Bug Bytes #98 – Imagemagick's comeback, Treasure trove of wordlists, Advent of Cyber & How to get more hours in your day

BY ANNA HAMMOND · NOVEMBER 25, 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.

This issue covers the week from 15 to 22 of November.

Intigriti News

Join us for an exclusive liveset performed by @realytcracker, this Friday 20:00 CET on our Youtube channel!

12 Cisco bugs, 200 most common passwords, Weird bounties & SAD DNS

Our favorite 5 hacking items

1. Videos of the week

Getting Organised: Making a //TODO list
Hacking 1Password | Episode 3 – Decrypting the data without Crypto Knowledge

@InsiderPhD shares the tools and time management techniques that allow her to get so much done as a PhD student, Youtuber and bug bounty hunter. If you'd like more hours in the day (who doesn't?), you'll probably find this insightful.

In the second video, @ngalongc continues his series on hacking 1password. It is helpful to see his method for breaking down such a complex topic (decrypting requests and responses of the 1password app).

2. Writeups of the week

ImageMagick – Shell injection via PDF password
Apache Unomi CVE-2020-13942: RCE Vulnerabilities Discovered & CVE-2020-13942 POC
Exploiting dynamic rendering engines to take control of web apps ($5,000)
Firefox: How a website could steal all your cookies & CVE-2020-15647 PoC (Mozilla, $5,000)

The first writeup is about OS command injection in ImageMagick. The payload is injected in the password passed with the "-authenticate" command line parameter to encrypt the PDF.

The second writeup is about two RCEs in Apache Unomi that got the maximum CVSS score of 10! I have a feeling some bug hunters are busy testing for "/context.json"...

The third writeup presents fantastic research on vulnerabilities in Web apps that use dynamic rendering engines. Everything is well explained, from what they are and how to identify them in black box testing to finding vulnerabilities and exploiting them.

The fourth finding is fixed, but it is very interesting for anyone who wants to see a real-life Android app vulnerability involving content providers, intents and the SOP.

3. Articles of the week

Privileged Container Escape – Control Groups release_agent
Real-life OIDC Security

The first article by @ajxchapman is about escaping privileged Docker containers to execute arbitrary commands on the container host. It is based on past work by @_fel1x. Pretty interesting for anyone who is into hacking CI/CD systems and containers!

The second article is the introduction to a 7 posts series on OpenID Connect and Single Sign-On security. It includes analysis of several implementations and attack patterns, and examples of bugs reported to five vendors. Great research by _lauritz_ as part of his master's thesis.

4. Resource of the week

Assetnote Wordlists

This is huge! Assetnote launched this collection of wordlist for assets and content discovery (DNS bruteforce, API routes, GET parameters, subdomains...). Some are automatically updated each month using Commonspeak2 and GitHub Actions, while others are curated manually.

The wordlists are cleaned with clean_wordlist.sh, a script suggested by @BonJarber to remove noise. It is worth checking out too if you want to curate your own wordlists.

5. Tools of the week

Webscan
CTFNote

Webscan is a browser-based internal network scanner by @samykamkar. Just by visiting a Web page, it remotely detects your LAN IPs using WebRTC and any live hosts. Mindblowing and dangerous if combined with other vulnerabilities such as NAT Slipstreaming!

CTFNote is a must for CTF players. It allows you to keep track of CTFs you're playing and who is available to participate or not, to assign tasks to team members, to shares notes, etc. This makes collaboration easier and would be nice to have for bug bounty too.

Other amazing things we stumbled upon this week

Videos

- BitK Talks about CTFNot, GoogleCTF Finals, CTF Tools, Hacker Mindset and more!
- Stealing your Github code with malicious YAML file – Bug Bounty Reports Explained
- h1-2010 Community Day
- How to Find and Exploit XSS DOM Cloberring – XSS in GMail
- Introduction To GraphQL | Penetration Test
- Discovering Email Addresses (OSINT) & Hunting Usernames and Accounts (OSINT)

Podcasts

- The InfoSec & OSINT Show 34 – John Strand & Moving Beyond 0-Days
- Security Now: SAD DNS – Malicious Android Apps, Ransomware-as-a-Service
- MangoPDF – The "Don't Get Arrested Challenge"
- Risky Business #605 — Trump fires CISA director Chris Krebs
- Creative Mindsets, Reaching Goals, & Encouraging Accountability – BSW #197
- Krebs Fired at CISA, DNS Is Not Your Friend, & 'Stone Panda' – Wrap Up – SWN #84
- IoT Cybersecurity Improvement Act, TCL Smart TV Flaw, & Popping Reverse Shells – PSW #675

Webinars & Webcasts

- Embrace Secure Defaults, Block Anti-patterns, and Kill Bug Classes with Semgrep with Clint Gibler

- StreamTitle Ep.1: XSS
- Accelerate Your Career By Building FIVE Critical Professional Skills – SANS@Mic
- Pen Test HackFest Summit – Cloud Penetration Testing Workshop

