Bug Bytes #147 – From won't fix to $100k+ bounties, HTTP Header Smuggling & ChaosDB

BY ANNA HAMMOND · NOVEMBER 17, 2021 · LAST UPDATED ON AUGUST 8, 2026

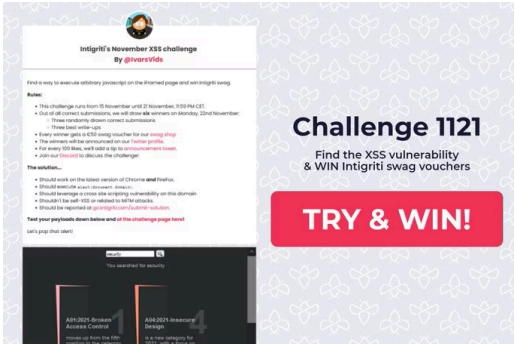
Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-147-from-wont-fix-to-100k-bounties-http-header-smuggling-chaosdb

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 8 to 15.

Intigriti news



Intigriti's November XSS challenge By @IvarsVids

Our favorite 5 hacking items

1. Article of the week

Practical HTTP Header Smuggling: Sneaking Past Reverse Proxies to Attack AWS and Beyond & Slides + Whitepaper

Daniel Thatcher presented a new technique called "HTTP header smuggling" at Black Hat Europe 2021. Basically, it is about attacking chains of servers and smuggling headers that will be hidden to some servers in the chain and visible to others.
This can lead to HTTP request smuggling, cache poisoning or IP restriction bypass (by leveraging a weakness in the AWS API Gateway).
As part of this research, Daniel released a Param Miner fork. However note that it was merged into the master branch.

2. Whitepaper of the week

T-Reqs: HTTP Request Smuggling with Differential Fuzzing & T-Reqs HTTP Fuzzer

This is a different take on HTTP Request Smuggling. It focuses on creating a generic framework and infrastructure to fully automate detecting HRS at scale using grammar-based fuzzing.
This is a neat paper/research that explores new areas, for instance finding web server and proxy pairs that are vulnerable even though each one individually is not.

3. Writeups of the week

ChaosDB Explained: Azure's Cosmos DB Vulnerability Walkthrough (Microsoft, $40,000)
Exploiting CSP in Webkit to Break Authentication & Authorization (Apple, $100k+)
Multiple Concrete CMS Vulnerabilities (Part1 – RCE)

Remember ChaosDB from a few weeks ago? It allowed @sagitz_ and @nirohfeld to gain unrestricted access to the databases of Microsoft Azure customers. The researchers finally released technical details on the chain of misconfigurations that made this impressive attack possible.

The second writeup is about a vulnerability in Safari's browser engine, Webkit. It did not adhere to the W3C specification when handling CSP violation reports, but Apple deemed this not severe enough to fix quickly. So, @sachinnthakuri and @1lastBr3ath found a way to use this and exploit multiple OAuth/SSO implementations, earning more than $100k bounties. Not bad for a *won't fix quickly* bug!

In the third writeup, FORTBRIDGE researchers combine file upload with two race conditions to get RCE. This is really worth reading, both creative and very informative.

4. Tool of the week

bugbounty-openvpn-socks

Let's say you need to use several VPNs simultaneously (e.g. corporate VPN + training platform VPN + bug bounty platform VPN).
What bugbounty-openvpn-socks allows you to do is expose each VPN via a local SOCKS proxy. So, when you run any tool, you can choose which VPN it should go through (e.g. `curl -x socks5://localhost:1000`).
This is a very useful tool by @honoki, that also integrates well with BBRF if you use it.

5. Resources of the week

Android App Hacking Workshop
@0xAwali's methodology for testing Secondary Contexts

The first resource is a slide deck by Google on Android app hacking for bug hunters. It is accompanied with two APKs that include challenges/flags, and a PDF for solutions.
If you want to dive into Android app security and like hands-on learning, this is fantastic. It is beginner friendly but also covers advanced topics, not just the basics.

Another amazing resource is @0xAwali's compilation of 110+ things to try when hacking secondary contexts. So many good tips, each one with its reference(s) if you want to find out more about it.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- BountyTraining [2] – Getting a feel for your target with BugBountyHunter
- HTTP/2 request smuggling (explained using beer)
- The MOST IMPORTANT advice for young hackers
- Scanning for hardcoded secrets in source code | Security Simplified
- SSD's CVE Deep Dive – IP-Board Stored XSS to RCE Chain
- #MentorshipMondays | Featuring @Achillean, Creator of Shodan

Podcasts

- Livestreaming a hacker's mind with Ben Sadeghipour
- Rust in the Web? A Special Guest and some Bad Crypto [Bounty Hunting Podcast]

Conferences

- Staying sane in bug bounties
- Adversary Village – Texas Cyber Summit IV
- ShellCon Livestreams & Program

