Bug Bytes #158 – postMessage XSS tips, API testing toolbox & Finding 100+ bugs in WordPress plugins

BY ANNA HAMMOND · FEBRUARY 9, 2022 · LAST UPDATED ON MARCH 6, 2025

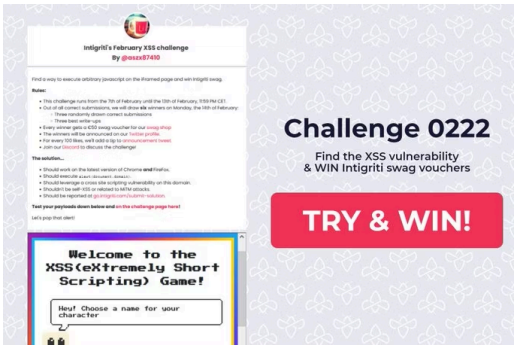
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from January 31 to February 07, 2022.

Intigriti news

Intigriti 1337UP LIVE 2022



Intigriti's February XSS challenge By @aszx87410

Our favorite 5 hacking items

1. Tutorial of the week

eventlistener-xss-recon

This is worth a read if you're interested in postMessage XSS. @oliverrickfors shares a methodology to easily find addEventListener in JS files (given a list of hosts as input), then what to do next to test and exploit them for XSS.

2. Writeups of the week

Solving DOM XSS Puzzles
CVE-2022-21703: cross-origin request forgery against Grafana

Can't get enough of postMessage XSS? Check out @spaceraccoonsec's writeup on two XSS vulnerabilities he found on bug bounty programs. They involve interesting bypasses and advanced tips worth adding to any DOM XSS methodology.

Another interesting finding is a CSRF found on Grafana by @jub0bs and @theabrahack. It could basically make a Grafana Admin unwittingly send you a user invite to become admin of their instance, demonstrating that CSRF is definitely not dead.

3. Video of the week

My API Testing Automated Toolbox

Testing a small intentionally vulnerable API is one thing, but where to start when you're looking for bugs in a large API with thousands of requests on a hardened bug bounty target?
Watch @InsiderPhD explain a sensible approach that combines automation and a manual workflow, with details on the tools she recommends.

4. Article of the week

A technique to semi-automatically find vulnerabilities in WordPress plugins

What is better than finding a vulnerability in a WordPress plugin? Finding over 100 vulnerabilities in dozens of popular WordPress plugins!
@kazet1234 details a semi-automatic approach used to scan for multiple vulnerability classes including XSS, SQL injection, CSRF, arbitrary file read and more. Amazing research that is interestingly transferable to other CMSes.

5. Tool & Tip of the week

fonetic-go
35 bytes PHP backdoor that's protected by a password & supports arbitrary function calls

@s0md3v just dropped these two beautiful gems. The first one is a Go tool that tells you whether a string is machine-generated or human readable. I'm not sure which use case he has mind, but I'd use this to programatically extract potential secrets from code.

The second tool is a neat PHP webshell that is protected by a password and supports arbitrary function calls despite being very short. From now on, this is my go-to PHP webshell!

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- OrwaGodFather Methodology
- 100 hours of bug bounty on a public Hackerone program. Bounty vlog #1 – Stripe
- Listen and learn from pentester Rana Khalil
- Bug Bounty Recap January 27 – February 2
- How to Be an Ethical Hacker in 2022 & Blog post
- Assembly – Pwn Zero To Hero 0x00
- Reverse Engineering 101 – Introduction to IDA PRO: Reversing/Patching a Binary from crackmes.one

Podcasts

- History of Hacking. Joe "Kingpin" Grand, Hardware Hacker. Former L0pht Member.

