Bug Bytes #139 – OMIGOD, Code review guides & A bug hunter's five year journey

BY ANNA HAMMOND · SEPTEMBER 22, 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 13 to 20.

Our favorite 5 hacking items

1. Conferences of the week

HacktivityCon2021 – Red Team Village
Shubham Shah – Hacking on Bug Bounties for Five Years (part of CrikeyCon 7 (2021))

H@cktivitycon was this weekend and featured a lot of amazing talks as expected. The main stage videos haven't made it to Youtube yet but there is enough to keep anyone busy for a while with the Red Team Village talks.
One talk that I find particularly interesting is a hands-on CodeQL workshop by @pwntester. Given how often he finds and publishes RCEs and critical bugs, it is a good opportunity to learn about code review and CodeQL from him.

Another excellent talk is @infosec_au sharing his five-year bug bounty journey. It is full of insights, bug examples and lessons for new bug hunters.

2. Writeups of the week

NSA Meeting Proposal for ProxyShell
PowerShell script, Unicode quotes and – a story of uncommon command injection

@irsdl explored combining the recent Exchange vulnerabilities named NSA Meeting and ProxyShell for maximum impact. Though he didn't publish the fully working exploit, the writeup includes a lot of juicy details on debugging Exchange, WAF bypass and bypassing limitations related to the 'Content-Type' header.

Another really good writeup is about an unusual RCE in ManageEngine ADSelfService Plus found by Krzysztof Andrusiak and Marcin Ogorzelski. It involves PowerShell script injection caused by Unicode characters not being properly sanitized.

3. Tutorials of the week

Beginners Guide to 0day/CVE AppSec Research
Vulnerability Digging With CodeQL

These are great guides to learn about source code review. One is @0xBoku's methodology for choosing a target app and discovering 0-days/CVEs. The other shows how @mtimo44 got his first CodeQL bounty by creating a query for CVE-2016-3427 (a Java JMX deserialization).

4. Vulnerability of the week

OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers

Wiz researchers discovered four bugs in OMI, a software agent used by many Azure services. Three are privilege escalations and one is an unauthenticated RCE where you get root just by removing the Authentication header. So critical yet so easy to exploit!

If you want to practice this, there is a free BugHuntrIO lab, or you can play with OMI locally like IppSec did.

In terms of public exploits, you can use a Nuclei template or this Python PoC.

Lastly if you need to advise defenders, Microsoft published this additional guidance and OMIcheck, a tool to detect vulnerable OMI installations.

5. Tools of the week

Haptyc
Trufflehog Chrome Extension & Intro

These tools are both very useful for Web app testers. Haptyc is a Python library by @defparam that adds support for payload positions and attack types (Sniper/Clusterbomb/Batteringram/Pitchfork) to Turbo Intruder. And @trufflesec's TruffleHog Chrome extension detects leaked API keys and other sensitives files in JavaScript code.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Pentester Diaries Ep8: Android Pentesting
- $4,211,006 for XSS
- Your "Secret" Folders Aren't Secret
- Post Exploitation – Transferring Files To Windows Targets
- SecuriTEA & Crumpets – Episode 12 – Ksenia Peguero

Podcasts

- Absolute AppSec Ep. #147 – James Kettle (@albinowax), Security Research
- A Flickr CSRF, GitLab, & OMIGOD, Azure again?
- NETGEAR smart switches, SpookJS, & Parallels Desktop [Binary Exploitation

Webinars

- [SecWed] Unusual Applications of OpenAI in Cybersecurity + How to get into CTFs & Accompanying blog post
- SiegeCast "COBALT STRIKE BASICS" with Tim Medin and Joe Vest

Slides & Workshop material

- An Attacker's Approach to Pentesting IBM Cloud – fwd:cloudsec 2021

Tutorials

Medium to advanced

- Cache-Control Recommendations
- ; echo "Shell Injection"
- Exploiting Jinja SSTI with limited payload size.
- Account Persistence – Certificates & PetitPotam – NTLM Relay to AD CS

