Bug Bytes #16 – Session fixation on Shopify by @filedescriptor, Keyhacks & How to Hunt Bugs in SAML

BY INTIGRITI · APRIL 30, 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 19 to 26 of April.

Our favorite 5 hacking items

1. Challenge of the week

> "CTF Challenge"

I haven't had the time yet to do this CTF, but it's on my todo list because it seems different. It's a Web CTF that involves multiple subdomains, directory bruteforce, and different attack vectors.
So it's a nice opportunity to practice recon. But make sure to respect the rules (attacking the infrastructure/ports other than 443 is not allowed).

2. Writeup of the week

> "Session fixation on Shopify ($5,000)"

This is an excellent session fixation report. It is well-written, detailed and a good example of a real-life session fixation attack. So it's a goodread if you want to learn about this kind of bugs.
Also, it's interesting to see how @filedescriptor found the bug and chained it with an out of scope vulnerability: He found an XSS but XSS was out of scope. So he kept playing with the apps and noticed that some session IDs generated didn't change after logging in, which meant session fixation. So he leveraged the XSS to exploit the session fixation.

3. Article of the week

> ""CI Knew There Would Be Bugs Here" — Exploring Continuous Integration Services as a Bug Bounty Hunter
> A list of the most common [secure] variables from 5,302,677 build logs on Travis CI"

This is awesome research and collaborative work! I loved reading about:

- How they came up with this research topic
- How they started with a list of bug bounty programs, found their Github organizations (using Google), then their Travis CI projects (using a bookmarklet)
- How they grepped through the sizeable data retrieved (using Ripgrep)

- How the tools they used to fetch build logs were created with availability in mind (to avoid causing any service disruption)
- Which kind of information to look for when analyzing Travis CI logs
- Several examples of bugs found on bug bounty programs

4. Resource of the week

> "Keyhacks"

Keyhacks is a Github repo listing ways in which API keys can be checked to see if they're valid.
It can be handy to quickly show the impact of API keys leaked by bug bounty targets. It's particularly interesting after reading the research about finding sensitive information in Travis CI logs.

5. Tutorial of the week

> "How to Hunt Bugs in SAML; a Methodology – Part I, Part II & Part III"

If you've come accross SAML during testing and didn't know which kinds of bugs to look for, these tutorials are for you!
They're a good introduction including how SAML works, common vulnerabilities, tools, a testing methodology, and resources.
5. Tutorial of the week

6. Intigriti News

6.1 XSS Challenge

After the big succes of the Twitter CTF, Intigriti published a new challenge. This time it is a XSS challenge. Are you able to execute javascript on challenge.intigriti.io?

> **"CHALLENGE: Can you find the XSS? Earn a Burp License, cool swag & private invites!**
> **https://t.co/EehqBfFmjA pic.twitter.com/sq8FIYgQOH**
> **— Intigriti (@intigriti) April 29, 2019"**

6.2 Program of the Week

Torfs – the well-known shoe retailer in Belgium – is still a 100% family business today. This family character guarantees a number of important values within the company where employees are central. With more than 80 stores in Flanders, 2 shops in the French part of Belgium and a growing online shop in Belgium, The Netherlands and several marketplaces, Torfs wants to be and remain the most customer-friendly optichannel shoe store chain. **They pay up to €5000 and have their full online store in scope.** Go have a look!

Start hunting here!

Other amazing things we stumbled upon this week

Videos

- GitLab 11.4.7 Remote Code Execution – Real World CTF 2018 & Blog post
- CarolinaCon 2019 – Much Ado About (Credential) Stuffing
- Zero to Hero Pentesting: Episode 6 – Enumeration (Kioptrix & Hack The Box)
- Hacker101 – Native Code Crash Course & Resources

Podcasts

- Security sandbox: Plain Language Web Hacking with Pete Yaworski
- Security Now 711 – DNSpionage
- Secure Digital Life #107 – Getting Started: Dark Web
- Smashing security 125: Pick of the thief!
- Hack Naked News #215 – Shopify, Intezer, & Weaponized Vuln.
- Risky Business #538 — Marcus Hutchins is a milkshake duck, Iranian APTs doxxed and more
- 7MS #360: Active Directory Security 101 – Part 2

Webinars & Webcasts

- Day in the Life of an Ethical Hacker: A Discussion w/ Callum Carney, SRT Member

Slides only

- OWASP Top 10 Like I'm Five – From a bug bounty hunter's perspective & Long version

Tutorials

Medium to advanced

- The most common OAuth 2.0 Hacks
- What else should you know about argument injection at OS commanding vulnerabilities
- Firmware Extraction 101
- Getting in the Zone: dumping Active Directory DNS using adidnsdump & Adidnsdump
- How to obtain Office 365 credentials on Mac OS

Beginners corner

- Top 7 Subdomain Scanner Tools: Find Subdomains in Seconds

- File Path Traversal and File Inclusions
- How to increase your chances of finding a hidden camera
- Exploring, Exploiting Active Directory Pen Test
- Pillaging Passwords from Service Accounts
- No installation packet capture—you might get credentials too!

