Bug Bytes #14 – Better Exfiltration via HTML Injection by @donutptr, Dell KACE K1000 RCE by @MrTuxracer & BurpFeed

BY INTIGRITI · APRIL 16, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 05 to 12 of April.

Our favorite 5 hacking items

1. Article of the week

> "Better Exfiltration via HTML Injection, tl;dr by @fransrosen & sic (Sequential Import Chaining tool)"

This is great example of how far collaboration can go for bug hunters, how to do research and invent a new attack.
André Baptista and Cache-Money found an HTML injection with clickjacking as the worst-case scenario. The bug wasn't an XSS because the target used DomPurify. But since DomPurify allows *style* tags by default, @donutptr started looked for a way to exfiltrate sensitive data using just a *style* tag.
It's similar to a CSS injection but the new attack has less prerequisites and works even though the target limits the payload's size.
The whole writeup is excellent to learn about CSS injection, and the kind of creativity/perseverence that makes you go from HTML injection to a 5 digit bounty despite many technical obstacles.

2. Writeup of the week

> "Dell KACE K1000 Remote Code Execution – the Story of Bug K1-18652"

This is a writeup of the bug that made @MrTuxracer winner of HackerOne's H1-3120 event.
It's an RCE on an in-scope Dropbox vendor. I find his process fascinating:

- During recon, he found a Dell Kace interface
- The same software is now distribted by "Quest Software Inc"
- The version detected is old. Free trials are only available for the last version of the app
- He tried to social engineer Quest to get a free trial of the same old version of the app that he found
- He still played with the latest version even though it was completely different from what he saw on the server
- He analyzed the app's source code and found a comment referencing a path traversal
- His code analysis showed that there was also an arbitrary command injection

- The bugs are fixed in the app's last version but they worked when he tried them on his target which wasn't up-to-date

Social engineering to get a demo app and taking the time to install an app locally and review its source code... remind me of this advice by @gwendallecoguic:

> **"You just need to do what other people don't, because they didn't think about it or because they were lazy, success guarantee."**

3. Tool of the week

> "BurpFeed"

I haven't had the opportunity to test this tool, but I will definitely do it ASAP. It's a Python script for mass feeding URLs to Burp suite's sitemap/target tab.
This can be handy to transition from automated recon (and enumeration of live domains) to manual testing with Burp.

4. Tutorial of the week

> "Linting For Bugs & Vulnerabilities"

This is a nice introduction to static analysis of JavaScript code using ESLint with custom rules. It can help detect issues like DOM XSS.
You can also add rules to detect other vulnerabilities, and play with the OWASP Juice Shop to test them.
I'd also combine such linting tools with manual anlysis because many bugs won't be found with automation.

5. Video of the week

> "How did Masato find the Google Search XSS?"

This is a follow-up video to last week's explanation of the mutation XSS found by @kinugawamasato on Google.
This time @LiveOverflow provides insight into how Masato found that XSS, and the kind of research he was involved in that allowed him to find it.
It's really interesting for anyone who wants to get into Web security research, or understand what make hackers like @albinowax, @sirdarckcat, @garethheyes or Mario Heiderich so good at research.

6. Intigriti News

6.1 EU FOSSA Bonuses

EU Commission is introducing EU FOSSA Bonuses for Keepass, glibc and Apache Tomcat. Up to a 50% bonus!

> "#EUFOSSA news: The European Commission raises bounty awards to challenge developers. Learn more at https://t.co/cK3sOvUGFr pic.twitter.com/Py4srNSYJq
>
> — intigriti (@intigriti) 10 april 2019"

6.2 Shop Apotheke

Shop Apotheke has introduced new In-scope domains due to a major relaunch based on new architecture and a new underlying infrastructure. The new pages mentioned in the In-scope section are delivered by a brand new frontend. This is based on a brand new backend, which is also part of the scope and also mentioned in the In-scope section. These new software solutions have been implemented using new technologies and are hosted in a brand new infrastructure, completely independent of the existing e-commerce platform. **Note: this is a registered only program!**

Start hunting here!

