Bug Bytes #116 – New OAuth attacks, Hacking Shopify with a single dot & Netmask SSRF

BY ANNA HAMMOND · MARCH 31, 2021 · 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 March 22 to 29.

Our favorite 5 hacking items

1. Articles of the week

Hidden OAuth attack vectors
Recovering A Full PEM Private Key When Half Of It Is Redacted

OAuth and SSRF are the gifts that keep on giving! @artsploit revealed three entirely new OAuth2 and OpenID Connect vulnerabilities: “Dynamic Client Registration: SSRF by design”, “redirect_uri Session Poisoning”, and “/.well-known/webfinger User Enumeration”. This is fantastic research, simply a must-read!
Also worth noting, ActiveScan++ was updated to detect and report these bugs.

The second article is the reason why you should never include a partially redacted PEM in a pentest report (or share it on social media). @CryptoHack__ was challenged to recover a full private key from a partially redacted private RSA key, and shows exactly how they did it.

2. Writeups of the week

From 500 to Account Takeover
[h1-2102] FQDN takeover on all Shopify wholesale customer domains by trailing dot (RFC 1034) (Shopify, $3,100)
Universal “netmask” npm package, used by 270,000+ projects, vulnerable to octal input data: server-side request forgery, remote file inclusion, local file inclusion, and more (CVE-2021-28918) & Serious Netmask vulnerability found to affect three Perl IP modules

Pentesters @skeltavik and @KoenClaes_ started with a goal, to steal users Session IDs that they noticed accessible in a JavaScript function. They detail in an excellent writeup how they managed to do it using an XSS on an HTTP 500 error page, a Cloudflare bypass, a CSP bypass and Google Analytics.

The second writeup is a cool FQDN takeover on Shopify that @securinti found during a live hacking event. The impact is similar to subdomain takeover except that it didn’t require access to DNS records. It only took adding a single dot... but it’s better explained with video!

The third writeup is about a vunerability affecting the Netmask NPM package used in almost 279k projects. If you like SSRF and IP validation bypasses, it's worth a read.

3. Resource of the week

MindAPI (online version) & Repo

dsopas published this cool mindmap of API hacking resources and methodology for all types of APIs. If you're into API hacking, this is a nice way to organize a lot of information on the topic (not only steps and tools, but also videos, writeups, labs, tutorials, etc).

4. Tutorials of the week

Poking At Elasticsearch: Beyond Just Dumping Data
SAML XML Injection

Elasticsearch is often associated with data dumps and information disclosure, but there is so much more to Elasticsearch security. The first tutorial shows how to bruteforce credentials when an Elasticsearch instance is using authentication and what to next after obtaining credentials (discovering user accounts and post-exploitation recon techniques).

The second article is about a vulnerability NCC Group pentesters detected in several assessments of SSO services. It is a great read about SSO / SAML hacking.

5. Tool of the week

masher & From Creative Password Hashes to Administrator: Gone in 60 Seconds (Or Thereabouts)

Masher stands for "**m**ultiple password '**asher**". It helps break password hashes when non obvious combinations of hashing algorithms are used.

Identifying the type of a hash is something I always struggle with. So, I find this very helpful. Since it's just a script using Python's hashlib, it's also easy to modify to add more combinations.

Other amazing things we stumbled upon this week

Videos

- XXE INJECTION Deep Dive with @0xTib3rius
- HACKING ANDROID WebViews (Static analysis – Part 2)
- SQL Injection – Lab #4 SQL injection UNION attack, finding a column containing text
- AMA with full-time bug hunter Alex Chapman

Podcasts

- DAY[0] Episode 70 – Google exposes an APT campaign, PHP owned, and Several Auth Issues
- GIT Me Some PHP – Spectre Returns to Linux, API Security, OpenSSL Flaws, SolarWinds
- The InfoSec & OSINT Show 50 – pdp (Petko Petkov) & Automating Pownage with PownJS
- Darknet Diaries Ep 88: Victor
- The Hacker Mind EP 17: Shellshock

Webinars & Webcasts

- @0xtavian presents “Axiom: A Distributed Hacking Framework for Pentesters and Red Teamers”
- Open Redirects – An Underestimated Vulnerability
- OPSEC Fundamentals for Remote Red Teams
- What Are BOF?

