Bug Bytes #13 – Shopify RCE, 0xpatrik's interview & XSS in Google Search

BY INTIGRITI · APRIL 9, 2019 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-13-shopify-rce-0xpatriks-interview-xss-in-google-search

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand**. Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

You can sign up for the newsletter here.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 29 of March to 05 of April.

Our favorite 5 hacking items

1. Resource of the week

Introducing the Web Security Academy

The Web Security Acedemy is a new online training on Web security. What's great about it that it's free, and it's from PortSwigger the company behind Burp Suite and The Daily Swig. Also, Dafydd Stuttard who is part of the team that created it, is the author of The Web Application Hacker's Handbook.
All this to say that it is high quality like everything that the company produces.
There are only 4 modules for now: SQL injection, XSS, OS command injection and Directory traversal.
Each one includes theory, resources and practical labs, plus related stories from The Daily Swig at the end of the page.
More vulnerabilities and labs will be added in the next months.

2. Writeup of the week

Handlebars template injection and RCE in a Shopify app & HackerOne report ($10,000)

This is an awesome writeup! What I love about it most us that @Zombiehelp54 initially reported a "possible template injection". He wasn't sure it was exploitable or even valid, and just explained the app's behaviour that led him to think it was vulnerable.
Then he kept trying and ~2 months later, he was able to identify the template used (handlebars) and escalate to a full SSTI/RCE.
So this is an excellent example of perseverence, a well-written report, escalating from an "almost bug" to RCE, and how to exploit an SSTI on an initially unknown template engine.

3. Tool of the week

Webanalyze

If you have tried automating your recon, you might have noticed that some interesting platform identification tools like Wappalyzer and BuiltWith have expensive APIs. There are many free alternatives like Webtech or Whatweb, but I like using different tools and combining their results to avoid erroneous results.
So Webanalyze is a good addition to my workflow. It's a port of Wappalyzer in Go. It doesn't require any API key because it uses the apps.json from the Wappalyzer project, which contains signatures to identify technologies.
Here are example outputs:
webanalyze -hosts hosts.txt -output csv
2019/04/07 20:54:37 Scanning with 4 workers.
Host,Category,App,Version
http://google.com,Web Servers,Google Web Server,
http://uber.com,"Web Servers,Reverse Proxy",Nginx,
http://microsoft.com,JavaScript Libraries,jQuery,
webanalyze -host yahoo.com
2019/04/07 20:55:29 Scanning with 4 workers.
2019/04/07 20:55:32 [+] http://yahoo.com (2.657574548s):
2019/04/07 20:55:32 – Apache Traffic Server, (Web Servers)
2019/04/07 20:55:32 – YUI, (JavaScript Libraries)
2019/04/07 20:55:32 – React, (JavaScript Frameworks)

4. Non technical item of the week

Bringing Cybersecurity into Academia: We Talk with Patrik Hudak

I'm a huge fan of Patrick Hudak's blog https://0xpatrik.com/. His articles on subdomain takeover, recon and OSINT are so detailed and well-written, they're like mini e-books!
So it was interesting to learn more about him through this interview. His work on subdomain takeovers and subdomain enumeration was actually part of his master thesis.
I really want to read that now, as not all theses are as practical and financially rewarding!
This might give you ideas if you're a student.

5. Video of the week

XSS on Google Search – Sanitizing HTML in The Client?

This is a mindblowing video writeup of an XSS on Google Search. The vulnerable parameter (*q*) and URL (*https://www.google.de/search?q=vuln*) are used by millions of people. It was vulnerable for almost 5 months until @kinugawamasato found the bug!
This shows that there are always bugs even in the most tested and secure apps.
Also, the video is full of interesting information on:
– Mutation XSS
– Why HTML parser libraries for XSS prevention are placed client-side
– Why the same tag can be interpreted in two different ways by the browser
– The reason is that <template> has JS disabled. And the browser parses <noscript> differently if JS is enabled or disabled.
– How to debug complex DOM XSS: Use `onerror=debugger;`. It triggers a breakpoint in the JS debugger when the XSS is executed.

