Bug Bytes #70 – Gmail XSS, Decrypting HTTPS without MiTM & Hakluke's TikTok Tips

BY INTIGRITI · MAY 12, 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 01 to 08 of May.

Intigriti news

We launched another XSS challenge! Find the XSS and WIN a Burp Suite Pro license (1 year):

> **"NEW CHALLENGE : Find the XSS and WIN a @Burp_Suite Pro License! As usual, we'll tweet a tip for every 100 likes. GO! https://t.co/dYnctSfAAq#HackWithIntigriti**
>
> **— Intigriti (@intigriti) May 11, 2020"**

Our favorite 5 hacking items

1. Article of the week

Decrypting and analyzing HTTPS traffic without MITM

This article revisits a known technique for decrypting TLS traffic of mobile apps. It shows why Man-in-The-Middle is not always the best method, since bypassing certificate pinning or client certificate authentication can be complicated.

The idea is to use Frida to steal the session key, sniff traffic with Wireshark and decrypt it in real time by providing Wireshark with the session key, and finally import the requests to Burp using the PDML importer for Burp Suite.

2. Writeup of the week

DOM XSS in Gmail with a little help from Chrome (Google, $5,000)

This is a cool DOM XSS found in Gmail. So, no recon, no looking for obscure or forgotten subdomains. @opnsec used the main site, focused on the postMessage API and understanding how the different iframes communicate with each other.He used postMessage-logger to make cross-frames messages visible in DevTools, and analyzed the different requests and JS code to get a working PoC.Moral of the story: DOM XSS is still a thing, complicated front-end code like Gmail's won't be confusing if you know exactly what to focus on (e.g. postMessage), and if DevTools is lacking a feature, develop your own extension!

3. Videos of the week

– James Kettle (albinowax) Talks About Request Smuggling, Security Research, Hacking, and More!

– API hacking for the Actually Pretty Inexperienced hacker with Katie Paxton-Fear – OWASP DevSlop

The first one is an interview of @albinowax. Anyone interested in Web app hacking, bug bounty or security research should watch it. He talk about his learning process, how he leverages automation and bug bounty for research, how he chooses research topics, etc.The second video is a talk by @InsiderPhD on API hacking. She shares her approach, the bugs to look for, with demonstrations using a custom vulnerable API.

4. Tool of the week

Transformations

Transformations is a new tool by @jobertabma that helps find out how inputs are transformed by Web apps. For instance, let's say that a server responds with `c1aa46d751f1ffa58481418667134109ac5f573c`, when you give it `test`. Feeding both strings to the tool will tell you that the transformations performed are `stringReverse(sha1(md5(md5("test"))))`.This can be useful for building payloads that bypass WAFs, or understanding seemingly random strings.

5. Tips of the week

Hackluke's hacking advice:- How to ACTUALLY get started with bug bounties– How to pick your first bug bounty program– What tools can you use to find critical vulnerabilities easily?– Do you need to be able to code to find bug bounties?– Which vulnerability should you learn first?!– What are the best resources for beginner hackers?– COMMUNITY. IS. IMPORTANT.– There is such thing as too much recon– How to stop finding duplicates– Abusing the "first mover advantage" in bug bounties– One of my best hacking tips: NEVER ASSUME ANYTHING!

These are the sweetest tips for bug hunters. @hakluke started tweeting short videos, each answering a specific question like the ones above. I love that he tells concise, no BS truths, in a light tone, the way only a real friend would do.

Make sure to follow him on Twitter to get any new ones!

Other amazing things we stumbled upon this week

Videos

- Android Directory Traversal Exploitation & Vulnerable app
- BOUNTY THURSDAYS – SSRF, OneForAll, tryhackme, Postmessage-tracker, LEVELUP0x06
- How to Build a Pentest Dropbox
- Introduction to CSRF

- Discord Hangout: AMSI Bypasses with Magic Unicorn and Defenses with David Kennedy
- Tips for an Information Security Analyst/Pentester- Ep.85: Weaponizing Windows Binaries (LOLBAS & C)
- Pentesting with Evil WinRM – Practical Exploitation

Podcasts

- Security Now 765 – An Authoritarian Internet?
- News Wrap: Microsoft Sway Phish, Malicious GIF and Spyware Attacks
- Python Pickling, Sophos 0-Day, & AWS RDS MySQL – PSW #649
- Psychic Paper, Salt RCE, & Love Bugs – ASW #106
- Learn how to write bug bounty reports that stand out!
- Layer 8 Podcast Episode 24: OSINT AMA with Noneprivacy and Ding0snax

