Bug Bytes #10 – Command Injection, Sublert by @yassineaboukir & Bypassing XSS Detection

BY INTIGRITI · MARCH 19, 2019 · LAST UPDATED ON JULY 16, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 8 to 15 of March.

Our favorite 5 hacking items

1. Conference of the week

> "OWASP AppSec California 2019, especially:
> – An Attacker's View of Serverless and GraphQL Apps & Slides
> – Endpoint Finder: A static analysis tool to find web endpoints, Slides & EndpointFinder
> – Pose a Threat: How Perceptual Analysis Helps Bug Hunters & Slides
> – Creating Accessible Security Testing with ZAP & Slides
> – Cache Me If You Can: Messing with Web Caching & Slides
> – Automated Account Takeover: The Rise of Single Request Attacks & Slides
> – Open-source OWASP tools to aid in penetration testing coverage & Slides
> – The Call is Coming From Inside the House: Lessons in Securing Internal Apps & Slides"

OWASP AppSec conferences are great for anyone interested in (both offensive and defensive) Web app security. This one is particularly good, as you can judge from the list of talks above that I'm planning to watch!
Some of the topics addressed are: extracting endpoints from JS files, FaaS & GraphQL security, Web Caching vulnerabilities, scaling visual identification for bug hunters, new features in ZAP, interesting OWASP tools for white box pentesting...
The only thing missing is the video/slides from workshops which look really interesting. Gonna have to go there myself some day!

2. Article of the week

> "Exploiting CVE-2018-1335: Command Injection in Apache Tika"

Have you ever found an open port on a target, and the service's version had a CVE but no disclosed exploit? This might happen a lot, especially on (internal) pentests where the number of open ports is generally higher than during bug bounty.
This article is a great example of you how to reverse engineer the patched version and locate the vulnerability – an RCE in this case, using **diff** (or **rcdiff**).

3. Tool of the week

> "Sublert & Introduction"

This is a new recon tool by @yassineaboukir who also wrote Asnlookup. They're both very handy tools for bug hunters.
Sublert monitors changes in CT logs, and notifies you via Slack when a new SSL/TLS was issued for the organization you're monitoring.
What's new compared to existing CT monitoring tools like Facebook's CT tool or CertSpotter is that it was created by a bug hunter for bug hunters. It won't spam you with irrelevant results, you can enable DNS resolution, disable monitoring for specific domains, and since it's in Python, you can integrate it with any bug hunting (automated) scripts you are already using.

4. Slides of the week

> "Pwning mobile apps without root or jailbreak"

This is an awesome presentation if you're into mobile app testing! It's understandable even without video.
The question answered is: how do you test the security of an app if for some reason you can't use a rooted/jailbroken device?
This happens when the app refuses to run on a rooted device, or when it requires an iOS version that doesn't have a public jailbreak.
Solutions explained including commands and resources are:

- For Android, modify the APK, enable backups, enable debugging, repackage the app, bypass certificate pinning manually using grep, bypass root detection manually, or do the same thing using Frida
- iOS repackaging or use Frida
- Use Objection (wrapper around Frida)

5. Resource of the week

> "Bypassing XSS Detection Mechanisms"

This is a great resource for learning how to bypass WAFs for XSS, by the author of XSStrike & Photon.
I often see people sharing complex XSS payload on Twitter. But without context, I don't find them very useful. This paper is a much better resource for understanding what filters do and how to bypass them with a solid methodology, as opposed to randomly running a list of payloads.
The steps proposed are:

1. Determining the payload structure based on the context where you are injecting (HTML inside or outside tag, JavaScript...)
2. Probing to determine the regex used
3. Obfuscation

Other amazing things we stumbled upon this week

Videos

- Snyking in – regular expression denial of service vulnerability exploit in the ms package #ReDoS
- 10 Minute Tip: Certificates: The OSINT Gift that Keeps on Giving...
- Python: XSS using SVG file
- Exploring Virustotal (Whitehat Foundation Series)
- Insider Threats Get Mean, Nasty and Very Personal
- RSAC 2019 – PenTest vs. RedTeam – Different or the Same? What is Purple Teaming?

Podcasts

- SPOILER – Security Now 705
- Sophos podcasts Ep. 023 – Facebook promises and Google Chrome patches [PODCAST]
- Absolute AppSec Ep. #50 – Eric Heitzman
- Security In Five Episode 449 – Citrix Hack Was Done Through Password Spraying, What Is That
- Overview of Hacking – Secure Digital Life #101
- Iranian APT, Equifax, & Crowdfense – Hack Naked News #210
- Application News – Application Security Weekly #53
- Tesla, YouTube, & Sexy Selfies – Paul's Security Weekly #597

Webinars & Webcasts

- Why You Need to CYA... Cover Your Apps!

