Bug Bytes #69 – @FransRosen's postMessage tracker, the @zseano files & SSRF in e-mail addresses

BY INTIGRITI · MAY 5, 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 24 of April to 01 of May.

Our favorite 5 hacking items

1. Tools of the week

- postMessage-tracker
- semgrep

postMessage-tracker is a Chrome extension presented by @fransrosen in his "Attacking Modern Web Technologies" talk. It monitors postMessage listeners in all subframes of the window and logs everything, helping find postMessage issues such as XSS and data extraction bugs.

Semgrep is like grep but for code. Both hackers and developers can use it to detect vulnerabilities by looking for anti-patterns in code. Here are two examples of patterns to look for in Go: 1 & 2. Languages supported are Python, JavaScript, Go, Java, C, and soon PHP and Typescript.

2. Writeup of the week

- Piercing the Veal: Short Stories to Read with Friends

This is a very well-written and informative writeup on SSRF. @d0nutptr shares what he looks for when testing SSRF, and 5 interesting bugs he found that earned hime more than $4,800 in total. My main takeaway is to start signing up to apps using Burp Collaborator emails like *user@abc123.burpcollaborator.net*.

If you receive an HTTP request in addition to the expected SMTP message (email), there is potential for SSRF.

3. Videos of the week

- Finally! HOW TO solve the INTIGRITI Easter XSS challenge using only Chrome DEVTOOLS!
- Mindset hacking with zseano – What am I thinking when I hack?

- Mayonaise Talks About His Recon Workflow, How to Learn Different Topics, and How to Bug Bounty!
- Mental Hacking 4 Better Bounties

Hackers are sharing so much good stuff these days! In this week's must-see videos:

@securinti solves Intigriti's latest XSS challenge. He based it on a bug found in a live hacking event, and shares so many cool tips on using Chrome DevTools.

@zseano hacks a Web app live and thinks out loud, sharing his mindset and approach.Mayonaise talks about his recon workflow and hacking approach, automation, learning process...

@stokfredrik shares advice on how to learn new skills, and dealing with duplicates. Personal development applied to hacking!

4. Non technical items of the week

- Raising your web hacking/bug bounty hunting game
- Bug Business #3 – Zseano's notes on hacking & mentoring

These are two interesting reads that can help get into a successful bug hunting mindset. @zseano is interviewed about his unique approach and experience, and @sharathsanketh shares some of his realizations as a beginner bug hunter trying to up his game.

5. Resources of the week

- Mobexler's Mobile Application Penetration Testing Checklist
- Daily-commonspeak2

Daily-commonspeak2 is an unofficial repo for Commonspeak2 wordlists generated daily. Useful for subdomains recon!

The mobile testing checklist covers both iOS and Android. I like its simple format that helps remember everything to test for, with references and the tools needed.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays – Automation, xss challenge, Getallurls, Burp Suite 2020.4, Logger++, hacker101.com
- Free Tools! How to Use Developer Tools and Javascript in Webapp Pentests
- How Deep Link RCE is possible on Android applications
- Switching To ZSH

- Interview With A 15 Year Old Bug Bounty Hunter
- Docker Security Failures
- VbScrub tutorials

Podcasts

- Darknet Diaries EP 64: The Athens Shadow Games
- How I approach a bug bounty program with this #bugbounty methodology & Transcript
- Security Now 764 – RPKI
- Risky Business #581 — Chinese telcos under fire in USA, spy firms pitch COVID-19 surveillance
- Hacked Off? 059. – Mike Jones: Anonymous, Suits, and Building Better Security
- Security Weekly News #28 – 0 Day Extravaganza, Zoom Can't Win, & Starbleed – Wrap Up
- Security Weekly News #29 – Shade Ransomware, FBI Warnings, & SCADA Attacks
- Application Security Weekly #105 – Nintendo Breach, NSA Advisory, & Security of IoMT
- Paul's Security Weekly #648 – iOS Mail Hijack, Hacking Satellites, & 0-Days for Days

Webinars & Webcasts

- Android App Reverse Engineering LIVE! – Part 1
- GitHub Security Lab Today (23-Apr) 4-7PM PT
- IDOR – what, where and how? – Vatika Mittal
- Kubernetes Post-Exploit – Live Code Session
- Q&A: Mental Health While Staying at Home
- IoT Hacking 101 – Firmware Funhouse! (Free registration required)

Conferences

- BSides Knoxville 2020 – Track 1 Live Stream, Track 2 & Schedule
- NSConclave 2020
- SARCON 2020 – DAY 3 – SECARMY
- HITB Lockdown & Slides
- HellaConf 2020

Tutorials

Medium to advanced

- Content Type Forcing – The XSS you may have missed.
- So, you can read WEB-INF/web.xml. How can you escalate this issue?
- Introducing Slacker: Monitoring subdomain additions in real time and automating directory scanning
- Abusing docker.sock exposure
- Remotely Host MSBuild Payloads
- Staying Off the Land: A Threat Actor Methodology
- Masquerading Windows processes like a DoubleAgent.

