BugBytes #18 – Information disclosure on Shopify, Awesome Asset Discovery & How To Work Smarter Not Harder with Bug Bounty

BY INTIGRITI · MAY 14, 2019 · LAST UPDATED ON MARCH 6, 2025

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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 3 to 10 of May.

Our favorite 5 hacking items

1. Challenge of the week

> "Authentication Lab (online), Source code & Walkthroughs"

This is a great lab if you want to practice finding authentication vulnerabilities. There are 5 bugs: IP based authentication bypass, Timing attack, Client side auth, Leaky JWT and JWT Signature Disclosure (CVE-2019-7644).
Also, if stuck, check out the walkthroughs. I don't want to read them before doing the challenges but they seem detailed (like 5 articles in 1!).

2. Writeup of the week

> "Information disclosure on Shopify ($802.20)"

This is a fun report! The vulnerability is that a GraphQL endpoint reveals sensitive information without authentication: that's the internal beer consumption (brands & quantities left) at Shopify's offices.
What's interesting is how @eraymitrani found the vulnerable GraphQL endpoint. I highly recommend reading the summary where he explains it.
Basically, he saw in a previous report by @rijalrojan that Shopify had an exposed GraphQL endpoint. So he set out to find other exposed endpoints, following these steps:

- Subdomain enumeration
- Request /graphql on all subdomains using wfuzz
- Filter by 200 responses
- Send introspection queries to all of them in Burp Repeater
- Got *"query string not present"* error

- Solve it by adding the "*content-type:*" header to the post request
- Look for a domain that leaks private information

3. Article of the week

> "Bug Chain Tales: P5+P5=P3"

If you're always hearing about chaining bugs and wondering how to do it in practice, this is a good example.
Self-XSS and login CSRF are generally not paying bugs by themselves. But, combined, they become more dangerous and worthy of a bounty.
The attack scenario in this case is to enter the XSS payload in the address details of the attacker's account, and make the victim open this account using the login CSRF. When the victim buys something and wants to select the delivery address, the XSS payload is triggered.

4. Resource of the week

> "Awesome-Asset-Discovery"

As its name indicates, this is an awesome asset discovery list. In other words, it's a list of resources to help find all kinds of assets for organization: IP addresses, (sub)domains, emails, open ports, cloud infrastructure, business communication infrastructure, data leaks, source code aggregators, and more. Some of the tools mentioned are classics that you probably already use, but you might also discover something new!

5. Slides of the week

> "Bug bounty – Work smarter not harder"

This is a nice introduction to bug bounty. But even if you're not a beginner, some resources mentioned might be helpful. Personally, I didn't know of dkimsc4n (a DKIM scanner) and can't wait to try it.
Also, thanks for mentioning Pentester Land @vavkamil!

6. Intigriti News

6.1 Platform Updates

We've added several new features to our platform:

- The submission title length is increased up to 50 characters.
- Researchers are now able to specify a preferred payment method (invoice, wire, Payoneer, Paypal) and enter their details. This setting is made available in the payout overview
- Researcher are now able to start their vetting procedure by one click via the profile view.

A blogpost about the platform's new features will be posted soon!

6.2 New Bug Bounty Tips

This week we received two bug bounty tips:

- Use Exiftool to extract metadata from documents. It might reveal vulnerable htmlopdf generators.

> "A PDF file can tell more than you think! Great advice from @QuintenBombeke! #BugBountyTip #HackWithIntigriti #BugBounty pic.twitter.com/73ZTUWlH0O
>
> — Intigriti (@intigriti) May 9, 2019"

- The Birthday Trick: If you sign up for a target, set your birthday to today or tomorrow! Then use birthday discount vouchers in your inbox to buy gift cards. Repeat!

> "BOUNTY TIP: Get yourself a nice bounty present by buying giftcards with birthday discounts ! Repeat & recycle your gift cards to generate infinite money. Thanks, and happy (real) birthday, @securinti! #BugBountyTip #HackWithIntigriti pic.twitter.com/cY1NcM3J4c
>
> — Intigriti (@intigriti) May 14, 2019"

Other amazing things we stumbled upon this week

Videos

- HackerOne Hacker Interviews: Jesse Kinser (@randomdeduction)
- A Day in the Life of an Ethical Hacker / Penetration Tester
- Zero to Hero: Week 8 – Building an AD Lab, LLMNR Poisoning, and NTLMv2 Cracking with Hashcat
- How do I prepare for a CTF Challenge? The Joe McCray Way for Beginners
- Heartbleed Exploit – Discovery & Exploitation
- Installing your own SAP Lab Part 1

