Echavarria, et al. v. Facebook, Inc.

3:18-cv-05982-WHA (and all related cases) Plaintiffs' Tutorial January 9, 2019

Introduction

- Plaintiffs' Counsel
 - Morgan & Morgan, P.A. Complex Litigation Group
 - Cohen Milstein Sellers & Toll PLLC
 - Milberg Tadler Phillips Grossman LLP
- Retained Experts
 - Mary T. Frantz will discuss:
 - PII, its Value, and Basic Security Against Hacking
 - Matt. B. Strebe will discuss:
 - Authentication, Access Tokens, and Hacking Tokens
- Some questions moving forward

PII, Its Value, and Basic Security Against Hacking

- Mary Frantz
 - Over 28 years experience in cyber security, corporate enterprise technology architecture, identity and access management
 - CEO of Enterprise Knowledge Partners, LLC
 - Has served as an expert witness in several data breach cases
 - Certified Ethical Hacker, Penetration Tester, Information Systems Auditor
 - CV provided for the Court and counsel

Personally Identifiable Information (PII)

- General Definition and California CalOPPA
 - PII Defined (California Online Privacy Protection Act (CalOPPA) Cal. Bus. & Prof. Code Sec. 2577(a))
 - Details collected on the Internet about an individual consumer, including an individual's first and last name, a physical street address, an email address, a telephone number, a Social Security number, or any other information that permits a specific individual to be contacted physically or online.
- Compromised PII has two major types
 - Temporary or "changeable" information short shelf life
 - Examples: passwords, credit card numbers, bank accounts, drivers license, email, phone numbers
 - Historical or "unchangeable" information long or infinite shelf life
 - Examples: original images/photos, passport numbers, current and previous addresses, mothers maiden name, relationships (family, contacts, challenge response questions), education, birth date, SSN, employment history, earnings and net worth, health history, purchase history, product designs, online comments, signed docs

<u>PII – Value</u>

- Aggregated Profiles or Fullz
 - Fullz complete "packages" of information
 - Combination of historical and temporary information
 - Highest value Fullz aggregated behavioral and personality profile descriptors
 - Opinions, contacts, family members, style and event choices, online and physical locations visited, interests (for example: music, movies, colors, auto purchases, and sites visited), "changeable" and "unchangeable" information
 - Confidential corporate information and IP, customer complaints, confidential electronic communication

• Value of PII

- Validated and/or recently updated Fullz PII = higher street price per profile
- Fullz is highly coveted by nation states, "phishers," malicious hackers, and spammers
- Neural-marketing: the process of mining Fullz for targeted influence and manipulation
- Collection and mining of Fullz has been used by nation state clandestine operations

PII – Darknet and Dark Web

- Darknet
 - System of routers and relay of devices that are not indexed or directly accessible
 - All communication between the relays use encryption
 - Cannot access Darknet using standard internet browsers; must know exact address or use Dark Web browsers
- Dark Web
 - A subset of the Darknet that works over HTML
 - Web services and specific browsers required to access Darknet
 - Built upon anonymous browsing
 - Specific, anonymous services available: messaging, emails, files sharing sites

PII – How It is Misused

- Big data repositories created from compromised and legitimate PII on Darknet
 - Combined and blended as needed
 - Sold off in pieces for continued revenue streams
 - Pieces sold rarely equate to exact copies of stolen data (obfuscates source and trail)
 - Complete Fullz NOT usually found or sold on Darknet auction sites
- Use of Dark Web for selling stolen data
 - "Changeable" information often sold on sales or auction sites; currency is BTC
 - Pieces of Fullz are sold on sales or auction sites
 - Usually copies (not original), with diminished value
 - Complete Fullz sales use private messaging, secure emails, burner phones

High Level Hacker Lifecycle



- Perform physical, logical reconnaissance (web site, employees, physical sites, etc.)
- Use web crawlers/spiders, NMAP
- Vulnerability scan
- Register as developer and gain insights
- Test possible vulnerabilities, learn from error messages/responses
- Test access see what works, what doesn't and why

- Access and create "backdoors"
- Open up ports
- Harvest and/or elevate credentials (impersonate real user and service accounts)
- Root
- Delete evidence as they go (advanced), time stomp
- Exfiltrate

- Leave back doors
- Delete logs
- May sell or share vulnerability to script kiddies to cover tracks, create noise (cause chaos)
- Come back after noise calms down or use noise as a cover
- Watch for reactions, method of remediation

