Bug Bytes #181 – SpookySSL, XSSHunter depreciated, and how to get a CVE

BY TRAVISINTIGRITI · NOVEMBER 9, 2022 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The second series is curated by InsiderPhD. Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the weeks from October 31st until November 6th.

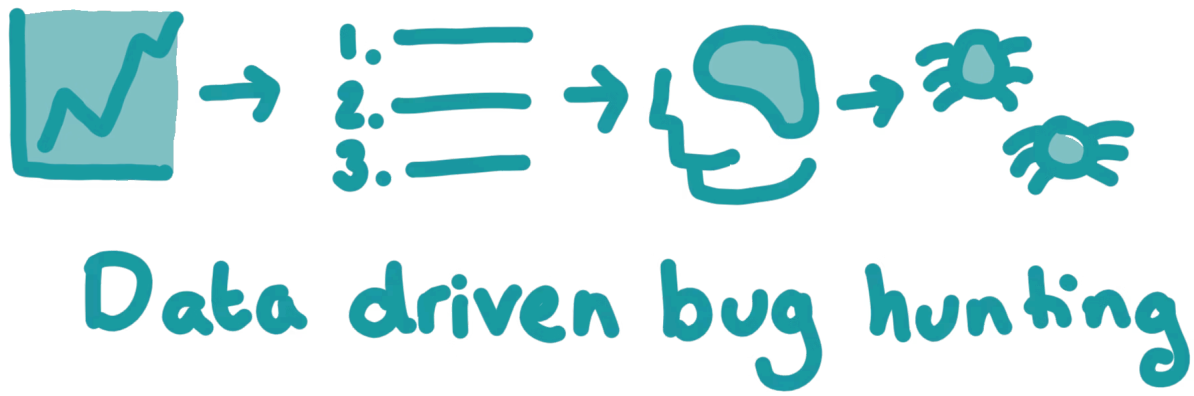
CLICK HERE TO SUBSCRIBE

Intigriti News

- Intigriti code review challenge and the solution!
- Happy Halloween!

From my notebook

This week I've been rather chaotic in what I've been reading and watching, so this week's top 5 resources are all around the theme of data-driven bug hunting. What I mean by this is using large amounts of data from things like disclosed reports or write-ups to try and understand larger trends in what bugs are common or uncommon, where to look, or how to change your bug-hunting style.



Data-driven bug hunting

- What I learnt from reading 217* Subdomain Takeover bug reports. – I love this article, I love how the author has really dived deep into the data to really try to understand it, I especially like their analysis of platforms for subdomain takeovers and key takeaways. Well worth a read!
- Exploiting Static Site Generators: When Static Is Not Actually Static – Honestly, every time I see a new Assetnote blog post I read it immediately, they are always full of really interesting and unique security research, and this is a great look into why static sites aren't always as static as they look!

- How I made a reliable hacking tools and resources search engine in two days (~6500 entries!) – IppSec.rocks but for GitHub tools! Highly recommend this if you're trying to figure out if your amazing new tool you're about to spend 100 hours making already exists.
- Awesome Cyber Security Newsletters – Awesome lists are fairly common around the tech community, this awesome list is of cyber security newsletters if you're looking for curated content with a slightly different vibe.
- XSS Hunter gets depreciated, new sign-ups are disabled, xss.ht domains can be redirected to local instances or a static payload until Feb 2023 and the announcement – XSS Hunter (the service) is shutting down, while you can host your own XSS Hunter (the product), new sign-ups are disabled and xss.ht domains will only be able to redirect or have a static XSS payload. Most people who've worked on the triage or client side of bug bounty hunting understand why, but XSS Hunter has a lot of confidential vulnerability information, and IAmMandatory is uncomfortable with this.
- CVE demystified, a quick guide to get your own CVE. – CVEs can be great social proof of your hacking skills, so here's how to get one!

Other Amazing Things

- @phillipwylie Talks About His Favorite Tools, Switching Careers
- Backup Server Hacked – SUPPLY CHAIN Code Execution
- Deep Dive into Kerberoasting Attack
- Server Griefed and New Beginnings
- Reversing with strings and tracing – Cult Meeting / EncodedPayload
- Enter the World of Haiku and Learn Hacking Through Video Games
- Learn Red Team Cybersecurity in a Gamified Way! (Guided Walkthrough)
- The King Of Malware is Back
- Deep Recursion Attack + Introspection | Damn Vulnerable GraphQL App
- Node.js "Pug" Server-Side Template Injection
- Exploiting Github to Mine Crypto
- HackTheBox – Moderators

- Dehashed |_| A Data Breah Search engine
- Cybercrime & Dark Web Conversations (w/ Shmuel!)
- Ditch LastPass and build your own password manager in python
- Full Time Bounty Hunter's Audit Methodology
- How I Automate My Subdomain Recon! (Automation Series)
- Mindset of a Hacker
- HTTP/3 Connection Contamination Made Simple – James Kettle (albinowax)

