Bug Bytes #146 – Driftwood, Trojan Source & XSS via smart contract

BY ANNA HAMMOND · NOVEMBER 10, 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 1 to 8.

Our favorite 5 hacking items

1. Tools of the week

Driftwood & Intro
Burp PAC Server

Driftwood is the result of A-M-A-Z-I-N-G research on asymmetric private keys, by the creators of TruffleHog. Identifying if and what private keys are used for, is a problem bug hunters and pentesters might often face. Driftwood will let you know quickly if the private key is used for TLS or as a GitHub SSH key.
I highly recommend the introductory video for details on the research and inner workings of the tool.

Another very useful tool is @honoki's Burp PAC Server. It is a Burp extensions that generates a PAC script to use in your browser. It makes it route only traffic that matches your Burp scope to Burp. So, no more noisy requests from the browser appearing in Burp!

2. Vulnerability of the week

Trojan Source: Invisible Vulnerabilities (CVE-2021-42572) & Rapid7 analysis

"Trojan Source" attacks described in this paper rely on Unicode Bidirectional control characters. Including them inside comments makes them invisible to humans, but most compilers don't support these characters and reorder them. This causes discrepancies in how the code is read by human reviewers and interpreted by compilers.

3. Conference of the week

OWASP Global AppSec Virtual 2020

You will love this playlist if you are interested in topics like AppSec, mass recon, OAuth, hacking APIs, mobile apps, WhatsApp, containers, code review, and crypto. I know I'm going to be busy for a while watching these.

4. Writeup of the week

Escalating XSS to Sainthood with Nagios

This is such a well written writeup! I love the "End-to-End Attack" examples that show how the different vulnerabilities can be chained to fully compromise Nagios servers. If you are a pentester, writing these sections that illustrate complete attack scenarios is a great way to convey both the technical and overall business risk to clients.

5. Tweet of the week

Using smart contracts to bypass front-end validation and register ENS names that contain XSS payloads

I am not into smart contract security but bugs like this are really cool. @theRaz0r found a way to register ENS (Ethereum Name Service) names with XSS, which is not allowed by the frontend on https://ens.domains. This can be bypassed using a smart contract and, makes any applications that integrate ENS vulnerable to XSS.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Can Hackers Get Into Every Device?
- Easy content discovery! GoBuster – Hacker Tools & Accompanying blog post

Podcasts

- A MacOS SIP Bypass & an XSS Fiesta [Bounty Hunting Podcast]

Webinars

- Containers in a nutshell — ähm pod! Containers in a pod
- WWHF | Advanced Phishing Threat (APT), The Reel Dangers of Surfing the Web | Payton Miller
- BHIS | Hack for Show, Report For Dough: Part 2 w/ BB King

Slides & Workshop material

- A Konami Code for Vuln Chaining Combos & Blog post

Tutorials

- Recon, Vulnerable Code Assessment, Exploit Automation, Bypasses & Patching all one. (Python, PHP)
- BOF2shellcode — a tutorial converting a stand-alone BOF loader into shellcode
- AD Delegation Attacks: Unconstrained Delegation
- Finding Privilege Escalation Vulnerabilities in Windows using Process Monitor

Writeups

Challenge writeups

- HTB: Explore (The first Android box on HTB)
- Roda – BSides Ahmedabad CTF 2021
- How to run an XXE injection via an SVG Image Upload!

Pentest writeups

- Pentaho Business Analytics Security Assessment Report & PoCs

Responsible(ish) disclosure writeups

- h1 vendor ATO
- How To Exploit CVE-2021-40539 On Manageengine Adselfservice Plus #CodeReview
- SmartStoreNET – Malicious Message leading to E-Commerce Takeover #CodeReview
- Chaining Three Zero-Day Exploits in ITSM Software ServiceTonic for Remote Code Execution
- HacktoberFest2k21 vulnerability: How users metadata can be changed via Auth JWT tokens leaking from waybackurls
- Rapid7 analysis: Pre-Auth Takeover of Build Pipelines in GoCD (CVE-2021-43287) #CI/CD

Bug bounty writeups

- Insufficient Redirect URI validation: The risk of allowing to dynamically add arbitrary query parameters and fragments to the redirect_uri (GitHub, Microsoft, StackExchange)
- Dangerous XSS bug in Google Chrome's 'New Tab' page bypassed security features (Google, $1,000)
- A Technical Analysis of CVE-2021-30864: Bypassing App Sandbox Restrictions (Apple)
- The Speckle Umbrella story — part 2 (Google)
- HackerOne Staging uses Production data for testing (HackerOne, $1,000)

- HTTP Request Smuggling due to ignoring chunk extensions (Node.js, $250)

See more writeups on The list of bug bounty writeups.

Tools

- ghorg: Quickly clone an entire org/users repositories into one directory – Supports GitHub, GitLab, Bitbucket, and more
- smbls & Intro: A simple Impacket-based tool to check a set of credentials against many Windows hosts and get permission for SMB shares
- CredMaster & Intro : Password spraying tool that uses FireProx APIs to rotate IP addresses, stay anonymous, and beat throttling

Tips & Tweets

- @theRaz0r used smart contracts to bypass front-end validation and register ENS names that contain XSS payloads
- css-fuzzer that helps find characters to break out of CSS strings
- If a Kubernetes user can change their username, setting it to "system:kube-controller-manager" will give them the rights of the controller manager
- Sneaky way to open/close CSS comments on Chrome
- Some payloads @bbuerhaus uses to detect vulnerabilities like XSS, HTML injection, template injection...
- Burp converts `\n` to `\r\n` if you copy and paste it

Misc. pentest & bug bounty resources

- Fuzzingbook 1.0
- MalAPI.io (maps Windows APIs to common techniques used by malware)
- Nmap Cheat Sheet – Reference Guide
- Computing fundamentals course
- Many passwords

Challenges

- Winja CTF | c0c0n 2021 (November 12-13)
- University CTF 2021 (November 19-21)
- Can you read filenames on our system? #CodeReview

Articles

- Finding and Fixing DOM-based XSS with Static Analysis & Related JScamp talk
- Automating DOM XSS Discovery & dump-scripts
- How SSL certificates are leaking sensitive information
- Shadow Credentials: Workstation Takeover Edition

Bug bounty & Pentest news

- Bug bounty
  - Pwn2Own Austin 2021: Synacktiv crowned Masters of Pwn after Sonos One, WD NAS exploits
- Upcoming events
  - HACKtheMACHINE Unmanned (November 16-19)
  - MystikCon 2021 (November 21)
  - INTENT (Security Research Summit) (November 16)
- Tech
  - Mozilla debuts Site Isolation technology with Firefox update
  - Microsoft brings JavaScript to Excel
- Tool updates
  - New gadgets added to the Client-Side Prototype Pollution repo
  - Refactoring of axiom-ssh, axiom-init, and axiom-fleet
  - Burp Professional / Community 2021.9.1 (New SSTI checks, Turbo Intruder "Deduplicate" button, and more)
  - Grep-Match in Burp isn't a boolean anymore (since v2021.9.1)
  - LOLBAS entries have been mapped to ATT&CK v10