Bug Bytes #8 – XML External Entities, Awesome WAF and Vulnreport

BY INTIGRITI · MARCH 5, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 22 of February to 1 of March.

Our favorite 5 hacking items

1. Webcast of the week

> "Top 10 Writing Mistakes in Cybersecurity and How You Can Avoid Them"

One of the first things I was told as a junior pentester was that writing a report is the most important part of a pentest. The reason is that even if you find the craziest vulnerabilities, they'll bring no value to the customer if you can't explain them clearly enough. Information like risks, impacts, how the bug works, and how to fix it must be crystal clear so that the client and developers know why they must fix the bug and how.
The good news is that writing good reports is not a magical art, it can be taught. This webcast by SANS has great tips on this topic. These are 10 mistakes to avoid and what to do instead. They apply whether you write your reports in english or any other language.
This is a must-read resource if want to improve the quality of your reports.

2. Writeup of the week

> "Typo in permission name allows to write contacts without user knowledge on Mail.ru ($150)"

I've never encountered this vulnerability type, so I thought it was very interesting. It is basically an Android app vulnerable to permission hijacking (the same idea link hijacking or subdomain takeover).
The app declares in its Manifest file the permission *write_contacts*. Then it defines a provider that gives access to the app's contacts database. The problem is that the provider definition uses the permission *write* which is not defined anywhere (instead of *write_contacts*).
So another malicious app could define this permission, using the same name and hence have access to the content provider. It could write contacts and users wouldn't see anywhere that the malicious app has this permission.

3. Resource of the week

> "Awesome WAF"

Wow, this is a pretty impressive collection on WAFs that @0xInfection open sourced this week. It contains:

- Fingerprints of almost all known WAFs (80+)
- Testing methodology for detecting WAFs

- Popular evasion techniques with examples
- Compiled list of known bypasses for WAFs
- Tools, research papers, blogs, writeups, videos & presentations

Also, the author recommends to keep an eye on it as he plans to update it regularly.

4. Tool of the week

> "Vulnreport & Tutorial"

This isn't a new tool, it's 2-year old. But I've just discovered it thanks to the tutorial above and it is the pentest reporting tool that I've been looking for.
It is a web app that you can self host and has great features: You can add applications (targets), multiple tests per application, vulnerabilities from custom defined vulnerability types, and a lot more (user roles, admin, exporting reports in PDF...).
Truth be told, I haven't tested it yet, but judging from the documentation and screenshots this is the most customizable and professional pentest reporting tool I've seen. And if it's still missing something you need, you can add it since it is open source.

5. Video of the week

> "XML External Entities ft. JohnHammond"

This is an excellent introduction to XXE. It's concise and contains most information you need to understand XXE and start hunting for it. The explanations include how XML works, what XXE is, the different types, how to detect it... It's very understandable even for people not familiar with XML.
Also, I love this quote:

> "'s' in 'xml' stands for 'security'"

Wait, there is no *s* in *xml*...!

Other amazing things we stumbled upon this week

Videos

- #1 GoodCode BadCode – XXE Code Review & Exploit | AppSec Academy
- Hacker101 – Android Quickstart
- HackerOne Hacker Inteviews: @smsecurity
- Snyking in – Directory traversal vulnerability exploit in the st package
- The Top 10 Things to Do After Installing Kali Linux on Your Computer & Tutorial
- Java: Random vs SecureRandom

Podcasts

- Security Now 703 Out in the Wild
- Sophos podcast Ep.021: Leaked calls, a social media virus and passwords exposed
- Hack Naked News #209: DNSSEC, TurboTax Hit, & DNS
- Application Security Weekly #52: Bugs, Breaches, and More!

Webinars & Webcasts

- BHIS Webcast: Endpoint Security Got You Down? No PowerShell? No Problem.

Conferences

- BSides Columbus 2019, especially:
  - Mobile App Vulnerabilities – The Bad, The Worse And The Ugly
  - API Security: Tokens, Flows and the Big Bad Wolf
  - Demystifying DMARC: A guide to preventing email spoofing
- Layer 8 Conference

Slides only

- Server-side template injection
- Hacking 101 Episode 2 – Web Recon
- Backdoors to the Kingdom: Changing the Way You Think about Organizational Reconnaissance
- Materials for Day of Shecurity Boston 2019 – Privilege Escalation Workshop
- Hack you a koober netty for great good
- Hacking the local internets

Tutorials

Medium to advanced

- Exploiting Regular Expressions
- Automate all the things! Postman + Python + Burp macros for the win — Part 1
- The RDP Through SSH Encyclopedia
- Setting up Frida Without Jailbreak on devices running Latest iOS 12.4

- OpenSSL Server Reverse Shell from Windows Client
- Modifying Empire to Evade Windows Defender
- Empire Domain Fronting With Microsoft Azure

Beginners corner

- How to Get Past The Wall Street Journal Paywall in a Few Seconds
- DNS & Web Enumeration Reference
- Commix-Command Injection Exploiter (Beginner's Guide)
- Getting Started with Kali Linux on Windows
- Post Exploitation on Saved Password with LaZagne
- Day 59: Windows API for Pentesting (Part 1)
- Day 60: Windows API Use in SpyEye Banking Trojan