Beginners corner

- Let's break into Payment Gateways
- Subdomain Takeover via GitHub steps [Point to IP Address] (Video)
- Subdomain Takeover via AWS Elastic Beanstalk with steps (Video)
- How to hook Android Native methods with Frida (Noob Friendly)
- Terminal Escape Injection
- Privilege Escalation in Windows
- Old Tricks Are Always Useful: Exploiting Arbitrary File Writes with Accessibility Tools
- RCE on Windows from Linux Part 1: Impacket
- Windows DLL Hijacking (Hopefully) Clarified

Writeups

Pentest writeups

- From directory deletion to SYSTEM shell
- Exploiting JD bugs in crypto contexts to achieve RCE and tampering with Java applets

Responsible(ish) disclosure writeups

- E-Learning Platforms Getting Schooled – Multiple Vulnerabilities in WordPress' Most Popular Learning Management System Plugins #Web #CodeReview
- CVE-2020-0932: Remote Code Execution on Microsoft SharePoint Using TypeConverters #Deserialization #RCE #Web #CodeReview

- Exploiting GlobalProtect for Privilege Escalation, Part One: Windows #Windows #PrivilegeEscalation #VPN #RCE
- Stealing your SMS messages with iOS 0day #iOS
- Exploiting Feedback Hub in Windows 10 # Windows #PrivilegeEscalation
- Open the Gates! The (In)Security of Cloudless Smart Door Systems #IoT
- Duplicated Vulnerabilities in WordPress Plugins #Web

Bug bounty writeups

- Arbitrary file read via the UploadsRewriter when moving and issue (GitLab, $20,000)
- Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams (Microsoft)
- Reflected XSS and sensitive data exposure, including payment details, on lioncityrentals.com.sg (Uber, $4,000)
- Stealing the Trello token by abusing a cross-iframe XSS on the Butler Plugin (Trello, $3,600)
- Researching Polymorphic Images for XSS on Google Scholar (Google, $9,401.1)
- Bitrix WAF bypass (Mail.ru, $300)
- [Bug Bounty Writeups] Exploiting SQL Injection Vulnerability ($2,000)
- Indirect UXSS issue on a private Android target app ($1,000)
- Account taken over in style !!!

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- github-secrets.py: Python script to do a regexp search on GitHub search results
- SonarSearch & Introduction: A MongoDB importer and API for Project Sonars DNS datasets
- VHosts Sieve: Searching for virtual hosts among non-resolvable domains
- Enemies Of Symfony (EOS): Debug mode Symfony looter
- @apps3c's ysoserial fork: Used to generate payloads for @Burp_Suite Java Deserialization Scanner. It adds time, DNS, OS-specific exec and reverse shell (@nickstadb) attack vectors, output transformation, xstream (Isaac Sears)
- download-networks.sh: Download all the Shodan data for a list of networks in a text file

More tools, if you have time

- Chrome Galvanizer & Introduction: A tool to generate Chrome enterprise policies to help users boost Chrome extension security
- CursedChrome
- Trishul: Burp Extension to hunt for common vulnerabilities including XSS, SQL injection & SSTI
- APKEnum & Introduction: A Python Utility For APK Enumeration
- WebIDL: New fuzzer to help identify security vulnerabilities in the implementation of WebAPIs in Firefox
- Nozaki: Security oriented HTTP fuzzer engine
- DevToolReader & Introduction: Python script that parses Indexeddb files – used to extract Firefox DevTools console history
- pwncat: Netcat on steroids with Firewall and IPS evasion, bind and reverse shell, local and remote port-forward
- SitRep: Extensible, configurable host triage
- jbosswidlyfly_to_hashcat.py: Python 3 script to convert JBoss/Wildfly user properties list to hashcat mode 20
- AzureADLateralMovement & Introduction: Bloodhound for Azure AD
- Pivotnacci: A tool to make socks connections through HTTP agents
- Wifipumpkin3: Powerful framework for rogue access point attack

