Bug Bytes #101 – XSS for PDFs, KringleCon & A whole bunch of fantabulous tools

BY ANNA HAMMOND · DECEMBER 16, 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 06 to 13 of December.

Intigriti News

FireEye hacked, Amnesia:33 & A device-bricking UEFI malware

Our favorite 5 hacking items

1. Article of the week

Portable Data exFiltration: XSS for PDFs & Presentation

This is @garethheyes's new research presented at Black Hat Europe. He developed a new injection technique based on controlling a single HTTP link in a PDF document. It allows for exfiltrating the PDF file's contents (like a Blind XSS via PDF) or SSRF. Several PDF libraries were found vulnerable including Acrobat and Chrome's PDFium.

This is really cool. PDFs files are used all the time, and they can be totally compromised with just one little link!

2. Writeups of the week

Content-Security-Policy Bypass to perform XSS using MIME sniffing
How I hacked Facebook: Part One (Facebook, $7,500)
The YouTube bug that allowed unlisted uploads to any channel (Google, $6,337)

The first one is about two impossible XSS, blocked by CSP, that became exploitable when chained together using MIME sniffing. The second writeup is about an admin account takeover (in a thefacebook.com subdomain) caused by an exposed password change endpoint. The third writeup is about a simple IDOR that would've allowed anyone to upload videos to someone's YouTube channel.

These are all proof that the best findings aren't necessarily the most complicated!

3. Tutorial of the week

Advanced Testing Of Web Application With Custom Message Signing Using Hackvertor

This tutorial shows how to use the Burp extension Hackvector to bypass replay protection mechanisms like message signing. This isn't a new problem but it is not extensively documented, so this can be helpful.

4. Conference of the week

KringleCon 2020

Y'all 've been nice this year, so Santa Claus has great talks for you! Topics range from S3 buckets weaknesses tocar hacking, adversary emulation, HID card hacking, red teaming, Kubernetes attacks, Offensive Security Tools and more.

Burp Suite Sequencer users will also be interested in the "Random Facts About Mersenne Twisters" talk on pseudo-random number generators and this thread on how Sequencer works.

5. Tools of the week

Depix & Intro
Proxify
HTTPSignatures & Intro

Depix is a Python tool that helps recover passwords from pixelized screenshots. It's worth trying when looking for information disclosure in public documents.

Proxify is a new Web proxy in Go by @pdiscoveryio. It looks interesting either as a standalone tool or chained with Burp/ZAP. It can dump all traffic to a file, replay traffic in Burp, match and replace requests and responses on-the-fly, match/filter traffic...

HTTPSignatures is a Burp extension that implements the Signing HTTP Messages draft-ietf-httpbis-message-signatures-01 specification draft. As apps start adopting HTTP Signatures, this extension will help test them seamlessly.

Other amazing things we stumbled upon this week

Videos

- Better Bug Bounty Tool Results with DNSValidator
- Gynvael Talks About Infosec Certificates, Playing Ctfs, Google's Ctf, and Getting Into Hacking!

- Bug Bounty (how to make money HACKING!!) // ft. STÖK
- Cybertalk EP8 – Better Bug Bounty Hunting, CTF's & Reverse Engineering
- "Profiling BurpSuite Spider/Crawler" Part 1
- Understanding Nat Slipstreaming
- How To Prevent IDORs | Security Simplified, Intro to Command Injection | Security Simplified & How to Prevent Command Injections
- My Life in Short/Shirt Stories (December 2020 Project)
- FAILING – motivational speech
- Distributed Recon – Axiom Scan Resolves 6M FQDNs in 10 Minutes

Podcasts

- Security Now: Amazon Sidewalk – Google Play Core Library, iOS Zero-Click Radio Proximity Exploit, Apple M1 Chip
- Risky Business #608 — FireEye discloses breach and tool exfil
- Atheris Python Fuzzer, Bronze Bit Attack, & FireEye Highlights – ASW #134
- Steam Flaws, Kerberos Exploit, Facebook Lawsuit, & Black Mirror – Wrap Up – SWN #88
- Layer 8 Podcast Episode 36: Inês Narciso – Teamwork Makes Dreamwork
- The Privacy, Security, & OSINT 199-Physical Security Assessments
- The InfoSec & OSINT Show 37 – Jenny Radcliffe & People Hacking

Webinars & Webcasts

- ZAP Deep Dive Series
- Webcast: Getting Started with Burp Suite & Webapp Pentesting
- Q&A: Finding & Reversing Malicious Mobile Apps with Kristina (chmodxx)

Conferences

- Wild West Hackin' Fest – The Roundup | 2020-10
- BSides Calgary 2020
- PasswordsCon 2020 virtual

