Bug Bytes #24 – VIM made easy by @TomNomnom, @jon_bottarini's hunt for hidden features & Rock-ON

BY INTIGRITI · JUNE 25, 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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 14 to 21 of June.

Our favorite 5 hacking items

1. Conference of the week

> "VIM tutorial: linux terminal tools for bug bounty pentest and redteams with @tomnomnom"

Oh my! We're really spoilt this week between this video tutorial with @tomnomnom and @nahamsec's recon tips video (see below).
@tomnomnom shares so many tips that are worthy to discover whether your are a beginner or seasoned bug hunter. This includes the tools he uses for recon (including custom ones like assetfinder and html-tool), BASH basics, how to manually search for secrets in Git repos, how to use (and exit) VIM and a lot more.
This is a must watch if you're into Web app security!

2. Writeup of the week

> "Using Burp Suite match and replace settings to escalate your user privileges and find hidden features ($500)"

@jon_bottarini shares here a technique that allowed multiple times to access unreleased beta and admin features (*i.e.* escalate his privileges).
The idea is that if you see the server always returning some "false" value, you can use Burp Suite's match and replace rule to change the server's response body from "false" to "true". Sometimes this triggers client-side code that was hidden or unaccesible.
Similarly, you can replace *"userlevel":READONLY* with *"userlevel":ADMIN*, or *"subscriptionlevel":"BASIC"* with *"subscriptionlevel":"PROFESSIONAL"*.
Pretty straightforward. Must try now!

3. Resource of the week

> "Collection of bug bounty tips"

This is a remarkable Twitter feed initiated by @intigriti who asked hackers to share their best bug bounty tip. A lot of people chimed in. Here are some of my favorite responses:

- "Create daily diffs of JavaScript files to find new features, endpoints and keep an eye on endpoints that disappear but still work, they might conflict with the future design of the product and induce a vulnerability."
- "Sometimes your target asks you to pay to access an account/premium features. If they use services like "Stripe", try paying with "test cards" and check if you can have a premium account/features, for free!"
- "Change the host header to "localhost", its IPv4/IPv6 equivalents or even better the internal IP of the server!" and "if you get a 403 with that, adding X-Fowarded-For:localhost might do the trick! :)"
- "If http://bugbountytarget.com does not verify e-mail addresses, try signing up with a @bugbountytarget.com email address! You may get access to special features or discounts!"

4. Tool of the week

> "Rock-ON"

If you're currently doing your recon manually, this will be a very handy tool. It's a wrapper around many staple tools and looks like a good basis to build upon and customize to your own needs.
I already have a custom recon tool. But regular readers of this newsletter know by now that I lo-o-ove going through repos like this one. I look for any good ideas that can be replicated and improve my own scripts.

5. Tutorial of the week

> "How to: Burp OpenVPN"

Bookmark this one. It will be really helpful if you need to direct all (and only) your Burp traffic through a remote VPN.
This is a little more complicated than running a VPN on your local machine, but sometimes you don't have a choice. Bug bounty program and pentest client can require that you use a remote VPN.
So check out this awesomly detailed guide. You will need PuTTY, OpenVPN, one VPS or two (if you have a dynamic IP) and the Switchy Omega browser extension.

Other amazing things we stumbled upon this week

Videos

- The Truth About Recon (Bug Bounty Tips)
- Interview with The Blind Hacker
- Exploiting Android Through ADB With PhoneSploit
- PowerShell Empire Complete Tutorial For Beginners – Mimikatz & Privilege Escalation

- Configuring the proxy

Podcasts

- 404 Podcast Not Found #1 /w John Hammond
- Security Now 719 – Exim Under Siege
- 7MS #366: Tales of Internal Pentest Pwnage – Part 3
- Hackable? 27 – Face the Fax
- Risky Business – Feature podcast: An interview with Jim Baker, former general counsel, FBI
- Purple Teaming, SCYTHE – Paul's Security Weekly #609
- Yubico, Tufin, & Venmo – Hack Naked News #223

Webinars & Webcasts

- So, You Wanna Be a Pen Tester? 3 Paths to Consider
- Web App Testing 101 – Getting the Lay of the Land
- A Day in the Life of a Pen Tester & Episode 2

Conferences

- SUE2019 – Entering NIPRNET: SSRF, cloud attacks & case study on abusing jira to gain internal network access on the US DoD (by @Alyssa_Herrera)
- How To Frida Good

Slides only

- The parts of JWT security nobody talks about
- Internet-Scale analysis of AWS Cognito Security
- Fridamania in Security – Using Frida as an Attacker
- IronPython... OMF v2.0 – An introduction to BYOI Payloads (Bring Your Own Interpreter)

Tutorials

Medium to advanced

- Pentesting Meteor Applications with Burp Suite
- Subdomain takeover via Ngrok service

- Deploy a private Burp Collaborator Server in Azure
- Attacking Docker Environments
- Active Directory Enumeration with PowerShell
- How to access RDP over SSH tunnel
- Antivirus Evasion with Python

Beginners corner

- Simplifying Password Spraying & Spray
- Linux for Pentester: CAT Privilege Escalation
- Linux for Pentester: xxd Privilege Escalation
- Linux for Pentester: Time Privilege Escalation
- OCSP: File transfer recipe for delicious post exploitation – Part 1 & Part 2

Writeups

Challenge writeups

- [CTF Write-up] Midnightsun CTF Finals Marcololo (web. mid)
- Facebook CTF 2019 Challenges: Source code & solutions
- Solving each and every fb-ctf challenge PART 1 – Write-up of all the challenges which were in fb-ctf web category

