Bug Bytes #11 – Insecure Deeplinks, new XS-techniques and @int0x33 ‘s 365DaysOfPWN

BY INTIGRITI · MARCH 26, 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 15 to 22 of March.

Our favorite 5 hacking items

1. Conference of the week

This is an awesome trick for any bug hunter who uses Chrome. You can create shortcuts to query sites like Shodan, VirusTotal, RiskIQ, etc.
For instance, you can type *s google* (for https://www.shodan.io/search?query=org%3Agoogle).
To do this, go to *Settings* in Chrome, then *Manage search engines*. Add a new one with *s* as the *Keyword* and https://www.shodan.io/search?query=org%3Agoogle as the URL.

2. Writeup of the week

> “[Grab Android/iOS] Insecure deeplink leads to sensitive information disclosure **($7,500)**”

This is a very interesting bug found on GrabTaxi’s Android and iOS apps. It’s the equivalent of an open redirect on mobile apps: some deeplinks missing validation “direct users to load any attacker-controlled URL within a webview”.
In case you’re wondering, a deep linking is a URI that links to a specific location within a mobile app rather than simply launching the app (Wikipedia definition).
One of the vulnerable deeplinks looks like this: grab://open?screenType=HELPCENTER&page=https://s3.amazonaws.com/edited/page2.html
The URL https://s3.amazonaws.com/edited/page2.html, created by the bug hunter, contains code that calls getGrabUser, a method defined within the app which returns sensitive information on the user.
So using the vulnerable deeplink, it is possible to execute attacker-controlled code that steals the victim’s sensitive information.

3. Article of the week

> “New XS-Leak techniques reveal fresh ways to expose user information”

I’ve encountered many articles on XS-Search this last couple of weeks. If, like me, you’re just hearing about this type of attack, this article is an excellent introduction.
It explains what it is briefly and references different publications about it. It’s worth to dive into each one, since XS-Search is said to be the next XSS.

4. Tool of the week

> “CommandGenInterface”

This is a simple vueJS app which generates commands based on what you choose: For example, you enter a target, select a wordlist and a list of extensions, and the app generates a complete dirsearch command for you.
Tis is great for anyone who uses several tools with different options each time (like nmap, sqlmap, dirsearch, wfuzz, massdns...).
A visual command generator allows for more flexibility than creating multiple aliases for the same command with different options.
But the app is meant to be customized to add tools based on your own testing workflow.

5. Resource of the week

> "P64labs: 365 DAYS OF PWN"

This is a site by the author of the #365DaysOfPWN Medium articles I've been sharing in the previous newsletters.
The site is more organized and is updated at least once a day. It's an amazing resource for pentesters and red teamers (and for OSCP)!

Other amazing things we stumbled upon this week

Videos

- Angular: XSS without HTML tags
- Zero to Hero Pentesting: Episode 1 – Course Introduction, Notekeeping, Introductory Linux, and AMA
- 10 Minute Tip: Searching Breach Data for OSINT
- DNS Enumeration Tutorial – Dig, Nslookup & Host
- Haxcellent Adventures: The Bird Feeder, Bash, and You
- Docstop: Team Whack – everything is hackable (in Finnish but English subtitles available)

Podcasts

- Security Now 706: Open Source eVoting
- 7MS #353: Tales of Internal Pentest Pwnage – Part 1
- Absolute AppSec Ep. #51 – Jessica Ryan (@Jhyp3)
- Security In Five Episode 455 – Tools, Tips and Tricks – Firefox Send
- Smashing Security 120: Silk Road with Deliveroo
- Darknet Diaries Ep 34: For Your Eyes Only
- VITB Podcast: Marcus Carey

Webinars & Webcasts

- Exploring the Top 15 Most Common Vulnerabilities with HackerOne and GitHub
- InfoSec Girls + OWASP WIA knowledge exchange webinar
- You are watching: Developing Burp Suite Extensions with Luca Carettoni
- BHIS Webcast: Py2k20 – Transitioning from Python2 to Python3

Conferences

- Catch Me If You Can: Ephemeral Vulnerabilities in Bug Bounties (44CON 2018)
- BSidesSF 2019, especially:
  - Automating Web Application Bug Hunting
  - Journey to Command Injection: Hacking the Lenovo ix4-300d
  - Offensive Javascript Techniques for Red Teamers
  - Navigating Passwordless Authentication with FIDO2 & WebAuthn
  - Abusing WCF Endpoint for RCE and Privilege Escalation
  - All Your Containers Are Belong to Us
  - Hacking with a Heads Up Display
  - Cats? In My Certificate Transparency Logs?
  - Ethical Hacking: DIY Mobile Security Workstation (For Cheap)
  - How to Fix the Diversity Gap in Cybersecurity
  - Don't Boil the Ocean: Using MITRE ATT&CK to Guide Hunting Activity
  - BADPDF: Stealing Windows Credentials via PDF Files
- OWASP Meetup – SF March 2019
- Shopify's $25k Bug Report, and the Cluster Takeover That Didn't... & Slides

