Bug Bytes #140 – The Great leak, Sandwich Attacks & Better InfoSec resumes

BY ANNA HAMMOND · SEPTEMBER 29, 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 20 to 27.

Intigriti news

5 insights into the recruitment & hiring process at Intigriti

Our favorite 5 hacking items

1. Tutorial of the week

How Secure Are Your Universally Unique IDentifiers (UUIDs)? & extract-uuid-infos

UUIDv1 Sandwich Attacks aren't new but I'm just discovering them thanks to @0xLupin. This led me to discover an excellent article by @VerSprite on UUID versions and their security implications. Also, @righettod has a PIPER script to automate the detection of UUIDs and extract info based on their version (all within Burp).

2. Writeups of the week

Autodiscovering the Great Leak (Microsoft)
"A tale of making internet pollution free" – Exploiting Client-Side Prototype Pollution in the wild
(Apple, Atlassian, Mozilla, HubSpot, Segment Analytics & others)

@0xAmit discovered that the Microsoft Autodiscover protocol used by Exchange leaks Windows domain credentials to autodiscover.[tld] domains. Some of these domains were available to purchase. By registering them, Amit received hundreds of thousands of domain credentials...

Another amazing piece of research is about prototype pollution at scale. A team of researchers scanned vulnerability disclosure programs looking for prototype pollution vulnerabilities, trying to find script gadgets for XSS. They found 18 vulnerable libraries, 80 bugs reported, and share lots of details on the methodology and tools they used.

3. Videos of the week

How To Search For DOM-Based XSS!
How to Create a Better Infosec Resume (with @jhaddix)!

@PascalSec's explanation of DOM XSS is just amazing. Everything is broken down including the basics of DOM XSS, sources and sinks, and how to track data flows from source to sink using the browser DevTools and JavaScript debugger.
If you struggle with this vulnerability type, this will clarify all the steps you need to detect and exploit it.

The second video is for anyone in InfoSec who wants to create or improve their resume. @NahamSec and @Jhaddix talk about the dos and don'ts, demonstrate the creation of a resume for a fake persona, then review some resumes sent by viewers.

4. Article / Tools of the week

SecurityTrails x Amass ReconMaster contest

@yougina came ninth in SecurityTrails's Recon Master contest and share how they did it. It is interesting to see that no intricate or obscure recon tools or techniques were used. It's all about *how* well-known tools were chained together, with custom scripts to overcome memory and storage space limitations.

5. Tip of the week

How to send remote VPS requests to your local BURP using SSH

Some of you may already know how to do this. For those who don't, this is good to know in case you need to run tools on your VPS and proxy the traffic through your local Burp.
The solution shared by @bsysop is simply to run `ssh -R 8080:127.0.0.1:8080 root@VPS_IP -f -N` locally, then use `http://127.0.0.1:8080` as a proxy when running tools on the VPS (e.g. `curl -k https://example.com -x http://127.0.0.1:8080`).

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Nosql Injection For Beginners!
- $50,000 Shopify access to source code via leaking GitHub token – Hackerone bug bounty
- Did you really find a vulnerability in Google? – ft. @PwnFunction

Podcasts

- Darknet Diaries Ep 101: Lotería
- Day[0]: iOS 0days, Apache Dubbo RCEs, and NPM bugs [Bounty Hunting]
- Day[0]: A Curl UAF, iPhone FORCEDENTRY, and a Crazy HP OMEN Driver [Binary Exploitation Podcast]

Webinars

- The Quest for the Kill Chain Killer Continues
- Webcast: Shellcode Execution with GoLang
- [SecWed] 8 Sep 21 | Firmware Bug hunting with Taint analysis, Slides & Blog post

Conferences

- h@cktivitycon 2021
- HTB x HacktivityCon 2021 Talks
- #RomHack2021

Tutorials

Medium to advanced

- How Secure Are Your Universally Unique IDentifiers (UUIDs)? & UUIDv1 Sandwich Attack example
- Easier URI Targeting With Metasploit Framework
- Linux X86 Assembly – How To Test Custom Shellcode Using A C Payload Tester
- Finding Number Related Memory Corruption Vulns
- A Short History of Chaosnet

Beginners corner

- Waybackurls – Hacker Tools: Time-traveling for bounties & Video
- AWS Cognito Misconfigurations in Android Apps
- nmapAutomator: Automating your Nmap Enumeration and Reconnaissance
- ASP.NET CORE Path Traversal