Podcasts

- SwigCast, Episode 1: HACKERS
- Security Now 713 – Post-Coinhive Cryptojacking
- Risky Business #540 — In depth: Hamas cyber unit destroyed in air strike
- Security In Five Episode 486 – The Different Types Of Malware
- Paul's Security Weekly #602 – Joshua Abraham, Praetorian
- Business Security Weekly #127 – Leadership Articles
- Secure Digital Life #109 – The Lair of the White Worm

Conferences

- OWASP NZ Day 2019: JWAT: Attacking JSON Web Tokens
- The Pentester Blueprint: A Guide to Becoming a Pentester

Slides only

- Attacking AWS: the full cyber kill chain
- OAuth: Where are we going?
- HITB 2019 materials, especially:
  - A decade of infosec tools from where we were to what we need now
  - Deep Confusables – Improving Unicode Encoding Attacks with Deep Learning
- Red Team Tools and Techniques – Red For Detection
- From Chump to Trump – Privilege Escalation By Stealing Elect^H^H^H^H Domain Credentials
- In and Out of the DNS Tunnel

Tutorials

Medium to advanced

- x-up-devcap-post-charset Header in ASP.NET to Bypass WAFs Again!
- Hack the JWT Token
- Danger of Stealing Auto Generated .NET Machine Keys
- What it is and where to go
- Introduction To Serverless Security: Part 2 – Input Validation
- MandaloreQuest: An Offensive Journey
- Network Redirections in Bash

Beginners corner

- Cross-Site Scripting (XSS) Exploitation
- Burp tip – How to share Burp Apps accross Linux Machines/Users.
- Web Services & API Pentesting-Part 1
- On the War Path! – Basic Application Recon
- Vulnerable Javascript Files

- Top 20 and 200 most scanned ports in the cybersecurity industry
- Network Penetration Testing-Part 1, Part 2, Part 3 & Part 4
- Pwning WordPress Passwords by Mitch Moser
- Metasploit Basics for Hackers, Part 25: Web Delivery with Linux/UNIX/OsX

Writeups

Challenge writeups

- INS Hack 2019 / Bypasses Everywhere

Pentest writeups

- IDOR Leads to Full Account Takeover

Responsible disclosure writeups

- Cricut Payment Bypass Vulnerability
- Pwning WordPress GraphQL
- Multiple vulnerabilities in jQuery Mobile
- Alpine Linux Docker Image root User Hard-Coded Credential Vulnerability
- [Advisory] Unpatched URL Address Bar Spoofing Vulnerability in UC Browser 12.11.2.1184 and UC Browser Mini 12.10.1.1192: With the same old one-liner payload...
- TYPO3-PSA-2019-007: By-passing protection of Phar Stream Wrapper Interceptor
- CVE-2018-20580: PoC for ReadyAPI RCE
- Alert logic Uncovers New Vulnerability in WordPress WP Live Chat – CVE-2019-11185

Bug bounty writeups

- Lazy writeup of a cool bug: OAuth token theft via XSS
- RCE on Aeternity ($10,000)
- XSS via Deeplink on Twitter ($2,940)
- DOM XSS on HackerOne ($565)
- DOM based CSS Injection on Grammarly ($250)
- Client-Side Enforcement of Server-Side Security on Dropbox ($216)
- SQL injection via User-Agent on private program
- CSRFs on private program ($3,000)

- Fider Subdomain takeover on ownCloud ($200)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- awesome-jenkins-rce-2019: There is no pre-auth RCE in Jenkins since May 2017, but this is the one!
- Natlas: Scaling Network Scanning
- ggroup.py: Check for public Google groups given a list of domains
- Horn3t: Powerful Visual Subdomain Enumeration at the Click of a Mouse

