Bug Bytes #29 – Why do Penetration Testing Teams Hate You, SSL/TLS vulnerabilities & A Deep Dive into XXE Injection

BY INTIGRITI · JULY 30, 2019 · LAST UPDATED ON JULY 31, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand.** Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

This issue covers the week from 19 to 26 of July.

Our favorite 5 hacking items

1. Tutorial of the week

> "Markdown For Penetration testers & Bug-bounty hunters"

This is an excellent tutorial on how to organize your pentest and bug bounty notes using a static website created with Mardown and Mkdocs.
I know... SwiftnessX and many other options already exist for taking notes. Why this one too?
Well, it's worth trying if you're looking for a self-hosted solution, want to use or learn markdown, want to share your notes with the world or make your site private, want a lightweight web-based tool to access your notes from any device...

2. Writeup of the week

> "Pwning child company to get access to ParentCompany's Slack Team"

Going out of scope while pentesting or bug hunting is a big no-no. You could end up with legal issues or upsetting your client/target. But it is sometimes tolerated in bug bounty, when the bug is critical or when it impacts an in-scope target.
That's what happened here: @Parth_Malhotra saw that he could sign up to his target's Slack URL either with a @parentcompany.com or @childcompany.com email address.
He looked at childcompany.com and found a cPanel on it. So if he could find an RCE on this server, he would use cPanel to edit the server's MX records and hijack emails sent to @childcompany.com.
Receiving these emails would allow him to access parentcompany.com's Slack (the in-scope target).
This scenario is exactly what ended up happening. I love how @Parth_Malhotra went backwards from a desired goal (Slack), to a needed vunerability (RCE). This is way more impactful than if he was just looking for a technical bug without thinking about business risk.

3. Webinar of the week

> "A BEAST and a POODLE celebrating SWEET32 **(Free registration needed)"**

SSL/TLS vulnerabilities can be a headache when you're writing a pentest report.
There's a lot of them like: POODLE, BEAST, BREACH, CRIME, DROWN, FREAK, SWEET32, etc. Some of them are really critical, but others are complicated to exploit in real life. So which ones are real threats? Should you report them as low/high findings, or not report them at all…?
If you're familiar with these questions, this webinar will help you have a better understanding of each vulnerability.

4. Video of the week

> "Live Bug Bounty Recon Session on Yahoo (Part 1 – 7/14/2019)"

@nahamsec is now doing a live on Twitch every sunday. They're usually great for bug hunters or anyone interested in Web app security testing.
This one shows Ben live hacking on Yahoo (with their permission). It's a unique opportunity to see a bug hunter in action and learn things like: how he uses a VPS for recon automation, how he does recon in a structured way on a target that has thousands of subdomains, how he uses crt.sh and certspotter.com, etc.
Weird confession: I (really) hate Twitch! So I wait for the streams to become available on Youtube. But you don't have to, here is Ben's Twitch account.

5. Non technical item of the week

> "Why Does the Penetration Testing Team Hate Me?"

Relationships between pentesters and developers can be tense for so many reasons: pentesters with a superior know-it-all attitude, developers who aren't briefed on the purpose of the pentest and their role in it, developers who aren't aware of security issues, or fear for their job…
If you've ever been in an opening/closing pentest meeting and felt such tensions, this article could help you understand the mindset of some developers. You'll also have ideas on how to deal with each situation or objection you are facing.

