Bug Bytes #59 – Exploiting Insecure XML and ZIP File Parsers to Create a Web Shell, Low Competition Bug Hunting & RCE on Tesla

BY INTIGRITI · FEBRUARY 25, 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 14 to 21 of February.

Our favorite 5 hacking items

1. Video of the week

> "Low Competition Bug Hunting (What to Learn) – ft. #AndroidHackingMonth"

If you are discouraged by bug bounty and think all the bugs are gone, watch this. @InsiderPhD gives an awesome explanation of why it is not true, and what you need to do to start finding bugs.
I love her way of thinking. She deconstruct the question into several chunks and tackles one after the other: Which targets/industry to choose? Which assets and bugs to focus on? Which techniques to learn? How to interpret and use bug bounty statistics?

2. Writeups of the week

> "– A Tale of Two Formats: Exploiting Insecure XML and ZIP File Parsers to Create a Web Shell
> – RCE on https://beta-partners.tesla.com due to CVE-2020-0618 ($10,000)"

The first writeup is an excellent breakdown of common vulnerabilities of XML and ZIP parsers.
@spaceraccoonsec was able to find an XXE and RCE via ZIP path traversal.
Mastering classic techniques can be as lucrative as monitoring and testing for new ones, which is what @parzel2 did. He got an impressive bounty by reporting CVE-2020-0618 on Tesla only 1 day after it was published!
I am amazed at his monitoring and historic data management that probably allowed for this speed. But I'm also surprised that the bug was accepted since some programs do not reward for CVEs discovered too recently.

3. Podcast of the week

> "Darknet Diaries – Ep 59: The Courthouse"

This episode goes over what happened during the Iowa-Coalfire pentesters debacle.
This is a must for anyone who loves pentest stories, Darknet Diaries, and was concerned over this shocking incident.

4. Tool of the week

> "Rule-Based Highlighter Plugin for BurpSuite"

This Burp extension automatically highlights or add a comment to requests based on user-defined rules. Use cases suggested are interesting. The tool allows you to highlight specific status codes, differentiate user sessions for authentication and authorization testing, hide requests with specific HTTP methods (e.g. CORS preflight OPTIONS requests), facilitate SOAP services tests by adding comments, and highlight requests containing sensitive information.

5. Non technical item of the week

> "How to Achieve Your Most Ambitious Goals | Stephen Duneier"

Do you know the common point between learning German, crochet world records, knitting, hedge fund management, reading challenges, skydiving, and losing weight by hiking? Stephen Duneier did all that and much much more just by making marginal adjustments to his daily routine.
It is amazing to see these concrete examples of making really ambitious goals and breaking them down into manageable decisions. By making one small good choice after another, the unattainable becomes easily reachable.
I think this is the best approach and mindset whether you're struggling with bug bounties, some complex hacking techniques, time management, weight loss or anything.

Videos

- Subnetting Made Easy
- Wifi Hacking Games with MicroPython
- Introduction to Docker for CTFs
- Kallithea – exploit git clone functionality
- Building with Azure Devops, Gadget to jscript & GadgetToJScript
- HackerSploit – The Home Of Open Source Cybersecurity Training
- SSH Port Forwarding

Podcasts

- Security Now 754 – The Internet of Troubles
- Risky Business #573 — Gas plant ransomware attack, Huawei mega-indictment and more
- Quantum Crypto Chaos, Cloud Vulnerabilities, Turkish RATs and Julian Assange. – SWN #13
- Docker, 42 Vulnerabilities, Backdoors, Spying on 100+ Foreign Govs. – PSW #639
- Arduino Hacking with Seytonic

Webinars & Webcasts

- Modern Web Application Penetration Testing Part 2, Hash Length Extension Attacks
- Enterprise Recon For Purple Teams
- Hacking RPA -1(UiPath) -A(Local Components) & 0-Day Hacking RPA -1(UiPath) B(Remote Components)

Conferences

- Owning the cloud through SSRF and PDF Generators – Ben Sadeghipour and Chris Holt
- GOTO 2019 • Taking Security Seriously • Michael Brunton-Spall
- BlueHat IL 2020

Tutorials

Medium to advanced

- WAF Bypassing with Unicode Compatibility
- HTTP Request Smuggling – 5 Practical Tips
- Hacking AWS Cognito Misconfigurations
- Gaining Lateral Movement with SSH Password Sniffing
- Introduction To Modern Routing For Red Team Infrastructure – using Traefik, Metasploit, Covenant and Docker
- NTLM Relaying for gMSA Passwords
- Kerberos (III): How does delegation work?
- Persistence – RID Hijacking

Beginners corner

- Make Your Own Custom OSINT Bookmarklet Tools (p1)
- A technique that a lot of SQL injection beginners don't know
- Jailbreak and stuff!! Kickstart tools and techniques for iOS application pentesting
- Shodan Pentesting Guide

Writeups

Challenge writeups

- [Writeup] Split second & TL;DR

Pentest writeups

- DNS Exfiltration through Blind SQL Injection in a MS-SQL Environment Using Burp Collaborator

Responsible(ish) disclosure writeups

- CVE-2020-0618: RCE in SQL Server Reporting Services (SSRS) #RCE
- Checkmarx Research: Apache Dubbo 2.7.3 – Unauthenticated RCE via Deserialization of Untrusted Data (CVE-2019-17564) #RCE