Pentest writeups

- Whoa! This is not a vulnerability
- Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk

Responsible(ish) disclosure writeups

- Hacking thousands of websites via third-party JavaScript libraries
- Why we shouldn't use sequential booking references
- Chaining Three Bugs to Get RCE in Microsoft AttackSurfaceAnalyzer
- Remote Code Execution via Ruby on Rails Active Storage Insecure Deserialization
- How I hacked into a website to prepare for my finals
- Ewon Flexy IoT Router. A Deep dive
- Sharing the Secrets: Pwning an industrial IoT router

- Operation Crack: Hacking IDA Pro Installer PRNG from an Unusual Way
- Fortinet FortiCam FCM-MB40 – Multiple Vulnerabilities

Bug bounty writeups

- SSRF on Snapchat (video)
- DOM XSS on Shopify ($500)
- Authorization flaw on Shopify ($500)
- Blind XSS on Google
- Parameter pollution
- IDOR / Payment tampering
- AWS flaw on Dropbox ($1,500)
- Cookie theft ($900)
- About a Sucuri RCE...and How Not to Handle Bug Bounty Reports ($750)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Redirector: Online open redirect / SSRF payload generator
- Droidstatx: Python tool that generates an Xmind map with all the information gathered and any evidence of possible vulnerabilities identified via static analysis. The map itself is an Android Application Pentesting Methodology component, which assists Pentesters to cover all important areas during an assessment.
- Konan: Advanced Web Application Dir Scanner
- Prithvi: Report Generation Tool

More tools, if you have time

- T1tl3: A simple python script which can check HTTP status of branch of URLs/Subdomains and grab URLs/Subdomain title
- Detect-techs.py: A simple tool written in python3 used to read a list of websites and enumerate WordPress sites, you can change WordPress to any other technology and use it
- EnumUserInFiles.sh: Script for searching usernames in files (nearly all filesystem) for getting sensitive files

- 0xsp-Mongoose: Privilege Escalation Enumeration Toolkit (ELF 64/32) , fast , intelligent enumeration with Web API integration
- Constole: Scan for and exploit Consul agents
- Sliver: A general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), & DNS
- Slackor & Introduction: A Golang implant that uses Slack as a command and control server

Misc. pentest & bug bounty resources

- Distrotest.net: Online operating system tester. Try 200+ Linux distributions without downloading or installing them
- Runbooks: Command references, posts, and resources for different topics
- Probable Wordlists – Version 2.0
- APIsecurity.io Issue 36: Vulnerabilities at TP-Link, Venmo, Amcrest, and GateHub
- League of Bounties
- Bug-Bounty-Bookmarks
- Grep cheatsheet
- Best Hacker and Security Blogs to Read
- Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities
- OSCP-Like vms for HackTheBox and VulnHub
- Application Security 101: Learn buffer overflows starting from CPU architecture, memory layout, programming & assembly
- CPR-Zero: Check Point Research Vulnerability Repository

Articles

- Dynamic Discovery of Mass Assignment Vulnerabilities
- Week in OSINT #2019–24: Interesting section about Facebook graph search changes
- New Kids On The Block (Part I)
- Introduction to AWS IAM Privilege Escalation – Escalating AWS IAM Privileges with an Undocumented CodeStar API
- Security of mobile OAuth 2.0
- A Primer for On-Site CTFs

- What You Need To Know About TCP "SACK Panic"
- Covert Keylogging: Sniping your Typing
- Bypassing Antivirus with Golang – Gopher it!

News

Bug bounty news

- New on Web Security Academy: SSRF course & labs
- New Bugcrowd Researcher Collaboration: Reward Splitting & Joint Submissions
- Speakers Wanted: Security@ San Francisco 2019
- Graph's not dead & SearchBook: A Firefox extension for executing some Graph-like searches against Facebook
- @naffy made roughly $550k USD in 365 days on 187 bugs & Spreadsheet of his bugs for the last 12 months

Reports

- Vulnerabilities and threats in mobile applications 2019

Vulnerabilities

- Oracle Warns of New Actively-Exploited WebLogic Flaw
- Netflix researcher spots TCP SACK flaws in Linux and FreeBSD
- Millions of Dell PCs Vulnerable to Flaw in Third-Party Component
- Widely used medical infusion pump can be remotely hijacked
- Used Nest cams were letting previous owners spy on you
- Pass the salt! Popular CMSs aren't securing passwords properly
- A bug in Wi-Fi 'extenders' could give a hacker full control over the devices
- Major HSM vulnerabilities impact banks, cloud providers, governments

Breaches & Attacks

- Malware sidesteps Google permissions policy with new 2FA bypass technique
- Mozilla releases fix for high-impact Firefox zero-day
- Mozilla Fixes Second Actively-Exploited Firefox Flaw
- NASA hacked because of unauthorized Raspberry Pi connected to its network

- Personal data of 2.7 million people leaked from Desjardins
- Millions of Venmo transactions scraped (again)
- Supply Chain Hackers Snuck Malware Into Videogames
- SIM swap horror story: I've lost decades of data and Google won't lift a finger

Malicious apps/sites

Other news

- Chrome adds features to improve protection against deceptive websites
- Facebook's Libra cryptocurrency is big news but will it be secure?
- Samsung asks users to please virus-scan their TVs

Non technical

- Research and Organization on the go and refinement when time permits
- Bug Bounty Insider
- Security, turns out it's hard
- The biggest data breaches of the last 15 years
- My Home Office
- Building blocks

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 06/14/2019 to 06/21/2019.

Subscribe to the newsletter here!

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