Other amazing things we stumbled upon this week

Videos

- OUT FOR BLOOD! (hacking Dropbox Hellosign Google Facebook)
- Open redirection: can automatic redirection be harmful?
- Website security vulnerabilities by Gwendal Le Coguic @ Yogosha · yesterday
- Free Food from Maccas

Podcasts

- Absolute AppSec Ep. #54 – Tim Tomes (@lanmaster53)
- Security Now 709 – URL "Ping" Tracking
- Risky Business #536 — Mar-a-Lago arrest, ASUS supply chain attack and more
- Simon Bennetts — OWASP ZAP: past, present, and future
- 7MS #357: 7 Minutes of IT and Security Tips
- Sophos podcast Ep. 027 – Honeypots, GPS rollover and the MySpace data vortex
- The Many Hats Club Ep. 56, I spy with my little SpyEar (with Rachel Tobac)

Webinars & Webcasts

- Zero to Hero Pentesting: Episode 4 – Five Phases of Hacking + Passive OSINT

Conferences

- Insomni'hack 2019, especially:
  - Vulnerabilities of mobile OAuth 2.0
  - Betrayed by the Android User Interface: Why a Trusted UI Matters & Slides
  - These are the Droids you are looking for – security research on Android
  - What every (IT | Security) Professional should know about the dark web
- BSides Rochester 2019, especially:
  - OWASP Amass Beyond Subdomain Enumeration
  - Jackson Deserialization Vulnerabilities
  - Pwning a cheap IP camera for fun, but not profit
  - How to Fix the Diversity Gap in Cybersecurity

Slides only

- Getting Started with API Security Testing
- Come to the Dark Side: Python's sinister secrets & Code snippets

Tutorials

Medium to advanced

- Exploiting CSRF on JSON endpoints with Flash and redirects

- Leveraging Expression Language Injection (EL Injection) for RCE
- AV WARS: Fighting fire with fire [AV Bypass Technique]
- Living Off the Land: Opening PowerShell When You Can't Open PowerShell
- An SMB Relay Race – How To Exploit LLMNR and SMB Message Signing for Fun and Profit
- Attacking QA platforms: Selenium Grid
- An intro into abusing and identifying WMI Event Subscriptions for persistence

Beginners corner

- A Pentester's Guide – Part 1 (OSINT – Passive Recon and Discovery of Assets), Part 2 (OSINT – LinkedIn is not just for jobs) & Part 3 (OSINT, Breach Dumps, & Password Spraying)
- Cross-site scripting: How to go beyond the alert
- OWASP ZAP | Automated Pen Test with Jenkins
- Commando VM: Looking Around
- How to Find Hidden Cameras in your AirBNB
- Oh, My Kerberos! Do Not Get Kerberoasted!
- PostgreSQL (Attack on default password)

Writeups

Challenge writeups

- Midnight Sun CTF (Challenges by @avlidienbrunn)

Pentest writeups

- SSRF vulnerability via FFmpeg HLS processing
- In-depth Freemarker Template Injection
- How customer collaboration during a pentest can lead to finding a Remote Code Execution (RCE)
- Finding Weaknesses Before the Attackers Do

Responsible disclosure writeups

- From CSRF to RCE
- CVE-2019-0227: Expired Domain to Remote Code Execution in Apache Axis
- Nagios XI 5.5.10: XSS to #
- Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis

Bug bounty writeups

- RCE on Gitlab ($12,000)
- OAuth flaw on Twitter ($5,040)
- Code injection on Starbucks ($4,000)
- SSRF on GitLab ($3,000)
- Logic flaw on Shopify ($1,837)
- Information disclosure on HackerOne ($1,500)
- Information disclosure on Slack ($1,500)
- SSRF & Path traversal on Uber
- MiTM on Burp Suite
- Logic flaw on Facebook ($1,000)
- SSRF/XSPA on Microsoft
- HTTP leak on private program

See more writeups on The list of bug bounty writeups.