Other amazing things we stumbled upon this week

Videos

- Bugcrowd Researcher Frans Rosen on collaboration, on Bug Bashes & on his approach to bug hunting
- Cross-Site Websocket Hijacking
- Teaching my Wife Linux

Podcasts

- Security Now 724 – Hide Your RDP Now!
- Risky Business #549 — FSB contractor breached, Equifax fined, NSO Group targets cloud
- Darknet Diaries Ep 43: PPP
- 7MS #373: Tales of Pentest Fail #2
- Hack Naked News #228
- Business Security Weekly #137 – Leadership Articles
- Application Security Weekly #70 – Application News
- Sophos podcast Series 2 launch episode – RDP exposed

Webinars & Webcasts

- Tips, Tricks, and Cheats Gathered from Red vs. Blue Team-Based Training (Free registration needed)
- Cloud Security and the Myths Around it.
- Life in Containers: The Big Picture by Pankaj Mouriya & GitBook

Conferences

- BSides Liverpool 2019
- ReconPi –
- The Good, The Bad And The Ugly Of Responsible Disclosure

Tutorials

Medium to advanced

- A Deep Dive into XXE Injection
- WebSocket Passive Scan using scripts with ZAP: New websockets add-on now available with passive scanning support
- A Pentesters Guide – Part 4 (Grabbing Hashes and Forging External Footholds)
- Insecure Deserialization: Finding Java Vulnerabilities with QL
- Browser plug-in
- Unhide a Hidden GPO
- MacOS Red Teaming 206: ARD (Apple Remote Desktop Protocol)

Beginners corner

- Dancing with OAuth: Understanding how Authorization Works
- Verifying SSL/TLS configuration (part 1)
- ExifTool : A Meta-Data Extractor
- Using Burp Suite with Android devices
- Exploiting JBoSS like a BOSS
- Using Lampyre for Basic Email and Phone Number OSINT

Writeups

Challenge writeups

- CVE-2019-8658 – Pwning Webkit.

Pentest writeups

- Axway SecureTransport 5.x XML Injection / XXE
- Exploiting UN-attended Web Servers To Get Domain Admin – Red Teaming
- Stories from the Shell: Episode One

Responsible(ish) disclosure writeups

- Axway SecureTransport 5.x Unauthenticated XML Injection / XXE
- InterSystems Cache 2017.2.2.865.0 and 2018.1.2 Multiple Vulnerabilities
- Livebox 3 – Weak password reset procedure
- LibreOffice – A Python Interpreter (code execution vulnerability CVE-2019-9848)
- Jackson gadgets – Anatomy of a vulnerability
- Apple bleee. Everyone knows What Happens on Your iPhone
- CVE-2019-7839: ColdFusion Code Execution Through JNBridge

Bug bounty writeups

- Information disclosure via GraphQL
- Authorization flaw on GitLab ($1,000)
- Race condition on HackerOne ($500)
- LFI on Google

- Clickjacking, XSS & DoS ($12,000)
- XSS to RCE on Github
- XSS on Twitter ($1,120)
- SQL injection
- Payment tampering

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Otxurls: Fetch known urls from AlienVault's Open Threat Exchange for given hosts
- O365-attack-toolkit & Introduction: A toolkit to attack Office365
- Graphql-introspection-analyzer.py: @gwendallecoguic's quick & dirty script to easily view GraphQL introspection results
- Hvazard Dictionary Modifier: Remove short passwords & duplicates, change lowercase to uppercase & reverse, combine wordlists!

More tools, if you have time

- CCrawlDNS: Retrieves unique subdomains for a given domain name from the CommonCrawl data
- Check_for_root_detection.py: Python3 script to help with bypassing root detection in Android apps. It recursively searches smali files for common strings that are use to check if the device is rooted and prints the filename, method, and root detection string found
- SubEnum: Small Python script used to bruteforce subdomain names of a specified domain
- Pdlist: A passive subdomain finder
- GetGithubRepoCloneUrls.py: This code snippet takes a Github organization name as input, crawls for all its public repositories and returns a list of all the "Git clone URLs" for those repos
- XSSwagger: A simple Swagger-ui scanner that can detect old versions vulnerable to various XSS attacks
- Fluxion & Introduction: A remake of linset. It attempts to retrieve the WPA/WPA2 key from a target access point by means of a social engineering (phishing) attack
- SUDO_KILLER: A tool to identify and exploit sudo rules' misconfigurations and vulnerabilities within sudo
- IPv6teal: Stealthy data exfiltration via IPv6 covert channel

