Bug Bytes #43 – Abusing HTTP hop-by-hop request headers, The Bug Bounty Podcast by @Regala_ & Live Bug Bounty Recon Session on Verizon Media's Yahoo.com W/ @Securinti

BY INTIGRITI · NOVEMBER 5, 2019 · 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.

This issue covers the week from 25th of October to 1st of November.

Our favorite 5 hacking items

1. Podcast of the week

> "Episode #1 ft. STÖK"

This podcast is made by Fisher and is A-M-A-Z-I-N-G! It makes you feel like you are at a live hacking event, sitting with two seasoned bug bounty hunters discussing all kinds of subjects. The podcast is about how to pronounce CSRF, how @stokfredrik overcame his depression, his research on race condition vulnerabilities and much more.
It is perfect for you when you feel like listening to something relaxing but still informational and related to bug bounties.

2. Writeup of the week

> "Abusing HTTP hop-by-hop request headers"

This is some cool research on hop-by-hop headers. These are headers that are used by proxies and not forwarded to the end server.
@nj_dav discovered a way to abuse them and basically remove other request headers. This can have unexpected results like authentication bypass, Cache poisoning DoS, etc.
The premise is simple to understand, but it would be interesting to practice this attack and take the research further by testing on common WAFs.

3. Tips of the week

> "What do you do when doing blackbox web testing that may be obvious to you but not so obvious to other people?"

This is an excellent question asked by @nnwakelam. Doing “not so obvious” tests is the best way to differentiate yourself and avoid duplicates.
The thread includes some very interesting responses, for instance: “Continuously scanning for surface will net you more $$$ in the long run. Looking at an asset once defeats the purpose of a BB, it might as well be a penetration test at that point”.
It’s good to know all these strategies and test them especially if stuck in dup’zone.

4. Video of the week

> “Live Bug Bounty Recon Session on Verizon Media’s Yahoo.com W/ @Securinti”

@securinti is most known for his crazy logic bugs. Since he is killing it at live hacking events and mostly shares unique creative bugs, it is interesting to get to know his mindset and approach. A recommended watch!

5. Conferences of the week

> “– Global AppSec Amsterdam 2019
> – SAINTCON 2019
> – Security@ 2019”

Wow, there are too many interesting talks to list and comment on here.
Let’s just say that Global AppSec and SAINTCON both offer a lot of talks on a large variety of topics and many of them are really captivating.
Security@ has two panels I find interesting for bug bounty hunters: one with bug bounty millionaires @nnwakelam, @thedawgyg and @santi_lopezz99. And another one on hacking the talent gap with @d0nut and @yaworsk.

Other amazing things we stumbled upon this week

Videos

- What to Expect in an Ethical Hacking Interview
- Developing Continuous Recon – !project, Continuous Reconnaissance and Red Teaming, Natlas & Context
- hacker:HUNTER – Wannacry: The Marcus Hutchins Story – All 3 Chapters

Podcasts

- Darknet Diaries EP 50: Operation Glowing Symphony
- Security Now 738 – A Foregone Conclusion
- Risky Business #560 — Facebook sues NSO Group
- InfoSec Career Podcast – Episode 3: Interview with Robin Wood

- Application Security Weekly #82 – Bug Bounties, Pentesting, & Scanners
- Hack Naked News #239
- Paul's Security Weekly – Format String Vulnerabilities

Webinars & Webcasts

- Infosecgirls Session by Andra: Hacking into developers' security consciousness
- Windows User Enumeration, Living off the land (free registration required)
- Life in Docker Containers – The Big Picture & Part II

Conferences

- BSides DC
- MITRE ATT&CKcon 2.0 Day One & Day Two

Slides only

- EYEBALLER
- C# Workshop
- Building a Product Security Team
- KazHackStan Doing The IoT Penetration Testing – Yogesh Ojha
- Let's Make Windows Defender Angry: Antivirus can be an oracle!
- [Attack]tive Directory #ActiveDirectory

Tutorials

Medium to advanced

- Exploiting prototype pollution – RCE in Kibana (CVE-2019-7609)
- Modern Wireless Tradecraft Pt I — Basic Rogue AP Theory — Evil Twin and Karma Attacks
- Persistence – Port Monitors, Netsh Helper DLL & BITS Jobs
- Process Injection – Part III

Beginners corner

- Security testing guide for JSON / REST APIs #1/3
- Race Condition in Web Applications