Misc. pentest & bug bounty resources

- Daily-commonspeak2
- Mobexler's Mobile Application Penetration Testing Checklist
- @GochaOqradze's Jaeles signatures
- The XSS rat's Youtube channel
- Offensive Security Cheatsheet
- The Extended AWS Security Ramp-Up Guide
- Hunting for credentials and building a credential type reference catalog
- Kusto Query Internals – Azure Sentinel Reference
- Wireless Penetration Testing Cheat Sheet
- Windows-Priviledge-Escalation-Resources
- Active Directory Exploitation Cheat Sheet

Challenges

- Introducing BetaFast – NetSPI's Vulnerable Thick Client
- Damn Vulnerable WordPress

Articles

- Writing a scanner to find reflected XSS vulnerabilities — Part 1, Part 2 & Code
- Working-As-Intended: RCE to IAM Privilege Escalation in GCP Cloud Build
- What is old is new again: The Relay Attack
- Kerberos Tickets on Linux Red Teams & SSSDKCMExtractor
- Sharing a Logon Session a Little Too Much

News

Bug bounty & Pentest news

- Amazon's new VDP
- Hack Your Resumé Workshop @ #LevelUp0x06
- Bug Bounty Q&A #4: How does Intigriti optimize bug bounty success?
- Professional / Community 2020.4
- Introducing YSoSerial.Net April 2020 Improvements

Reports

- Microsoft: Ransomware groups continue to target healthcare, critical services; here's how to reduce risk
- Top Attacks Against Financial Services Organizations 2017–2019
- Kaspersky: RDP brute-force attacks have gone up since start of COVID-19
- Android OEM patch rates have improved, with Nokia and Google leading the charge
- We're going on a vuln hunt. We're going catch a big one: Researchers find Windows bugs dominate – but fixes are fast

Vulnerabilities

- What's worse than an annoying internet filter? How about one with a pre-auth remote-command execution hole and there's no patch?
- Microsoft Teams accounts could be hijacked via malicious GIFs & TL;DR

- Salt peppered with holes? Automation tool vulnerable to auth bypass: Patch now
- "Zero-click" mobile phone attacks – and how to avoid them
- In trying times like these, it's reassuring to know you can still get pwned five different ways by Adobe Illustrator files

Breaches & Attacks

- The 2020 URL Querystring Data Leaks — Millions of User Emails Leaking from Popular Websites to Advertising & Analytics Companies
- Sophos XG Firewall zero-day vulnerability gets patched & CVE-2020-12271: Sophos XG Firewall Pre-Auth SQL Injection Vulnerability Remediation Guidance and Exposure Overview
- GDPR.EU has er... a data leakage issue
- Sophisticated Android Spyware Attack Spreads via Google Play
- This new Android mobile malware targets banks, financial services across Europe
- Lucy malware for Android adds file-encryption for ransomware ops
- PerSwaysion Campaign – Playbook of Microsoft Document Sharing-Based Phishing Attack

Other news

- Twitter turns off SMS-based tweeting in most countries
- ICANN has voted to REJECT the sale of the .ORG registry to private equity firm Ethos Capital
- Shade (Troldesh) ransomware shuts down and releases decryption keys
- Here's the NSA's guide for choosing a safe text chat and video conferencing service
- Facebook-NSO lawsuit: Hundreds of WhatsApp attacks linked to one IP address
- NSO Employee Abused Phone Hacking Tech to Target a Love Interest

Coronavirus

- Cybersecurity professionals being sidetracked by coronavirus home-working drive
- Microsoft warns of malware surprise pushed via pirated movies
- Malicious advertising slingers up the ante during Covid-19 pandemic
- Split opens up in Europe on privacy control for Covid-19 contact-tracing apps
- Australian contact-tracing app leaks telling info and increases chances of third-party tracking, say security folks

Non technical

- YESWEHACK PROPHILE ON HISXO
- Honeysploit: Exploiting the Exploiters
- Payment Card Industry (PCI) – Recurring Requirements Require Attention!
- The Duality of Attackers – Or Why Bad Guys are a Good Thing™
- Why Cloud Is Impossible without Open Source
- A game changer technology – Quantum Security Series – Part 1
- InfoSec questions

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 04/24/2020 to 05/01/2020.

Curated by Pentester Land & Sponsored by Intigriti