Bug Bytes #44 – New platform, new programs and a $25K HEAD CSRF

BY INTIGRITI · NOVEMBER 12, 2019 · LAST UPDATED ON JULY 30, 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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 01 to 08 of November.

Intigriti news

- We've launched our brand new platform, check it out!
- KULeuven launched 2 new public programs:
  - www.kuleuven.be (responsible disclosure)
  - Online enrollment for students (up to €2.500 bounty)

Our favorite 5 hacking items

1. Conference of the week

> "Piercing The Veil: Server Side Request Forgery Attacks On Internal Networks – Alyssa Herrera & Other Hack.lu 2019 talks"

The slides for this talk were published months ago, and I was really hoping for the talk to be public too.
Alyssa is known for focusing on server-side bugs, especially SSRF.
So, this is a must watch for anyone who wants to learn about this bug class. It is also a good example on the kind of thinking and focus you need to find critical bugs and become an expert at a specific topic.

2. Writeup of the week

> "Bypassing GitHub's OAuth flow & TL;DR ($25,000)"

Who would have thought that playing with HTTP methods could bypass OAuth on GitHub and yield a $25,000 bounty?!
The bug exists because the same controller handles both GET & POST requests, and using a HEAD request instead is unexpected.
The controller relies on the HTTP method to determine whether it will grant access to the app or serve an OAuth authorization page. @not_aardvark used the HEAD method. It was routed as GET (Rails behavior) and at the same time, the controller treated it as an authenticated POST request, bypassing authorization.

3. Non technical item of the week

> "Deliberate Practice: What It Is and How to Use It"

It is very easy for hackers to get distracted by all the information and topics out there and keep hopping from one subject to another. If you think you have the Shiny Object Syndrome, or if you find yourself spending a lot of time learning and practicing without seeing the results you would expect, then you probably need "deliberate practice".
This article is a great introduction to this concept, with many resources to go further.

4. Tip of the week

> "I get asked how I manage a full time job, content, steam, hacking on top of my personal life. I'm going to answer this once and only once: if you have time to waste on YouTube/Reddit you have time to learn how to hack. I go to bed an hour later and wake up an hour earlier by @nahamsec"

Every time I hear of some accomplishement by bug hunters like @nahamsec, @stokfredrik, @nnwakelam, etc, I can't help but wonder how they do it all.
A lot of bug hunters juggle between multiple jobs and/or passions. It is what I do myself, but self-doubt creeps up sometimes: Why does it take me so much time to learn X? It seems easier for Y person... Is it just about the talent/intelligence you're born with? Is it because they don't have a family life like you? Or because they don't need to sleep as much as you do?
@nahamsec shares his unambiguous take on the matter: sleep one hour later and wake up an hour earlier. Make the time and stop with the excuses!

5. Resource of the week

> "IntelX Tools"

This is not a new site, but I've just discovered it while looking for good OSINT resources. And it is amazing whether you do OSINT, or reconnaissance for pentest/bug bounty.
It has a lot of categories: Email, Domain, IP, Username, Person, Phone Number, File... For each one, you can find a lot of tools at the same place and search them all at once.

Other amazing things we stumbled upon this week

Videos

- Live Bug Bounty Recon Session on Verizon Media's Yahoo.com with @phwd
- The Anatomy of C2
- SQL Injection PHP Code Review [22] #CodeReview
- PHP command Injection Vulnerability Code review [23] #CodeReview
- Reflected Cross Site Scripting PHP Code Review [24] #CodeReview
- CISSP vs. CEH, Cybersecurity Degrees, CTFs vs. Real-Life – Cybertalk with HackerSploit

- Common Linux Privilege Escalation: Exploiting Sudo Access & Exploiting Sudo Access
- Sudo Vulnerability CVE 2019-14287 | Privilege escalation in kali Linux

Podcasts

- 7MS #386: Interview with Ryan Manship and Dave Dobrotka – Part 4
- Security Now 739 – DOH and Bluekeep
- Risky Business #561 — Report: NSO exploits used against politicians, senior military targets
- Hackable? 34 – False Charges
- LadyBug Podcast – Working Remotely
- Hack Naked News #240
- Application Security Weekly #83

Webinars & Webcasts

- Research on the dangers of copy/pasting code
- Attacking and Defending Cloud Metadata Services

Conferences

- Secure Coding Workshop
- BlueHat Seattle 2019 || I'm in your cloud: A year of hacking Azure AD
- BsidesTLV 2019
- Does remote work really work?