Slides & Workshop material

- Retrospective (and some new tricks) for cross-site browsing history leaks
- Black Hat Europe 2021, especially:
  - HTTP/2: The Sequel is Always Worse
  - How Your E-book Might Be Reading You: Exploiting EPUB Reading Systems
  - Re-route Your Intent for Privilege Escalation: A Universal Way to Exploit Android PendingIntents in High-profile and System Apps
  - Is This My Domain Controller: A New Class of Active Directory Protocol Injection Attacks
  - Practical Attacks Against Attribute-based Encryption & Blog post

Tutorials

- Windows Security Updates for Hackers
- Attacking SAML implementations & saml-practice

- Uniscan: An RFI, LFI, and RCE Vulnerability Scanner
- Golden Certificate

Writeups

Challenge writeups

- SecurityMB's October 2021 Prototype Pollution Challenge
- CSP Porfavor (bughuntr.io walkthrough)
- How to exploit a blind SSRF?
- HTH 2021 CTF Solves

Responsible(ish) disclosure writeups

- JavaScript type confusion: Bypassed input validation (and how to remediate) #Web
- Laravel 8.x image upload bypass #Web
- Multiple Vulnerabilities in ResourceSpace #Web #CodeReview
- Unboxing BusyBox – 14 new vulnerabilities uncovered by Claroty and JFrog #Linux #MemoryCorruption
- Independently Secure, Together Not So Much – A Story Of 2 WP Plugins #Web #CodeReview

0-day & N-day vulnerabilities

- Zero-Day Disclosure: Palo Alto Networks GlobalProtect VPN CVE-2021-3064

Bug bounty writeups

- Becoming A Super Admin In Someone Elses Gsuite Organization And Taking It Over (Google)
- Write Up – Google VRP Bug Bounty: /etc/environment Local Variables Exfiltrated On Linux Google Earth Pro Desktop App – $1,337 USD (Google, $1,337)
- Pre-Auth POST Based Reflected XSS in Microsoft Exchange (CVE-2021-41349) & Microsoft fixes reflected XSS in Exchange Server (Microsoft)
- Simple SSRF Allows Access To Internal Assets
- From URL dumps digging to IDOR , BAC, Massive Phishing in Udemy (Udemy, $1,300)
- Fix for CVE-2021-22151 (Kibana path traversal issue) can be bypassed on Windows (Elastic, $584)

See more writeups on The list of bug bounty writeups.

Tools

- GrepAddr: Python script that extracts different kinds of addresses (URLs, IPs, e-mail addresses, MAC addresses, etc) from stdin

- lsarelayx: NTLM relaying for Windows made easy
- dnsline: Tool for making it easy to collect dns results from the CLI

Tips & Tweets

- A technique to bypass file signature checks in file uploads
- Lateral SQL Injection Revisited – Exploiting NUMBERs & More whitepapers by the same author
- Search Burp history for JS sinks to find DOM XSS
- Another use-case for Burp Intruder's Grep-Extract
- Pre-auth XXE on software using Apache XML-RPC versions prior to 3.1.3
- Deleted S3 objects with versioning enabled and public access can still be accessed
- SQL injection and XPath injection testing polyglots

Misc. pentest & bug bounty resources

- Pythonizing Nmap
- All about bug bounty
- Useful sed, Simple Awk & Quick Grep
- Example pentest reports (by finalists of the Collegiate Penetration Testing Competition) & CPTC – Better Pentest Reports w/ Examples!

Challenges

- Intigriti's November XSS challenge By @IvarsVids
- "1 Day XSLeak and a trailer for ElectronJS bugs" & Author's writeup
- XSS challenge @itszn13 created for CSAW finals

Articles

- The Invisible JavaScript Backdoor & Smuggling hidden backdoors into JavaScript with homoglyphs and invisible Unicode characters
- The Kerberos Key List Attack: The return of the Read Only Domain Controllers
- CVE-2021-22205: It Was A GitLab Smash (includes a method for fingerprinting GitLab versions by looking at the names of publicly available CSS files)

Bug bounty & Pentest news

- Cybersecurity

    - PortSwigger Black Friday offer: Take the Burp Suite Certified Practitioner exam for $9 and get refunded if you pass before Dec. 15
    - PSA: Apple isn't actually patching all the security holes in older versions of macOS
    - GitHub's commitment to npm ecosystem security
    - HTML smuggling: Fresh attack technique is being used to increasingly target banking sector
- Upcoming events
    - DAMNCON 2021 (November 20)
    - Digital Meetup — "Report Medley — What Makes a Bug Report Great?" (December 8)
- Tool updates
    - gau rewrite + new provider
    - New Release: FullHunt Public API!
    - Hashcat now supports cracking Windows "Hello" PIN/Password authentication

Non technical

- Some Thoughts on Teaching Hacking
- A Cybersecurity Professional's review of the M1 Pro Macbook
- Practical Security Recommendations for Start-ups with Limited Budgets
- Cybersecurity Career Path