Slides & Workshop material

- Weaponized XSS Workshop

Tutorials

Medium to advanced

- Abusing exposed Docker Registry APIs
- 4 Free Easy Wins That Make Red Teams Harder
- Connecting GoPhish with Office365

Beginners corner

- A Pentester's Guide to Command Injection
- Finding bugs at limited scope programs (Single Domain Websites)
- Alternative ways to Pass the Hash (PtH)
- Bypassing IP Based Rate-Limit
- Don't Hesitate, Isolate (Your Virtual Machine)

Writeups

Challenge writeups

- SSD Secure Disclosure December – 2020 challenge
- Intigriti's December XSS Challenge winners & writeups

Responsible(ish) disclosure writeups

- SRC-2020-0031 : Microsoft Exchange Server EWS RouteComplaint ParseComplaintData XML External Entity Processing Information Disclosure Vulnerability #Web
- GHSL-2020-205: Remote Code Execution in Apache Struts 2 – S2-061 – CVE-2020-17530 #Web
- Watchcom Discovers New Cisco Jabber Vulnerabilities #Web
- Prototype Pollution in ini package #Web
- Vulnerabilities in McAfee ePolicy Orchestrator #Web
- CVE-2020-17049: Kerberos Bronze Bit Attack – Overview, Theory & Practical Exploitation #AD
- Novel Abuses On Wi-Fi Direct Mobile File Transfers #Wifi
- PsExec Local Privilege Escalation #Windows #LPE

Bug bounty writeups

- Game On – Finding vulnerabilities in Valve's "Steam Sockets" (Valve)
- How I dumped PII information of customers in an ecommerce site?
- A very long name in hey.com can prevent anyone from accessing their contacts and probably can cause denial of service (Basecamp, $1,000)
- How i got my First Bug Bounty in Intersting Target (LFI to SXSS)
- CVE-2020-8286: Inferior OCSP verification (Curl, $900)

See more writeups on The list of bug bounty writeups.

Tools

- Solarflare & Intro: SolarWinds Orion Account Audit / Password Dumping Utility
- Cloudlist: A Go tool for listing Assets from multiple Cloud Providers
- FlyDNS: Related subdomains finder
- JNDI-Exploit-Kit: A modified version of @welk1n's JNDI-Injection-Exploit. It can be used to start an HTTP Server, RMI Server and LDAP Server to exploit java web apps vulnerable to JNDI Injection
- CornerShot: Amplify network visibility from multiple POV of other hosts
- pstf^2 & Intro: Passive Security Tools Fingerprinting Framework
- SnitchDNS & Intro: Database Driven DNS Server with a Web UI, that makes DNS admin easier for red teams & pentesters
- rga / ripgrep-all: ripgrep wrapper that can also search in PDFs, E-Books, Office documents, zip, tar.gz, etc
  - "Wraps ripgrep, the fastest grep-like tool, but enables it to search pdf, docx, sqlite, jpg, movie subtitles (mkv, mp4), etc."
- rawsec_cli: Rawsec's Cybersecurity Inventory cli. Search pentesting tools, resources, ctf, os.

Tools updates

- Lessons Learned on Brute-forcing RMI-IIOP With RMIScout
- Professional / Community 2020.12

Misc. pentest & bug bounty resources

- @irsdl research notes
- OpenSSF CVE Benchmark project & Intro

- OWASP GraphQL Cheat Sheet
- Twitter SecLists
- cloudpentest-aws-gcp
- Infrastructure as Code: Dynamic Systems for the Cloud Age
- WADComs
- Bugs found by Cryptofuzz
- Week in OSINT #2020-49

Challenges

- 12 Days Of Hacky Holidays CTF
- The 2020 Sans Holiday Hack Challenge
- sconwar – sensecon 2020 & Szensecon Discord Bot

Articles

- Web Almanac by HTTP Archive – Security
- Deciphering Google's mysterious 'batchexecute' system
- Using The UK Planning System For OSINT
- ABSTRACT SHIMMER (CVE-2020-15257): Host Networking is root-Equivalent, Again
- Web fuzzers review
- Adventures in Dynamic Evasion
- BlindSide
- Improving DNS Privacy with Oblivious DoH in 1.1.1.1

Bug bounty & Pentest news

- Good News: SANS Virtual Summits Will Be FREE for the Community in 2021
- Pwine Award Winners 2020
- The World's Largest Live Hacking Event
- SANS Open-Source Intelligence Summit 2021 – Live Online

Non technical

- Questions a mentor will want to ask you
- Communication In Bug Bounty Programs (As Triager, Researcher, Manager)
- Analysis of the RECON/Attack Surface Management Space
- Hacker Spotlight: Interview With Tolo7010
- A CVE in our Executive Summary
- Bad CTF Bingo
- Get your work recognized: write a brag document
- Summary: The Pentester's BluePrint

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 12/06/2020 to 12/13/2020.