Beginners corner

- Fuzzing WebSocket messages on Burpsuite
- Thinking About Simple SQL Injections

Writeups

Challenge writeups

- HackTheBox – Sink
- XSS to RCE? CrossFit by Hack The Box
- H@cktivityCon walkthroughs: Bumblebee, Race Car, Unpugify,Titanic & Go Blog
- The hardest PHP challenge ever? Race To Win – Typhooncon CTF – Web
- CSRF – Lab #3 CSRF where token validation depends on token being present

Pentest writeups

- Discovering and Exploiting Multiple Vulnerabilities in Avaya Aura #Web

Responsible(ish) disclosure writeups

- Apache Dubbo: All roads lead to RCE
- All Your (d)Base Are Belong To Us, Part 1: Code Execution in Apache OpenOffice (CVE-2021–33035) #MemoryCorruption
- SSD Advisory – macOS Finder RCE #MacOS #RCE
- Nuclei v2.5.2 – First Security Release
- Unauthenticated Remote Code Execution in Motorola Baby Monitors #IoT
- Pardus 21 Linux Distro – Remote Code Execution 0day 2021 #Linux

0-day & N-day vulnerabilities

- Technical details on ManageEngine ADSelfService Plus CVE-2021-40539
- Analyzing The ForcedEntry Zero-Click iPhone Exploit Used By Pegasus & FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild

Bug bounty writeups

- A Facebook bug that exposes email/phone number to your friends (Facebook, $19,250)
- 5 RCEs in npm for $15,000 (GitHub, $15,000)
- Mistuned Part 1: Client-side XSS to Calculator and More, Mistuned Part 2: Butterfly Effect & Part 3
- This is why you shouldn't trust your Federated Identity Provider ($1,500)
- From phpinfo page to many P1 bugs and RCE. [Symfony]
- Stored XSS in main page of a project caused by arbitrary script payload in group "Default initial branch name" (GitLab, $3,000)
- Escalating Azure Privileges with the Log Analytics Contributor Role (Microsoft)

See more writeups on The list of bug bounty writeups.

Tools

- rpckiller: xmlrpc.php pingback checker
- cswsh-scanner & Usage tip: Scanner for Cross-Site WebSocket Hijacking
- FAV/E: Search for vulnerabilities and exposures while filtering based on age, keywords, and other parameters

- CVESearch: Query various sources for CVE proof-of-concepts

Tips & Tweets

- How to dump information on all Drupal installed modules
- Network misconfigurations on internally used domains
- Using htmlq as a zero false-positive HTML Injection finder
- iOS 15 launched today with official support for Safari extensions
- TIL you can echo lists into nmap

Misc. pentest & bug bounty resources

- Dorks collections list
- @0xAwali's tips for bypassing 403 and 401 pages
- Microsoft Azure & O365 CLI Tool Cheatsheet, Pentest Notes: Google Cloud Edition, Useful Pentest Notes: Cloud Edition, Active Directory penetration testing cheatsheet & Part 2
- AD Pentest mindmap
- CryptoHack courses
- Subnet Calculator by @JackRhysider

Challenges

- WebSploit Labs
- OWASP VulnerableApp
- hacksec.in

Articles

- Hunting nonce-based CSP bypasses with dynamic analysis
- If You Copied Any Of These Popular Stackoverflow Encryption Code Snippets, Then You Coded It Wrong
- Cracking Radmin Server 3 Passwords
- Security Implication of Root principal in AWS
- Building a C2 Implant in Nim – Considerations and Lessons Learned

Bug bounty & Pentest news

- Bug bounty
  - Researcher discloses iPhone lock screen bypass on iOS 15 launch day
- Cybersecurity
  - Google is partnering with Open Source Technology Improvement Fund, Inc to sponsor security reviews of critical open source software.
- MSHTML Zero Day Exploits Used Shared Infrastructure With Ransomware Group
- Tool updates
  - If you run an instance of xsshunter-express, please update ASAP
  - Kali Linux 2021.3 Release (OpenSSL, Kali-Tools, Kali Live VM Support, Kali NetHunter Smartwatch)
  - AutoRecon v2 is officially released

Non technical

- Missing Critical Vulnerabilities Through Narrow Scoping