Bug Bytes #143 – Building an Apache SSRF exploit, Thesis on HTTP Request Smuggling & Turbo Intruder go brrr

BY ANNA HAMMOND · OCTOBER 20, 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 October 11 to 18.

Intigriti News

How Artificial Intelligence is being used to match researchers with bug bounty programs

Our favorite 5 hacking items

1. Resource of the week

Bachelor's thesis on HTTP Request Smuggling

Mattias Grenfeldt (@mgrenfeldt) and Asta Olofsson published their Bachelor's thesis on HTTP Request Smuggling. After it was published, they also discovered a new technique that uses chunk extensions and affected Node.js.
There is a lot to unpack here but if you can't get enough of this vulnerability, they also have a writeup on HRS in Gunicorn.

2. Writeups of the week

Bypassing required reviews using GitHub Actions (GitHub)
Stored XSS in markdown via the DesignReferenceFilter (GitLab, $16,000)

@omer_gil discovered a creative way to bypass required reviews on GitHub. Users with "write" permissions on a repo could create a GitHub Action that approves their pull request, allowing them to bypass required reviews.

The second writeup is an interesting bug chain on GitLab. @wcbowling found a stored XSS with CSP bypass that could ne escalated to Arbitrary file read / SSRF.

3. Vulnerability of the week

Building a POC for CVE-2021-40438, one-liner PoC & Nuclei template

CVE-2021-40438 is an SSRF in Apache HTTP Server 2.4.48 and earlier. It's was discovered by the Apache HTTP security team and patched back in September, but there wasn't any public proof of concept until now.
@Firzen14 details in an excellent article how they reverse engineered the patch and constructed the exploit.

4. Tip of the week

How to make Turbo Intruder attacks go as fast as possible

PortSwigger shared tips for making Turbo Intruder go as fast as possible. These can make all the difference when you are testing a vulnerability and speed is an important factor (e.g. race conditions).

5. Tutorial of the week

How to win at CORS

The first step to hack anything is understanding how it works, right? If you are interested in client-side vulnerabilities or browser security, you might enjoy this introduction to CORS. It is full of information on this fundamental Web mechanism, its history, how it works, with a playground for practice.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- How to Reset Forgotten Password on Kali Linux
- Introduction to Bash Programming (GIVEAWAY)
- $2,500 Leaking parts of private Hackerone reports – timeless cross-site leaks
- How to conduct a basic security code review | Security Simplified

Webinars

- How to Analyze Code for Vulnerabilities using Joern
- A week in the life of a pentester

Conferences

- DC9111 0x04 SAFE MODE
- fwd:cloudsec
- BruCON 0x0D

Tutorials

- Azure Privilege Escalation via Service Principal Abuse
- Creating A Malicious Azure Ad OAuth2 Application
- Creating (almost) perfect Hackintosh VM
- 0-Day Hunting (Chaining Bugs/Methodology)
- Resource Based Constrained Delegation

Writeups

Challenge writeups

- PBCTF 2021 – RCE 0-Day in Goahead Webserver
- InsecureShop Write-up, all vulnerabilities explained
- Solstice VM – Walkthrough with S1REN.
- CSRF – Lab #7 CSRF where Referer validation depends on header being present
- How To Search For CSRF!

Pentest writeups

- ICMP Tunneling

Responsible(ish) disclosure writeups

- GHSL-2021-1012: Poor random number generation in keypair – CVE-2021-41117 #Crypto #CodeReview
- Multiple Vulnerabilities In WP Fastest Cache Plugin #Web
- Check Point Research Prevents Theft of Crypto Wallets on OpenSea, the World's Largest NFT Marketplace #Web #Ethereum

0-day & N-day vulnerabilities

- CVE-2021-20034: Rapid7 analysis

Bug bounty writeups

- Abusing Slack's file-sharing functionality to de-anonymise fellow workspace members (Slack)
- Write Up – Google VRP N/A: Arbitrary Local File Read (Macos) Via <a> Tag And Null Byte (%00) In Google Earth Pro Desktop App (Google)
- Auth Bypass in Google Assistant (Google, $8,133.70)
- Stored XSS in Mermaid when viewing Markdown files (GitLab, $3,000)

See more writeups on The list of bug bounty writeups.

Tools

- RIO & Guide: A handy plugin for copying requests/responses or generating reports directly from Burp
- gh-dork: Github dorking tool
- Snowcat & Intro: A Go tool to audit the Istio Service Mesh
- Gorgo: A multi-threaded password sprayer based on Medusa, built for distributed spraying
- LDAP Monitor: Monitor creation, deletion and changes to LDAP objects live during your pentest or system administration
- SAML2Spray: Python Script for SAML2 Authentication Passwordspray

Tips & Tweets

- Cloudflare bypass for RCE via Unrestricted file upload & Stored XSS
- DevTools command for taking screenshots
- Save/load Burp Match/Replace rules as project options

- If you find a S3 subdomain takeover, you need to set up the S3 bucket in the correct region
- Interactsh server can be used to query cloud metadata services

Misc. pentest & bug bounty resources

- Bug bounty changelogs
- container-security.site
- Mobile Application Penetration Testing Cheat Sheet
- OffensiveRust
- Learn Burp Suite Plugin Development from Scratch. ($5 pre-launch, $8 post-launch)

Challenges

- Totally Insecure Web Application Project (TIWAP)

Articles

- AWS WAF's Dangerous Defaults
- Don't let Prometheus Steal your Fire
- Mozilla: Implementing form filling and accessibility in the Firefox PDF viewer
- Creating a Basic Python Reverse Shell Listener
- Bugs in our Pockets: The Risks of Client-Side Scanning

Bug bounty & Pentest news

- Cybersecurity
  - Windows 10, iOS 15, Ubuntu, Chrome fall at China's Tianfu hacking contest
  - Missouri governor criticized for confusing vulnerability disclosure with criminal hacking
- Upcoming events
  - Ekoparty 2021 (November 2-6)
- Tool updates
  - Backslash Powered Scanner will now recognise and flag iterable inputs for easier IDOR testing
  - L0phtCrack 7.2.0 has been released as an open source project
  - Cobalt Strike Sleep Python Bridge

Non technical

- Bug bounty hunter to working at Microsoft

- PROMPT#: Choose Wisely

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com