# Bug Bytes #60 - Bypassing AWS signing, @samwcyo's secrets and WordPress leaks

BY INTIGRITI · MARCH 5, 2020 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

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 21 to 28 of February.

## Our favorite 5 hacking items

### 1. Conference of the week

> "AppSec California 2020"

So many good talks and prestigious speakers! Topics range from Web security to Cloud, Kubernetes, Credential stuffing, DevSecOps, Car hacking and more.

I'm starting with JWT Parkour – Louis Nyffenegger and Are You Properly Using JWTs? – Dmitry Sotnikov. What about you?

### 2. Writeup of the week

> "Write-up: AWS Document Signing Security Control Bypass ($1,000)"

This is a writeup of an interesting bug found by analyzing a file upload functionality. It used AWS for storing documents uploaded, and AWS signing to authorize access to files.

By manipulating a request parameter, @ozgur_bbh was able to bypass the signing mechanism and access all documents in the S3 bucket.

### 3. Videos of the week

> "– @zlz Talks About How He Got Started, Recon, Hacking @Tesla, and Working With @Theparanoids
> – How to Use Firefox Containers for Easy IDOR Hunting (With Demo!)"

I don't think I will ever get bored of watching interviews with hackers. This one is with @zlz. It is fascinating to learn about his thought process, his unique recon process, how he approaches full-time bug hunting, how he is able to get a sense of applications that are probably vulnerable based on past experience, etc.

The second video may be the fastest way to learn how to use Firefox Containers. They are very useful for both Web hacking (IDOR and authorization tests) and segregating accounts during normal navigation.

## 4. Article of the week

> "Gehaxelt – How WordPress Plugins Leak Sensitive Information Without You Noticing"

This in an interesting read for anyone interested in doing research and submitting new modules to Detectify. @gehaxelt explains his process for analyzing the most popular WordPress plugins and finding information leaks.

## 5. Tutorial of the week

> "Bypassing OkHttp Certificate Pinning & Reddit discussion"

This tutorial might be helpful if you are struggling with certificate pinning bypass. @CaptMeelo shows a nice trick he used when Xposed Modules and Frida were not working.

He looked at the system log while the app was running. Certificate fingerprints appeared in the log. He decompiled the app, identified where the fingerprints were located and added one for his Burp certificate. Recompiling the app and running this patched version allowed him to bypass certificate pinning without having to modify smali code.

# Other amazing things we stumbled upon this week

## Videos

- How Docker Works – Intro to Namespaces & Deepdive Containers – Kernel Sources and nsenter
- Penetration Testing Bootcamp
- Overview of .json Firebase database information disclosure
- NGINX: misconfigurations examples
- My Entrepreneurial Journey – Episode 6: Revenue, Advertising, and Mayor Joe the Intern

## Podcasts

- CoalCast #12 – What's Happwning? w/ Ryan Villarreal
- SwigCast, Episode 5: EDUCATION
- The Many Hats Club – Ep. 39, I am Notdan (with notdan)
- Security Now 755 – Apple's Cert Surprise
- Security Weekly News #14 – Citrix Hacks, RSA Sold, IBM Runs In Terror, D-List Celebrities

## Webinars & Webcasts

- Adversary Emulation and the C2 Matrix (Free registration required)

## Conferences

- BSides Tampa 2020 Videos
- File Upload Security (February OWASP Meetup) & Updated OWASP File Upload Cheat Sheet
- CS3STHLM 2019 #ICS/SCADA

## Slides & Workshop material

- Android Pentesting

## Tutorials

### Medium to advanced

- Other Security Features of Content Security Policy
- DNS Exfiltration using SQLMap in a Microsoft SQL Environment
- Simple DLP for AWS S3
- Finding Pwned Passwords in Active Directory
- Parent PID Spoofing
- Persistence via Shims
- PyRDP on Autopilot – Unattended Credential Harvesting and Client-Side File Stealing
- Getting DNS Client Cached Entries with CIM/WMI
- Adaptive DLL Hijacking

### Beginners corner

- Fiddling with Windows: Proxy tools for Win10
- Faster nmap scanning with the help of GNU parallel
- SSH Tricks
- AngularJS Client Side Template Injection (XSS)
- Running-up and organizing CTF events — Nginx & Docker
- How to Use OWASP Amass: An Extensive Tutorial
- Multiple Ways to Exploit Windows Systems using Macros
- Pass-the-Hash is still a nuclear bomb

## Writeups

### Pentest writeups

- Hiding In Plain Sight
- From 0 to 1337. brief security analysis of a large service provider
- Interesting Bugs — 1

### Responsible(ish) disclosure writeups

- The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections & FAQ
- CVE-2020-1938: Ghostcat #Web
- CVE-2020-0688: Microsoft Exchange deserialization/RCE vuln #RCE
- CVE-2020-8818: Magento Payment Process Bypass #Web
- Cacti v1.2.8 authenticated Remote Code Execution (CVE-2020-8813) #CodeReview #RCE
- RCE via Apache Struts2 – Still out there. #Web
- Cache poisoning DoS in CloudFoundry gorouter (CVE-2020-5401) #Web
- Signature Validation Bypass Leading to RCE In Electron-Updater #RCE
- [EN] A-Z: GWTUpload – DoS #CodeReview

