Bug Bytes #77 – Exploiting unexploitable XSS, Wordlists galore & RCE from any website with Bitdefender

BY ANNA HAMMOND · JULY 1, 2020 · 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.

This issue covers the week from 19 to 26 of June.

Our favorite 5 hacking items

1. Tip of the week

JS frameworks which simulate events and can turn an XSS that requires user-interaction into an XSS that doesn't & Demo

This is crazy. @freddyb had the idea to leverage events simulation in JavaScript frameworks, to bypass the user interaction required to exploit some XSS vulnerabilities. In other words, the XSS is triggered by simulating user actions instead of waiting for victims to actually perform the corresponding actions themselves.

This technique also works for hidden inputs. Time to revisit any old unexploitable XSS!

2. Writeups of the week

Exploiting Bitdefender Antivirus: RCE from any website

Simple story of some complicated XSS on Facebook

The first writeup by @WPalant is a cool combination of antivirus exploitation and remote Web vulnerabilities. The gist is that Bitdefender handles HTTPS certificate errors itself (instead of delegating it to the browser), and leaks some sensitive tokens. Any website can read them and use them to start a session with the Safepay browser. RCE is then obtained by opening URLs like `data:text/html,nada --utility-cmd-prefix=\"cmd.exe /k whoami & echo\"` .

The second writeup is about two reflected XSS bugs found on Facebook. It reads like a fascinating investigation. @win3zz identified that MicroStrategy Web SDK was used, downloaded its source code, analyzed it, and transformed the bugs found into working exploits.

3. Tool of the week

Pencode

Pencode is a command line tool for creating complex encoding chains (e.g. `urlencode(b64encode(hexencode(string)))`). It can be used as a standalone tool or as a Go library. Handy for handling complex encoding in scripts!

@joohoi is also planning to add integration with ffuf.

4. Resources of the week

Golang HandleFunc wordlisr by @d0nutptr

@NahamSec & @_StaticFlow_'s 1stleveldomainsbycount

PWDB – New generation of Password Mass-Analysis

Crafting a custom wordlist for python-flask webservers

This week's been all about wordlists!

@d0nutptr shared the most used HTTP endpoints, found by analyzing 500 popular Golang repositories. This inspired @r0bre to build a similar wordlist for python-flask webservers by analyzing Github repositories. He shares both the resulting wordlist and details of the whole process.

@NahamSec & @_StaticFlow_ shared a list of subdomains built by scanning ~200 million IPs from bug bounty targets.

And @ahakcil collected 100 million leaked credentials and published stats on what he found, as well as wordlists of the most common passwords.

5. Tutorial of the week

Exploiting SSTI in Thymeleaf

This is a nice tutorial to bookmark. If you come across Thymeleaf, a Java template engine, you'll know exactly how to test for SSTI, from detection payloads to real-world exploitation.

Other amazing things we stumbled upon this week

Videos

- h1-2006 Virtual Live Hacking Event: Meet the Hackers who #HackForGood, Community Day – CTF, Kickoff, Recap & Closing Ceremonies
- Interview with Joona Hoikkala aka. @joohoi, creator of ffuf
- Interview with Peter Yaworski
- BOUNTY THURSDAYS – India EK NUMBER!
- Burp for Beginners: How to Use Repeater
- ATTACKING JWT FOR BEGINNERS!
- Modern Webapp Pentesting: How to Attack a JWT w BB King 1 Hour BHIS HEVC
- Igniting Creativity for a (Hacking) Game – Game Devlog #2
- @bsidesahmedabad Live with Bhavuk Jain

- Upload Scanner Burp extension: Level up your file upload hacking skills #bugbounty #upload #hacking
- Hacking Sunday ep. 2 (Deserialization)
- Beacon Object Files – Luser Demo

Podcasts

- Security Now 772 – Ripple20
- Darknet Diaries EP 68: Triton
- Layer 8 Podcast Episode 30: Brent White and Tim Roberts
- Risky Business #589 — Why Microsoft's steep E5 license pricing is a national security risk
- How to Prevent Account Takeover Attacks – John Chirhart – ASW #109

Webinars & Webcasts

- Webcast: IPv6: How to Securely Start Deploying
- ATT&CK® Deep Dive: Process Injection
- SANS webinars:
  - Post Modern Web Attacks: Kubernetes Attack Matrix
  - SANS@MIC – Catch and release: phishing techniques for the good guys
  - Overt Operations | When the Red Team gets in your Face!

