Bug Bytes #38 – New XSS Challenge, {{7*7}} to {{P1}} & the ultimate XSS payload generator

BY INTIGRITI · OCTOBER 1, 2019 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-38-live-bug-bounty-with-yaworsk-77-to-p1-the-ultimate-xss-payload-generator

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 20 to 27 of September.

Intigriti news

- Tomorrowland added https://winterpackages.tomorrowland.com/en to their scope
- A new vetted program launched on intigriti. Learn how to become vetted.
- We've launched another XSS challenge! Solve it and win a Burp Suite Pro license and private invitations!
  - **TIP 1:** // is more than a comment!
  - **TIP 2:** Go back to your roots
  - **TIP 3:** It's a name game
  - **TIP 4:** Like an onion, this challenge has multiple layers.

Our favorite 5 hacking items

1. Slide/tool of the week

Manual JavaScript Anaylsis Is A Bug & MetaSec.js

I hope this talk's video will be released soon. But even without it, this presentation is very helpful in understanding what to look for in JavaScript files, existing tools for automation, and what can/cannot be automated.
Techniques mentioned include endpoint discovery, reversing source maps, technology fingerprinting, detecting sources and sinks, detecting ReDoS, detecting secrets, detecting vulnerable third-party components, etc.
As a bonus, LewisArdern provides MetaSec.js, a wrapper around several open source tools to automate JS file analysis

2. Writeup of the week

> Fuzzing {{7*7}} Till {{P1}}

This is an SSTI writeup. Detection was pretty straightforward: @err0rrrrr injected *{{7*7}}{{7*7}}* as a comment and received an email notification containing *4949*.
The interesting part is that exploitation was hindered by some kind of blacklisting. He could bypass it by bruteforcing local variable names using this custom wordlist. That's worth adding to Burp to help with stubborn SSTIs!

3. Article of the week

> Application Enumeration Tips using Aquatone and Burp Suite

This is an excellent article on automation using Burp and Aquatone.
The novel idea is to use visual identification, not for checking subdomains, but when you're testing a large Web app. When you're limited on time as a pentester, you want to quickly assess a lot of URLs to cover the maximum surface.
@ryanwendel explains how he gets a list of URLs from Burp's proxy history, and passes them to Aquatone to take screenshots. If authentication is required, he makes Aquatone use Burp as a proxy, and leverages Session Handling rules to maintain an authenticated state. So handy!

4. Resource of the week

> One XSS cheatsheet to rule them all

This is the most comprehensive XSS cheatsheet I've seen.
What is also unique about it, apart from the number of payloads, is that it is interactive. You can filter payloads by tag, event handler and browser.
It also features entirely new XSS payloads that @garethheyes found and presented at Global AppSec 2019. The talk wasn't recorded but the slides are available: XSS Magic tricks.
All this should be really helpful with HTML filter and WAF bypass.

5. Video of the week

> 09/15/2019 – Live Bug Bounty Recon Session on Yahoo (Censys, Crtsh, Sublist3r) w/ @Yaworsk

If you're a fan of @Yaworsk, his books "Real-World Bug Hunting: A Field Guide to Web Hacking" and Web Hacking 101, or his Youtube channel, then you will love this video!
For, once he is the interviewee not the interviewer. The discussion starts at 1h55m00s and covers many topics: Peter's way of doing recon, his testing methodology, his areas of improvements, how he does JS analysis, why he doesn't set Burp scope to only the target app, burnout and way more.

