Bug Bytes #94 – Breaking Symfony apps, Why Cyber Security is so hard to learn & how best to approach it

BY ANNA HAMMOND · OCTOBER 28, 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 18 to 25 of October.

Intigriti News

Security Snacks #3 – 2020 Threat landscape, Top 25 exploited vulnerabilities & The cost of a data breach

Our favorite 5 hacking items

1. Article of the week

Secret Fragments: Remote Code Execution On Symfony Based Websites

This is excellent research by @ambionics on a misconfiguration that leads to RCE on Symfony-based applications. The idea is to guess, bruteforce or bypass the secret used to sign /_fragment requests that allow running arbitrary PHP code. Everything is detailed in this thorough article, from theory on how fragments work to obtaining the secret and exploiting it in practice.

2. Writeups of the week

Samsung S20 – RCE via Samsung Galaxy Store App (Samsung)
GitHub Pages – Multiple RCEs via insecure Kramdown configuration – $25,000 Bounty (Github, $25,000)

These are brilliant writeups on vulnerabilities that led to RCE. F-Secure Labs found a bug chain that allowed attackers to install any application on the Galaxy Store without user consent. They intended to use it for Pwn2Own 2020, but Samsung patched it before the event.

The second writeup by William Bowling (@wcbowling) shows how he found a couple of RCEs on Github Pages. They allowed anyone with permission to create and build a Github Pages site to execute commands on the GitHub Enterprise Server instance. He actually found three bugs recently that got him $61k in total, including an interesting GitHub Gist – Account takeover via open redirect.

3. Tools of the week

GWTMap & Intro
LiveDOM++

GWTMap is a Python tool for reverse engineering Google Web Toolkit applications. Its introduction article is worth reading as it sums up the state of the art of GWT hacking, existing tools and how this new one can help map the attack surface of GWT apps.

LiveDOM+++ is an online tool by Michał Bentkowski (@SecurityMB) who specializes in browser security and recently published a cool DOMPurify bypass. This tool helps him "compare various HTML parsers in browsers (DOMParser, template.innerHTML and others) and to easily test sanitizers (like DOMPurify)". A nice playground for anyone interested in XSS or bypassing sanitizers.

4. Tutorial of the week

Android Adb Reverse Tethering MiTM Setup

This is about setting up an Android app testing environment when you're using a physical device and have to use a corporate VPN. The setup leverages Gnirehtet and proxychains to make the mobile device use the Internet connection of your PC over ADB, while routig traffic to Burp.

5. Video of the week

Why Cyber Security is Hard to Learn (Tips For Success!)

This is a great piece on why Cyber Security is so hard to learn. Beyond the difficulties most of us already know, it offers excellent advice including three different effective learning strategies, and the long-term mindset to be successful on your journey.

Other amazing things we stumbled upon this week

Videos

- Mattibijnens Talks About Doing Bug Bounties Full Time, Buying a Tesla and Hacking on Intigriti!
- My Learning Workflow as a Developer & Content Creator
- $10k+5k Web cache poisoning – Github + Firefox – Bug Bounty Reports Explained

- Educational Barriers in Cyber Security
- What after Recon? : URLs – Easy $$$
- Most Popular Burp Extensions Explained: Request Smuggler, Logger++ and others #burpsuite #hacking
- 10 Minute Tip: How to find Facebook data when a profile is private

Podcasts

- The InfoSec & OSINT Show 30 – Hakluke & The Bug Bounty Mindset
- Security Now: Anatomy of a Ryuk Attack – Zoom End-to-End Encryption, Windows 10 God Mode, Manifest v3
- Risky Business #602 — US DoJ hooks Sandworm
- SWN #77 – 'KashmirBlack' Botnet, Winston Privacy Vulns, IoT, & Roger Hale
- ASW #127 – Nvidia GeForce Experience Flaws, Firefox 'Site Isolation', & Chrome 0-Day Bug

Conferences

- ShellCon 2020 Live Streams & Schedule
- BSidesMunich 2020

Slides & Workshop material

- Burp suite "ninja moves"

Tutorials

Medium to advanced

- Pass-the-hash WiFi
- Abusing RDP's Remote Credential Guard with Rubeus PTT
- Signed Binary Proxy Execution via PyCharm
- Leveraging LD_AUDIT to Beat the Traditional Linux Library Preloading Technique

