Bug Bytes #149 – WordPress plugin confusion, Bug bounty automation & CTF tricks

BY ANNA HAMMOND · DECEMBER 1, 2021 · LAST UPDATED ON MARCH 6, 2025

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

CLICK HERE TO SUBSCRIBE

This issue covers the week from November 22 to 29.

Our favorite 5 hacking items

1. Resource of the week

xvnpw.github.io

@xvnpw has been sharing interesting research, writeups and tips on path traversal vulnerabilities. The blog is worth a read if you're interested in this bug class, or in older articles on hacking Azure and SpEL.

2. Writeup of the week

WordPress Plugin Confusion: How an update can get you pwned, WordPress Plugin Update Confusion – The full guide how to scan and mitigate the next big Supply Chain Attack & Traffic Factory example

@vavkamil took the idea of dependency confusion and transposed it to WordPress themes and plugins. Then he partenered with @naglinagli to search for this new vulnerability at scale on bug bounty programs.
I love this type of research, both so clever and obvious AFTER you've read about it. Who would've thought that WordPress and package registries like NPM had anything in common?!

3. Challenge writeup of the week

The InfoSecurity Challenge 2021 Full Writeup: Battle Royale for $30k

@spaceraccoonsec solved all 10 levels in The InfoSecurity Challenge that involved web, mobile, cryptography, pwn, forensics, steganography, and more. He wrote a detailed walkthrough of all tasks and it is full of interesting techniques worth knowing.
With all the CTFs running this December, it might help to learn some of these advanced CTF tricks.

4. Tools of the week

cero
Scavenger

These tools both perform common bug bounty taskd but with a twist.

@blegmore's cero scrapes domain names from SSL/TLS certificates. This sounds like something that tons of other tools already do, right? What makes cero interesting is that it can scrape certificates from any protocol that uses TLS, not just HTTPS.
Thank you @Six2dez1 for highlighting this awesome tool!

Scavenger by @0xDexter0us is a Burp extension that creates target-specific wordlists from Burp history. The cool part is that it can create a parameter wordlist (based on URL, body, cookie, and JSON parameters), an endpoint wordlist (based on URLs in the sitemap and JavaScript files) or a wordlist of JSON response keys.

5. Article of the week

Hakluke: Creating the Perfect Bug Bounty Automation

This reads like a short history of automation through the eyes of a bug hunter. @hakluke describes different types of architectures he tried, their limits, and how he plans on solving them.
If you're thinking of building your first bug bounty automation solution, it can be useful to learn about someone else's experience and mistakes.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Web Fundamentals for Cyber Security Series
- What's in the pipeline for the Burp Suite message inspector?
- $16k Stealing secrets.yaml from GitLab using stored XSS – Hackerone bug bounty
- #MentorshipMondays | Mobile Hacking
- Pentester Diaries Ep10: Journey into Reverse Engineering and Exploit Development
- HTB Stories #5: Let's Chat with LiveOverflow

Podcasts

- A Conversation With Pentesting And Bug Bounty Expert Jason Haddix | The Hacker Factory With Phillip Wylie
- GitLab Prototype Pollution and Some Authentication Bypasses [Bug Bounty Podcast]

Conferences

- Become an Ethical Hacker for $0 (BSides Ahmedabad keynote)
- Mystikcon 2021
- GreHack 2021, especially:
  - Optimizing Server Side Template Injection Payloads for jinja2
  - Exploiting CSP in WebKit to break Authentication/Authorization
  - DNSpooq: Does DNS cache poisoning still matter?