- Advanced attackers do not want to get caught, maximize "time on target"
- "Scriptkiddies" are not advanced, they often make noise that is [sometimes] easily detected

Sample Crawl or Spider

Т								_	
Contexts Context Context Sites			Welcome to the OWASP Zed Attack Proxy (ZAP) ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. Please be aware that you should only attack applications that you have been specifically been given permission to test. To quickly test an application, enter its URL below and press 'Attack. URL to attack: https://www.facebook.com Image:						
y 🔍 Search р Alerts 📄 Output w Scan 🗄 Progress: 1: https://wwww.face	券 Spider े Active Scan ≠ ≭ =	F]	0% 🗸 Current Scans: 1 : Num requests: 187 🦑 Export					i i i i i i i i i i i i i i i i i i i	
Req. Timestamp	Resp. Timestamp	Method	URL	Code Reason	RTT	Size Resp. Header	Size Resp. Body		
695 1/8/19 12:17:32 PM	1/8/19 12:17:32 PM	GET	https://www.facebook.com/ajax?query=thishouldnotexistandhopefullyitwillnot	404 Not Found	218 ms	1,380 bytes	582,355 bytes		
696 1/8/19 12:17:32 PM	1/8/19 12:17:32 PM	GET	https://www.facebook.com/ajax/pagelet?query=%2F	404 Not Found	90 ms	1,172 bytes	579,682 bytes		
697 1/8/19 12:17:32 PM	1/8/19 12:17:33 PM	GET	https://wwww.facebook.com/ajax/pagelet/generic.php?query=c%3A%5CWindows%5Csystem.ini	404 Not Found	823 ms	1,182 bytes	580,765 bytes		
698 1/8/19 12:17:32 PM	1/8/19 12:17:32 PM	GET	https://www.facebook.com/ad_campaign/landing.php?campaign_id=%2Flanding.php&extra_1=autr	o& 200 OK	177 ms	1,311 bytes	616,402 bytes		
699 1/8/19 12:17:32 PM	1/8/19 12:17:33 PM	GET	https://www.facebook.com/ajax/pagelet?query=%2F%2F%2F%2F%2F%2F%2F%2	.% 404 Not Found	83 ms	1,172 bytes	582,949 bytes		
700 1/8/19 12:17:34 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax/pagelet?query=WEB-INF%2Fweb.xml	404 Not Found	117 ms	996 bytes	72 bytes		
701 1/8/19 12:17:33 PM	1/8/19 12:17:33 PM	GET	https://www.facebook.com/ajax?query=ajax	404 Not Found	206 ms	1,380 bytes	579,428 bytes		
702 1/8/19 12:17:33 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax/pagelet/generic.php?query=%5C%5C%5C%5C%5C%5C%5C%5	5C 404 Not Found	633 ms	1,182 bytes	583,469 bytes		
703 1/8/19 12:17:34 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax/pagelet?query=WEB-INF%5Cweb.xml	404 Not Found	94 ms	996 bytes	72 bytes		
704 1/8/19 12:17:33 PM	1/8/19 12:17:33 PM	GET	https://www.facebook.com/ajax/pagelet?query=c%3A%5C	404 Not Found	182 ms	1,172 bytes	580,294 bytes		
705 1/8/19 12:17:34 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax/pagelet?query=%2FWEB-INF%2Fweb.xml	404 Not Found	87 ms	996 bytes	72 bytes		
706 1/8/19 12:17:33 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ad_campaign/landing.php?campaign_id=%5Clanding.php&extra_1=aut	to& 200 OK	101 ms	1,311 bytes	616,383 bytes		
707 1/8/19 12:17:34 PM	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax?query=%2Fajax	404 Not Found	121 ms	1,380 bytes	579,602 bytes		
	1/8/19 12:17:34 PM	GET	https://www.facebook.com/ajax/pagelet?query=%5CWEB-INF%5Cweb.xml	404 Not Found	92 ms	996 bytes	72 bytes		
708 1/8/19 12:17:34 PM					E00 ma	1,182 bytes	580,430 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM	1/8/19 12:17:35 PM	GET	https://www.facebook.com/ajax/pagelet/generic.php?query=%2Fetc%2Fpasswd	404 Not Found	002 1115		592,009 buton		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM	GET	https://wwww.facebook.com/ajax/pagelet/generic.php?query=%2Fetc%2Fpasswd https://wwww.facebook.com/ajax/pagelet?query=.%2F%2F%2F%2F%2F%2F%2F%2F	404 Not Found .% 404 Not Found	95 ms	1,172 bytes	565,006 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM	GET GET GET	https://www.facebook.com/ajax/pagele/generic.php?quurp=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagele?quurp=%4E_%2F_%2F_%2F_%2F_%2F_%2F_%2F_%2F_%2F_%2F	404 Not Found .% 404 Not Found 404 Not Found	95 ms 92 ms	1,172 bytes 1,380 bytes	579,562 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET	https://www.facebook.com/ajax/pagelet/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelet/?query=.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F	404 Not Found .