Bug Bytes #141 – Sesh Gremlin attack, RCE via password field & Pwning XMLSec for info disclosure and bounties

BY ANNA HAMMOND · OCTOBER 6, 2021 · 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 September 27 to October 4.

Intigriti news

Always wanted to be part of an @intigriti live hacking event? Now is your chance!

Everybody can win a 40€ swag voucher (King of the Hill 102021)

Our favorite 5 hacking items

1. Video of the week

Bug Bounty | $2000 for SSRF bypass using DNS rebinding & Lab

If you want to practice SSRF or DNS rebinding attacks, this is a great resource. "Leet Cipher" shares details of an SSRF bypass via DNS rebinding found in a bug bounty program. The lab provided reproduces the issue and is easy to deploy using Docker. Make sure to try first before watching the solution!

2. Writeups of the week

Ping'ing XMLSec
Cisco Hyperflex: How We Got RCE Through Login Form and Other Findings

© Intigriti

The first writeup is about an ingenious attack chain involving XSLT and XXE that @_tint0 discovered in PingFederate. Pwning this popular SSO product led to critical information disclosure bugs on many programs and bounties from Netflix, Paypal, Ping, etc.

The second writeup by @Ankorik and @__mn1__ relates (among other vulnerabilities) an interesting RCE via password field in Cisco HyperFlex.

3. Tip of the week

"Sesh Gremlin" attack

@SlandailLtd shared an interesting excerpt from a pentest report on what they call a "Sesh Gremlin" attack. The idea is to keep an eye on all endpoints that return a session cookie, then re-use each cookie collected to access authenticated areas.

4. Resource of the week

Burp Suite documentation

The official Burp documentation was recently updated and is worth the detour. It includes extensive details on generic Burp usage, all the features including advanced ones you may not know about, how to use the tool for penetration testing or mobile testing, and more.

5. Conference of the week

BSides Berlin 2021

This conference includes many interesting talks on all kinds of topics such as attacking cookie-based authentication or webinar platforms. I especially recommend the keynote by @niemand_sec. He shares some bug examples and the approach/mindset used to find them, the types of questions he asks himself when doing research or when reading writeups.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- How to get Hacked by making random requests? | SSRF
- Intent Redirection (Access to Protected Components) | Android Pentesting
- HTB Stories 3 – 0xdf – Creating HTB Machines
- LiveOverflow's bug bounty playlist

© Intigriti

Podcasts

- Accidentally finding a $50,000 vulnerability – Augusto Zanellato – Bug Bounty Reports Discussed #2
- Day[0]: Gatekeeper Bypass, Opera RCE, and Prototype Pollution [Bounty Hunting Podcast]
- Day[0]: Kernel UAFs and a Parallels VM Escape [Binary Exploitation Podcast]

Webinars

- BHIS | Getting Started in Covert .NET Tradecraft for Post-Exploitation – Kyle Avery
- Windows Command Line & Intro to PowerShell

Conferences

- BSides Singapore Conference 2021

Slides & Workshop material

- VolgaCTF 2021, especially:
  - New ways to alert: prototype pollution
  - Bypass CSP? No problem

Tutorials

- Improper Spring @Query Usage Allows N1QL Injection
- CRLFuzz – Hacker Tools: Injecting CRLF for bounties & Video
- Information Gathering&scanning for sensitive information[Reloaded]
- How to get started Hacking WordPress Plugins
- iOS certificate pinning bypass (Unc0ver + AltStore + Frida)
- An Intro to Fuzzing (AKA Fuzz Testing)

Writeups

Challenge writeups

- How To Circumvent SSRF Protection!
- CSRF – Lab #5 CSRF where token is tied to non-session cookie
- Can't Contain Poop — Container Security CTF
- Google's Beginner Quest 2021 – all tasks solved recording