Slides only

- Fast Recon-NG [from global to granular] [and how I got a P1 in Google VRP]
- A Purple-Team View of Serverless and GraphQL & The Hard Way: Security Learnings from Real-world GraphQL
- Breaking & Pwning Docker Containers & Kubernetes Clusters – All Day DevOps 2019
- Mix and match to bypass the same-origin policy
- ATT&CKing #Koadic with EQL
- An Analysis Of the BlueKeep Vulnerability

Tutorials

Medium to advanced

- Serving custom HTML on private collaborator domain
- Vulnerability hunting with Semmle QL: DOM XSS
- Publicly Exposed AWS SNS Topics
- Android Frida hooking: disabling FLAG_SECURE
- Hacking Tricks: Identifying Outgoing TCP Port for Reverse Shell
- How to Use CCAT: An Analysis Tool for Cisco Configuration Files
- Persistence – Scheduled Tasks & PowerShell Profile
- Part 2: Living Off The Land
- Finding and Identifying JScript/VBScript Callable COM Objects

Beginners corner

- A Deep Dive On The Most Critical API Vulnerability — BOLA
- Python 3.7 Asyncio For Hackers & dirbuster-asyncio.py
- How to easily find Reflected XSS vulnerabilities!
- How to Set up Certificate-Based SSH for Bug Hunting (+ bonus!)
- How to make Firefox an essential tool for OSINT
- OSINT Investigations on TikTok & TikTok Bookmarklet Tools
- Spot Fake Businesses & Find the Signature of CEOs with OSINT
- Same-Origin Policy And Cross-Origin Resource Sharing (CORS)
- Better Privacy: Encrypting DNS

Writeups

Challenge writeups

Pentest writeups

- XML Signature Validation Bypass in simpleSAMLphp and xmlseclibs

Responsible(ish) disclosure writeups

- Microsoft Office for Mac cannot properly disable XLM macros
- Text-To-Speech speaks pwned #Android #PrivilegeEscalation

- Breaching the perimeter – PhantomJs Arbitrary file read #Web
- CVE-2019-12415: XML processing vulnerability in Apache POI #Web
- Insecure Defaults in Adobe's Mobile SDKs #Mobile
- CVE-2019-1414 — a Local Command Execution in Visual Studio Code #PrivilegeEscalation #RCE
- Backend SQL Injection in BigTree CMS 4.4.6 #Web #CodeReview

Bug bounty writeups

- SSRF & DNS Rebinding on private program
- MiTM / Logic flaw on Shopify ($13,337)
- Information disclosure on Shopify ($1,000)
- Information disclosure on HackerOne ($2,500)
- Privilege escalation on Ubiquiti Inc. ($16,109)
- Stored XSS via CSV file upload on Shopify ($1,000)
- Token for changing email leaked on Shopify ($500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Jandroid & Introduction: A tool for template matching against apps. Current use case is to identify potential logic bug exploit chains on Android
- LiveTargetsFinder: Generates lists of live hosts and URLs for targeting, automating the usage of MassDNS, Masscan and nmap to filter out unreachable hosts and gather service information
- Github-endpoints.py: Search endpoints on GitHub for a given (sub)domain

More tools, if you have time

- Getallurls: Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl
- BlackWidow: A Python based web application scanner to gather OSINT and fuzz for OWASP vulnerabilities on a target website (by the creator of Sn1per)
- Paramuda: A python tool designed to enumerate hidden parameters on a target URL through a wordlist. It is designed to scan for URL by counting the existence of the payload in the response body
- SRLabs Gobuster: File & directry bruteforcer based on Gobuster with enhanced false positives detection

