Bugbytes #28 – Wireshark over SSH, Pwning New Relic & Filter Fun with @zseano

BY INTIGRITI · JULY 23, 2019 · LAST UPDATED ON JULY 17, 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 12 to 19 of July.

Our favorite 5 hacking items

1. Tutorial of the week

> "Using Wireshark over SSH (WS on Windows traffic on Linux)"

This is a short how-to for using Wireshark over SSH. It'll be really handy if your main host is Windows, and you are using a Linux VPS for tests.
The steps described will allow you to run Wireshark locally, and use it to analyze traffic captured on the remote Linux server (even if you don't have a GUI on the latter!).

2. Writeup of the week

> "Privilege escalation via mass assignment on New Relic"

What a fun bug! @samwcyo bought a Tesla, tried to hack it, didn't find anything, cracked his windshield, then accidentally triggered a blind XSS when he wanted to report the accident.
My takeaways are:
– Put blind XSS payloads everywhere
– Own a Tesla one day
– Then damage it intentionally to find new bugs

3. Video of the week

> "Understanding & bypassing filters with @zseano"

@zseano walks us through why all XSSes are not low hanging fruits, and how he proceeds to find edge cases by bypassing filters.
If you want to stop trying random payloads grabbed from the Internet and learn how to manually find interesting XSSes like a pro, this is the video to watch!
Also, it's a good idea to focus on one bug at a time. That's what @zseano and @nahamsec did and recommend.

4. Conference of the week

> "SteelCon 2019, especially:
> – SteelCon 2019: Hunting Sh*T Up: Red Teaming With A Bug Hunter's Mindset – Andy Gill
> – TLS 1.3 For Penetration Testers
> – WordPress Isn't A Security Dumpster Fire, Fight Me!"

These talks go to my top list of things to watch really soon. Especially the one by Andy Gill because it's about three aspects of offensive security in which I'm very interested: Pentesting, Bug bounty and Red teaming.
Applying a bug hunter's mindset to pentest and red teaming can only be a good idea: bug hunting pushes you to automate as much as you can, go for the most impactful bugs and PoCs, work fast by using report templates, use/create the best tools... But many tools used for Web security today were created by bug hunters and aren't known by many pentesters.
So I can't wait to learn Andy's take on this subject, and learn about TLS 1.3 and WordPress security.

5. Non technical item of the week

> "Web Application Penetration Testing: Minimum Checklist Based on the OWASP Testing Guide"

This article is aimed at QA specialists. But I think it's also a good read for beginner pentesters who don't have the time to go trough the whole OWASP Testing Guide and need a quick summary.
Not that I don't encourage reading the whole thing (on the contrary!). But it can be overwhelming when you're just starting out.
The cheatsheet is useful to use during tests or as a basis for your own customized cheatsheet. I love how each test is accompanied with a concise comment that's like the most important thing that you need to know about that test.

Other amazing things we stumbled upon this week

Videos

- @nahamsec stream: Bug bounty basics, Automation, Recon, Q&A & Stream 2
- Infosecgirls Discussion with Kavya Pearlman
- Post Exploitation With Windows Credentials Editor (WCE) – Dump Windows Password Hashes

Podcasts

- 7MS #372: Tales of Internal Pentest Pwnage – Part 5
- Hackable? 29 – Dead Drops
- SwigCast Ep. 3: 'This is not something that you ask for random advice on at a cocktail party'
- Security Now 723 – Encrypting DNS
- Risky Business #548 — Zoom RCE details and all the week's news

- Smashing Security 137: Porn trolling lawyers, Insta hacking, and Ctrl-Alt-LED
- Hacking cars, getting arrested and a career in cybersecurity
- Security In Five Episode 538 – Facebook Hit With A $5 Billion Fine, It Won't Change Anything
- Absolute AppSec Ep. #65 – Adam Baldwin (@adam_baldwin)
- Paul's Security Weekly #612 – Topic Segment: Security Roundtable, MITRE ATT&CK: Katie Nickels, MITRE & Security News: July 18, 2019
- Hack Naked News #227
- Application Security Weekly #69 – Application News

Webinars & Webcasts

- You can rest easy when protecting REST APIs
- Getting started with Netcat (SECARMY)
- Attack Tactics 7: The logs you are looking for.