Conferences

- Nullcon Goa 2019:
  - Getting to $10,000 – How you can craft your reports for higher impact and bigger bounty awards
  - Interview with Robert Baptiste aka Elliot Alderson [@fs0c131y] by Antriksh Shah
- Can I hack your android app, please? (in French, no English subtitles yet

Slides only

- Pwning mobile apps without root or jailbreak
- DevSecCon Singapore 2019, especially:
  - Burp Suite Extension Writing Workshop
  - Web Services aren't as secure as we think
  - An attacker's view of Serverless and GraphQL apps

Tutorials

Medium to advanced

- Burp Extension Python Tutorial – Generate a Forced Browsing Wordlist
- ClickAnywhere: An Advanced Clickjacking Script & clickjacking_full.html
- Using Terraform to set up a VPC with vulnerability scanners (Tenable Nessus & Rapid7 Nexpose)
- Automating GHIDRA: Writing a Script to Find Banned Functions
- Day 74: From PHP (s)HELL to Powershell Heaven
- Day 72: Monitor Nix Processes for Privilege Escalation Opportunities

Beginners corner

- API Penetration Testing with OWASP 2017 Test Cases
- NMAP Tips: RTFM?
- Finding S3 Buckets by accident....
- How to Discover MongoDB and Elasticsearch Open Databases
- Certificates: The OSINT Gift that Keeps on Giving...
- Web Hacking with Burp Suite (Part 3: The Power of a Proxy)
- Automobile Hacking, Part 5: Hacking the Car Alarm Systems to Take Control of the Vehicle
- Penetration Testing Active Directory, Part II
- MouseJack: From Mouse to Shell – Part 2
- Day 70: Hijacking VNC (Enum, Brute, Access and Crack)
- Day 69: Hijacking Tmux Sessions 2 Priv. Esc.

Writeups

Challenge writeups

- Simple JWT hacking

Pentest writeups

- Escalating SSRF to RCE
- Tale of Account Takeover in Multiple Website

Responsible disclosure writeups

- StackStorm – From Originull to RCE – CVE-2019-9580 #RCE #CORS
- From RCE to LDAP Access #RCE #Ldap
- CVE-2019-0604: Details of a Microsoft SharePoint RCE Vulnerability #SourceCodeAnalysis #RCE
- A Saga of Code Executions on Zimbra #RCE
- Flexpaper <= 2.3.6 RCE #RCE
- Blind Cross-Site scripting to RCE in Cerberus FTP version 9 and 10 #RCE #BlindXSS
- WordPress 5.1 CSRF to Remote Code Execution # CSRF #RCE
- A Wormable XSS on HackMD! (Original in Chinese) #XSS
- How I hacked my Xiaomi MiBand 2 fitness tracker — a step-by-step Linux guide by Andrey Nikishaev #BLE #IoT

Bug bounty writeups

- RCE on Steam client (Valve) via Buffer Overflow on server ($18,000)
- Blind SSRF in OAuth on GitLab ($4,000)
- Stored XSS on Keybase ($3,000)
- SSRF on Shopify ($1,000)
- Path traversal on Vanilla ($900) #SourceCodeAnalysis
- SSRF escalated to RCE on private program
- Blind stored XSS on private program ($800)
- Stored XSS on Microsoft triggered by opening ppt file in iOS ($1,000)
- Password reset flaw on private program
- Authorization flaw, IDOR, XSS on Google (clever chain of bugs but strangely $0!)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Stepper: A natural evolution of the Repeater tool for Burp Suite! Create sequences of requests to simplify testing of multi-stage endpoints, and create regular expressions to define variables for use in later steps.

More tools, if you have time

- Graudit: Grep rough audit – source code auditing tool
- TLS-Attacker-BurpExtension: Tool based on TLS-Attacker to assist pentesters and security researchers in the evaluation of TLS Server configurations with Burp Suite
- VulEdiWi & Introduction: A tool to find all publicly editable Github wikis of an organisation and publish your demo page on it
- PandorasBox & Writeup: Find Enterprise Box accounts and enumerate for shared files and folders
- Goca: a [FOCA](https://github.com/ElevenPaths/FOCA) fork written in Go, which is a tool that finds metadata and hidden information in the documents its scans. These documents may be on web pages, and can be downloaded and analyzed with Goca
- HashSlack: Small utility script to notify via Slack about Hashcat's progress during a password cracking session & [How to specify which channel to use] (https://twitter.com/Sec_GroundZero/status/1104837509215911937
- Cat-nip: Automated Basic Pentest Tool – Designed For Kali Linux
- Initial scan: A tool for performing an initial, information-gathering scan of websites for penetration tests
- PWSP : ClickJack Test: Online tool to test if a given URL is vulnerable to clickjacking
- Frida-extract-keystore.py & Introduction: Automatically extract KeyStore objects and relative password from Android applications with Frida
- BuildReview-Windows: A PowerShell script for performing a build review of a Windows host
- Wesng](https://github.com/bitsadmin/wesng): Windows Exploit Suggester (based on *systeminfo*)
- RootOS: macOS Root Helper. Tries to use various CVEs to gain sudo or root access