Other amazing things we stumbled upon this week

Videos

- Cross-Site Request Forgery Attack
- Zero to Hero Pentesting: Episode 3 – Python 102, Building a Terrible Port Scanner, and a Giveaway
- Get Any Wi-Fi Password Without Any Cracking Using Wifiphisher's Social Engineering Attack [Tutorial]

Podcasts

- Security Now 708 – Android Security
- TrustedSec Podcast Episode 3.12 – Money, Malware, and Facebook Reads Your Mail
- The Many Hats Club – Ep. 38, Take care of yourself while reversing malware (with Amit Serper)
- The Many Hats Club – Ep. 55, The Beer Farmers Monthly Special No. 4
- Application Security Podcast: Georgia Weidman — Mobile, IoT, and Pen Testing
- Paul's Security Weekly #599 – OceanLotus, Russia, & Google
- Paul's Security Weekly #599 – Bugs, Breaches, and More!
- Hack Naked News #212 – ASUS, Microsoft, & Tesla
- Sophos podcast Ep. 026 – Android bloatware, hackable routers and website attacks
- Darknet Diaries Ep 35: Carbanak

Webinars & Webcasts

- InfoSec Girls + OWASP WIA knowledge exchange webinar – 06 April 2019
- Intro to Cracking Hashes

Conferences

- BSides Columbus 2019, especially:
  - Mobile App Vulnerabilities – The Bad, The Worse And The Ugly
  - Battling Magecart: The Risks of Third-Party Scripts
- TROOPERS19

Slides only

- Weaponizing Corporate Intel: This Time, It's Personal!
- Browsers – For better or worse ...
- BlackHat Asia 2019
- Attacking Java RMI services after JEP 290 & blog post

Tutorials

Medium to advanced

- GraphQL Voyager as a tool for API security testing
- Circumventing SSL Pinning in obfuscated apps with OkHttp
- Going Phishing with Terraform
- Post Exploitation with KOADIC
- Rethinking the inotify API as an offensive helper

Beginners corner

- Better API Penetration Testing with Postman – Part 1 & Part 2
- Exploitation of Mis-configured Cross-Origin Resource Sharing (CORS)
- Advanced SSRF exploitation and prevention (Original in Dutch)
- Using Wireshark: Identifying Hosts and Users
- Hack Excel passwords
- Comprehensive Guide on Netcat
- Hashcat Tutorial – Rule Writing
- Network Basics for Hackers: Server Message Block (SMB) and Samba

Writeups

Challenge writeups

- Solution for "A Weird XSS Case"
- VolgaCTF 2019 Quals: web 300 — Gallery [EN]
- HackLab ESGI Security Day 7th Edition – Write-ups

Responsible disclosure writeups

- CARPE (DIEM): CVE-2019-0211 Apache Root Privilege Escalation

- Multiple Vulnerabilities in Android's Download Provider (CVE-2018-9468, CVE-2018-9493, CVE-2018-9546)
- Vulnerability in Xiaomi Pre-Installed Security App
- Xiaomi URL spoofing w/ SSL vulnerability or, CVE-2019-10875 – Was it intentionally kept in the global versions by Xiaomi?
- Content provider injection in Xiaomi stock browser
- Go get -u CVE-2018-16873
- Hacking College Admissions
- SQL Injection in Duplicate-Page WordPress Plugin
- Malicious remote code execution backdoor discovered in the popular bootstrap-sass Ruby gem

Bug bounty writeups

- Client-Side Race Condition on HackerOne ($1,250)
- Subdomain takeover on HackerOne ($500)
- SSRF on Shopify ($500)
- Information disclosure on Shopify ($500)
- Blind SSRF/XSPA on Lob
- Authorization flaw on GitLab ($2,000)
- Logic flaw on GitLab ($1,000)
- Logic flaw on Google
- SQL injection on private program ($10,000)
- Information disclosure on Facebook ($10,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Anew: A tool for adding new lines to files, skipping duplicates. Useful for recon automation
- GenerateParameterWordlist.py: Burp Extension that extracts the parameters from sites in scope or from a selected site so you can use them in Intruder (useful to test for mass assignments)
- Graphqlschema2payload: Helps recreate GraphQL payloads from a GraphQL Schema

More tools, if you have time

- Pastebin dump: A website listing daily Pastebin dumps

- Shodan-Seeker: Command-line tool using Shodan API. Generates and downloads CSV results, diffing of historic scanning results, alerts and monitoring of specific ports/IPs, etc
- Giggity: Wraps github api for openly available information about an organization, user, or repo
- Fracker: PHP function tracker
- Android-ks-decryptor.py: Script to decode and decrypt Android Keystores (only software) & Slides (in French)
- Fireprox: AWS API Gateway management tool for creating on the fly HTTP pass-through proxies for unique IP rotation
- SharpGPOAbuse: A .NET application written in C# that can be used to take advantage of a user's edit rights on a Group Policy Object (GPO) in order to compromise the objects that are controlled by that GPO
- KatzKatz: Python script to parse txt files containing Mimikatz output & generate the valid creds into a CSV file
- QRLJacker: QRLJacking Exploitation Framework
- APC-PPID: Adds a user-mode asynchronous procedure call (APC) object to the APC queue of the specified thread and spoof the Parent Process (for red teamers)