Other amazing things we stumbled upon this week

Videos

- Using BurpSuite's Intruder to find bugs and solve Bug Bounty Notes & Hacker101 CTFs
- Owning Cody's First Blog (RCE) on Hacker101 and hacking on FFH from BugBountyNotes.com (IDOR)

- The Top 5 Ways I Hacked Your Internal Network in 2019
- How to Get Started in Infosec – with Michael LaSalvia – Cybertalk 1
- H1-604 Hot Sauce Challenge

Podcasts

- Security Now 733 – Top 25 Bug Classes
- Risky Business #557 — 26 nations release cyber norms statement at UN
- Business Security Weekly #144 – Leadership Articlesusiness
- Paul's Security Weekly #621
- Hackable? Mousejacked
- 7MS #382: Tales of Internal Network Pentest Pwnage – Part 9
- #StateOfTheHack: #DerbyCon Edition with Dave Kennedy (@HackingDave)

Webinars & Webcasts

- Easing Into Consulting; Consulting on The Side & Other Approaches
- The State of Kubernetes Security

Conferences

- OWASP Bay Area – Mobile AppSec 101
- USENIX Security '19 Technical Sessions
- BSides SATX 2019, especially:
  - There's no place like 169.254.169.254 – (Ab)using cloud metadata URLs
  - Challenged by Your Job Search? So Are We All! Learn Key Job Search Tips!
  - Hacker MBA Soft Skills For hackers

Slides only

- Pentest Application With GraphQL
- Application Security Workflow Automation using Docker and Kubernetes & KubeSecO

Tutorials

Medium to advanced

- Why Websites Need HTTP Strict Transport Security (HSTS)

- If HttpOnly You Could Still CSRF... Of CORS you can!
- Subdomains listing techniques
- Exploiting unusual Referer based XSS
- Diving into unserialize(): POP Chains
- A Pivot Cheatsheet for Pentesters
- Nessus Through a Transparent Proxy
- MacOS Red Teaming 209: macOS Frameworks for Command and Control
- Bypassing MacOS Privacy Controls

Beginners corner

- Understanding Cross-Origin Resource Sharing (CORS)
- Security Testing for Android Cross Platform Application (Xamarin & Cordova) – Part 1 & Part 2
- Web Shells Penetration Testing
- Fixing EyeWitness Install Errors on Kali Linux
- ASN Lookup Tools, Strategies and Techniques
- What is Reverse DNS? Top Tools for Performing a Reverse DNS Lookup
- Understanding Java De-serialization

Writeups

Pentest writeups

- Splunk Service Misuse
- Pentesting an IOT based Biometric Attendance device
- Out of Band XXE Injection Via gopher

Responsible(ish) disclosure writeups

- Second order SQL injection in ZoneMinder
- WordPress Privilege Escalation from an Editor to Administrator
- WordPress (Core) Stored XSS Vulnerability
- Write-up of DOMPurify 2.0.0 bypass using mutation XSS
- XSS in The Digital #ClimateStrike Widget
- CVE-2019-0801: Microsoft Office Uri Hyperlink Hijinks

- The Time I Chased a Cab (File): Zip Slip and Certificate Cloning

Bug bounty writeups

- Path traversal on Atlassian ($11,000)
- Information disclosure, SQL injection, Authentication bypass, Unrestricted file upload, RCE & XSS
- Path traversal on Valve ($1,250)
- Stored XSS on Rockstar Games ($1,000)
- XSS & Open redirect on Twitter ($1,540)
- Logic flaws on Twitter

Tools

If you don't have time

- Mongo-objectid-predict: Predict Mongo ObjectIds to exploit IDORs
- Keyhacks.sh: No matter what tool you use to find secrets in Github, this Bash script will help test your findings

More tools, if you have time

- Secret-bridge, Introduction & TOOLS.md: Monitors Github for leaked secrets
- Shhgit Live: Live stream of shhgit (Github monitoring tool) in action
- WaybackRust: A tool written in Rust to query the WaybackMachine
- Andromeda: Interactive Reverse Engineering Tool for Android Applications
- CredNijna: A multithreaded tool designed to identify if credentials are valid, invalid, or local admin valid credentials within a network at-scale via SMB
- Thetick: A simple embedded Linux backdoor
- Navi: An interactive cheatsheet tool for the command-line
- SKA: Simple Karma Attack
- nmapAutomator: A script that you can run in the background!
- SearchOpenFileShares & Introduction: Searches open files shares for potentially sensitive information (password files, database backups, etc)