Misc. pentest & bug bounty resources

- ArchiveBox: Open-source self-hosted web archive. Useful for archiving interesting writeps, tutorials, etc, in case they're taken offline (happens a lot!)
- OSINT Guide Part 2: Identified Personnel Reconnaissance

- Bountyhq.secapps.com: Pre-compiled Bug Bounty Recon Datasets
- Browser Side Channels
- Red Team Project & Github projects: Project sponsored by the Linux Foundation to help make open source software safer to use. Among other things, it includes offers meetups and open source cybersecurity tools for pentesters & red teamers
- Scylla: Passive port scans data & database dumps. Recently updated to include all historical results from PunkSPIDER (5.5GB of webapp vulns).
- Mobilesecurity-docker: WIP Docker Image for Mobile Security Training and Assessments
- Hackle.dev: "Yet another Search Engine for hackers / security professionals. No JS, Privacy-Friendly, scalable, not unhackable. Doesn't use blockchain or A.I. but I like it." by @WawaSeb
- Day 73: OSCP Notes from IPPSEC OSCP Style Videos
- CFP Time: Never miss Call For Papers (CFP) for Security Conferences again!
- APIsecurity.io Issue 22: SANS SWAT list, 42Crunch Platform launch

Challenges

- WebsitesVulnerableToSSTI: Simple websites vulnerable to Server Side Template Injections(SSTI)
- XSS challenge & XSS in Limited Input Formats (Tutorial)
- Xss-game.appspot.com

Articles

- Transforming Self-XSS Into Exploitable XSS
- The Most Common Protocol You've Never Heard Of
- Bug Hunting Methodology(Part-2)
- How to write secure code? Protect yourself against Broken Auth & Session Management!
- How to write secure code? Protecting yourself against Injection Attacks!
- WHOIS XSS
- Further attack surface of WordPress PHAR injection: "In extended research about PHAR deserialization attack, we found roughly 300 WordPress plugins can be exploited to attack WordPress 4.9."
- How to Learn Penetration Testing: A Beginners Tutorial
- The Hitchhiker's Guide To Initial Access
- Day 73: OSCP Exam Tips

News

Bug bounty news

- @naffy close to be the third bug hunter millionaire!, following @BugBountyHQ & @santi_lopezz99
- Crowdfense, a company that buys zero day exploits from researchers and then sells them to government agencies, announced it is now offering a total of $15 million to hackers who have particular exploits for sale. On their site, they're selling it as bug bounty...
- On disclosure, confidentiality, and norms...

Breaches & Vulnerabilities

- Misconfigured Box accounts leak terabytes of companies' sensitive data
- Researchers Find Critical Backdoor in Swiss Online Voting System: "I don't think this was deliberate. However, if I set out to design a backdoor that allowed someone to compromise the election, it would look exactly like this."
- New Android adware found in 200 apps on Google Play: Malware masquerading as an ad-serving platform infected more than 200 legitimate apps
- Patched WinRAR Bug Still Under Active Attack—Thanks to No Auto-Updates
- UltraHack: The Security Risks of Medical IoT
- Citrix admits attackers breached its network – what we know: "a company estimated to manage the VPN access of 400,000 large global organisations"
- Hacked Sex Robots Could Murder People, Security Expert Warns
- MAGA 'Safe Space' App Developer Threatens Security Researcher](https://threatpost.com/maga-safe-space-app-data-leak/142771/
- Gearbest security lapse exposed millions of shopping orders: "Not only are the exposed orders a breach of customer privacy, the exposed data could endanger customers in parts of the world where freedom of speech and expression is limited"
- Threatlist: IMAP-Based Attacks Compromising Accounts at 'Unprecedented Scale'
- A legal analytics company exposed passwordless database with sensitive documents
- BEWARE – New 'Creative' Phishing Attack You Really Should Pay Attention To

Other news

- SANS reveals the top attacks for 2019 at RSA Conference: DNS hijacking, domain fronting, attacks against cloud services & DNS information leakage. But no Web vuln!
- Android Q privacy checklist: What's new in Android Q's privacy features
- ThreatList: Phishing Attacks Doubled in 2018

- World Wide Web marks its 30th birthday
- Two-thirds of all Android antivirus apps are frauds: “Only 23 Android antivirus apps had a 100 percent detection rate with no false positives”
- Fresh U.S presidential candidate @BetoORourke was a member of the country’s oldest hacking group, which has kept his role a secret for decades – until now: Not only was he one of the founding members of the cDc (Cult of the Dead Cow), but he also came up with the name!
- You left WHAT on that USB drive?!: Two-thirds of secondhand USB drives still contain previous owners’ data

Non technical

- Lessons from a Pen Test: The Power of a Well-Researched and Well-Timed Phishing Email
- Meet the Hacker: EdOverflow, motivated by community and knowledge sharing
- Meet our CTF master – Chamli
- The Zero Day Initiative

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 03/08/2019 to 03/15/2019.

Curated by Pentester Land & Sponsored by Intigriti