Conferences

- Global AppSec Tel Aviv 2019, especially:
  - Testing and Hacking APIs
  - Common API Security Pitfalls
  - Security for Modern Webapps: New Web Platform Security Features to Protect your Application
  - NOSQL web application vulnerabilities and mitigation
  - Webhooks Hookups Abusing API Developers
  - OWASP Top 10 for JavaScript Developers
  - Building & Hacking Modern iOS Apps
  - OWASP Serverless Top 10
- OISF 2019 Videos, especially:
  - Continuous Skills Improvement For Everyone & Slides
  - A Discussion of Secrets
- Hack in, Cash out – Hacking and Securing Payment Technologies – OWASP London (40m15s)

Tutorials

Medium to advanced

- Advanced Blind XSS Payloads
- HQL Injection Exploitation in MySQL
- SSH tunneling as a VPN alternative
- Delegating Like a Boss: Abusing Kerberos Delegation in Active Directory
- GPO Abuse: "You can't see me": How to create a backdoor through GPO to remain hidden in Active Directory

Beginners corner

- Exploiting SSL Vulnerabilities in Mobile Apps
- What is a blind vulnerability and how can it be exploited and detected?
- Subdomain Takeover Explained with Practical
- What Is a CSRF Attack
- How to Install Kali Linux in the Cloud
- Linux for Pentester: ed Privilege Escalation

Writeups

Challenge writeups

- Google XSS game walkthrough

Pentest writeups

- Exploring the Power of Phished Persistent Cookies in AWS
- Bypassing a restrictive JS sandbox

Responsible(ish) disclosure writeups

- Attacking SSL VPN – Part 1: PreAuth RCE on Palo Alto GlobalProtect, with Uber as Case Study!
- Symantec Mobile Threat: Attackers Can Manipulate Your WhatsApp and Telegram Media Files
- Analysis of an Atlassian Crowd RCE – CVE-2019-11580
- Zoom Zero Day Followup: Getting the RCE
- TYPO3 9.5.7: Overriding the Database to Execute Code
- RCE in Jira(CVE-2019–11581)
- Burning down the house with IoT
- Tmux privilege escalation abusing send-keys

- An Exploit Chain Against Citrix SD-WAN

Bug bounty writeups

- Race condition on Facebook (Instagram) ($30,000)
- Subdomain takeover on Facebook ($500)
- CSRF on Facebook ($3,000)
- Stealing CSRF token with Clickjacking ($1,250)
- CSRF through GraphQL on Tokopedia
- IDOR, SSRF, Information disclosure & CORS misconfiguration ($9,000)
- MiTM on Slack ($500)
- Logic flaw on Uber ($1,500)
- Authorization flaw on GitLab ($1,000)
- RCE / Browser extension flaw on Grammarly & PoC ($1,500)
- RCE on GitLab ($12,000)

Tools

If you don't have time

- GitGot& Introduction: Semi-automated, feedback-driven tool to rapidly search through troves of public data on GitHub for sensitive secrets
- Git-Scrapers: Collect OSINT from git repositories
- Entro.py: Tool that recursively searches directories for files containing strings with high shannon entropy (by @healthyoutlet) & How to reduce false positives

More tools, if you have time

- git-ls: List (or plunder) private repos/gists to which a token has access, including those of other users
- Git-hound: Find exposed keys across GitHub using code search keywords. Git Hound is a pattern-matching, batch-catching secret snatcher.
- jLoot: JIRA Secure Attachment Looter
- RacePWN (Race Condition framework) & Introduction: Race Condition framework
- ORtester:
- XSpear: Powerfull XSS Scanning and Parameter Analysis tool&gem