Writeups

Challenge writeups

- Asis CTF Quals 2019 – Fort Knox
- Bugcrowd University CTF
- ångstromCTF 2019 — quick write-ups by @terjanq (Web)

Pentest writeups

- Gaining Access to Card Data Using the Windows Domain to Bypass Firewalls

Responsible disclosure writeups

- How I found 5 ReDOS Vulnerabilities in Mod Security CRS & Unpatched ModSecurity CRS vulnerabilities leave web servers open to denial-of-service attacks
- This is how (easily) Indiamart gave away access to their Internal corporate secrets and Dev Instances
- Stealing Bear Notes With Url Schemes
- On insecure zip handling, Rubyzip and Metasploit RCE (CVE-2019-5624)
- Uncovering CVE-2019-0232: A Remote Code Execution Vulnerability in Apache Tomcat
- Security flaws uncovered in Sony Smart TVs

Bug bounty writeups

- Information disclosure on GitLab ($12,000)
- DoS on Twitter ($5,040)
- Information disclosure on HackerOne ($3,000)
- Use After Free on Lob ($1,500)

- Privilege escalation on Shopify ($500)
- Information disclosure on Discourse ($128)
- Information disclosure on Zendesk ($3,000)
- Information disclosure on Facebook ($5,000)
- Stored XSS on private program ($800)
- Ssrf on private program
- 2FA bypass using X-Forwarded-For on private program
- Logout CSRF on private program

See more writeups on The list of bug bounty writeups.

Tools

- X41 BeanStack & Introduction: Java Fingerprinting using Stack Traces
- SmartProxy: SmartProxy will automatically enable/disable proxy for the sites you visit, based on customizable patterns
- BugHunter: A Bug management project for Bug Hunters
- RCEvil.NET & Slides: A tool for signing malicious ViewStates with a known validationKey
- Viewgen: ASP.NET ViewState generator, When to use it & Related research
- Thief: Subdomain hijack automation. Wrapper around Sublist3r & Subjack
- Findomain: A tool that use Certificate Transparency logs to find subdomains
- Reverie: Wrapper around pentest tools with automated reporting (for Parrot Linux)
- GitHacker: A Git source leak exploit tool that restores the entire Git repository, including data from stash, for white-box auditing and analysis of developers' mind
- Csp-analyzer.py: Python script that displays the Content-Security-Policy of a given url
- Netmap.js: Fast browser-based network discovery & port-scanning module
- Termshark: A terminal user-interface for tshark
- SAP Gateway RCE exploits

Misc. pentest & bug bounty resources

- APIsecurity.io Issue 28: Breaches in Tchap, Shopify, and JustDial
- Angular and the OWASP Top 10 Cheat sheet

- JSON Web Tokens (JWT) Cheat sheet
- Underdog Discord server

Challenges

- Target Practice #Android
- XSS challenge by @intigriti: Submit answer before May 2nd. Winner gets a Burp license, swag & private invites
- DOM & reflective XSS challenge by @bl4ckh4ck5
- XSS challenge by @s3c_krd & Solution
- XSS challenge & A harder one by @brutelogic
- XSS challenges by @LooseSecurity
- Locomocosec CTF

Articles

- Attacking Cloud Containers Using SSRF
- What stealthy attacks are hiding in API data—and why do most WAF miss them?!
- Stop Using Python for Subdomain Enumeration & Twitter discussion
- XSS-Auditor—the protector of unprotected & tl;dr
- Exploiting Deserialisation in ASP.NET via ViewState
- After three years of silence, a new jQuery prototype pollution vulnerability emerges once again
- My Personal OSINT Techniques, Volume 2: The Kitchen Sink
- How Google Is Using Content Security Policy to Mitigate Web Flaws
- Achieving DevSecOps with Open-Source Tools
- Name (mDNS) Poisoning Attacks Inside The LAN & mDNS server/spoofer

News

Bug bounty news

- Goodbye to CloudFront subdomain takeovers

Vulnerabilities

- Hacker Finds He Can Remotely Kill Car Engines After Breaking Into GPS Tracking Apps
- Hotspot finder app blabs 2 million Wi-Fi network passwords
- Phone fingerprint scanner fooled by chewing gum packet
- France's 'Secure' Telegram Replacement Hacked in an Hour

Breaches & Attacks

- Threat actors leverage credential dumps, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide
- Docker Hub Database Hack Exposes Sensitive Data of 190K Users
- P2P Weakness Exposes Millions of IoT Devices
- Researchers checked 34 billion insufficiently random Ethereum keys, and found that 732 of the associated addresses had already been emptied, likely by thieves. One of those thieves had amassed a fortune that was at one point worth $54 million.
- Evil TeamViewer Attacks Under the Guise of the U.S. State Department
- Android apps on Google Play Store come with nasty surprise

Other news

- These Are The World's Most Hacked Passwords — Is Yours On The List?
- DNS over HTTPS is coming whether ISPs and governments like it or not
- EU votes to create gigantic biometrics database
- Facial Recognition is Here: But Are We Ready?
- Password1, Password2, Password3 no more: Microsoft drops password expiration rec
- Google to block sign-in attempts from embedded browsers
- Carbanak Source Code Unveils a Startlingly Complex Malware
- Amazon Employees Given 'Broad Access' to Personal Alexa Info

Non technical

- From Grey to White – An Unspoken Ethical Journey in Cyber Security
- An Idiot's Guide to Dealing with Hackers
- All Eyes On You: How To Grab And Hold An Audience's Attention
- Why Rest Is Essential To High Performance

- Job burnout: How to spot it and take action

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

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.