Bug Bytes #92 – Pwning Apple for three months, XSS in VueJS, Hacking Salesforce Lightning & Unicode by□tes

BY ANNA HAMMOND · OCTOBER 14, 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 04 to 11 of October.

Intigriti News

Our new weekly digest of notable InfoSec news

NEW HOODIES: Embrace the hacker stereotype, but do it with style!

Our favorite 5 hacking items

1. Videos of the week

Unicode vulnerabilities that could by_te you (Part of NorthSec 2020)
Masonhck3571 Talks About Being Disciplined, His Learning Process, and Full Time Bug Hunting!

These are two very informational videos. One is on Unicode vulnerabilities including the latest research such as HostSplit and HostBond attacks. The other is an interview with @Masonhck3571 on transitionning from a non IT job to full-time bug hunting, how he chooses targets, his learning process, etc.

2. Writeups of the week

We Hacked Apple for 3 Months: Here's What We Found

What an incredible writeup! A crew of five bug hunters (@samwcyo, @bbuerhaus, @nahamsec, @erbbysam and @*StaticFlow*) hacked on Apple for 3 months and found 55 vulnerabilities. They shared how it went, the list of vulnerabilities detected, with detailed writeups on 12 of them. It's so impressive when you know that some of them have full-time job and not all the bugs were disclosed (maybe including some new research).

As @hakluke says, an apple doesn't taste as good now, it just tastes like vulnerabilities.

3. Tools of the week

bbrf-client & Intro
jwt-heartbreaker & Intro

BBRF is Pieter Hiele's (@honoki) tool for storing bug bounty data. It is in Python, uses CouchDB and has a client-server architecture. It is meant to be combined with other recon tools to store/read the data collected on a program (subdomains, domains, IPs...). A very handy and well-documented tool!

JWT is a Burp extension to passively scan for JWT tokens signed with a weak secret. I haven't tried it yet but it looks interesting, especially if customized to even more JWT secrets to test.

4. Article of the week

Evading defences using VueJS script gadgets

This is an excellent article on XSS in VuesJS. It is packed with information on identifying and exploiting XSS created from VueJS script gadgets. A must if you're into XSS or plan on testing VueJS sites!

5. Tutorial of the week

Salesforce Lightning – An in-depth look at exploitation vectors for the everyday community

Aaron Costello (@ConspiracyProof) published this in-depth tutorial on hacking Salesforce Lightning by exploiting common misconfigurations of the CRM. This offensive approach hasn't been documented before, so it is very interesting for bug hunters and pentesters.

Other amazing things we stumbled upon this week

Videos

- Cybertalk ep13 – @hakluke Talks About Creating Content, Bug Hunting, Pentest, Automation & Resources
- Finding Your First Bug: Reading JSON and XML for Information Disclosure
- Getting started with Github for Security Professionals and Bug Bounty Hunters & Written guide
- What after Recon? – Demystifying JavaScript Files
- $12,000 Grafana SSRF in Gitlab – Bug Bounty Reports Explained
- ZeroLogon Exploit – Abusing CVE-2020-1472 (Way Too Easy!)
- Giving Effective Presentations: A Crash Course with Chris Crowley

Podcasts

- The InfoSec & OSINT Show 28 – STÖK and Hunting Bug Bounties
- Security Now: Why Win7 Lives On – Android Security, Windows 7 Security, Microsoft Defender
- Risky Business #600 — Who's messing with TrickBot?
- Targeting Trickbot, Static Kitten, & 'Raccine' Ransomware – SWN #71
- Hacked Off 076. Joe Thorpe: Hacking Mobile Apps
- ASW #124 – Things Every Developer Should Know About Security – Chris Romeo
- SWN #72 – Stuxnet Redux, Fancy Bear, & UEFI Bootkits – Wrap Up
- PSW #669 – Assembling Your First Infosec Home Lab – Tony "tjnull" Punturiero

Webinars & Webcasts

- Hacking JWTs for Beginners with Farah Hawa
- Managing containers with Google Kubernetes Engine (GKE)

Conferences

- ARPCon Conference 2020 | Day 1 & Day 2

Slides & Workshop material

- A Hacker's perspective on AEM applications security

Tutorials

Medium to advanced

- Firebase: Google Cloud's Evil Twin – Excerpt
- I Like to Move It: Windows Lateral Movement Part 3: DLL Hijacking
- MITRE ATT&CK turned purple – Part 1: Hijack execution flow

Beginners corner

- How to Store Session Tokens in a Browser (and the impacts of each)
- IOS Pentesing Guide From A N00bs Perspective.1
- Java RMI for pentesters: structure, recon and communication (non-JMX Registries). & Part two — reconnaissance & attack against non-JMX registries
- How to Find Vulnerabilities in Code: Bad Words
- Escape Restricted Shell Environments on Linux
- Proxies, Pivots, and Tunnels – Oh My!
- dumpco.re – asreqroast