Webinars & Webcasts

- HelSec virtual meetup #1
- SQL Server Hacking Tips for Active Directory Environments
- Linux Command Line Dojo II – Return of the Sensei
- Webinar 3 Passive recon – Tyrone Wilson
- SANS webinars
  - Develop Technical Recall Skills: Spaced Repetition with Anki
  - Mobile Assessments : Attack Surface and Frameworks
  - Multi-factor authentication bypass techniques you need to know about.
  - Adversary emulation using CALDERA – Building custom plugins – Part #3

Conferences

- DERPCON 2020 Red Team Track, Blue Team Track & Tales from the Trenches
- AirGap2020
- DISC – SANS ICS Virtual Conference

Tutorials

Medium to advanced

- Security of Data processing libraries Part 1, Part 2 & Set of exploits for data processing open source libraries
- Introduction to GCP Privilege Escalation & Part 2
- Bypass Instagram SSL Certificate Pinning for iOS
- Post-Exploitation: Abusing Chrome's debugging feature to observe and control browsing sessions remotely
- Windows authentication attacks part 2 – kerberos
- Abusing Kerberos Resource-Based Constrained Delegation
- T1111: Two Factor Interception, RSA SecurID Software Tokens

Beginners corner

- Towards a Quieter Burp History
- Closing the Loop: Practical Attacks and Defences for GraphQL APIs
- Getting Started API Penetration Testing with Insomnia
- Bypassing SSRFs like a King
- Developing with VBA for Script Kiddies
- What Are Format String Vulnerabilities?
- A crash course into WPA Enterprise security and deployment
- How to Type Less and Do More in Terminals

Writeups

Pentest writeups

- SQL Injection and Postgres – An adventure to eventual RCE

Responsible(ish) disclosure writeups

- "Psychic Paper" #IoS
- Remote Command Execution on RemotePC for Windows #MiTM #RCE
- Instacart Patches SMS Spoofing Vulnerability Discovered by Tenable Research #Web
- Pentesting Cisco SD-WAN Part 2: Breaking routers #Linux #PrivilegeEscalation
- A simple way to break into Cisco Webex Meeting Rooms!! #Web
- SSD Advisory – Unauthenticated Access API Key Access leads to RCE #Java #RCE #CodeReview

Bug bounty writeups

- Potential stored Cross-Site Scripting vulnerability in Support Backend (HackerOne)
- Character limitation bypass can lead to DoS on Twitter App and 500 Internal Server Error (Twitter, $560)
- Remote Code Execution via Insecure Deserialization in Telerik UI
- DOM-Based XSS at accounts.google.com by Google Voice Extension. (Google, $3,133.7)
- Hacking Razer Pay Ewallet App (Razer, $6,000)
- A tale of verbose error message and a JWT token
- DOM XSS Walkthrough
- How we Hijacked 26+ Subdomains

See more writeups on The list of bug bounty writeups.

Tools

- Differer: Finds how URLs are parsed by different languages in order to help bug hunters break filters
- Fridax: Enables you to read variables and intercept/hook functions in Xamarin/Mono JIT and AOT compiled iOS/Android apps
- gwen001/wordgrab.sh: Create a wordlist from the target itself
- hussein98d/ssrf.sh: Bash script that takes a domain name and a callback server, parses links, appends SSRF parameters & fires the requests
- OneForAll: A Powerful Chinese Subdomain Enumeration Tool
- vmdkReader: .NET 4.0 Console App to browse VMDK images and extract files
- Slack Watchman: Monitoring Slack workspaces for sensitive information
- Whispers: Identify hardcoded secrets and dangerous behaviours
- NSDetect: A Python Utility To Detect AWS NS Takeover
- vps_setup/offensive_script.sh: Auto deployment of VPS
- Evil SQL Client (ESC) & Introduction
- nmap-query-xml: Python tool to query nmap xml files in the terminal
- YAS (Yet Another Sniffer): A Scapy-based network analyzer
- SharpHose: Asynchronous Password Spraying Tool in C# for Windows Environments
- SSH PuTTY login bruteforcer: Turn PuTTY / Plink into an SSH login bruteforcing tool