- Investigating TikTok Accounts
- Hacking JSON Web Tokens (JWTs)
- Practical Approaches for Testing and Breaking JWT Authentication & Reddit discussion
- GitHub Wiki – Access Restriction
- How to Detect CVEs Using Nmap Vulnerability Scan Scripts
- Intro to Software Defined Radio and GSM/LTE

Writeups

Challenge writeups

- How I solved the Unlockme APK Challenge at c0c0n XII (Dome CTF) #Android
- NorzhCTF 2019 & RedHackCTF 2019 – Windows AD – Game of Pwn #ActiveDirectory
- Video walkthrough for Web Security Academy challenges

Pentest writeups

- Exploiting an old noVNC XSS (CVE-2017-18635) in OpenStack
- Jira Username Enumeration (CVE-2019-8446)

Responsible(ish) disclosure writeups

- Abusing the SYLK file format #Phishing
- Vulnerabilities Leading to RCE in LabKey Server Biomedical Research Platform #Web #RCE
- Vulnerability in EU cross-border authentication software (eIDAS Node) #Web
- rConfig v3.9.2 authenticated and unauthenticated RCE (CVE-2019-16663) and (CVE-2019-16662) #Web #CodeReview
- Stealing private keys from a secure file sharing service #Crypto #Web
- Moxa EDR-810 Command Injection and Logs disclosure #Router #Web
- Breaking a smart lock #IoT #Android
- RouterOS: Chain to Root #Router
- WebLogic EJBTaglibDescriptor XXE Vulnerability Analysis(CVE-2019–2888) #Web #CodeReview
- Proof of Concept for “WordPress <=5.2.3: viewing unauthenticated posts” (CVE-2019-17671) #Web #PatchDiffing
- Proof of Concept for “Apache Httpd Limited cross-site scripting in mod_proxy error page (CVE-2019-10092)” #Web #PatchDiffing

- WordPress Visualizer plugin XSS and SSRF #Web #CodeReview
- CVE-2019-1306: Are you my Index? #RCE #Deserialization #.NET
- Drive By RCE Exploit in Pimcore 6.2.0 #Web #CodeReview #RCE

Bug bounty writeups

- Through stopping the redirect in /admin/* the attacker able to bypass Authentication & HowTo
- XSS and CSRF bypass
- Information disclosure
- CVE-2019–3396 found with Google dorks
- Stored XSS on Shopify ($1,000)
- CORS misconfiguration / CSRF on Grammarly ($750)
- Clickjacking on Twitter ($1,120)
- Unrestricted file upload on Central Security Project

Tools

If you don't have time

- BugReplay: Browser extension to record bugs with network traffic and JS console (commercial tool)
- XORpass: Encoder to bypass WAF filters using XOR operations
- Femida: Burp extension for automated blind-xss testing (both passive & active)
- UhOh365: A script that can see if an email address is valid in Office365 (user/email enumeration). This does not perform any login attempts, is unthrottled and is useful for social engineering assessments to find which emails exist and which don't. See Reddit discussion on the weakness exploited by this tool

More tools, if you have time

- Decoder Improved (update): Burp extension that includes all Decoder modes plus other features
- Cloud-service-enum & Introduction: Cloud enumeration scripts to validate which cloud tokens (API keys, OAuth tokens and more) can access which cloud service (for AWS, Azure & GCP)
- userrecon-py: Username recognition on various websites
- Amazon-AWS-Hack: Fully Automated Remote Hacking Tool for Amazon AWS
- Is-website-vulnerable: CLI tool that finds publicly known security vulnerabilities in a website's frontend JavaScript libraries

- OffensiveCloudDistribution: Leverage the ability of Terraform and AWS to distribute large security scans across numerous cloud instances
- Jwtear: Module command-line tool to parse, create and manipulate JWT tokens for hackers
- TSQL example scripts for identifying insecure use of global temp tables in SQL Server as an unprivileged login
- SauronEye: A search tool built to aid red teams in finding files containing specific keywords
- p12Cracker: A simple tool to brute force a password for a password-protected PFX/P12 file
- CloudUnflare: Find origin IP address for Cloudflare Bypass using CompleteDNS DNS History
- SharpLoginPrompt & Introduction: Post exploitation credential gathering tool. Useful for getting the current user's username & password without touching lsass and having administrator credentials on the system. Instead, it creates a login prompt to phish credentials.

