRF + Phishing chain

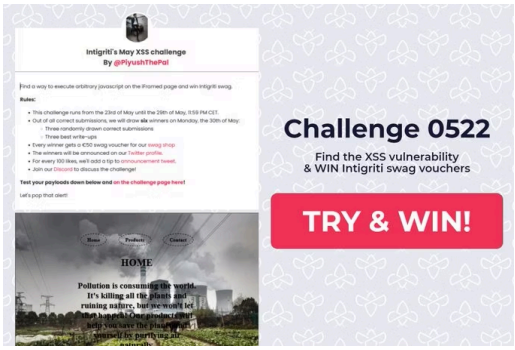
BY ANNA HAMMOND · JUNE 1, 2022 · LAST UPDATED ON MARCH 6, 2025

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 weeks from May 23 to 30.

Intigriti news



Intigriti's May XSS challenge By @PiyushThePal

Our favorite 5 hacking items

1. Article of the week

Bypass CSP Using WordPress By Abusing Same Origin Method Execution

@PaulosYibelo discovered two scenarios in which CSP can be bypassed if WordPress is hosted on the target website.
In a gist: HTML injection on the main domain + WordPress endpoint on a subdomain = XSS with CSP bypass that can be escalated to RCE.

2. Writeups of the week

Pre-hijacked accounts: An Empirical Study of Security Failures in User Account Creation on the Web (Dropbox, Meta / Facebook (Instagram), LinkedIn, WordPress & Zoom)
From open redirect to RCE in one week (Mail.ru)

The first link is a research paper by @ajpaverd and @sudoavi. They explored the topic of account hijacking, focused on five types of account pre-hijacking attacks, and discovered that 35 out of 75 services tested (including Instagram, Zoom, LinkedIn and DropBox) were vulnerable to these attacks.

The second writeup is a fantastic tale of persistence by @ByQwert. It reads like a detective story that started with open redirect and ended with RCE, with LFI, SSRF and insecure deserialization in between.

3. Vulnerabilities of the week

VMware Authentication Bypass Vulnerability (CVE-2022-22972)

- Technical Deep Dive by @Horizon3Attack
- @assetnote's code review to find the root cause
- Nuclei template

Microsoft Windows Support Diagnostic Tool RCE (CVE-2022-30190 / Follina)

- Analyses by Rapid7, Huntress & @GossiTheDog
- Videos by @_JohnHammond & SANS
- PoCs by @_johnhammond & @chvancooten
- Remediation Guidance by Microsoft

CVE-2022-22972 is an authentication bypass in some VMware products. Basically, they send authentication requests to the server specified in the Host header. Since this header can be controlled by the user, it is possible to point it to a server that always returns the 200 HTTP response code, validating all authentication requests (without having correct credentials).
The vulnerability is simple to exploit, but it is worth going through the analyses if you are interested in finding this type of bugs with code review and patch analysis.

Follina a.k.a. CVE-2022-30190 is an RCE vector that allows apps like Word to execute code (without macros) by calling MSDT using the URL protocol. It was noticed as a 0-day being exploited in the wild, but was first mentioned in 2020 in a rather interesting thesis on Electron security.

4. Videos of the week

This is my coolest bug bounty report (SSRF Phishing)
@YassineAboukir Talks About His Recon Flow, Bug Bounty, Mental Health and More!

@gregxsunday explains his coolest exploit, an SSRF chained with phishing. An unusual combination that escalated the SSRF's impact and doubled his bounty.

@Yassineaboukir's interview is one of those where I took a lot of notes. So many good insights shared on recon, content discovery, learning, favorite tools, Burp plugins, etc.

5. Resources of the week

Example of using Turbo Intruder in a "listen and attack" mode
Finding command execution sinks in decompiled JVM languages

Did you know that Turbo Intruder could use Burp's plugin API? That is what @defparam shows with this example script that listens while you're browsing, and re-plays requests with different HTTP methods.

The second resource is @dee__see's cheatsheet for reverse engineering apps written in Scala, Clojure, Groovy and Kotllin.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty 101: #19 – Android Mobile App Testing with Burpsuite
- SSRF in 100 seconds
- Wireshark for Cybersecurity w/ Chris Greer!
- HTB Stories #9: AmA with IppSec
- Manually Parse Bloodhound Data with JQ to Create Lists of Potentially Vulnerable Users and Computers

Webinars

- Hacking JavaScript: ELECTRON Applications w/ 7ASecurity
- Getting The Most Out Of The SANS Pivot Cheat Sheet
- What C2 do I need?