Slides & Workshop material

- A tale of making internet pollution free – BSides Ahmedabad 2021

Tutorials

Medium to advanced

- Chronolocation of Media
- Persistence Through Service Workers-part 3: Easy Javascript Payload Deployment
- Hunting for Persistence in Linux (Part 1): Auditd, Sysmon, Osquery, and Webshells & Hunting for Persistence in Linux (Part 2): Account Creation and Manipulation
- Active Directory Sites and Subnets enumeration

Beginners corner

- Hunting for Bugs in Shopping/Billing Feature.
- Don't Search by Port
- Simplifying Authorization Testing in Burp Part 1 & Part 2

Writeups

Challenge writeups

- The InfoSecurity Challenge 2021 Full Writeup: Battle Royale for $30k
- Synack 2021 Open Invitational CTF Crypto Writeup
- UHC- Union
- SSRF – Lab #1 Basic SSRF against the local server | Long Version
- XXE to RCE? BountyHunter by Hack The Box

Responsible(ish) disclosure writeups

- Exploiting Vulnerabilities in a TLD Registrar to Takeover Tether, Google, and Amazon
- Discovering Full Read SSRF in Jamf (CVE-2021-39303 & CVE-2021-40809) #CodeReview
- Insecure default configuration in Redash that leads to authentication bypass
- Moodle Blind SQL injection via MNet authentication
- RocketChat – Monitor User Messages
- Unlocking the Vault :: Unauthenticated Remote Code Execution against CommVault Command Center #CodeReview
- RCE with SSRF and File Write as an exploit chain on Apache Guacamole

0-day & N-day vulnerabilities

- Dedecms GetCookie Type Juggling Authentication Bypass Vulnerability
- Windows installer LPE 0day (bypasses the incomplete fix for CVE-2021-41379)

Bug bounty writeups

- Finding XSS on .apple.com and building a proof of concept to leak your PII information (Apple)
- Price Manipulation Bypass Using Integer Overflow Method
- A business logic error bug worth 600$
- GoSecure Investigates Abusing Windows Server Update Services (WSUS) to Enable NTLM Relaying Attacks (Microsoft)
- How I Found My First XSS Bug (Atlassian, $600)

See more writeups on The list of bug bounty writeups.

Tools

- GoMapEnum: User enumeration and password bruteforce on Azure, ADFS, OWA, O365 and gather emails on Linkedin
- STEWS: A Security Tool for Enumerating WebSockets
- AuRA: Auth. Request Analyser: Chromium extension to to support the analysis of OAuth 2.0 and OpenID Connect 1.0 SSO flows & Custom and flexible OAuth/OIDC SP and IdP implementations
- GAP (Get All Params): An evolution of the getAllParams Burp extension for collecting parameters

Tips & Tweets

- CSRF and CORS bypass tricks
- New cases added to the "Make JDBC Attack Brilliant Again" paper
- Using HTML tags attributes without any separators
- Oneliner to manually grep through JS files
- From unrestricted file upload with no access to the uploaded shell to blind OOB RCE
- Outlook attachments can be directly downloaded (useful for phishing engagements)

Misc. pentest & bug bounty resources

- CVE Trends
- @0xAwali's workflow for pasing JS files
- The Cyber Plumber's Handbook – The definitive guide to Secure Shell (SSH) tunneling, port redirection, and bending traffic like a boss (Free) & Practice lab ($9.99)
- SalmonSec cheatsheets
- Bishop Fox: The Pen Testing Tools We're Thankful for in 2021

Articles

- Data Exfiltration via CSS + SVG Font
- A Bit Of A Fixer Upper – Testing Fix-backed Applications & FixerUpper
- Is running legacy software with no publicly known exploits safe?
- Gadget reduction using zero-call-user-regs

Challenges

- HTB Cyber Santa (December 1-5)
- Code Security Advent Calendar 2021 (Starts on December 1)
- HITCON CTF 2021 (December 4-5)

Bug bounty & Pentest news

- Cyber Security Awareness Month Extravaganza! Bug Bounty CTF (Public-009)
- Hacking Book Bundle
- OWASP Timisoara #20 – AI, Bug Bounty & Web Fuzzing (Online) (December 9)

- Tool updates
  - SecLists 2021.4 (Final release of 2021)
  - Brida 0.5 released for Hack In Paris 2021!
  - OWASP ZAP: Launching Browsers with Extensions
  - "X-Forwarded-Prefix" header added to Param Miner to detect Symfony cache poisoning
  - New features added to Auth Analyzer

Non technical

- Passing OSCP 2021 within 12 hours
- An OSINT Story: It's late Friday evening...