### Bug bounty writeups

- Periscope android app deeplink leads to CSRF in follow action (Twitter, $1,540)
- Twitter Source Label allow 'mongolian vowel separator' U+180E (app name) (Twitter, $560)
- Ad Builder Display Ads Path Traversal (SEMrush, $500)
- Tale of Account Takeovers (Part-1)
- iOS app crashed by specially crafted direct message reactions (Twitter, $560)
- Password Reset Link Works Multiple Times (NordVPN, $100)
- Long String DoS ($100)
- The Tricky XSS

## Tools

- Progress: Burp Suite extension to track vulnerability assessment progress

- 1u.ms: A small set of zero-configuration DNS utilities for assisting in detection and exploitation of SSRF-related vulnerabilities
- shuffleDNS: Wrapper around massdns written in go that allows you to enumerate valid subdomains using active bruteforce as well as resolve subdomains with wildcard handling and easy input-output support
- Jiraffe: One stop place for exploiting Jira instances in your proximity
- PassiveHunter: Subdomain discovery using the power of 'The Rapid7 Project Sonar datasets'
- udp-hunter & Introduction: Network assessment tool for various UDP Services covering both IPv4 and IPv6 protocols
- Weakpass_generator & Weak in, Weak out: Keeping Password Lists Current: Generates weak passwords to try in brute-force attempts, based on current date with a 90 day window.
- IIS-Raid & Backdooring IIS Using Native Modules

## Misc. pentest & bug bounty resources

- Clicker-service: Clicker service docker container that assists in developing intentionally vulnerable web apps that need a user to "click" on malicious payloads
- CPR evasion encyclopedia: The Check Point evasion repository
- Choose Your Own Red Team Adventure
- So you want to learn Azure Security?
- How to Hack Like a GHOST: A detailed account of a breach to remember (Hacking the Planet Book 8): New ebook from the author of How to Hack Like a Pornst*r. Looks interesting!
- Reverse XSShell
- The network protocol cheatsheet

## Challenges

- Hacking Unicode Like a Boss
- CyberSoc CTF Platform (OSINT)

## Articles

- Twitter Recap #1 – Bug Bounty Tips by the Intigriti Community
- Twitter Recap #2 – Polls by the Intigriti Community
- The Curse of Old Java Libraries
- SMB is Dead, Long Live SMB!

- Interesting Recon Script
- Azure Privilege Escalation Using Managed Identities
- Building a bypass with MSBuild

## News

### Bug bounty & Pentest news

- Humble Book Bundle: Cybersecurity 2020 by Wiley
- Nullcon AMA
- The 2020 Hacker Report
- Duplicates & self-closed reports do not affect reputation on H1 anymore (Retroactive change)
- We found 6 critical PayPal vulnerabilities – and PayPal punished us for it

### Reports

- Mobile malware evolution 2019

### Vulnerabilities

- How one man could have flooded your phone with Microsoft spam
- iPhone and iPad apps can snoop on everything you copy to the clipboard& Show me Your Clipboard Data!
- WhatsApp, Telegram Group Invite Links Leaked in Public Searches
- New Kr00k vulnerability lets attackers decrypt WiFi packets
- Checkmarx Research: Smart Vacuum Security Flaws May Leave Users Exposed
- Microsoft Exchange Server admins urged to treat crypto key flaw as 'critical' (CVE-2020-0688)
- Ghostcat bug impacts all Apache Tomcat versions released in the last 13 years (CVE-2020-1938)
- LTE vulnerability allows impersonation of other mobile devices
- Google patches Chrome zero-day under active attacks

### Breaches & Attacks

- PayPal accounts abused en-masse for unauthorized payments
- Ransomware wipes evidence, lets suspected drug dealers walk free
- A 'stalkerware' app leaked phone data from thousands of victims
- The "Cloud Snooper" malware that sneaks into your Linux servers

- Clearview AI loses entire database of faceprint-buying clients to hackers & Here's the File Clearview AI Has Been Keeping on Me, and Probably on You Too

### Malicious apps/sites

### Other news

- Brave Browser Integrates Wayback Machine to View Deleted Web Pages
- Report identifies the most dangerous mobile app store on the internet
- How a Hacker's Mom Broke Into a Prison—and the Warden's Computer
- When speakers are all ears: Understanding when smart speakers mistakenly record conversations
- SSL/TLS certificate validity chopped down to one year by Apple's Safari
- Biohackers Encoded Malware in a Strand of DNA
- Meet the white-hat group fighting Emotet, the world's most dangerous malware
- Hiding Windows File Extensions is a Security Risk, Enable Now

## Non technical

- #AndroidHackingMonth Q&A With Android Hacker bagipro
- Congratulations, Cosmin! The world's seventh million-dollar bug bounty hacker
- Todayisnew Crosses $1M in Bounties at h1-415 in San Francisco
- Malicious Insider Scenarios
- The Future of Adversaries is Software Development

## 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 02/21/2020 to 02/28/2020.

*Curated by Pentester Land & Sponsored by Intigriti*