- Frida Android Helper: Several handy commands to facilitate common Android pentesting tasks
- Droidlysis: Property extractor for Android apps. It automatically disassembles apps and looks for various properties within the package or its disassembly
- WitnessMe: Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier
- NTLM Challenger: Parse NTLM over HTTP challenge messages
- _amerka GUI & Introduction: Internet of Things/Industrial Control Systems reconnaissance tool
- PostMessage_Fuzz_Tool & PostMessage Xss Fuzz using Chrome App

Misc. pentest & bug bounty resources

- OSINT tools and resources bookmark collection
- The Cyber Mentor Discord Server
- EC2 Security Strategy
- Build a new Windows Domain with a (semi) easy button & Alternative
- Exchange-AD-Privesc
- OWASP Firmware Security Testing Methodology

Challenges

- Privilege Escalation in AWS – Labs & Slides

Articles

- Bypassing AngularJS bind HTML
- #ProTips: Bug Bounty Hunting with Random Robbie
- Anatomy of Scalable Vector Graphics (SVG) Attack Surface on the Web
- HTTP smuggling via fake WebSocket connection
- Intro to Chrome's (g)old features & If you are ever able to upload files to a site and want to XSS but are blocked by a CSP whitelist, you should try PNaCl! It requires you to control a JSON and a binary of any content-type (nosniff is ignored).
- Bypassing a Firewall with Encrypted DNS Tunneling
- The Ethereal Beauty of a Missing Header
- Security assessment techniques for Go projects
- C2 Over RDP Virtual Channels

News

Bug bounty & Pentest news

- The end for BugBountyNotes
- Burp Suite Pro 2.1.05 released, with experimental support for using Burp's embedded Chromium browser to perform all navigation while scanning. This new approach will provide a robust basis for future capabilities.
- Coalfire arrests: Charges against US pen testers reduced but not dropped & The Primary Documents relating to the Coalfire Pentest in Iowa
- Facebook Portal survives Pwn2Own hacking contest, Amazon Echo got hacked
- Hacking the Singapore Government: A Q&A With A Top Hacker & MINDEF 2.0 Results

Reports

- Strategies for Building and Growing Strong Cybersecurity Teams
- Spear Phishing: A Law Enforcement and Cross-Industry Perspective

Vulnerabilities

- Apple Mail on macOS leaves parts of encrypted emails in plaintext
- Site Isolation bypass discovered in Google Chrome's Payment Handler API
- Smartphone and speaker voice assistants can be hacked using lasers
- Exclusive: Bitdefender Discovers Ring Doorbell Vulnerability

Breaches & Attacks

- BlueKeep Attacks Have Arrived, Are Initially Underwhelming
- TrendMicro Employee Sold Customer Info to Tech Support Scammers
- Ex-Twitter Employees Spied on Saudi Dissidents: DoJ
- Specially Crafted ZIP Files Used to Bypass Secure Email Gateways
- An inside look at WP-VCD, today's largest WordPress hacking operation

Other news

- Open source tool predicts which security vulnerabilities are most likely to be exploited
- How data breaches affect stock market share prices
- Undercover reporter tells all after working for a Polish troll farm
- Huawei calls hackers to Munich for secret bug bounty meeting

- DNS-over-HTTPS will eventually roll out in all major browsers, despite ISP opposition
- A guide to cryptojacking – how to prevent your computer from being turned into a money-making tool

Non technical

- Dirsearch wordlists – how big is too big?
- What nobody tells you about documentation
- What's the Difference Between a URI and a URL?
- How to Make Better Infosec Presentation Slides
- How to Look and Sound Confident During a Presentation
- Gartner: Of the 4 manager types, only 1 boosts employee performance 26%

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 11/01/2019 to 11/08/2019.

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