Conferences

- Social Engineer Your Way Into Your First InfoSec Job with Volkis
- Getting Into Penetration Testing for Beginners
- [FR] Sthack 2022 : Tales from a successful bug bounty hunter – Daniel Le Gall
- Ben Sadeghipour – Would I even be here if it wasn't for the Internet?

Tutorials

Medium to advanced

- Using a cloud Mac with a local iOS device
- Guidance for Choosing an Elliptic Curve Signature Algorithm in 2022
- Capitalizing on BloodHound's Data: Cypher, Object Ownerships and Trusts
- BloodHound Inner Workings & Limitations – Part 1: User Rights Enumeration Through SAMR & GPOLocalGroup, Part 2: Session Enumeration Through NetWkstaUserEnum & NetSessionEnum & Part 3: Session Enumeration Through Remote Registry & Summary

Beginners corner

- Customized Hacker Shell Prompts
- Intro To Web App Security Testing: Burp Suite Tips & Tricks
- Social Media Take Over = Easy Money
- Sniffing TLS traffic on Android
- Testing Non-Proxy Aware Mobile Applications Through a VPN

Writeups

Challenge writeups

- HackTheBox – AdmirerToo & Blog post
- Approaching CTF OSINT Challenges — Learn by Example (NahamCon CTF)
- Solving "Click Me" & "Secure Notes" (mobile) (NahamCon CTF)
- Heap BINARY EXPLOITATION w/ Matt E!

Pentest writeups

- Breaking out of Windows Kiosks using only Microsoft Edge
- Reversing an Android App to Code Execution on their Server
- DOMAIN ADMIN Compromise in 3 HOURS

Responsible(ish) disclosure writeups

- 2nd RCE and XSS in Apache Struts 2.5.0 – 2.5.29 #Web
- Android apps with millions of downloads exposed to high-severity vulnerabilities #Android
- Hijacking webcams with Screencastify #BrowserExtension #Web
- Mass Account Takeover In The Yunmai Smart Scale API
- CVE-2022-25237: Bonitasoft Authorization Bypass and RCE #Web #CodeReview

Known vulnerabilities

- Analysis of CVE-2022-22978 – Authorization Bypass in Spring Security RegexRequestMatcher
- A New Exploit Method for CVE-2021-3560 PolicyKit Linux Privilege Escalation

Bug bounty writeups

- Zoom: Remote Code Execution with XMPP Stanza Smuggling (Zoom)
- Stored XSS in Notes (with CSP bypass for gitlab.com) (GitLab, $13,950)
- CVE-2022-21404: Another Story Of Developers Fixing Vulnerabilities Unknowingly Because Of CodeQL (Oracle)

See more writeups on The list of bug bounty writeups.

Tools

- goodfaith: Stay within program scope
- IISRecon: IIS shortname scanner (uses *ffuf*, *sns* and *arjun*)
- PyHackTheBox: Unofficial Python library to interact with the Hack The Box API
- UPnProxyChain & Intro: A tool to create a SOCKS proxy server out of UPnProxy vulnerable device(s)
- Max: Maximizing BloodHound with a simple suite of tools

Tips & Tweets

- A fascinating file upload trick
- Bruteforcing directories and parameters at the same time
- Internal assets = sensitive
- @Melotover's last P1 submission
- Using URL hash fragments for Reflected XSS without user interaction
- How to access photos, videos, and audio on mobile using HTML file inputs
- @tabaahi_'s life changing bug bounties

Misc. pentest & bug bounty resources

- Breaking Into Cloud Security
- Practical Web Application Security & Testing (New TCM Security Academy course, $29.99)
- zap-scripts: OWASP ZAP Scripts for finding CVEs and Secrets

- UNREDACTED Magazine – Issue 002

Articles

- Kubernetes Privilege Escalation: Excessive Permissions in Popular Platforms
- Customising Blacklist3r for OWIN OAuth Access Tokens
- Exploiting Leaked Handles for LPE & LHF – Leaked Handles Finder
- Spoofing Microsoft 365 Like It's 1995

Challenges

- Intigriti's May XSS challenge By @PiyushThePal
- NorthSec CTF Mini-Challenge
- CyberHeroes (TryHackMe free room)

Bug bounty & Pentest news

- Cybersecurity
  - Security 'researcher' hits back against claims of malicious CTX file uploads
  - npm security update: Attack campaign using stolen OAuth tokens
- Tool updates
  - Blackbox Protobuf v1.0.0
  - AWS support added to Axiom (dev branch)
  - Welcome to the next generation of ngrok

Non technical

- Learnings from 5 years of tech startup code audits
- Preventing burnout: A manager's toolkit