Misc. pentest & bug bounty resources

- Open Source Intelligence Techniques – 7th Edition (2019) (~ $46, not paid to advertise it but it looks interesting for OSINT, especially for the self-reliance credo)
- How to Secure Your App – The ULTIMATE Reference
- Command Injection Payload List
- Awesome iOS Application Security
- Android Pentesting CheatSheet
- Ten Books to Start Your Penetration Testing Journey
- Arabic Web Application Penetration Testing Course & Github repo
- DNS Cheatsheet & DNS Record crash course
- Hacking Tools Cheat Sheet
- APIsecurity.io Issue 55: Vulnerabilities in eIDAS and Cisco routers, Instagram API program locked down

Challenges

- Sadcloud & Introduction: Tool to spin up intentionally insecure AWS infrastructure with Terraform
- White-box-pentesting lab to demonstrate pass-the-hash, blind sql and SSTI vulnerabilities
    - https://twitter.com/trouble1_raunak/status/1189917440274157569

Articles

- An analysis and thought about recently PHP-FPM RCE(CVE-2019-11043), TL;DR of the bug & [How to set up a CVE-2019-11043 testing lab with LXD system containers]
- Get out of the limited OWASP TOP-10/SANS TOP-25/Bug Bounty mindset
- Patching Android apps: what could possibly go wrong
- Burp Suite Team Collaborator Plugin
- De-anonymization via Clickjacking in 2019
- Fuzzer gets us new functions to bypass PHP disable_functions
- HTTP Desync Attacks in the Wild and How to Defend Against Them
- Open Redirects In Improperly Configured mod_rewrite Rules (PoC for CVE-2019-10098?)

News

Bug bounty & Pentest news

- Turbo Intruder 1.0.15 has a major quality of life enhancement: it now remembers your window size! Also you can use ctrl+enter to start/stop attacks.
- @mubix is giving away 3 OSCP Vouchers
- Slack Increases Minimum Bounties for High and Critical Bugs for 30 Days
- Facebook, Mozilla and Cloudflare announce new TLS Delegated Credentials standard: New TLS protocol extension will shorten the window an attacker has to perform a man-in-the-middle attack.
- Introducing http://canidisclose.it, the largest directory for security contacts. Made for security researchers attempting to disclose vulnerabilities, the list contains over 2,000 organization contacts
- Developers: Get Ready for New SameSite=None; Secure Cookie Settings
- Coalfire's CEO statement & The Coalfire employees have pleaded not guilty to reduced trespassing charges and are requesting a jury trial. Their attorney said they won't rest until their names are cleared.
- Pwn2Own to launch industrial control systems contest at 2020 Miami event

Reports

- JavaScript frameworks security report 2019
- The State of Retail Cybersecurity – 2019 Edition
- State of Stolen Credentials in the Dark Web from Fortune 500 Companies

Vulnerabilities

- Office for Mac Users Warned of Malicious SYLK Files
- Project Zero discloses UXSS in Safari WebKit
- Security researcher gets access to all FurryTail pet feeders around the world
- Five months after returning rental car, man still has remote control
- Android bug lets hackers plant malware via NFC beaming
- Major vulnerability patched in the EU's eIDAS authentication system
- RCE vulnerability impacts XML developer environments
- ELK Stack: Exploit for Kibana remote code execution flaw released on GitHub

Breaches & Attacks

- Office 365 Users Targeted by Voicemail Scam Pages #Phishing
- Nasty PHP7 remote code execution bug exploited in the wild
- Massive stolen credit card sale features 1.3m mostly Indian records
- BlueKeep attacks are happening, but it's not a worm
- On Halloween night, Google discloses Chrome zero-day exploited in the wild
- Confirmed: North Korean malware found on Indian nuclear plant's network
- Ransomware with a difference as hackers threaten to release city data: @thegrugq's old prediction coming true
- China-Linked Hackers Spy on Texts With MessageTap Malware

Other news

- How NSO Group Helps Countries Hack Targets
- This is how malicious Android apps avoid Google's security vetting
- A guide to spear-phishing – how to protect against targeted attacks
- Hackers who extorted Uber and LinkedIn plead guilty
- The scariest hacks and vulnerabilities of 2019
- Remember that competition for non-hoodie hacker pics? Here's their best entries

Non technical

- Bug Bounty Programs: Enterprise Implementation

- How are people finding hundreds/thousands of bugs so quickly?
- This One Time on a Pen Test, Halloween Edition: An Ode to Our Favorite Pen Tester Disguises
- Top 10 Hacker Movies of all Time
- The journey from web server to browser
- @j_opdenakker's #CyberSecurityAwarenessMonth blogs

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 10/25/2019 to 11/01/2019.

Curated by Pentester Land & Sponsored by IntigritiDisclaimer:The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.