Bug Bytes #138 – Web app security roadmap, OWASP Top 10 & Request smuggling via integer overflow

BY ANNA HAMMOND · SEPTEMBER 15, 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 6 to 13.

Intigriti news

Atos and Intigriti launch new integrated Bug Bounty service

Our favorite 5 hacking items

1. Resource of the week

Web Application Security Roadmap

The number of resources for hackers and skills to learn can be intimidating. This roadmap created by @HolyBugx compiles interesting resources and books for all levels. Most importantly, they are divided into tiers which helps choose what to focus on without getting overwhelmed.

2. Writeups of the week

Critical Vulnerability in HAProxy (CVE-2021-40346): Integer Overflow Enables HTTP Smuggling
Hacking CloudKit – How I accidentally deleted your Apple Shortcuts (Apple, $64,000)
Finding Azurescape – Cross-Account Container Takeover in Azure Container Instances (Microsoft)
GitHub Actions check-spelling community workflow – GITHUB_TOKEN leakage via advice.txt symlink (GitHub)

The first writeup is about an integer overflow in HAProxy that was exploited to enable request smuggling. An interesting crossover of different types of vulnerabilities.

The second writeup is @fransrosen's story of hacking Apple, which clarifies why Apple shortcuts broke back in March...

Next is a writeup on Azure Container Instances. @yuval_avrahami found a cross-account container takeover that could've allowed a malicious Azure user to attack other customers.

Another interesting finding is a vulnerability in GitHub Actions. @justinsteven found a way to leak GITHUB_TOKEN API keys and introduce malicious code to Microsoft, NASA, PowerDNS and Jekyll repos.

3. Vulnerability of the week

CVE-2021-40444: Microsoft MSHTML Remote Code Execution Vulnerability

CVE-2021-40444 is an RCE in Microsoft MSHTML (the Internet Explorer browser engine). It is triggered simply by opening a malicious Microsoft Office document (without macros) and was discovered as a a zero-day actually being exploited in the wild.
Here are a few resources if you want to know more:

- @RET2_pwn's Analysis/Exploit
- @lasq88's analysis in video
- @lockedbyte's malicious docx generator

4. Non technical item of the week

Obsidian, Taming A Collective Consciousness

This is an excellent post on the knowledge management system used by TrustedSec's red team. The article details how they leverage Obsidian and the Zettelkasten method for efficient note-taking as a team.

5. Article of the week

Introduction to OWASP Top 10 2021 & Intigriti's insights on it

The draft OWASP Top 10 2021 is out. Among other changes, injection lost its first place for the first time since 2007 and SSRF made it to the list. Also, some vulnerabilities were included in broader categories, for instance XSS is now in the "Injection" category, XXE in "Security Misconfiguration", etc.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- 0day Shares His Journey on Becoming #1 on TryHackMe, Learning How to Hack, Resources and more!
- LiveStream – Avinash Jain – Journey To Security Engineer @Microsoft
- "Automation Is Going To Play Huge Role" with @kapytein (Hacker Heroes #13)
- How to search for XSS (with blacklisted HTML tags)
- PowerShell for Pentesters
- How to learn anything in Computer Science or Cybersecurity | Security Simplified
- Talking about File Formats with Ange "Corkami" Albertini

Podcasts

- Radio Hack Ep5: Bug Bounty & Triaging – Ebrahem Hegazy (In Arabic)
- Reused VMWare exploits & Escaping Azure Container Instances [Bug Bounty Podcast]
- The Mēris Botnet – 0-Day Attack on Office Docs, WFH and Security, Return of REvil

Webinars

- Docker Hacking
- Hacker School Reboot – insights from leading API hackers [VIDEO]
- BHIS | Getting Started in Blockchain Security and Smart Contract Auditing | Beau Bullock & Slides

Conferences

- Evolution of application Security – Louis Nyffenegger | SecConf 2021
- DEF CON 29 Cloud Village & IoT Village

Tutorials

Medium to advanced

- ADExplorer Exporting Quick Tip
- Offensive WMI – The Basics (Part 1), Exploring Namespaces, Classes & Methods (Part 2) & Interacting with Windows Registry (Part 3)

- Active Directory virtualization safeguard deactivation

Beginners corner

- Dalfox – Hacker Tools: XSS Scanning Made Easy
- How malicious applications abuse Android permissions
- Metasploit for Pentester: Clipboard

Writeups

Challenge writeups

- Obfuscated Password Manager?! Solution to September '21 XSS Challenge
- CSRF – Lab #2 CSRF where token validation depends on request method
- Cyber Mentoring Monday (8/30/21) – Knife & Bank
- Entry Level Pentesting Lab Walkthrough

Pentest writeups

- Why are developers so vulnerable to drive-by attacks?
- PKINIT FTW – Chaining Shadow Credentials and ADCS Template Abuse

Responsible(ish) disclosure writeups

- SSD Advisory – NETGEAR D7000 Authentication Bypass #Web
- CVE-2021-3546[78]: Akkadian Console Server Vulnerabilities (FIXED) #Web

Bug bounty writeups

- Spook.js: Attacking Google Chrome's Strict Site Isolation via Speculative Execution and Type Confusion (Google)
- Facebook email disclosure and account takeover (Facebook)
- Bug Bounty Guest Post: Local File Read via Stored XSS in The Opera Browser (Opera, $4,000)
- Bypassing GCP Org Policy with Custom Metadata & GCP AI Notebooks Vulnerability – Remediation (Google, $1,337)

See more writeups on The list of bug bounty writeups.

Tools

- cspp-tools: Client-Side Prototype Pollution Tools

- Apkeep: CLI for downloading APK files from various sources
- Lazydroid: Bash script to facilitate some aspects of an Android application assessment
- gcpHound: A Swiss Army Knife Offensive Toolkit for Google Cloud Platform (GCP)
- htmlq: Like jq, but for HTML
- WWWGrep: A rapid search "grepping" mechanism that examines HTML elements by type

Tips & Tweets

- Leaking source code or auth bypass using alternate data streams
- Client side path traversal
- Api tip for finding new endpoints
- RCE via exposed AEM Groovy console
- Did you know that ssh tries to authenticate with stored keys BEFORE the key specified with -i?

Misc. pentest & bug bounty resources

- Complete Jailbreak Chart
- Awesome Ruby Security & Ruby On Rails Security Guide
- Fresh-Resolvers: List of Hourly Updated Fresh DNS resolvers
- CodePath Web Security Guides
- pwn.college

Challenges

- IAM Vulnerable – An AWS IAM Privilege Escalation Playground & Repo
- Detectify Lisp to HTML Converter

Articles

- Mass assignment and learning new things
- A different way to attack certain reverse proxies
- Introducing Process Hiving & RunPE
- Google Cloud Build — under the hood (Google)

Bug bounty & Pentest news

- Bug bounty
  - Atos and Intigriti launch new integrated Bug Bounty service
- Upcoming events
  - h@cktivitycon 2021 (September 18) & H@cktivityCon 2021 CTF (September 16-18)
- Tool updates
  - Hackvector added support for custom tags, local and global variable tags & Here's how to use them
  - Kali Linux 2021.3 Release (OpenSSL, Kali-Tools, Kali Live VM Support, Kali NetHunter Smartwatch)
  - Frida 15.1 Released ∞
  - dirsearch v0.4.2
  - Nuclei v2.5.1

Non technical

- Top 5 OSINT Sources for Penetration Testing and Bug Bounties
- An analysis on developer-security researcher interactions in the vulnerability disclosure process