Webinars

- OAuth 2.0 Hacking for Beginners with Farah Hawa
- Vulns Unleashed: Pwnkit
- [SecWed] 26 Jan 22 | Automate Reverse Engineering CTF with Angr & An introduction to container hacking

Conferences

- DefCamp 2021, especially:
  - Abusing postMessage API for 6 figures/year
  - What it takes to be good at bug bounty hunting
  - Recipe for a beginner in bug bounty hunting
- ChaosDB: How We Hacked Databases of Thousands of Azure Customers (rev)
- CactusCon 10

Slides & Workshop material

- Attacking JavaScript Engines in 2022

Tutorials

- Nmap: Host Discovery
- How to restrict XXE resolving? #BlueTeam
- Vulnerabilities that aren't. ETag headers
- OSINT without APIs
- I'm Bringing Relaying Back: A Comprehensive Guide On Relaying Anno 2022

Writeups

Challenge writeups

- SSTI Method Confusion in Go.
- UHC – Pressed
- SQLi, SSTI & Docker Escapes / Mounted Folders – HackTheBox University CTF "GoodGame"
- H1-CTF Hacky Holidays Writeups by akshansh & w31rd0

Pentest writeups

- How We "Forced" Our Client To Fix A Low Severity Security Bug And Still Got Appreciated!

Responsible(ish) disclosure writeups

- My experience of Hacking The Dutch Government #Web
- Don't trust comments #Web
- A misconfigured Apache Airflow to AWS Account Compromise
- Malicious Kubernetes Helm Charts can be used to steal sensitive information from Argo CD deployments #CI/CD
- CoronaCheck App TLS certificate vulnerabilities #iOS #Android

Bug bounty writeups

- What Bypassing Razer's DOM-based XSS Patch Can Teach Us
- How I approached Dependency Confusion!
- Abusing Facebooks `Call To Action` To Launch Internal Deeplinks (Facebook, $4,000)
- My first bounty, IDOR + Self XSS [€3000] (Intigriti, $3,000)
- HigherLogic Community RCE Vulnerability ($1,250)

- A *wontfix* request header injection vulnerability in net/http (Ruby)
- CVE-2021-44142: Details On A Samba Code Execution Bug Demonstrated At Pwn2Own Austin ($45,000)

Tools

- LFIDump: A simple python script to dump remote files through a local file read or local file inclusion web vulnerability
- Aerides & Intro: An implementation of infrastructure-as-code scanning using dynamic tooling
- SMBSR: Lookup for interesting stuff in SMB shares
- SMBeagle: SMB fileshare auditing tool that hunts out all files it can see in the network and reports if the file can be read and/or written (useful for lateral movement and privilege escalation)
- EvilSelenium: A C# tool that weaponizes Selenium to attack Chrome

Tips & Tweets

- @mrtuxracer, @equat0rium & @samm0uda's inspiring success stories
- Get an alert(1) by swearing at JavaScript
- Bypass for XSS filters that allow SVG tags
- XSS filter bypass
- How to limit the RAM used by Burp

Misc. pentest & bug bounty resources

- InsecureProgrammingDB: Insecure programming functions database
- Awesome Cyber Security Newsletters
- Linux /proc/ virtual file system in one single page
- Top 25 Browser Extensions for Pentesters and Bugbounty Hunters (2022)
- File formats, Techniques and Tools that can be used to execute code in MS Office
- reapoc

Articles

- GitHub: The Red-Teamer's Cheat-Sheet
- Windows Drivers Reverse Engineering Methodology
- How Android updates work: A peek behind the curtains from an insider

- Linux (In)security
- Windows Persistence Using WSL2

Challenges

- Intigriti's February XSS challenge By @aszx87410
- wrongsecrets: Examples with how to not use secrets

Bug bounty & Pentest news

- Bug bounty
  - Intel Launches Project Circuit Breaker (A new expansion of its Bug Bounty program)
  - Announcing the public launch of Cloudflare's bug bounty program
- Cybersecurity
  - Bittersweet Symfony: Devs accidentally turn off CSRF protection in PHP framework
  - Microsoft to block internet macros by default in five Office applications
  - Open Source Security Foundation launches new initiative to stem the tide of software supply chain attacks
- Upcoming events
  - Intigriti 1337UP LIVE (March 12)
  - Hacking Battlegrounds #4: Valentine's Special – Hacking Will Tear Us Apart! (Live stream on February 18)
- Tool updates
  - Findomain v6.0.0 (Breaking changes)
  - reconFTW v2.2
  - Mythic 2.3 — An Interface Reborn & Apollo 2.0 — New Year, New Features

Non technical

- CVELE: Wordle but for CVE!
- Stop Storing Secrets In Environment Variables!