- LabMD Vs. The FTC
- EP94 Meet Cloud Security Acronyms with Anna Belak
- 127: Maddie
- 163 – A Galaxy Store Bug, Facebook CSRF, and Google IDOR
- Risky Business #683 — OpenSSL bug is a fizzer, ASD responds to Medibank hack
- 164 – XNU's kalloc_type, Stranger Strings, and a NetBSD Bug

- Prerequisite bug bounty knowledge by Rhynorater
- Upcoming content creators by InsiderPhD
- XSSHunter depreciation
- What sucks about doing recon? By Bug Bounty Reports Explained
- What programming languages should every hacker know?

- What is a JWT – JSON Web Token?
- Android Pentesting 101—Part 3
- Wanna Learn Basics of Programming for Bug Bounty?
- WordPress 6.0.3 Patch Analysis
- Finding SQL injection vulnerabilities using Ghauri
- Google Dorks for Hackers
- FUZZING FOR HIDDEN PARAMS
- Bug Bounty / Cybersecurity Resource Management Guide
- The Complete Guide to PortSwigger Directory Traversal and How to Prevent It
- Making HTTP header injection critical via response queue poisoning
- Guess Your Enemies' Passwords With Python (Brute Force Attack)
- Login CSRF—What is it and how to prevent it?
- Write-up: Information disclosure in error messages @ PortSwigger Academy
- OS Banner Grabbing & Identifying Target System OS.
- 4 Videos From 4 Infosec Experts to Explain Web3 Hacking
- BUG BOUNTY: FIND HIDDEN PARAMETERS
- Automation of Buffer-Overflow
- Python Source Code Analysis
- The Ultimate Bug Bounty Checklist For 2FA
- Web Enumeration -WPScan
- Web Security Academy—Blind OS command injection with time delays
- 403 Forbidden: Access Control Bug Hunting
- $1000 BAC: The Complete Guide to Exploiting Broken Access Control
- Gift Card Hacking
- Awesome Cyber Security conferences

- How Uber social engineering hack compromised Uber's Hackerone bug bounty reports
- A $250 Entirely Automated Bug Bounty
- How to Find Escalating HTML to SSRF. I instantly got the Hall of Fame within 5minutes.
- Blind SQL Injection on Delete Request
- P1 Bounties: File Upload to RCE == $$
- Improper Access Control—My Third Finding on Hackerone!
- Sensitive data exposure through GitHub Leads to Dev team accounts compromise.
- Getting P1 Bug Only With My Cellphone
- How I Get 5x Swag From Sony
- How 403 Forbidden Bypass got me NOKIA Hall Of Fame (HOF)
- Chaining Multiple Vulnerabilities Leads to Remote Code Execution (RCE).
- The easiest bug to get a Hall of fame from a Billion dollar company.
- Get Blind XSS within 5 Minutes—$100
- Invitation Hijacking
- CSRF Leads to Delete User Account
- HTML INJECTION LEADS TO OPEN REDIRECT
- Multiple IDORs on same API family
- Exploit Feature To Get High Bug impact
- Directory traversal in PDF viewing application. Leading to full database takeover
- IDOR on Unsubscribe emails to $200 bounty.
- Caiyon.com (Dall-E Mini) Reflected XSS Vulnerability
- Case of Admin Bypass for RCE, XSS, and Information Disclosure

- Fun with TurboIntruder,
- XSS Catcher – A blind XSS detection framework
- Appshark – Static Taint Analysis Platform To Scan Vulnerabilities In An Android App
- XSS Hunter Express

- TOP 5 AWESOME BUG BOUNTY BOOKS FOR BEGINNERS THAT YOU SHOULD KNOW
- Bug bounty zero to hero
- ngrok without ngrok
- Self-hosted blind XSS with ezXSS
- Don't use X-Custom-IP-Authorization, it was just a placeholder for a web security academy lab, oops
- PHP filter_var shenanigans
- Using google and copyright notices to find old assets

- DOJO CHALLENGE #18 Winners!
- pentesting.cloud part 1: "Open To The Public" CTF walkthrough
- Cicd-Goat – A Deliberately Vulnerable CI/CD Environment

- VuCSA – Vulnerable Client-Server Application – Made For Learning/Presenting How To Perform Penetration Tests Of Non-Http Thick Clients

- XSS Hunter Depreciated
- OpenSSL 3.0 vulnerability overblown
- The OpenSSL security update story – how can you tell what needs fixing?
- Layoffs across the US tech industry
- Pentester Land gets a makeover!
- Dropbox discloses breach after hacker stole 130 GitHub repositories

- Cyber Laws In Pakistan!
- Android Apps With a Million Downloads Led Users to Phishing Sites