Bug Bytes #150 – CMS wordlists, Lesser known Python bugs & Containers learning path

BY ANNA HAMMOND · DECEMBER 8, 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 November 29 to December 6.

Intigriti news

Intel chooses Intigriti as its bug bounty vulnerability management platform

Our favorite 5 hacking items

1. Challenge of the week

Orange Tsai's HITCON CTF 2021 Challenges

@orange_8361 published the code for some HITCON CTF 2021 challenges. I found Metamon-Verse really interesting, but I won't say more to avoid spoiling it.

If you're stuck, here is a writeup for Metamon-Verse and a hint for W3rmup-PHP.

2. Writeups of the week

SSRF vulnerability in AppSheet – Google VRP (Google, $6,267.4)
AWS SageMaker Jupyter Notebook Instance Takeover (Amazon)

@david_nechuta shared a cool SSRF on Google AppSheet, with an interesting bypass involving HTTP headers.

The other noteworthy writeup is about self-XSS that can be chained with CSRF to completely take over AWS SageMaker Jupyter Notebook instances. The technique is similar to @S1r1u5_'s Cookie Tossing to RCE on Google Cloud JupyterLab .

3. Tutorial of the week

10 Unknown Security Pitfalls for Python

This article is about ten lesser known bad coding practices that SonarSource researchers encounter when doing Python code review assessments.
Before diving into the article, make sure to try solving this code review challenge that is related.

4. Tools of the week

csg ("Credential Storage with Go") & Intro
Proxy Agent & Intro

csg is a Go tool that helps organize and store credentials. Think of it like a password manager in command line, for credentials that you only need temporarily for the duration of a CTF for instance.

Another handy tool is Proxy Agent. If you find yourself often needing to set up Burp on your rooted Android device, it will help speed up the process.

5. Resources of the week

Learning Containers From The Bottom Up: Efficient Learning Path to Grasp Containers Fundamentals
webapp-wordlists & @podalirius_'s Cyber Advent 2021

After years spent studying containers, @iximiuz created a learning path to walk us through this complex topic. Whether you want to hack containers or just use them in your day-to-day life, check out the first resource. It is amazing, both informative and dealing with advanced topics yet beginner friendly.

@podalirius_ has been posting one new article or tool everyday, and will continue doing so until Christmas.
One of them is webapp-wordlists, a repository of path and directory wordlists for many CMSs. Having this collection of endpoints is valuable for fingerprinting CMSs when testing Web apps.
The Python scripts used to generate the wordlists are also included, so you can tweak them to generate wordlists for any missing CMS.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Authorization vs. Authentication (Google Bug Bounty)
- Why do you Duplicate so much with Bug Bounties?
- $28k IDOR that broke Apple Shortcuts – Apple bug bounty
- I Hacked Red Bull and All I Got Was This!
- Fuzzing for beginners! FFuF – Hacker Tools
- Back to the Basics of Security Practices
- #MentorshipMondays: Breaking Into Pentesting with @TheCyberMentor & @PhillipWylie & Part 2

Podcasts

- Bypassing MFA, WebCache Poisoning, and AWS SageMaker [Bounty Hunting Podcast]
- Hack'n Speak 0x14 – Podalirius | Retour sur LDAPMonitor, pydsinternals et le rebuild d'un AS400 (in French)

Conferences

- The Infinite Game of Vulnerability Research (and other No Hat 2021 talks)
- BSides Calgary 2021
- Black Hat USA 2021 – Many new videos added, including:
  - Timeless Timing Attacks
  - Diving in to Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer
  - Internal Affairs: Hacking File System Access from the Web
  - MFA-ing the Un-MFA-ble: Protecting Auth Systems' Core Secrets
  - Certified Pre-Owned: Abusing Active Directory Certificate Services
  - ALPACA: Application Layer Protocol Confusion – Analyzing and Mitigating Cracks in TLS Authentication
  - ProxyLogon is Just the Tip of the Iceberg: A New Attack Surface on Microsoft Exchange Server!