Writeups

Challenge writeups

- How To Search For SSRF!
- [::ACSC Quals 2021::] — Breaking Logics
- CSRF – Lab #4 CSRF where token is not tied to user session | Long Version
- HackTheBox – Pit

Responsible(ish) disclosure writeups

- CVE-2021-38112: AWS Workspaces Remote Code Execution #Desktop
- Cachet 2.4: Code Execution via Laravel Configuration Injection
- The Ultimate Guide to Crashing Your Friend's Wedding – The Knot, Business Logic Flaw #Web
- CVE-2021-40875: Improper Access Control in Gurock TestRail versions ≤ 7.2.0.3014 results in sensitive file exposure #Web
- PandoraFMS 755 – Chained XSS + .htaccess RCE #Web
- iOS 15 iCloud Private Relay Vulnerability Identified #Privacy #iOS

0-day & N-day vulnerabilities

- New Azure Active Directory password brute-forcing flaw has no fix
- VMware CVE-2021-22005 Technical analyses by Censys, by Randori, by @testanull & Nuclei template for detection
- Disclosure of three 0-day iOS vulnerabilities and critique of Apple Security Bounty program (Apple)
- CVE-2021-26084: Details On The Recently Exploited Atlassian Confluence OGNL Injection Bug
- Analysis of CVE-2021-35211 (Part 1) & Part 2
- Fully Weaponized CVE-2021-40444

Bug bounty writeups

- Remote Command Execution in Visual Studio Code Remote Development Extension (Microsoft)
- Attack Surface Analysis – Part 3 – Resurrected Code Execution ($8,500)
- $8,000 Bug Bounty Highlight: XSS to RCE in the Opera Browser (Opera, $8,000)
- Facebook Messenger for MacOS contained valid hardcoded FB access token (employee's token?) (Facebook, $625)
- RCE in Citrix ShareFile Storage Zones Controller (CVE-2021-22941) – A Walk-Through (Citrix Systems)
- Pwn2Own 2021: Parallels Desktop Guest To Host Escape (Parallels)
- mXSS in support.mozilla.org (Mozilla)

See more writeups on The list of bug bounty writeups.

Tools

- fullhunt.io & Intro
- Chronos: Extract pieces of info from a web page's Wayback Machine history
- ssh-key-confirmer: Test if a public key would theoretically be allowed on a SSH target if you had the private key
- crawlergo: A powerful browser crawler for web vulnerability scanners
- Mitra: A generator of weird files (binary polyglots, near polyglots...)
- Cariddi: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more...

Tips & Tweets

- Proxying curl traffic through Burp when burp doesn't work
- XSS when target="_blank"
- With iOS 15 supporting Safari extensions, you can use WebInspector extension to hack on iPad
- WAF bypass using multiple fields
- A contrived solution for the "Basic context length limit, arbitrary code" impossible lab
- When reviewing a new project/framework/library...
- Use this to build a quick GraphQL schema from Facebook Android and iOS apps

Misc. pentest & bug bounty resources

- Defense against Client-Side Attacks (Whitepaper)

- @HolyBugx's recommended resources for learning GraphQL
- List of API endpoints & objects
- Bookt of Tips ft. Aditya Shende
- Game Hacking Academy

Challenges

- Training XSS Muscles
- PyGoat: Intentionally vuln web Application Security in django
- HTB Retired Machines free for two weeks, the current one is Jarmis

Articles

- IAM Vulnerable – Assessing the AWS Assessment Tools
- New XSLeaks technique: CSP violation based on form-action
- Using CodeQL to detect client-side vulnerabilities in web applications
- Resetting Expired Passwords Remotely
- Bug Bounty Cloud Automation at Scale & AWS Step Functions to accelerate bug bounty recon workflows (follow-ups to @ryanelkins's DEFCON 29 talk)

Bug bounty & Pentest news

- Bug bounty
  - Google: Announcing New Patch Reward Program for Tsunami Security Scanner
- Cybersecurity
  - Google TAG: Financially motivated actor breaks certificate parsing to avoid detection
  - NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs
- Tech
  - AWS federation comes to GitHub Actions
- Upcoming events
  - AMA with 0xdf_: Creating HTB machines
- Tool updates
  - ReconFTW v2.1.0
  - Anew added output options
  - Dalfox v2.5.0 released

- Subfinder v2.4.9
- Feroxbuster has a new documentation site

Non technical

- Meet a Hacker Hero – Eva Galperin
- 20 productivity hacks that will change your life