Bug Bytes #100 – Apache XSS trick, Google in CLI without Captcha & How to easily fetch bug bounty scopes

BY ANNA HAMMOND · DECEMBER 9, 2020 · 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.

Before we dive into the meat of this newsletter, we'd like to acknowledge some of our favorite sources of information as a means of celebrating this 100th issue.

This publication would not exist without all you hackers and content creators who share your knowledge and help others improve each in your own different ways. This short list won't do justice to all, it is just a tiny fraction of the sources on which we keep a close eye for their regularity and excellent quality. Immense gratitude and respect to all:

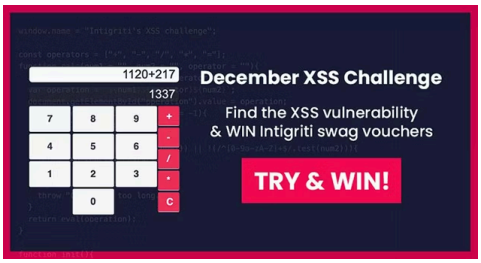
- PortSwigger for the incredible research, invaluable training academy and daily news (Daily Swig);
- Darknet Diaries for entertaining us with fascinating real-life hacker stories;
- ProjectDiscovery.io for the many sweet well-polished tools;
- NahamSec for allowing us to "meet" so many talented hackers in delicious interviews;
- Daniel Miessler for the bubbly mix of technical topics and thought-provoking essays;
- NCCGroup for the numerous and quality responsible disclosure advisories, tools and research;
- InfoSec Write-Ups for helping us keep up with the latest bug bounty writeups;
- SANS Information Security Webcasts for regularly offering free high-quality webcasts on all kinds of Information Security topics;
- Bishop Fox research labs for the excellent tools, guides, security advisories and fantastic research;
- Rhino Security Labs for your unique tools, challenges, guides and writeups on all things penetration testing, especially cloud security.

Lastly, an honourable mention to Appsecco for insightful presentations, writeups and free trainings on Cloud and Web security.

To everyone else who did not make the list, we also love you and appreciate your work <3

That said, let's look at what the week (from 29 of November to 06 of December) brought us.

Intigriti News



Intigriti's December XSS Challenge

The ultimate iPhone hack, The new threat of cyber-biological attacks & 2021 threats forecast

Our favorite 5 hacking items

1. Challenge of the week

Orange Tsai's HITCON CTF 2020 XSS challenge & Solution

This XSS challenge shows a cool trick for getting XSS in Apache installations. Without spoiling it, here's a little indication: It affects file upload functionalities when Apache supports content negotiation.

2. Writeups of the week

$10000 Facebook SSRF (Bug Bounty) (Facebook, $10,000)
Don't Scan My Website I: Exploiting an Old Version of Wappalyzer #Web

How do people still find SSRF on Facebook? @amineaboud did it using a series of common bug hunting techniques (subdomains enumeration, file bruteforcing and JS analysis), yet the magic was in their combination, his thoroughness and perseverance. Hats off for a beautiful finding!

The second writeup answers the question: can you be pwned by running Wappalyzer against a malicious server? Malicious JavaScript hosted on a remote server cannot read local files in Web browsers because of the Same Origin Policy. Wappalyzer however uses on Zombie.js, a headless browser, with a default setting that made it possible to load and exfiltrate local files. It is fixed now but it is a very interesting read.

3. Resource of the week

xsleaks.dev

This is a new wiki by Google on Cross-site leaks (XS-Leaks). It's a great resource for learning about this vulnerability class, common attacks and how to mitigate them. Also good to know, the project is open source and welcomes new contributions.

4. Tools of the week

bbscope

Degoogle

bbscope is a Go tool for fetching the scope of bug bounty programs from Intigriti, Bugcrowd and Hackerone. It has handy options that allow you to fetch only private programs, those that offer bounties, or to filter results by scope category (URL, CIDR, mobile, code, hardware...). Awesome work by @sw33tLie!

Degoogle is a Python script for querying Google and extracting result URLs. I haven't dived into the code, so I'm not sure how it does it but somehow it avoids bot detection. No captcha is served even after running it for weeks.

5. Videos of the week

Finding Your Next Bug: GraphQL
Hacking Tips – Finding new Tools and Techniques Using Github
Hacking 1Password | Episode 4 – Two Simple Bugs that Worth $3,300

The sweet videos to watch this week are about a comprehensive introduction to GraphQL for bug hunters, a welcome reminder to leverage Github for discovering new tools and techniques, and (finally!) the overlooked bugs @ngalongc found in 1Password after decrypting it.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays – DNS? XSS? DOMXSS? SSRF?
- RCE via Prototype Pollution in kibana – CVE-2019-7609 – Bug Bounty Reports Explained
- Multi 0-Day Exploits Expose Millions Of Routers
- How to grow as a HACKER // ft. NahamSec (a hacker)
- Local Recon Machine – Kali on Windows ft. WSL | Final Part – Pt.2 | Recon on a live site
- Attacking Active Directory – AS-REP Roasting & Attacking Active Directory – Bloodhound

Podcasts

- Security Now: DNS Consolidation – Generic Smart Doorbells, Tesla Model X Key Fobs, Critical Drupal Flaw, Spotify
- Risky Business #607 — Trump lawyer calls for Krebs' execution, ransomware insurance getting wobbly
- Darknet Diaries EP 80: THE WHISTLEBLOWER
- The InfoSec & OSINT Show 36 – Tracy Maleeff & Empathy Based InfoSec
- Joshua Richards – Buying/Selling Body Parts on the Dark Web
- SIGRED: Hijacking Microsoft Windows Server