Misc. pentest & bug bounty resources

- Gf-Patterns
- Cookie database
- Getting Started with OAuth and OpenID Connect
- Awesome Bugbounty Writeups
- @securibee's bug bounty twitter list & Creators list
- Project TJ-JPT
- Advanced Wireless Attacks Against Enterprise Networks (AWAE)
- Docker Security Playground

Challenges

- Intigriti May XSS Challenge: Until May 17
- CYBAR OSINT CTF: June 6
- puzzle.nahomies.com & Walkthrough
- 5 minute Express.js Web Security challenge, Level 2 & Level 3
- GitHub Security Lab CTF 4: CodeQL and Chill – The Java Edition: Until June 12

Articles

- Exploring macOS Calendar Alerts: Part 1 – Attempting to execute code
- PrintSpoofer – Abusing Impersonation Privileges on Windows 10 and Server 2019 & PrintSpoofer
- From NETWORK SERVICE to SYSTEM
- Crossing Trusts 4 Delegation

News

Bug bounty & Pentest news

- Black Hat and DEF CON security conferences go virtual due to pandemic
- Azure Sphere Security Research Challenge Now Open
- Kicking off the Azure Sentinel Hackathon!
- Polymorphic payloads: New image processing test suite snags Google Scholar
- Second Order Chaos Presents: Bucks For Belize: May 15

- Hacker Days: FRIDA — Inside Mobile App Reverse Engineering: May 14
- Did you know @metasploit recently added functionality for creating .NET Deserialization payloads like #YSoSerialNet does?

Reports

- Video killed the conferencing star
- Mandiant Security Effectiveness Report 2020
- ATT&CK Evaluation results: visual perspective
- Microsoft: 150 million people are using passwordless logins each month

Vulnerabilities

- Samsung patches 0-click vulnerability impacting all smartphones sold since 2014
- Air gap security beaten by turning PC capacitors into speakers
- If you miss the happier times of the 2000s, just look up today's SCADA gear which still have Stuxnet-style holes
- Airplane Hack Exposes Weaknesses of Alert and Avoidance Systems
- Oracle warns of attacks against recently patched WebLogic security bug
- JQuery XSS vulnerability affects other apps, warns security researcher
- Gmail XSS vulnerability placed under the microscope

Breaches & Attacks

- Salt framework security flaws used to attack multiple targets
- CAM4 adult cam site exposes 11 million emails, private chats
- GoDaddy hack: Miscreant goes AWOL with 28,000 users' SSH login creds after vandalizing server-side file
- Hackers sell stolen user data from HomeChef, ChatBooks, and Chronicle: They also claim hacks of Microsoft's private github repos, Tokopedia & Unacademy
- Hackers breach company's MDM server to spread Android malware
- Massive campaign targets 900,000 WordPress sites in a week
- Now we know what the P really stands for in PwC: X-rated ads plastered over derelict corner of accountants' website
- New Kaiji malware targets IoT devices via SSH brute-force attacks
- Hacker Bribed 'Roblox' Insider to Access User Data

- Game patch gives hackers access to development content on Amazon S3
- A passwordless server run by NSO Group sparks contact-tracing privacy concerns

Other news

- Google Authenticator app gets a much needed update, but only on Android
- New Firefox service will generate unique email aliases to enter in online forms
- Xiaomi tracks private browser and phone usage, defends behavior
- It has been 20 years since cybercrims woke up to social engineering with an intriguing little email titled 'ILOVEYOU'
- Zoom acquires encryption startup Keybase
- GitHub showcases new code-scanning security tools at virtual event
- UK NCSC to stop using 'whitelist' and 'blacklist' due to racial stereotyping
- FYI: Your browser can pick up ultrasonic signals you can't hear, and that sounds like a privacy nightmare to some

Coronavirus

- Apple-Google COVID-19 virus contact-tracing API to bar location-tracking access
- Cyber volunteers release blocklists for 26,000 COVID-19 threats
- Surprise surprise! Hostile states are hacking coronavirus vaccine research, warn UK and USA intelligence

Non technical

- Undetected e.02 recap: Fredrik N. Almroth – Bug Bounties
- Things to do at home – Pandemic Movies
- Effective Vulnerability Report Writing — Quick Triages to Bonus $$$ (Always a Win)
- Why You Fail at Bug Bounties
- PWK Gone Rogue (A PWN Story)
- Getting Your First job in OSINT
- Housemates. The new Red Team?
- Let's Play Virtual Sticker Swap!!! & #virtualstickerswap

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 05/01/2020 to 05/08/2020.

Curated by Pentester Land & Sponsored by Intigriti