Writeups

Pentest writeups

- Remote Code Execution — Gaining Domain Admin due to a typo

Responsible disclosure writeups

- SHAREit Multiple Vulnerabilities Enable Unrestricted Access to Adjacent Devices' Files & Exploit
- Video Downloader and Video Downloader Plus Chrome Extension Hijack Exploit – UXSS via CSP Bypass (~15.5 Million Affected)
- Host Header Poisoning in IBM Websphere
- Can your Printer Hack your Secrets: Appweb Authorization Bypass
- How To Spoof PDF Signatures

Bug bounty writeups

- SSRF in Slack ($500)
- Bypass of SSRF protection in Slack ($500)
- Web cache poisoning on Postmates ($500)
- CSRF on Instacart ($300)
- LFI & SSRF on private program
- Web Cache Deception leading to info disclosure on private program ($300)

- Information disclosure on sli.do ($150)
- Horizontal Privilege Escalation on Quora
- XSS & CSP bypass on Microsoft

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- AutoRecon
- GCPBucketBrute: A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated & Google Cloud Platform (GCP) Bucket Enumeration and Privilege Escalation
- Tarnish: A Chrome extension static analysis tool to help aide in security reviews & Introduction
- Yawast: Antecedent Web Application Security Toolkit, an app meant to simplify initial analysis and information gathering for penetration testers

More tools, if you have time

- Hell Blazer: Automated recon tool
- GenerateForcedBrowseWordlist.py: Burp extension that builds a wordlist for forced browsing from host(s) in the sitemap or for all in scope
- Tripped.it](https://tripped.it/): New tool to test for Blind XSS (commercial tool with a free version)
- Certrip: Subdomain recon tool for pulling Subject Alternative Names from hosts TLS certificates
- Sherlock: Find usernames across social networks (136 sites supported)
- SplunkWhisperer2 & Introduction: Local privilege escalation, or remote code execution, through Splunk Universal Forwarder (UF) misconfigurations
- Whori.sh: Bash script that attempts zone transfers for rwhois (i.e. scraping rwhois data from permissive environments)

Misc. pentest & bug bounty resources

- Advanced Recon Automation (Subdomains) case 1
- Does_email_address_exist.py: Useful Python script to know if an email address exists, based on Inti's Medium post
- APIsecurity.io Issue 20: Drupal APIs hacked, EU releases IoT standards
- List of resources for people asking "I want to get into information security, where do I start?"

- Building Virtual Machine Labs: A Hands-On Guide (Free book)
- The Ultimate Guide For Subdomain Takeover with Practical
- Awesome Frida
- Mobile Security Penetration Testing List
- Everything about XSS is in this source!
- Jenkins Master Post: A collection of posts on attacking Jenkins
- Reverse Shell Reference
- OffensiveCSharp: Collection of Offensive C# Tooling

Challenges

- HackerOne CTF for h1-702: "All of the information is included in that tweet"
- @s0md3v's XSS challenge

Articles

- Top 10 web hacking techniques of 2018
- Day 61: My Top 5 Web Hacking Tools
- Pushing Left, Like a Boss, Part 5.9 Error Handling and Logging
- Sound Hijacking – Abusing Missing XFO
- Thinking outside of the password manager box
- Exploiting Spring Boot Actuators
- WordPress 5.0 RCE detailed analysis
- The Stoic Approach To OSINT

News

Bug bounty news

- "Effective immediately, AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services."
- @klikkioy got $10,000 for a stored XSS in Yahoo Mail
- @try_to_hack Makes History as First Bug Bounty Hacker to Earn over $1 Million although he may not be the first
- Bugcrowd Announces Fourth Annual Buggy Awards Finalists

Breaches & Vulnerabilities

- Bug Allows Bypass of Face ID and Touch ID Authentication of WhatsApp iOS version
- Plain wrong: Millions of utility customers' passwords stored in plain text
- How a Hacking Group is Stealing Popular Instagram Profiles
- Drupal Vulnerability (CVE-2019-6340) Can Be Exploited for Remote Code Execution & WAF bypass
- Latest WinRAR Flaw Being Exploited in the Wild to Hack Windows Computers
- IIS Vulnerability Triggers a Denial-of-Service
- Padding Oracles: New padding oracle attacks against TLS with CBC. "We tried to get in contact with security teams via common BugBounty sites but had very bad experiences. Man-in-the-Middle attacks are usually out of scope for most website owners, and security teams did not know how to deal with this kind of issue. We lost a lot of "Points" on Hackerone and BugCrowd for reporting such issues"

Other news

- Full DNSSEC adoption needed to repel state-sponsored DNS hijackers – ICANN
- New flaws in 4G, 5G allow attackers to intercept calls and track phone locations
- WordPress 5.1 launches with Site Health security feature: "WordPress 5.1 will start showing notices to administrators of sites that run on long outdated PHP versions"

Non technical

- Salary Negotiation Tips from White Men in Tech: Part 2
- Information Security Assessment Types
- Just My Routine As A Remote Worker
- Interview With the Developer of Spiderfoot – Steve Micallef
- End User Security Cheatsheet

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 02/22/2019 to 03/01/2019.

Curated by Pentester Land & Sponsored by Intigriti