Webinars & Webcasts

- Why So Serious? Insecure Object Deserialization Demystified
- Binary and Patch Diffing for Bug Hunting and Weaponization – SANS@Mic
- Webcast: Pretty Little Python Secrets – Episode 2 – Python Development & Packaging as Beautiful as a Poem

Conferences

- BSides Islamabad, especially:
  - The road towards O365 bugs in Microsoft Office365, By Ashar Javed & Slides
- PasswordsCon 2020 virtual
- Converge Detroit, especially:
  - Improving the Landscape and Messaging of Offensive Tooling and Techniques & Slides
  - Déjà vu in the cloud

Tutorials

Medium to advanced

- Abusing SSRF on Selenium Grid
- Abusing Application Layer Gateways (NAT Slipstreaming) & New PoC
- Machine Learning Attack Series: Overview
- Building C2 Implants in C++: A Primer
- Weaponizing Windows Sandbox To Bypass Defender

Beginners corner

- Hacking into an AWS Account – Part 2: Jenkins & Hacking into an AWS Account – Part 3: Kubernetes
- Introducing Monsoon A Lean And Versatile HTTP Enumerator
- Simple Recon Methodology
- CSP bypasses, and how developers can build a strict CSP!
- State of the art of network pivoting in 2019

Writeups

Challenge writeups

- XSSworm.dev ~ Self-replication contest [write-up]
- Imposter Alert: Extracting and Reversing Metasploit Payloads (Flare-On 2020 Challenge 7)

Pentest writeups

- A 3D Printed Shell

Responsible(ish) disclosure writeups

- Multiple (RCE) Vulnerabilities in Micro Focus Operations Bridge Manager #Web
- Technical Advisory: containerd – containerd-shim API Exposed to Host Network Containers (CVE-2020-15257) #Containers
- Drupal Core: Behind the Vulnerability #Web
- Multiple vulnerabilities through filename manipulation (CVE-2020-28948 and CVE-2020-28949) #33 #Web
- Bug Or Feature: Privilege Escalation In Windows Autopilot #Windows #LPE

Bug bounty writeups

- An iOS zero-click radio proximity exploit odyssey
- Site Wide CSRF On Glassdoor (Glassdor, $3,000)
- Exploiting Blind Postgresql Injection And Exfiltrating Data In Psycopg2 ($3,000)
- "Important, Spoofing" – zero-click, wormable, cross-platform remote code execution in Microsoft Teams (Microsoft)
- Leaking Browser URL/Protocol Handlers (Google, Microsoft, Mozilla)
- RCE via LFI Log Poisoning – The Death Potion

- Websites Can Run Arbitrary Code on Machines Running the 'PlayStation Now' Application (PlayStation, $15,000)

See more writeups on The list of bug bounty writeups.

Tools

- Windows Registry .burp file handler & Intro: Windows Registry file that adds handling of .burp files by allowing double-click to open projects directly. Also adds context menu options to launch with extensions disabled, spider and scanner paused, or both.
- antiburl.py: Python tool inspired by @TomNomNom's anti-burl, with advanced options
- HackerOne Scripts: Collection of scripts to automate HackerOne things using their GraphQL API
- CastleBravo: @m4ll0k's BugBounty Automation Tool
- metahttp: A bash script that automates the scanning of a target network for HTTP resources through XXE
- galer: A fast tool to fetch URLs from HTML attributes by crawl-in
- PyOracle2 & Intro: A python-based padding oracle tool
- powersploit_portscan_db_import & Intro: Metasploit db importer for PowerSploit Invoke-Portscan
- IAMFinder & Intro: Open Source Tool to Identify Information Leaked from AWS IAM Reconnaissance
- BackBomb: Dockerized penetration-testing/bugbounty/app-sec testing environment
- WriteHat & Intro: A pentest reporting tool written in Python. Markdown –> HTML –> PDF
- Carnivore: Tool for assessing on-premises Microsoft servers authentication such as ADFS, Skype, Exchange, and RDWeb
- Distillo.io: Tracking website updates, automated and simplified

Tools updates

- All hail HunterSuite , A year later.
- Arjun v2.0
- Kubernetes is deprecating Docker support
- dnsprobe reworked as dnsx

Misc. pentest & bug bounty resources

- Awesome Electron.js hacking & pentesting resources
- Web Security Testing Guide v4.2 Released

- Humble Book Bundle: Hacking 101 By No Starch Press (Starting at $1)
- Web Security Academy – your questions answered
- iOS pentesting mindmap & SAML security mindmap

Challenges

- Intigriti December XSS Challenge
- Damn Vulnerable WooCommerce Plugins & Security Advisory to Exploit – A Hands-On Approach with WooCommerce Plugins
- Advent of CTF

Articles

- Single Sign-On Security: Security Analysis of real-life OpenID Connect Implementations & Full thesis
- Improving OAuth App-to-App Security
- PHP8, from a security point of view
- Whac-A-Mole: Six Years of DNS Spoofing
- Tried and True Hacker Technique: DOS Obfuscation
- Hacking in Among Us

Bug bounty & Pentest news

- $40 bounty for the first person to implement findomain on reNgine
- BSidesRDU/DC919 Weaponized XSS workshop: Dec 13th
- Priority One Report 2021 Edition: A New Decade In Crowdsourced Cybersecurity
- Announcing The Hackerone Brand Ambassadors
- Excellerate Your Hunting With Bugcrowd And Microsoft!
- Announcing the Winners of Pentester Lab Pro Subscription Giveaway — November 2020
- Dropbox: Protecting Security Researchers

Non technical

- Hacker Spotlight: Interview With Jensec
- Reddit RSS Functionality Explained

- Exploiting APT data for fun and (no) profit
- More Motivated in Minutes: 5 Science-Backed Tricks To Get You Going
- When you need to confirm you're not a robot

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 11/29/2020 to 12/06/2020.