Slides & Workshop material

- Key Details Phrasing
- GreHack workshops: Finding security vulnerabilities with CodeQL

Tutorials

- Android APK security analyzer
- Binary Reversing Methodologies
- Hunting for Persistence in Linux (Part 1): Auditd, Sysmon, Osquery, and Webshells & Hunting for Persistence in Linux (Part 2): Account Creation and Manipulation
- Operating with AutoIt & OffensiveAutoIt

Writeups

Challenge writeups

- CSAW Finals – Grande
- HackTheBox – Pikaboo
- Craft Walkthrough with S1REN
- ZipSlip w/ TAR & Server-Side Template Injection – HackTheBox University CTF – "Slippy"
- CyberSecLabs – Spray – Active Directory [Walkthrough]

Responsible(ish) disclosure writeups

- Grafana path traversal (CVE-2021-43798), PoC by @jas502n, Nuclei template & The vulnerable function
- uBlock, I exfiltrate: exploiting ad blockers with CSS
- Arbitrary package tampering in Deno registry + Code Injection in encoding/yaml #CodeReview
- F-Secure discovers vulnerabilities affecting over 150 HP printer models #Printer
- How PwC found a zero-day vulnerability during a penetration test for a client (CVE-2021-21234) & CVE-2021-21234 Spring Boot Actuator Logview Directory Traversal
- CVE-2021-21980: Unauthenticated AMF deserialization in VMware vCenter Server
- Notes and PoC for ManageEngine ADManager Plus CVE-2021-37928

Bug bounty writeups

- NodeBB 1.18.4 – Remote Code Execution With One Shot (NodeBB, $1,536)
- Write Up – XSS Stored In files.slack.com Via XML/SVG File (iOS) – $1,000 USD (Slack, $1,000)
- Easy SQLi in Amazon subsidiary using Sqlmap (Amazon, $1,500)
- Full read SSRF in www.evernote.com that can leak aws metadata and local file inclusion (Evernote, $5,000)

- Windows 10 RCE: The exploit is in the link (Microsoft, $5,000)
- This shouldn't have happened: A vulnerability postmortem (Mozilla)

See more writeups on The list of bug bounty writeups.

Tools

- Eval Villain & Intro: ZAP / Firefox add-on to inspect arguments to arbitrary native JavaScript functions (similar use cases to DOM Invader in Burp but with more configuration options)
- pip-audit & Intro: A tool for scanning Python environments for known vulnerabilities
- Cracken: A fast password wordlist generator, Smartlist creation and password hybrid-mask analysis tool written in Rust
- ipsourcebypass: Python script that checks for IP source restrictions bypass using HTTP headers

Tips & Tweets

- Response manipulation to bypass paywalls
- Something to try when you find an external SSRF and can't hit internal URLs
- Script to fingerprint Script Gadgets to use to exploit Prototype Pollution
- How @GodfatherOrwa finds 90% of their SQL injection vulnerabilities
- How to get #burpsuitecertified on your first try
- GitLab default login credentials

Misc. pentest & bug bounty resources

- New Web Security Academy topic: File upload vulnerabilities
- Subdomain Enumeration Guide 2021 (new update)
- A First Introduction to System Exploitation (With Georgia Tech's "pwnable" challenges)
- awesome-kubernetes-security

Challenges

- HTB Starting Point Machines are free until December 31
- Can you create the shortest XSS vector that triggers in all contexts?
- XMGoat & Intro: Terraform templates that build insecure Azure environments

Articles

- Azure Privilege Escalation via Azure API Permissions Abuse, Recording of the talk & Slides
- Compromising the email supply chain of 190 Australian organisations through a single IT Managed Service Provider
- Lateral Movement With Managed Identities Of Azure Virtual Machines
- Gaining Persistency on Vulnerable Lambdas & Splash

Bug bounty & Pentest news

- Bug bounty
  - Verizon Information Disclosure + Race condition
- Upcoming events
  - 2021 SANS Holiday Hack Challenge & KringleCon (December 10)
  - Introduction to Azure Penetration Testing (December 18)
  - BountyConEDU 2022 (Spain) (deadline to apply is December 31)
- Tool updates
  - Troy Hunt is offering 50% Off on 1Password Families
  - Burp Professional / Community 2021.10.3 & The mystery of the missing Mac release
  - Nuclei v2.5.4
  - httpx v1.1.4

Non technical

- Dive into the world of vulnerability research