Misc. pentest & bug bounty resources

- swf_json_csrf
- Xsshop: Scripts for exploiting XSS

- A Pentester's Favorite Vulnerability Scanning Tools
- @nahamsec Discord channel
- Bug Bounty Chat: Telegram channel to talk and help about bugbounty
- Info Sec Pics: Telegram channel sharing infosecurity related pics
- Web Application Cheatsheet (Vulnhub): List of Vulnhub VMs by exploit/vulnerability

Challenges

- CSP bypass challenge & Nonce-based CSP + Service Worker = CSP bypass?
- Server-Side Request Forgery (SSRF) vulnerable Lab
- C0delabs.com (XSS labs)
- HackerOne ekoparty CTF

Articles

- Random Thoughts After Nearly 9 years Pentesting/Red Teaming: 2019
- OSCP: Developing a Methodology
- 10 Java security best practices
- Cyber Kill Chain – Part 2
- Tracking The OSINT Hunter

News

Bug bounty & Pentest news

- New on Web Security Academy: WebSockets
- Burp Suite Pro/Community 2.1.04 released: new options to reopen closed Repeater tabs, close a tab, close all other tabs...
- Here's what it's like being a hacker millionaire under the age of 25
- @daeken's Bounty Progress – September 2019
- Basic Authentication will be turned off in Exchange Online for Exchange ActiveSync (EAS), POP, IMAP & Remote PowerShell on October 13, 2020
- From now until November 1st. The Internal Security Assessment: Field Guide will be on sale for $4.99

Vulnerabilities

- High-severity vulnerability in vBulletin is being actively exploited

- Syntax error in Go programming language conjugates security vulnerability
- Apple to Fix iOS Bug Granting Full Access to 3rd Party Keyboards
- Adobe issues emergency patch for critical ColdFusion vulnerabilities & Microsoft releases emergy patch for 2 critical bugs
- Patch released for Windows-pwning VPN bug

Breaches & Attacks

- Magecart Group Targets Routers Behind Public Wi-Fi Networks
- Massive wave of account hijacks hits YouTube creators
- Tibetans hit by the same mobile malware targeting Uyghurs
- Instagram phish poses as copyright infringement warning – don't click!
- Russian national confesses to biggest bank hack in US history
- Hackers Exploit Unpatched Bug in Rich Reviews WordPress Plugin
- Chinese Hackers Suspected Of Airbus Cyberattacks—A350 Among Targets
- Advanced hackers are infecting IT providers in hopes of hitting their customers
- Microsoft Phishing Attack Uses Google Redirects to Evade Detection
- DoorDash confirms data breach affected 4.9 million customers, workers and merchants
- Hackers Replace Windows Narrator to Get SYSTEM Level Access
- These Hackers Were Hiding Malware Behind a Captcha

Malicious apps/sites

- Malicious Android Apps Evade Google Play Protect via Remote Commands
- New Android Warning: 500 Million Users Have Installed Apps Hiding Nasty Malware—Uninstall Now
- 'Fleeceware' Play store apps quietly charging up to $250
- Fake ad blockers that attempted fraud get blocked

Other news

- Microsoft Blacklists Dozens of New File Extensions in Outlook
- How Google Changed the Secretive Market for the Most Dangerous Hacks in the World
- AT&T redirected pen-test payloads to the FBI's Tips portal
- How The U.S. Hacked ISIS
- What Is CrowdStrike and Why Is Donald Trump Blabbering About It to Ukraine

- Medicine show: Crown Sterling demos 256-bit RSA key-cracking at private event

Non technical

- Meet our hackers – Borja
- YesWeHack profile on Ak1t4
- Personal Branding Workbook: A guide for InfoSec professionals
- A security researcher has made contact. What do I do?
- Cyber Entrepreneur PitFalls You Can Avoid

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 09/20/2019 to 09/27/2019.

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