Misc. pentest & bug bounty resources

- In Plain Sight:: The Vulnerability Epidemic in Financial Mobile Apps
- Poc-graphql: Research on GraphQL from an AppSec point of view
- Whitepaper: Deobfuscating JavaScript Code: A Steam Phishing Website
- Automating Discovery and Exploiting DOM (Client) XSS Vulnerabilities using Sboxr
- APIsecurity.io Issue 25: NIST microservices guidelines, Facebook opens up to pentesting
- Web Application Penetration Testing Course URLs
- Reverse Engineering iOS Applications: A completely free, open source and online course about Reverse Engineering iOS Applications
- Android Penetration Testing Courses: Free course with examples from Diva (Damn Insecure Vulnerable Application
- 6,000+ HackerOne Disclosed Reports
- My Wireshark Display Filters Cheat Sheet

Challenges

- Intigriti Community challenge: Can you spot the open redirect?
- Can you trick this browser extension into revealing its data? (Hard)

Articles

- Same-Origin Policy: From birth until today
- The Journey to Try Harder: TJnull's Preparation Guide for PWK/OSCP
- CLI on steroids: Productivity boost on the linux command-line
- Server side request forgery in different manner
- Bug-Hunting-Day-5, Day 6 & Day 7
- CVE-2019–5418: on WAF bypass and caching
- Clickjacking the reCAPTCHA in the suspicious activity context
- Subverting Electron Apps via Insecure Preload
- How to Guard Against Mobile App Deep Link Abuse
- Security in Sciter-based applications
- What you see is not what you get: when homographs attack
- How to Implement DMARC/DKIM/SPF to Stop Email Spoofing/Phishing: The Definitive Guide
- DNS Ping Scans via Open Resolvers & Rumble tools: Useful when testing segmented network environments
- What Application Developers Need To Know About TLS Early Data (0RTT)

News

Bug bounty news

- Microsoft Bounty Program Updates: Faster bounty review, faster payments, and higher rewards: "The first researcher to report a bounty-eligible vulnerability will receive the full eligible bounty award, even if it is internally known."
- Bugrcrowd New Platform Feature – Advanced Program Search
- Bugcrowd University

Breaches

- Hackers Abuse Google Cloud Platform to Attack D-Link Routers
- Ransomware attack on Black Hat Asia halted by NOC
- Losing Face: Two More Cases of Third-Party Facebook App Data Exposure

Vulnerabilities

- Apache web server bug grants root access on shared hosting environments

- Is your hard drive exposed online?
- Zero-day hole in Microsoft Edge exposes users' secrets
- Swiss Post puts e-voting on hold after researchers uncover critical security errors
- TP-Link router zero-day offers your network up to hackers
- WordPress iOS app leaked authentication tokens
- Tesla cars keep more data than you think, including this video of a crash that totaled a Model 3
- Hackers Can Access Pacemakers, but Don't Panic Just Yet

Breaches

- Hackers Abuse Google Cloud Platform to Attack D-Link Routers
- Ransomware attack on Black Hat Asia halted by NOC
- Losing Face: Two More Cases of Third-Party Facebook App Data Exposure

Malicious apps/sites

- Researchers Find Google Play Store Apps Were Actually Government Malware
- Huawei laptop 'backdoor' flaw raises concerns
- Russia accused of massive GPS spoofing campaign

Other news

- Android Security Monthly Recap #3 | March 2019
- Introducing Warp: Fixing Mobile Internet Performance and Security: Cloudflare is launching Warp, a free VPN for mobile devices
- North Korea's elite hackers are funding nukes with crypto raids
- JavaScript sniffer slingers duke it out to control vulnerable websites
- Hidden code gives plugin developers admin access to WordPress sites
- Crooks use hidden directories of compromised HTTPS sites to deliver malware
- Google Warns of Growing Android Attack Vector: Backdoored SDKs and Pre-Installed Apps

Non technical

- My Story: From Business Development Rep to Security Consultant-in-Training at Rapid7
- Researcher Spotlight: Ambassador Hagai Sason
- Our take on social engineering

- How Hackers Define “Hacker”
- Hacker/Infosec Con Types & Getting More Out Of Hacker/Infosec Conferences
- Tactical Advice for Clearing Depression
- How do you overcome the tough times & self-doubt?

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 03/22/2019 to 03/29/2019.

Curated by Pentester Land & Sponsored by IntigritiDisclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.