© Intigriti

Pentest writeups

- Hello Neighbor

Responsible(ish) disclosure writeups

- Chasing a Dream :: Pre-authenticated Remote Code Execution in Dedecms #Web #CodeReview
- Heap-based Buffer Overflow in vim/vim #Linux #MemoryCorruption
- The fugitive in Java: Escaping to Java to escape the Chrome sandbox #MemoryCorruption #Browser
- Breaking Custom Cursor to p0wn the web #Web #BrowserExtension

0-day & N-day vulnerabilities

- CVE-2021-41773: Path Traversal Zero-Day in Apache HTTP Server Exploited
- Python & PowerShell PoCs for the won't fix Azure AD bruteforce technique that evades logging
- Chrome in-the-wild bug analysis: CVE-2021-30632

Bug bounty writeups

- CVE-2021-26084 (Atlassian)
- Expect The Unexpected: Discovering fresh ZeroDay for Bounty
- Multiple bugs allowed malicious Android Applications to takeover Facebook/Workplace accounts (Facebook, $10,000)
- The Discovery Of Gatekeeper Bypass CVE-2021-1810 & Analysis Of CVE-2021-1810 Gatekeeper Bypass (Apple)
- Denial of Service via Hyperlinks in Posts (Slack, $1,500)
- HTTP Request Smuggling on api.flocktory.com Leads to XSS on Customer Sites (QIWI, $300)
- Telegram bug in terminated sessions (Telegram)

See more writeups on The list of bug bounty writeups.

Tools

- Mariana Trench: Facebook's security focused static analysis tool for Android and Java applications
- Certgraph & Intro: An open source intelligence tool to crawl the graph of certificate Alternate Names
- GitOops!: A tool to help attackers and defenders identify lateral movement and privilege escalation paths in GitHub organizations by abusing CI/CD pipelines and GitHub access controls (Inspired from Bloodhound and Cartography)
- interactsh-web: Web Client for Interactsh

© Intigriti

- Gowap: Wappalyzer implementation in Go
- DonPAPI: Dumping DPAPI credz remotely
- Weggli & Difference with CodeQL: A fast and robust semantic search tool for C and C++ codebases. It is designed to help security researchers identify interesting functionality in large codebases

Tips & Tweets

- How @putersarehard got 3rd spot in the SecurityTrails ReconMaster contest
- Endpoint-based CSRF tokens
- Bookmarklets for quick Base64/URL encoding and decoding
- Combine reflected HTTP headers with XSS to bypass (HTTPOnly) cookie flags

Misc. pentest & bug bounty resources

- SSRF-Testing
- Deserialization on Rails (in Japanese)
- nuclei-templates directory
- AEM-List
- Phrack #70

Challenges

- HTB Starting Point (Complete free machines for a chance to win an annual VIP+ subscription)
- HackBack 2021: The Future of Cyber Operations (October 14-15)
- #RedTeamFive Open Invitational CTF Details (November 5-7)
- New Hacker101 CTF level by @adamtlangley (focused on content discovery)
- GOAD (Game Of Active Directory)

Articles

- 10 Types of Web Vulnerabilities that are Often Missed
- Automated Cloud Based Recon
- How malware gets into the App Store and why Apple can't stop that
- Revisiting Lambda Persistence

© Intigriti

Bug bounty & Pentest news

- Bug bounty
  - Google: Introducing the Secure Open Source Pilot Program
- Cybersecurity
  - Get Burp Suite Certified for free (before December 15)
  - Understanding How Facebook Disappeared from the Internet
  - What does the future hold for browser security? Check out the latest features destined for mobile and desktop
- Upcoming events
  - Hacktoberfest 2021 (Participating security-related projects include PayloadsAllTheThings, Subfinder, reconFTW, OWASP Amass / MSTG / WSTG...)
  - Your Personal Brand Speaks Louder than Your CV! (October 6)
- Tool updates
  - interactsh v0.0.5
  - OWASP Amass v3.14.0
  - jwt-hack v1.1.0
  - GTFOBLookup (Added support for WADComs)

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

© Intigriti