Slides only

- GDG Toulouse: Can I hack your Android app, please?
- Ironing out Docker
- I'm in your cloud... reading everyone's email. Hacking Azure AD via Active Directory
- I am AD FS and So Can You, ADFSDump & ADFSpoof

Tutorials

Medium to advanced

- From SSRF to Port Scanner

- An introduction to privileged file operation abuse on Windows & Abusing Privileged File Manipulation
- Java Serialization: A Practical Exploitation Guide
- SQL Injection Data Extraction through .NET framework error
- Jenkins – More than Just Target Practice: Automate tests
- Extracting NTLM Hashes from keytab files & KeyTabExtract
- Exploiting OGNL Injection in Apache Struts
- MacOS Red Teaming 201: Introduction
- Using HTTP Pipelining to hide requests
- Building an Office macro to spoof parent processes and command line arguments

Beginners corner

- How to rotate your source IP address & alternative
- Cache-Control for Civilians
- DNS Toolbox: How to Perform a Full DNS Enumeration and Domain Research
- Git clone all organizational repos
- Bypass OTP validation and Phone Number authentication
- Efficient way to pentest Android Chat Applications
- A technique that a lot of SQL injection beginners don't know
- Kerberos (I): How does Kerberos work? – Theory
- Command & Control: Silenttrinity Post-Exploitation Agent
- OSX Exploitation with Powershell Empire
- Command & Control Tool: Pupy
- Multiple Ways to Exploiting OSX using PowerShell Empire

Writeups

Challenge writeups

- BsidesSF CTF — Challenge Write-up Part 1
- CONFidence CTF 2019 Teaser – Write-up

Pentest writeups

- A story of one not-a-bug SQL injection
- Finding and Exploiting .NET Remoting over HTTP using Deserialisation

Responsible disclosure writeups

- Authenticated Arbitrary Command Execution on PostgreSQL 9.3 > Latest #PostgreSQL #Database
- Rails-doubletap-exploit #RCE #PathTraversal #Deserialization #Rails
- MiniBlog Remote Code Execution #RCE
- Ghidra From XXE to RCE #RCE #Decompiler
- RCE in Slanger, a Ruby implementation of Pusher #RCE #WebSockets #Ruby
- Remote command injection through an endpoint security product #IoT
- Find My Contacts (or personal data of 650,000 people) #Mobile #IDOR
- Connected camera cock up #Mobile
- Vulnerability Spotlight: Multiple Vulnerabilities in CUJO Smart Firewall, Das U-Boot, OCTEON SDK, Webroot BrightCloud #Firewall
- Exploitation of Remote WCF Vulnerabilities #WCF
- Multiple vulnerabilities in the web interface of the Cisco IP Phone 7800 and 8800 series #IPPhone #BufferOverflow #FileUpload #PathTraversal #CSRF #Authorization
- Analysis for CVE-2019-5418 File Content Disclosure on Rails & Exploit #Rails #PathTraversal

Bug bounty writeups

- SQL injection via User-Agent HTTP header on TTS Bug Bounty ($2,000)
- DoS on Twitter ($1,120): “How to break Twitter using only 3 characters”
- Payment bypass on Zomato ($1,000)
- Information disclosure via Pastebin on Zomato ($400)
- DoS due to Integer overflow on Facebook ($10,000)
- XS-Search on Google ($1,337)
- DoS on Facebook ($750)
- RCE on Mozilla ($500)

See more writeups on The list of bug bounty writeups.

Tools

If you don’t have time

- PowerHub: A web application to transfer PowerShell modules, executables, snippets and files while bypassing AV and application whitelisting
- Anubis: Subdomain enumeration and information gathering tool

- NPK, Introduction & demo: A mostly-serverless distributed hash cracking platform that provides unprecedented password cracking capabilities

More tools, if you have time

- Pastebin_scraper & Introduction: Automated tool to monitor Pastebin for interesting information like emails and passwords. Project created after Dumpmon went dark last October
- RapidRepoPull: The goal of this program is to quickly pull and install repos from its list
- Bug Hunter: Tools for Bug Hunting
- InjectMate.py: Burp Extension that generates payloads for XSS, SQLi, and Header injection vulns (for Burp Pro)
- InjectMateCommunity: same thing minus collaborator (for Burp Community)
- Pocsuite3 & PoCs: Open-sourced remote vulnerability testing framework developed by the Knownsec 404 Team
- TrustMeAlready: Disable SSL verification and pinning on Android, system-wide
- APK Utilities](https://github.com/ViRb3/apk-utilities): Tools and scripts to manipulate Android APKs
- Hashboy-tool: A hash query tool
- Cloud Crack & Introduction: Crack passwords using Terraform and AWS
- AnsiblePlaybooks: A collection of Ansible Playbooks that configure Kali to use Fish & install a number of tools
- PoshNmap](https://github.com/justingrote/poshnmap): A Powershell Wrapper for Nmap
- Bettercap/hydra: Official Bettercap Web UI
- Kerbrute: A tool to perform Kerberos pre-auth bruteforcing. “A cross platform standalone binary for bruteforcing and enumerating AD users through Kerberos AS requests. Definitely the fastest way to brute force (or lockout a user in an AD domain”
- Cyberlens: Free ICS Asset Identification and Assessment tools for industrial cybersecurity
- Platypus: A modern multiple reverse shell sessions manager written in go