More tools, if you have time

- doNmap.sh: Bash wrapper for nmap scans
- Final Recon: OSINT Tool for All-In-One Web Reconnaissance
- awsEmailCheck.py: Determines if there is an AWS account associated with a given email address
- Scan.sh: Initial recon automation (masscan + nmap import into metasploit db)
- wpBullet Build Status: A static code analysis for WordPress Plugins/Themes (and PHP)
- autOSINT: Recon tool. Uses recon-ng & hunter.io
- ReconT: Reconnaisance, footprinting & information disclosure
- Shiva: An Ansible playbook to provision a host for penetration testing and CTF challenges
- QRGen: Simple script for generating Malformed QRCodes
- Jalesc: Just Another Linux Enumeration Script: A Bash script for locally enumerating a compromised Linux box
- LDAP_Search: Python3 script to perform LDAP queries and enumerate users, groups, and computers from Windows Domains. Ldap_Search can also perform brute force/password spraying to identify valid accounts via LDAP.
- SharpClipHistory: A .NET application written in C# that can be used to read the contents of a user's clipboard history in Windows 10 starting from the 1809 Build

Misc. pentest & bug bounty resources

- Nina Zakharenko's Fundamentals & Intermediate Python Courses (Free Until May 16th), learnpython.dev (Accompanying website) & Repo
- OSINT Collection Tools for Pastebin

- All in one Recon Methodology PDF: PDF bundle of multiple recon presentations listed here
- Church of Hackers
- APIsecurity.io Issue 30: 5G going to REST. Breaches in Dell, Cisco, WebLogic, DockerHub, JustDial, iLnkP2P
- Infosec – Infographics
- Android Security & Malware: Telegram channel by @LukasStefanko on "Security & privacy, malware on Google Play, vulnerabilities, bug bounty hunting, security tips, tutorials, penetration testing.."
- Active Directory Kill Chain Attack & Defense
- Mobile App Sec Assemble: Slack workplace for people interested in Mobile Application Security
- Kaonashi: Wordlist, rules and masks from Kaonashi project (RootedCON 2019)

Challenges

- Infiltrate 19 AWS related CTF: Available until 05/31/2019

Articles

- The XSS challenge that +100k people saw but only 90 solved
- Finding Unlisted Public Bounty and Vulnerability Disclosure Programs with Google Dorks
- Chrome switching the XSSAuditor to filter mode re-enables old attack
- Bug Bounty Adventures: This Is the Wrong Porn!
- Why Go? – Key advantages you may have overlooked
- Accessibility vs Security: Breaking CAPTCHAs by exploiting their accessibility features by Gautam Krishnan
- Medical Device Security, Part 2: How to Give Medical Devices a Security Checkup

News

Bug bounty / Pentest news

- Win a Trip to Las Vegas – Our May 2019 Promotion: The two reports to Facebook during May that are of better quality & with highest reward value will get a paid trip to Las Vegas for DEFCON
- Congratulations to our most dedicated researchers in Q1 2019!
- Amazon S3 Path Deprecation Plan – The Rest of the Story

Reports

- Verizon's 2019 Data Breach Investigations Report & Summary of findings
- Who's Afraid of the Dark? Hype Versus Reality on the Dark Web

Vulnerabilities

- Sinister secret backdoor found in networking gear perfect for government espionage: The Chinese are – oh no, wait, it's Cisco again
- 'Unhackable' Biometric USB Offers Up Passwords in Plain Text
- Flaws in a popular GPS tracker leak real-time locations and can remotely activate its microphone

Breaches & Attacks

- Cybercrooks steal $40m in Bitcoin from crypto-exchange Binance
- Freedom Mobile leaked millions of card data with CVV codes in plain text
- A development lab used by Samsung engineers was leaking highly sensitive source code, credentials and secret keys for several internal projects — including its SmartThings platform via their GitLab instance
- Hackers breached 3 US antivirus companies, researchers reveal

Other news

- Announcing WSL 2
- Google I/O 2019: Upcoming browser features to help you secure your web application
- Microsoft launches Internet Explorer Mode for Edge
- A Chinese hacking group was using NSA exploits a ~year before~ they were leaked publicly by the Shadow Brokersfv
- Japanese government to create and maintain defensive malware
- IDF air strike against Hamas hackers shocks infosec world
- Mozilla bug throws Tor Browser users into chaos

Non technical

- ICS Security – IT vs OT
- Improving Infosec (or any Community/Industry) in One Simple but Mindful Step
- How To Be More Disciplined With Your Goals: 7 Simple Strategies You Should Learn
- Security Researcher: A Road Less Frequently Traveled

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 05/03/2019 to 05/10/2019.

Subscribe to the newsletter here!*Disclaimer:*
*The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.****Curated by Pentester Land & Sponsored by Intigriti***