Conferences

- NahamCon 2020 (on Youtube)
- Security BSides Athens 2020, especially:
  - A Less Known Attack Vector, Second Order IDOR Attacks – Ozgur Alp
  - NoSQL Means No Security? – Philipp Krenn
- BSides Greenville 2020 – Track #1, Track #2, Track #3, Track #4 & Schedule
- Open Security Summit
- All The Talks 2020 – Security & MyDevSecOps Virtual Sessions, especially:
  - How to Hack OAuth – Aaron Parecki
  - Basics of OAuth 2.0 and OpenID Connect – Andreas Falk
  - Web Components for Authentication: The what, the how and the why – Ana Cidre

Tutorials

Medium to advanced

- Hacking with Environment Variables: Interesting environment variables to supply to scripting language interpreters
- External IP domain reconnaissance and attack surface visualization in under 2 minutes.
- How to Create a Disposable Email Address with Gmail
- Bypassing string base XSS protection with Optional chaining
- Hardcoded secrets, unverified tokens, and other common JWT mistakes
- IoT hacking field notes #2: Using bind mounts to temporarily modify read-only files
- EternalRed aka Sambacry without Metasploit & EternalBlue without Metasploit

Beginners corner

- Introduction to Hacking Thick Clients: Part 6 – The Memory
- Thick Client Proxying – Part 11 – GOG Galaxy and Extract-SNI
- Let's Reverse Engineer an Android App!
- Disable clipboard events override in Firefox
- How to install Kali Linux [All possible ways 2020]
- A Guide To Social Media Intelligence Gathering (SOCMINT)

Writeups

Challenge writeups

- Intigriti June XSS challenge solutions & winner
- The Tangled Browsers: Beyond XSS (Part 1)

Pentest writeups

- MSBuild: A Profitable Sidekick!
- Bypassing External Mail Forwarding Restrictions with Power Automate
- Java Deserialization Exploitation With Customized Ysoserial Payloads

Responsible(ish) disclosure writeups

- CVE-2020-8163: Partial Remote Code Execution #Web #Rails
- Exploiting a Webroot Type Confusion Bug #Web

- SecureAuth Version 9.3 #Web
- Bring your own .NET Core Garbage Collector #.NET
- Crashing VMware Guests with a Silly Filesystem Bug #MacOS
- CVE-2020-1170 – Microsoft Windows Defender Elevation of Privilege Vulnerability #PrivEsc #Windows
- Zoom In: Emulating 'Exploit Purchase' in Simulated Targeted Attacks #PrivExc #Windows
- eLection 2.0 Authenticated Remote Code Execution Vulnerability #Web
- DLL Hijacking at the Trend Micro Password Manager (CVE-2020–8469) #Windows #PrivEsc
- My Adventures Hacking the iParcelBox #IoT

Bug bounty writeups

- Bypassing Digits origin validation which leads to account takeover (Twitter, $5,040)
- Uploading large payload on domain instructions causes server-side DoS (HackerOne, $2,500)
- Keybase client (Windows 10): Write files anywhere in userland using relative path in "download attachement" feature (Keybase, $5,000)
- From Recon to Bypassing MFA Implementation in OWA by Using EWS Misconfiguration ($500)
- How i hacked worldwide ZOOM users (Zoom)
- Leveraging an SSRF to leak a secret API key ($1,000)
- Chaining an IDOR with a business-logic error to achieve critical impact
- Hackerone Bug Bounty Report: Hinge (Hinge, $250)

See more writeups on The list of bug bounty writeups.

Tools

- Getrelationship.py: Python script to get domain relationships using BuiltWith
- Shaggy-rogers: Clojure lambda to scan blob files for sensitive content
- Travis Grabber: Grabs all logs for all builds for any given Organisation from Travis CI. Similar to CILeek, but in Go
- BugPoC: Burp Suite Extension to send raw HTTP Requests to the BugPoC HTTP PoC Generator (BugPoC.com)
- ChopChop: Go tool for dynamic application security testing on web applications
- disas-apk: All-in-one tool for automating Android app reverse engineering
- Subvenkon: Subdomain enumerator which gathers information from Venkon

- Physmem2profit: Create a minidump of a target hosts LSASS process by analysing physical memory remotely
- seeker: Accurately locate smartphones using social engineering
- Securing Active Directory: Performing an Active Directory Security Review
- Max & Intro: Scripts for maximizing BloodHound with a simple suite of tools
- Talon & Intro: A tool designed to perform automated password guessing attacks while remaining undetected

Misc. pentest & bug bounty resources

- Pretty print nmap grepable files
- Docker image for running any Python 3 scripts
- The Bug Hunter Methodology v4 summed up in a picture
- OAuth in one picture & JWT Authentication
- The Rajappan Project
- @CircleNinja's "Mental Health for Hackers" Discord channel
- The Art of Packet Crafting with Scapy & Repo
- Library of Resources for Industrial Control System Cyber Security
- Active Directory Cheat Sheet
- CVE-2020-10665 Docker Desktop Local Privilege Escalation: First public exploit by @spaceraccoonsec