Beginners corner

- Brute Force Attacks: Protection and Mitigation Measures
- Finding OSINT Eggs In Mobile Apps
- Phone numbers investigation, the open source way

- Google Cloud IAM for Security Teams #BlueTeam

Writeups

Challenge writeups

- Hack this repository: The EkoParty 2020 GitHub CTF challenges
- Hacker101 CTF walkthrough of "Model E1337 – Rolling Code Lock" (+ hardened) (video)

Pentest writeups

- Bypassing WAF to do advanced Error-Based SQL Injection

Responsible(ish) disclosure writeups

- CVE-2020-15906 #Web
- Multiple Address Bar Spoofing Vulnerabilities In Mobile Browsers & Vulntober: Multiple Mobile Browser Address Bar Spoofing Vulnerabilities #WEB
- Enumerate AWS API Permissions Without Logging to CloudTrail & PoC/Helper scripts #Cloud
- Vulnerability Spotlight: A deep dive into WAGO's cloud connectivity and the vulnerabilities that arise #RCE #Web
- How I Found An alg=none JWT Vulnerability in the NHS Contact Tracing App #Web #CodeReview
- Gateway2Hell – Multiple Privilege Escalation Vulnerabilities in Citrix Gateway Plug-In #LPE
- When ntuser.pol leads you to SYSTEM #LPE

Bug bounty writeups

- Accidental Observation to Critical IDOR
- Undocumented fileCopy GraphQL API (Shopify, $2,000)
- Broken OAuth leads to change photo profile users . (Dropbox, $512)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- prys-hacks/image-to-text: Keybind to copy-paste through images. It takes an image from your clipboard, runs it through OCR (extract the text), and then copies the output to the clipboard
- android_frida_scripts/file_exists.js: Frida script to identify potential arbitrary code execution dynamically

More tools, if you have time

- Orkestra: Android Inspection framework
- tlds_hunt: DNS permutation tool to hunt for TLDs
- Procrustes: A bash script that automates the exfiltration of data over dns in case we have a blind command execution on a server where all outbound connections except DNS are blocked
- BountyIt: A fuzzer made in golang for finding issues like xss, lfi, rce, ssti...that detects issues using change in content length and verify it using signatures
- Substr3am: Passive reconnaissance/enumeration of interesting targets by watching for SSL certificates being issued
- Taken: Takeover AWS ips and have a working POC for Subdomain Takeover
- PwnDoc: Pentest Report Generator
- PyRDP 1.0: RDP man-in-the-middle (mitm) and library for Python with the ability to watch connections live or after the fact
- wsb-detect: C library to detect if you are running in Windows Sandbox

Misc. pentest & bug bounty resources

- Bug Hunter Handbook
- CloudSecDocs & Intro
- Cloud Security Tools
- Adversarial ML Threat Matrix & Intro
- Advanced Level Resources For Web Application Penetration Testing
- Getting Started as a Penetration Tester in NZ (2020 Edition)
- six2dez Pentest Book

Challenges

- @LiveOverflow XSS challenge
- @RenwaX23's "alert(23) to win" XSS challenge
- YesWeHack DOJO
- Chrome hacking challenge

Articles

- New client-side prototype pollution gadget using a reddit embed post
- Segmentation Vault: Cloning Thick Client Access
- Introducing a new phishing technique for compromising Office 365 accounts
- Exploring an Assembly Loading Technique and Detection Mechanism for the GfxDownloadWrapper.exe LOLBIN
- Let's build a high-performance fuzzer with GPUs!
- Build a Face Recognition System for $60 with the New Nvidia Jetson Nano 2GB and Python

Bug bounty & Pentest news

- Critical new defenses for Microsoft OAuth consent phishing
- Update To Bugcrowd Points System & Private Commenting On Submissions

Non technical

- Switching "sides" in security – How does product security work differ from pen testing and hacking all the things?
- Hacker Spotlight: Interview With Mrtuxracer
- Penetration Testing and Low-Cost Freelancing – The Story of How I Hired 7 Freelancers to Exploit this Weird Vulnerability
- MITRE ATT&CK Tactics Are Not Tactics
- How I got hacked, lost crypto and what it says about Apple's security. Part 1

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 10/18/2020 to 10/25/2020.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com