Misc. pentest & bug bounty resources

- Bug-Hunting-Mentaility
- Bug Bounty Hunting Struggle (2BHS)
- Pentest compilation
- WebHunt: @GochaOqradze’s bug hunting notes
- “Domain Name” section of IntelTechniques
- OWASP Cheat Sheet Series

- Awesome Node.js for penetration testers
- APIsecurity.io Issue 23: Hacking ML, AWS Gateway Security, Gartner advice to CISO
- Red Team References
- DeadPixelSec Discord server: “Cyber security discord community with lots of helpful people to help you start your career in cyber security”

Challenges

- The unescape() room by @jobertabma
- Yes We Hack XSS challenge

Articles

- Designing Distributed Systems for Security Workflow — Learning from our Nullcon Workshop
- Attacking the internal network from the public Internet using a browser as a proxy
- HTTP Cache Cross-Site Leaks
- How to get private invitation in HackerOne?
- SAML – Want to pen-test?
- Apache Struts Vulnerabilities
- How to write secure code? Protect yourself against Cross-Site Scripting!
- How Do I Prepare to Join a Red Team?
- IPv6 unmasking via UPnP
- Buy One Device, Get Data Free: Private Information Remains on Donated Tech

News

Bug bounty news

- OWASP ZAP Questionnaire to help make it better
- Kringle Con Winners and Answers
- Bugcrowd’s LevelUp 4 CFP: “Topics desired: Hacker Collaboration/How to Hack w/Others, Pentesting Methodologies, Advanced Web Hacking & Recon Techniques, and more.””
- Finalists of Hackerone’s T-shirt contest: Vote before 31 of March
- New features for quicker and improved Bug Reporting !: You can add your on report templates on Yes We Hack
- Researcher settings on Facebook & Help: New Facebook functionality for whitehats to help analyze traffic in the mobile apps

- Sonatype and HackerOne eliminate the pain of reporting open source software vulnerabilities
- GitLab now automatically warns against merging API keys into your codebase
- Pwn2Own Vancouver 2019 – The Schedule and Live Results: The @fluoroacetate duo found bugs on Safari, Virtualbox, VMware Workstation, Firefox, Edge & Chromium, and left with $375,000 plus a Tesla Model 3!

Reports

- Threat detection report 2019: The most used ATT&CK technique by far is PowerShell
- Top 10 vulnerabilities 2018
- What Are The Most Secure Programming Languages: "Vulnerabilities in C amounted to 50% of all reported open source security vulnerabilities"

Vulnerabilities

- Flaw in popular PDF creation library enabled remote code execution
- Researcher finds new way to sniff Windows BitLocker encryption keys
- Researchers fret over Netflix interactive TV traffic snooping
- Critical flaw lets hackers control lifesaving devices implanted inside patients
- Now-Patched Google Photos Vulnerability Let Hackers Track Your Friends and Location History: via browser-based timing attacks

Breaches

- Why you should "never EVER install spyware on anyone's phone unless you're willing to accept that everything captured may one day become public"
- Change your Facebook password now!
- FEMA Breach Exposes Personal Data and Banking Information of 2.3 Million Disaster Survivors
- Hacked tornado warning systems leave Texans in the dark
- Round 4 — Hacker Puts 26 Million New Accounts Up For Sale On Dark Web
- How Hackers Pulled Off a $20 Million Mexican Bank Heist
- Norsk Hydro Calls Ransomware Attack 'Severe': "This is the first time I can recall a cyberattack impacting the spot price of a global commodity like aluminum"
- Elsevier exposes users' emails and passwords online: "The credentials were displayed on Kibana"
- Scammer pleads guilty to fleecing Facebook and Google of $121m

Other news

- Microsoft Windows 7 patch warns of coming patchocalypse

- MySpace loses 50 million songs in server migration: Always do your own backups...
- CEOs more likely to receive pay rise after a cyber attack. Wait, what?
- Uber used secret spyware to try to crush Australian start-up GoCatch: “Surfcam allowed Uber Australia to see in real time all of the competitor cars online and to scrape data such as the driver’s name, car registration, and so on.” It allowed Uber to directly approach the GoCatch drivers and lure them to work for Uber.

Non technical

- Researcher Spotlight: Ambassador Justin Gardner
- Lucas aka BitK: high level bug hunter and the brand new YesWeHack Tech Ambassador
- An Argument that Cybersecurity Is Basically Okay
- OSINT is Maturing: Our Interview with Steve Micallef from SpiderFoot
- FIRST for security: Non-profit looks ahead to another 15 years of CVSS ratings
- RSAC 2019: Better than what?
- Red Teaming VS Penetration Testing VS Vulnerability Testing

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 03/15/2019 to 03/22/2019.

Curated by Pentester Land & Sponsored by Intigriti