- Exploiting Jira for Host Discovery #Web
- Combining DOM and reflected XSS to bypass input sanitation in Checkpoint.com #Web
- Critical Issue In ThemeGrill Demo Importer Leads To Database Wipe and Auth Bypass #Web #CodeReview
- BreakingApp – WhatsApp Crash & Data Loss Bug #XMPP
- Hackers Can Gain Active Directory Privileges Through New Vulnerability in Xerox Printers #LDAP #Printer
- Bypass Windows 10 User Group Policy (and more) with this One Weird Trick #Windows

Bug bounty writeups

- Filesystem Writes via `yarn install` via symlinks and tar transforms inside a crafted malicious package
- Email address of any user can be queried on Report Invitation GraphQL type when username is known ($8,500)
- From Recon to Optimizing RCE Results – Simple Story with One of the Biggest ICT Company in the World
- Exploiting WebSocket [Application Wide XSS / CSRF]
- Uploading Backdoor For Fun And Profit.

Tools

If you don't have time

- GadgetProbe & GadgetProbe: Exploiting Deserialization to Brute-Force the Remote Classpath: Probe endpoints consuming Java serialized objects to identify classes, libraries, and library versions on remote Java classpaths
- [EnumJavaLibs]_Remote Java classpath enumerator

More tools, if you have time

- BurpSuite Random User-Agents: Burp Suite extension for generating random user-agents
- GoSpider: Fast web spider written in Go
- Cve-api: Unofficial api for cve.mitre.org
- VTSCAN: Scan a file directly from your terminal using VirusTotal API
- TugaRecon: Fast subdomains enumeration tool for penetration testers
- XSS'OR: Hack with JavaScript
- Onedrive_user_enum & Achieving Passive User Enumeration with OneDrive: pentest tool to enumerate valid onedrive users
- Updog: A replacement for Python's SimpleHTTPServer. It allows uploading and downloading via HTTP/S, can set ad hoc SSL certificates and use http basic auth

- Online Brute Force WPA Cracking Tool – Kraken
- HTTP Asynchronous Reverse Shell
- OpenRelayMagic: Tool to find SMTP servers vulnerable to open relay
- icmpsh-s-linux: GNU/Linux version of the *icmpsh* reverse ICMP shell client

Misc. pentest & bug bounty resources

- OSWE/AWAE Preparation
- OSINT, Security, CTI, Social Engineering, Darkweb podcasts and more
- Phar Deserialization Exploit on CVE-2019-18889 Sample
- FREE hands-on OWASP Top 10 training Lab

Challenges

- 0l4bs: XSS labs

Articles

- Finding Python ReDoS bugs at scale using Dlint and r2c
  - https://www.reddit.com/r/netsec/comments/f6h1ij/finding_python_redos_bugs_at_scale_using_dlint/
- Attacking Jenkins
- Analysis of Network Security Configuration bypasses with Frida
- Exploring Microsoft Teams Rooms (MTR) Console as a Potential Attack Vector
- Attacker's Tactics and Techniques in Unsecured Docker Daemons Revealed
- Passwords are dead? Long live WebAuthn!
- How to Prevent the OWASP Top 10
- Getting What You're Entitled To: A Journey Into MacOS Stored Credentials

News

Bug bounty & Pentest news

- Meet the bug bounty platform putting community into crowdsourced security
- Top 10 web hacking techniques of 2019
- Next LevelUp Coming Soon!
- Sub-Technique Update Part Deux

Reports

- M-Trends 2020 Report

Vulnerabilities

- Security flaws belatedly fixed in open source SuiteCRM software
- Microsoft has a subdomain hijacking problem
- Windows, Linux Devices at Risk Due to Unsigned Peripheral Firmware
- CoTURN patches denial-of-service and memory corruption flaws

Breaches & Attacks

- Slickwraps says customer trust was 'violated' in data breach caused by glaring security holes
- Hacker Scheme Threatens AdSense Customers with Account Suspension
- Hackers exploit vulnerability in IOTA wallet to steal $1.6M
- Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum
- PAN enumeration attacks
- Phishing scammers pose as World Health Organization to exploit coronavirus fears
- Cybergang Favors G Suite and Physical Checks For BEC Attacks
- Over 20,000 WordPress Sites Run Trojanized Premium Themes
- Iranian hackers have been hacking VPN servers to plant backdoors in companies around the world

Other news

- Microsoft: Linux Defender antivirus now in public preview, iOS and Android are next
- New infrastructure will enhance privacy in today's Internet of Things
- How Saudi Arabia Infiltrated Twitter
- Protect yourself from coronavirus with a mask that looks like your face
- Facebook was repeatedly warned of security flaw that led to biggest data breach in its history
- Privacy Concerns Raised Over New Google Chrome Feature

Non technical

- LTR101: Writing or Receiving Your First Pentest Report
- The Difficult Decision to Switch Jobs
- Software Development Principals for Offensive Developers — Part 1 (Fundamentals)
- Sharenting, BYOD and Kids Online: 10 Digital Tips for Modern Day Parents
- The Science of A Great First Impression

- Ships can’t be hacked. Wrong

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 02/14/2020 to 02/21/2020.

Curated by Pentester Land & Sponsored by IntigritiThe views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.