Misc. pentest & bug bounty resources

- Event handler for mobile used in XSS (ontouch*)
- 11 top DEF CON and Black Hat talks of all time
- SecHub
- Web-fuzz-wordlists
- Bug Bounty Hunter Den (BBHD)
- APIsecurity.io Issue 41: Tinder and Axway API Vulnerability, Equifax fined
- Jobert Abma on Quora Sessions
- The HTML Handbook

Challenges

- Vulnerable stand & Source code
- Hacker Test: 20 levels to test your hacking skills
- Xsslabs.tech: Online labs to learn and practice different XSS filter evasion & character blacklisting bypass techniques
- Owasp-TOP-10-Training-Panel
- CyberTruckChallenge19

Articles

- Improving WordPress plugin security from both attack and defense sides
- What does it mean when they say React is XSS protected?
- AWS IAM Privilege Escalation – Methods and Mitigation – Part 2 & Repo of AWS IAM Privilege Escalation Methods
- Illusion of Randomness & Exploiting RNGs
- Introduction to physical penetration tests
- Things to do before you conduct a 'red team' assessment
- Securing your Geckoboard
- Underscoring the "private" in private key
- PEAP Relay Attacks with wpa_sycophant
- DataSpii: The catastrophic data leak via browser extensions

News

Bug bounty & Pentest news

- Burp Repeater now has a new WebSockets connection wizard letting you attach, reconnect, clone, and manually configure WebSockets connections.
- A quick update on Yes We Hack's ranking point system

Reports

- [Research] Under the Hoodie, 2019 Edition: Lessons Learned from 180 Penetration Tests
- 2019 Global Developer Report: DevSecOps
- Unique to the .NET ecosystem, 75% of the top twenty vulnerabilities have a high severity rating

Vulnerabilities

- Chances of destructive BlueKeep exploit rise with new explainer posted online
- A US company selling a weaponized BlueKeep exploit with RCE capabilities as part of a pen-testing tool (named CANVAS)
- Concern over 'unpatched' Comodo Antivirus flaws
- Your Android's accelerometer could be used to eavesdrop on your calls: New attack called Spearphone uses the motion sensors in Android phones as a listening device (without asking for microphone permission)
- Big password hole in iOS 13 beta spotted by testers
- Facebook design flaw let thousands of kids join chats with unauthorized users
- Flaws in widely used corporate VPNs put company secrets at risk

Breaches & Attacks

- Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach In Its History'
- Advanced mobile surveillanceware, made in Russia, found in the wild
- EvilGnome – Linux malware aimed at your desktop, not your servers
- Rare Steganography Hack Can Compromise Fully Patched Websites
- Popular File-Sharing Service WeTransfer Used in Malicious Spam Campaigns
- Hackers Exploit Recent WordPress Plugin Bugs for Malvertising
- Telegram voicemail hack used against Brazil's president, ministers

Malicious apps/sites

- Browser plug-ins peddled personal data from over 4m browsers

Other news

- WannaCry hero gets off lightly, avoids prison – was justice done?
- Non “security issue” on VLC
- Equifax to pay up to $700m to settle 2017 data breach
- Gamers Are Easy Prey for Credential Thieves
- ThreatList: Human Error is Behind One Quarter of Data Breaches
- Concern Over ‘Russian’ FaceApp Ignores That American Companies Sell Our Data Abroad
- Greece, Spain to Be Fined for Not Transposing EU Data Protection Law

Non technical

- Social engineering. When you’re the mark…
- Security risks of Have I Been Pwned
- How to answer (shitty) security questions
- Recent Talk: How To Crash & Burn…And Recover!
- Your Posture Is Awful. Here’s How To Fix It.
- A woman’s greatest enemy? A lack of time to herself

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 07/19/2019 to 07/26/2019.

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.