- RedGhost: Linux post exploitation framework designed to assist red teams in gaining persistence, reconnaissance and leaving no trace
- Very Complete Management (VCM): A small script to automate project folder management and basic tool output
- ReportingTool: PHP Laravel Based Pentesting Report Writing Tool
- Kali-ptf: A Kali container with custom set of tools installed
- Revssl: A simple script that automates generation of OpenSSL reverse shells
- Find-LOLBAS & Introduction: Simple powershell script to find living off land binaries and scripts on a system
- Vulnrep: Java tool that collects vulnerabilities (from vulners.com and/or wpvulndb.com) for defined keywords generates an HTML report

Misc. pentest & bug bounty resources

- Trufflehog.json: High signal patterns from trufflehog refactored to work with tomnomnom's gf
- Pentest Notes – Approaching a Target
- Cloud Security Alliance Releases Cloud Penetration Testing Playbook
- Sqlinjection.net
- OWASP cheat sheet series project (new website)
- Awesome Mitre ATT&CK™ Framework
- One-liner Mimikatz Parser
- APIsecurity.io Issue 40: Vulnerabilities in Instagram, 7-Eleven, Zipato

Challenges

- CORS misconfiguration vulnerable Lab
- New Android challenges on challs.reyammer.io
- Page containing a set of DOM XSSes

Articles

- Automating local DTD discovery for XXE exploitation
- Eavesdropping in the era of Web Applications!
- Docker for Pentesters
- Improve Your JavaScript Knowledge By Reading Source Code

- Protecting Your Website Using an Anti-CSRF Token
- The Strange Case of the Malicious Favicon
- Understanding Docker container escapes
- Fails and Fixes with IoT
- Linux Privilege Escalation Basics

News

Bug bounty & Pentest news

- Tell @naffy what you'd like to hear him explain / cover in Live streams
- Real-World Bug Hunting: A Field Guide to Web Hacking, Peter Yaworski @yaworsk's new book is out
- Burp Suite Pro/Community 2.1.01 released, with support for WebSockets in Burp Repeater & Here's how to use Burp Repeater with WebSockets
- Google deprecates XSS Auditor for Chrome
- End of Sale Announced for Metasploit Community
- Kali NetHunter App Store, a new Android store dedicated to free security apps
- Live Hacking Events: Stats, invitations, and what's next & @luketucker answering live hacking questions on Twitter
- Bigger Rewards for Security Bugs: Google is tripling the maximum baseline reward amount from $5,000 to $15,000 and doubling the maximum reward amount for high quality reports from $15,000 to $30,000
- Equifax launches a vulnerability disclosure policy, the first major credit reporting agency to do so

Reports

- RDP exposed: the wolves already at your door
- State of Application Security at S&P Global World's 100 Largest Banks

Vulnerabilities

- Researchers Easily Trick Cylance's AI-Based Antivirus Into Thinking Malware Is 'Goodware'
- WhatsApp, Telegram had security flaws that let hackers change what you see

Breaches & Attacks

- New EvilGnome Backdoor Spies on Linux Users, Steals Their Files
- Firmware Bugs Plague Server Supply Chain, 7 Vendors Impacted

- Massive Malvertising Campaign Reaches 100M Ads, Manipulates Supply Chain
- Microsoft warns 10,000 customers they're targeted by nation-sponsored hackers
- Russia's Kaspersky Lab Finds Says Notorious 'FinSpy' Malware Can Read Secret Chats
- Slack Resets Account Passwords Compromised During 2015 Hack

Other news

- FaceApp privacy panic sets internet alight
- 'My job application was withdrawn by someone pretending to be me'
- Lessons learned from ransomware authors' crypto mistakes
- Privacy Experts: Facebook's $5B Fine Unlikely to Do Much
- CALM DOWN: Discord hasn't been hacked
- Kazakhstan government is now intercepting all HTTPS traffic
- Palantir's Surveillance Service for Law Enforcement
- Security Watch: Elon Musk's NeuraLink Links Brains to iPhones via Bluetooth

Non technical

- Time Speeds Up When You're Wasting It
- Swag Store
- I turned my procrastination habit into a productivity hack
- Burnout Prevention and Treatment – Techniques for Dealing with Overwhelming Stress
- No, You Don't Need a Burner Phone at a Hacking Conference
- Anne-Marie Eklund Löwinder: "I was good at making others' code stop running very early on."

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 07/12/2019 to 07/19/2019

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