Challenges

- New @PwnFunction XSS challenge
- New topic with 10 labs on Web Security Academy: Insecure deserialization

Articles

- The problem with Parse: A low-code server that endangers over 63,000,000 users.
- A recap of the Q&A session on Twitter
- AWS IAM Assume Role Vulnerabilities Found in Many Top Vendors
- Denial of Wallet Attacks on AWS
- Things I learned after rooting 25+ Hack the Box machines!
- Hijacking DLLs in Windows

- The Case of BusyBox Wget: A Long Overdue Fix
- Engineering antivirus evasion
- Further Evasion in the Forgotten Corners of MS-XLS
- IndigoDrop spreads via military-themed lures to deliver Cobalt Strike

News

Bug bounty & Pentest news

- Crowdsourced ethical hacking platform Intigriti raises €4M+
- OffSec Giving Program
- LiveQL episode 1: finding non-intuitive string manipulation vulnerabilities in C code: July 7
- Sony launches PlayStation bug bounty ahead of PS5 rollout
- Bug hunter problems

Reports

- Demystifying Hackers: Bugcrowd's 2020 Inside the Mind of a Hacker Report
- Snyk – The State of Open Source Security 2020
- Academics studied DDoS takedowns and said they're ineffective, recommend patching vulnerable servers

Vulnerabilities

- Unpatched regex bug leaves Node.js apps open to ReDoS attacks
- Backdoor wide open: critical vulnerabilities uncovered in GeoVision
- Web admins urged to update Magento stores as first release line reaches end of life
- Adobe, Mastercard, Visa warn online store owners of Magento 1.x EOL: "Almost 110,000 online stores are still running the soon-to-be-outdated Magento 1.x CMS."
- Twitter apologizes for business user data leak

Breaches & Attacks

- Glupteba – the malware that gets secret messages from the Bitcoin blockchain
- Credit card skimmers are now being buried in image file metadata on e-commerce websites & Technical details
- Docker servers infected with DDoS malware in extremely rare attacks
- Chinese bank forced western companies to install malware-laced tax software

- There are DDoS attacks, then there's this 809 million packet-per-second tsunami Akamai says it just caught
- Evil Corp blocked from deploying ransomware on 30 major US firms
- REvil ransomware scans victim's network for Point of Sale systems
- Microsoft: Attackers increasingly exploit Exchange servers
- BlueLeaks: Data from 200 US police departments & fusion centers published online
- New Mac malware uses 'novel' tactic to bypass macOS Catalina security
- Hackers use fake Windows error logs to hide malicious payload
- Fxmsp hackers made $1.5M selling access to corporate networks
- Oracle's BlueKai tracks you across the web. That data spilled online

Other news

- 400 organizations sign open letter to save Open Technology Fund (OTF)
- Microsoft quietly created a Windows 10 File Recovery tool, how to use
- US govt: Julian Assange tried to recruit hacker to steal hush-hush dirt and we should know – the hacker was an informant
- Adobe wants users to uninstall Flash Player by the end of the year
- TikTok To Stop Clipboard Snooping After Apple Privacy Feature Exposes Behavior & Penetrum Security Analysis of TikTok versions 10.0.8 – 15.2.3
- Here's a headline we never thought we'd write 20 years ago: Microsoft readies antivirus for Linux, Android
- Safari 14 removes Flash, gets support for breach alerts, HTTP/3, and WebP
- FBI uses T-shirt, tattoo and Vimeo clips to track down alleged arsonist
- Career Choice Tip: Cybercrime is Mostly Boring
- Experts Denounce Racial Bias of Crime-Predictive Facial-Recognition AI

Non technical

- Hacker Spotlight: Interview with randomdeduction
- Toward Applied Andragogy in Cyber Security Education #ForContentCreators
- MFA v2.0: Improving the State of Multifactor Authentication
- Why API Security Is Different and How the OpenAPI Spec Can Help
- A Guide to Digital Reconnaissance
- Remote Workforce is NOT the New Norm, but "Secure Work Anywhere" Should Be

- So You Want to Learn ICS Security...
- The top 10 best hacking documentaries of all time
- Why More Than Half of Email Phishing Leaks Happen on Mobile Devices
- Mental Fatigue and Decision Making in a Time of Crisis & Social Engineering Red Flags document
- Sketch 403 – "Private Browsing" – A high level view of what it does and does not do!

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 06/19/2020 to 06/26/2020.