Conferences

- FuzzCon Europe – WebSecurity Edition
- Dave Aitel – Dry Run of Adding Value by Being Annoying Talk

Tutorials

Medium to advanced

- Old But Gold – Attack And Defend The Sys Admins
- Red Team Privilege Escalation – RBCD Based Privilege Escalation – Part 2

Beginners corner

- The Ultimate Guide To Finding And Escalating XSS Bugs
- Cloud Storage Security: Attacking & Auditing
- Comprehensive Guide on ffuf
- 6 ways to enumerate WordPress Users

Writeups

Challenge writeups

- Challenge writer POV: BSidesSF 2021 CTF (Cloud)

- Intigriti — XSS Challenge 0321

Pentest writeups

- Bypassing VPN MFA During a Pentest via Duo Inline Self-Enrollment
- Second independent audit of SecureDrop Workstation completed #PentestReport

Responsible(ish) disclosure writeups

- CVE-2021-3449 OpenSSL <1.1.1k DoS exploit
- Pentester's tricks: Local privilege escalation in OpenVAS #LPE #Linux
- CVE-2021-23888 – McAfee ePolicy Orchestrator HTML Injection #Web
- CVE-2020-27199 (Magic Home Pro – Authentication Bypass) #Web

Bug bounty writeups

- PHP fopen() function to local file inclusion
- Multiple Authorization bypass issues in Google's Richmedia Studio (Google, $6,000)
- Google Chrome Bug Bounty: $5,000 – File System Access API – vulnerabilities (Google, $5,000)
- HTML Injection in Swing can disclose netNTLM hash or cause DoS (PortSwigger Web Security, $1,000)
- Unrestricted access to quiesce functionality in dss.api.playstation.com REST API leads to unavailability of application (PlayStation, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- S3 Account Search & Intro: Python tool that finds the AWS account ID of any public S3 object/bucket
- SQLMap DNS Collaborator: Burp Extension that lets you perform DNS exfiltration with Sqlmap with zero configuration needed
- gitrecon: OSINT tool to get information from a Github and Gitlab profile and find user's email addresses leaked on commits
- nsdp-discover: Nmap NSE script to discover NSDP service and retrieve basic information
- harlogger: Simple utlity for sniffing decrypted HTTP/HTTPS traffic on a jailbroken iOS device into an HAR format

Tips & Tweets

- If you like XSS, and do not know where to start WAF Bypassing...

- Code snippet disclosure
- Techniques @nnwakelam uses to bypass admin interface authentication
- Ever find a phpMyAdmin login portal and default creds won't work?
- Why Hackvertor JavaScript custom tags are broken in newer Burp versions & A temporary fix
- No NTB-NS/ARP/LLMNR? Use DHCP.py in Responder's tools/ folder

Misc. pentest & bug bounty resources

- Web wordlists in 2021
- Wordlists for Pentester
- Awesome Kubernetes (K8s) Security

Articles

- Detecting dangerous Spring service exporters with CodeQL
- More Options For Response Modification -with Responsetinker & ResponseTinker
- Eliminating XSS from WebUI with Trusted Types & Trusted Types bypass challenge solutions
- Dumping LSASS in memory undetected using MirrorDump
- Restricted Environment IoT Hacking: All You Need Is a Remote Shell

Bug bounty & Pentest news

- TLS 1.0 and TLS 1.1 are officially deprecated
- Microsoft: Introducing Bounty Awards for Teams Desktop Client Security Research
- Hack Alongside Hackers: AWS and HackerOne CTF (April 5-12)
- Hackers Who Paint (May 15)
- Security researcher launches GoFundMe campaign to fight legal threat over vulnerability disclosure
- Backdoor planted in PHP Git repository after server hack
- Tool updates:
  - BBRF v1.1.1
  - ZAP 2.10.0
  - SAML Raider Release 1.4.0

Non technical

- Bug Bounties: Tips from the Triager
- Infosec job thread
- The Consumer Authentication Strength Maturity Model (CASMM)
- Bug hunters sharing stats on their reports in terms of severity (check out the “Quote Tweets”)

Community pick of the week

So happy for you @sumgr0! Keep it up

Want to share your bug bounty wins, swag and joys with other Bug Bytes readers? Tag us on social media, we’d love to hear from you too!