Tools

- Http-prompt: An interactive command-line HTTP client featuring autocomplete & syntax highlighting, built on HTTPie & prompt_toolkit
- Git-Pwned: Wrapper around *subfinder* & *git-dumper*
- Denumerator: Finds servers responding on port 80/HTTP
- LFI-Enum: Scripts to exploit LFI & extract information from Linux servers
- Dirble: Directory scanning & scraping tool in Rust, based on Dirb but faster
- Domain-to-webapp: Web application Enumerator
- EmailGen: Email Generation from Bing using LinkedIn Dorks
- Adconnectdump: Dump Azure AD Connect credentials for Azure AD & Active Directory
- PEPE (Post Exploitation Pastebin Emails) & Introduction: Collect information about email addresses from Pastebin for advanced credential stuffing
- SharpExec & Introduction: Offensive security C# tool designed to aid with lateral movement

Misc. pentest & bug bounty resources

- Bug Bounty Methodology
- Bug Hunting Methodology(Part-3)
- The Android Platform Security Model
- iOS/macOS penetration testing cheatsheet
- AWS Security Maturity Roadmap
- Can you hack your government?: A list of governments with Vulnerability Disclosure Policies
- Microsoft publishes SECCON framework for securing Windows 10

Challenges

- The Unescape Room (source code): Source of the online XSS game by @jobertabma
- 10 levels of XSS challenges by @haxel0rd

Articles

- Apple's App-Site Association – The New robots.txt & aasa.sh (Script that generates URL list from App-Site Association file)
- Online shoplifting – exploiting e-commerce basket and voucher faults for five-finger discount
- A Novel CSP Bypass Using data: URI
- Don't trust the locals: investigating the prevalence of persistent client-side cross-site scripting in the wild
- The Danger of Exposing Docker.Sock
- Exploiting ScriptInjection Flaws in ReactJS Apps
- Don't leak sensitive data via security scanning tools
- Sudo_inject: New Linux privilege escalation technique abusing sudo token

News

Bug bounty news

- For the next two weeks, the European Commission is raising its EU-FOSSA bug bounty awards!
- Winners of HackerOne's 50M CTF
- BugCrowd Image embedding

Vulnerabilities

- The Ping is the Thing: Popular HTML5 Feature Used to Trick Chinese Mobile Users into Joining Latest DDoS Attack
- Phar out: PHP deserialization techniques offer rich pickings for security researchers
- App could have let attackers locate and take control of users' cars: Hard-coded credentials
- Internet Explorer zero-day lets hackers steal files from Windows PCs. Microsoft refused to patch issue so security researcher released exploit code online.
- Some enterprise VPN apps store authentication/session cookies insecurely
- Facebook app developers leaked millions of user records on cloud servers, researchers say
- Check your Verizon FiOS Quantum Gateway G1100 router now
- Dragonblood – several design flaws discovered in WPA3

Breaches

- Microsoft: Hackers compromised support agent's credentials to access customer email accounts
- SAS 2019: Exodus Spyware Found Targeting Apple iOS Users
- Matrix security breached because of running an outdated Jenkins instance and the attacker hijacked SSH keys to gain access to their production infrastructure
- Berkeley High student tried to rig his own election, exposing flaw in district's cybersecurity: A user's email is always a his/her first and last name. The default password is "Berkeley" followed by the student's identification number.
- The international companies official newsletters are used to steal money from bank accounts
- Stealthy spyware steals data from printer queues
- WordPress Yellow Pencil Plugin Flaws Actively Exploited

Other news

- Android phones transformed into anti-phishing security tokens
- Assange arrested, faces extradition for hacking
- Mar-a-Lago intruder had instant-malware-inflicting thumb drive

Non technical

- 1 big thing: How Heartbleed turned vulnerabilities into brands
- 60 Must-Know Cybersecurity Statistics for 2019
- 5 of the Biggest Security Breaches in the 2010s.

- The key to loving your job in the age of burnout
- Chronic Stress and a Life: How Stress Almost Killed Me

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 04/05/2019 to 04/12/2019.

Curated by Pentester Land & Sponsored by Intigriti