Conferences

- BSides CT 2020
- API Specifications Conference (ASC) 2020

Tutorials

Medium to advanced

- Purgalicious VBA: Macro Obfuscation With VBA Purging & OfficePurge
- Customizing Python's SimpleHTTPServer
- A Fresh Outlook on Mail Based Persistence
- Dynamic Invocation in .NET to bypass hooks
- Customizing C2-Frameworks for AV-Evasion
- Exploits in The Attic – Visiting Forgotten Metasploit Modules

Beginners corner

- Why embedding secrets in mobile apps is not a good idea
- Proxying Android app traffic – Common issues / checklist
- Exploiting OAuth 2.0 — Authorization Code Grants
- What to do when a Facebook profile is private?
- Quick Guide to Security Headers – Part Two
- SQL Injection Attack And Exploiting SQL Injection Part – 2

Writeups

Challenge writeups

- wacky & BugPoC XSS Challenge – Wacky Text Generator

Pentest writeups

- The tale of Restricted Shell bypass leading to Arbitrary Code Execution
- Pentest-Story: Empirum password decryption

Responsible(ish) disclosure writeups

- Cisco pre-auth RCEs #Web
- Path Traversal on Citrix XenMobile Server #Web
- Consul by HashiCorp: from Infoleak to RCE #Web
- Windows RpcEptMapper Service Insecure Registry Permissions EoP #Windows #LPE
- CVE-2020-16995: Microsoft Azure Network Watcher Linux Extension EoP #LPE
- Microsoft Teams For Macos Local Privilege Escalation #Windows #LPE

Bug bounty writeups

- Tale of 3 vulnerabilities to account takeover!
- Bypassing the Redirect filters with 7 ways
- Turning Blind Error Based SQL Injection into Exploitable Boolean One
- Security@ email forwarding and Embedded Submission drafts can be used to obtain copy of deleted attachments from other HackerOne users (HackerOne)
- @bugraeskici's bug reports to Automattic (Automattic, $3,100)
- Staff with no permissions can listen to Shopify Ping conversations by registering to its different WebSocket Events (Shopify, $800)
- Access token stealing. (PlayStation, $1,200)
- Authorization Token on PlayStation Network Leaks via postMessage function (PlayStation, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- Urlhunter: Recon tool that allows searching for URLs exposed via shortener services (using URLTeam data)
- exclude-cdn: Wraps projectdiscovery's cdncheck library to exclude CDN hosts from input passed over stdin
- 403Bypasser: Burpsuite Extension to bypass 403 restricted directory
- Phonerator: A search engine that allows you to provide a few digits and generate a list of possible valid phone numbers for #OSINT
- Nimplant & Implant Roulette Part 1: Nimplant: A cross-platform implant written in Nim
- Goshs: A SimpleHTTPServer written in Go, enhanced with features and with a nice design

Tools updates

- Nuclei – Fuzz all the things
- Kali Linux 2020.4 Release
- Open Azure blobs search on grayhatwarfare.com and other updates
- InQL Scanner v3 – Just Released!
- Introducing BloodHound 4.0: The Azure Update

Misc. pentest & bug bounty resources

- Disclosed HackerOne reports by vulnerability type
- Infosec Bugbounty AMA with zseano & with Sreeram KL
- hahwul/DevSecOps
- New gadget chain for deserialization in Zend Framework applications
- OffensiveNim
- Open-Source Intelligence (OSINT) Fundamentals ($29.99)

Challenges

- Advent of Cyber: Start on December 1st
- Announcing the 2020 December Metasploit community CTF
- Bluetooth Low Energy hardware-less HackMe

Articles

- Project Resonance Wave 1: Internet-Wide Analysis of Subdomain Takeover & Top vulnerable subdomain names
- Good Luck, I'm Behind Two Proxies
- Information Leakage in AWS Resource-Based Policy APIs
- NTLM relay of ADWS (WCF) connections with Impacket
- Detecting Cobalt Strike Default Modules via Named Pipe Analysis
- Windows Terminal Profile Fun
- The Strange Case of the Malformed Shebang

Bug bounty & Pentest news

- Intigriti 1337UP live session starring YTCracker

- Facebook: Marking the 10th Anniversary of Our Bug Bounty Program
- Bugcrowd Platform Updates: Portfolio Accounts And Security Settings & Introducing Our New Researcher Dashboard!
- Porchetta Industries / byt3bl33d3r is partnering up with Kali Linux

Non technical

- AWS access keys leak in GitHub repository and some improvements in Amazon reaction
- Organizing Feedly by Tags
- Hacker Spotlight: Interview With InsiderPhD
- 'As long as people are the ones writing code, there's going to be insecure code' – Tommy DeVoss on his post-jail bug bounty exploits
- How to tackle impostor syndrome while working remotely

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 11/15/2020 to 11/22/2020.