Writeups

Challenge writeups

- BugPoC LFI Challenge
- Misc CTF – Request Smuggling
- Chaining Script Gadgets to Full XSS – All The Little Things 2/2 (web) Google CTF 2020

Pentest writeups

- Shell Wars: Episode II – Attack of the Code {Review}
- Breaking JCaptcha using Tensorflow and AOCR

Responsible(ish) disclosure writeups

- Research: Can you build spyware for a Fitbit? #IoT
- Enter the Vault: Authentication Issues in HashiCorp Vault #Web #Cloud
- HP Device Manager – CVE-2020-6925, CVE-2020-6926, CVE-2020-6927
- Smart male chastity lock cock-up #IoT
- CVE-2019-0230: Apache Struts OGNL Remote Code Execution #Web

- A brief encounter with Leostream Connect Broker #Reverse #Web
- Pulse Connect Secure – RCE via Template Injection (CVE-2020-8243) #RCE #Web
- c0ntextomy – Let's Debug Together: CVE-2020-9992 #iOS #RCE
- Anti-Virus Vulnerabilities: Who's Guarding the Watch Tower? #AV #Windows #PrivEsc

Bug bounty writeups

- Research: The mass CSRFing of *.google.com/* products. (Google, $30,000)
- Watch your requests! Open redirect to a complete account takeover
- 6k$ Worth Account Takeover via IDOR in Starbucks Singapore (Starbucks, $6,000)
- JS is l0ve . ($5,000)
- SVE-2020-18025: Unauthorised access to Samsung secure folder files (Samsung, $3,750)
- Our Experiences Participating in Microsoft's Azure Sphere Bounty Program (Microsoft, $160,000)
- Kud I Enter Your Server? New Vulnerabilities in Microsoft Azure (Microsoft)
- Transferring a public group to a private group doesn't remove code from the Elastichsearch API search result (GitLab, $3,000)
- Windows only: arbitrary file read vulnerability in openssl s_server (OpenSSL)

See more writeups on The list of bug bounty writeups.

Tools

- GitLab Watchman & GitHub Watchman : Monitoring GitLab & GitHub for sensitive data shared publicly
- GLORP: A CLI-based HTTP intercept and replay proxy
- reesolve (ree): Tool to do dual-stack IPv4/IPv6 lookups for A & AAAA DNS records
- Asnap: Go tool that aims to render recon phase easier by providing regularly updated data about which companies owns which ipv4 or ipv6 addresses and allows the user to automate initial port and service scanning
- tojson.py: Python tool to convert simple string (find in js file) to JSON body – for brute force api endpoint with many json parameters
- Trident: Automated password spraying tool
- A CrowdSec Primer: A Modern Replacement for Fail2Ban #BlueTeam
- rpc2socks: Post-exploitation client-server solution that allows to drop and remotely run a custom RPC + SOCKS-through-SMB server application on a #Windows target, from a Unix or Windows host

- SwiftBelt: A macOS enumeration tool inspired by harmjoy's Windows-based Seatbelt enumeration tool
- Vulmap: Online Local Vulnerability Scanners Project for Windows & Linux
- WMIHACKER: A Bypass Anti-virus Software Lateral Movement Command Execution Tool

Misc. pentest & bug bounty resources

- Hacky af long term monitoring of Burp Collaborator
- stop-firefox-automatic-connections
- Open Source Intelligence Tools And Resources Handbook 2020
- cvebase.com
- Project Cobrat: A Centralised Searchable Open Source Project Sonar DNS Database
- Chrome Extension manifest.json Dataset (>100K Extensions)
- 30-Days-Of-Python & 30-Days-Of-JavaScript
- A BIG collection of Unix/Linux 'grep' command examples

Challenges

- Goof: Snyk's vulnerable Node.js demo app
- Vulnerability Cybersecurity Challenges

Articles

- OAuth 2.0 Security Best Current Practice
- Mutation XSS via namespace confusion – DOMPurify < 2.0.17 bypass
- Bypassing DOMPurify again with mutation XSS
- Now you C me, now you don't: An introduction to the hidden attack surface of interpreted languages
- Bug Bounty Recon: Perform Faster Port Scan
- Sandbox evasion: Identifying Blue Teams

Bug bounty & Pentest news

- Hacker Plus: Facebook's new bug bounty loyalty program
- Making bug triage faster and simpler: rolling out Facebook's Bug Description Language (FBDL)

- Security@ 2020
- HackerSploit Linux Security Series
- HackerOne incident report of a Credential Stuffing Attack
- New Search Tokens For Faster Filtering! (Bugcrowd)
- Concluding the Azure Sphere Security Research Challenge, Microsoft Awards $374,300 to Global Security Research Community & Why we invite security researchers to hack Azure Sphere

Non technical

- Why is prod down – Penetration testing edition
- These Are The Bugs You Should Look For In Late 2020
- Hacker Spotlight: Interview With Arneswinnen
- You don't need SMS-2FA.
- Why Software Remains Insecure
- Social Media around the World
- The Stress and Joy of Security Jobs

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 10/04/2020 to 10/11/2020.