% 404 Not Found 404 Not Found 404 Not Found	95 ms 92 ms 96 ms	1,172 bytes 1,380 bytes 996 bytes	579,562 bytes 72 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:35 PM 713 1/8/19 12:17:34 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET	https://www.facebook.com/ajax/pagelet/gueryi=.tp/p?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelet?query=.%2F%2F%2F%2F%2F%2F%2F%2F	404 Not Found % 404 Not Found 404 Not Found 404 Not Found 404 Not Found	95 ms 92 ms 96 ms 90 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes	579,562 bytes 72 bytes 580,498 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:35 PM 712 1/8/19 12:17:35 PM 713 1/8/19 12:17:34 PM 714 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET	https://www.facebook.com/ajax/pagele/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/guery=%5Cajax https://www.facebook.com/ajax?query=%5Cajax https://www.facebook.com/ajax/pagele7query=WEB-INF%2Fwbe.xml https://www.facebook.com/ajax/pagele7query=thishouldnotexistandhopefullyitwillnot https://www.facebook.com/ajax/pagele7query=%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.	404 NotFound % 404 NotFound 404 NotFound 404 NotFound 404 NotFound 5 404 NotFound	95 ms 95 ms 92 ms 96 ms 90 ms 500 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,182 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:35 PM 713 1/8/19 12:17:35 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelet/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelet?query=%62F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%	404 NotFound % 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound	95 ms 95 ms 92 ms 96 ms 90 ms 500 ms 97 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,182 bytes 1,182 bytes 1,172 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes		
708 1/8/19 12.17:34 PM 709 1/8/19 12.17:34 PM 710 1/8/19 12.17:34 PM 711 1/8/19 12.17:34 PM 712 1/8/19 12.17:34 PM 713 1/8/19 12.17:35 PM 714 1/8/19 12.17:35 PM 715 1/8/19 12.17:35 PM 716 1/8/19 12.17:34 PM 715 1/8/19 12.17:35 PM 716 1/8/19 12.17:34 PM	1/8/19 12:17:35 PM 1/8/19 12:17:34 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelet/guery=is/2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelet/guery=is/2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%	404 Not Found % 404 Not Found 404 Not Found	95 ms 95 ms 92 ms 96 ms 90 ms 500 ms 97 ms 105 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,182 bytes 1,172 bytes 1,519 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes 588,443 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:35 PM 712 1/8/19 12:17:34 PM 713 1/8/19 12:17:35 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET GET GET	https://www.facebook.com/ajav/pagele/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajav?query=%5Cajax https://www.facebook.com/ajav?query=%5Cajax https://www.facebook.com/ajav/pagele?query=WEB-INF%2Fweb.xml https://www.facebook.com/ajav/pagele?query=thishouldnotestiandhopelulytiwillinot https://www.facebook.com/ajav/pagele?query=%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=pagelet https://www.facebook.com/ajav/pagele?query=bagelet https://www.facebook.com/ajav/pageleVgeneric.php?pagePostSectionPagele?query=c%3A%2FWi	404 NotFound % 404 NotFound 404 NotFound	95 ms 95 ms 96 ms 90 ms 500 ms 97 ms 105 ms 106 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,182 bytes 1,519 bytes 1,519 bytes 1,173 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes 588,443 bytes 0 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:35 PM 713 1/8/19 12:17:35 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelet/generic.php?querp=%2/Fetc%2/Fpasswd https://www.facebook.com/ajax/pagelet?query=%2/F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2	404 Not Found % 404 Not Found 404 Not Found	95 ms 95 ms 96 ms 90 ms 500 ms 97 ms 105 ms 106 ms 91 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,519 bytes 1,173 bytes 996 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes 588,443 bytes 0 bytes 72 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:34 PM 713 1/8/19 12:17:35 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM	1/8/19 12:17:35 PM 1/8/19 12:17:35 PM	GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelef/generic.php?query=%2Fet%2Fpasswd https://www.facebook.com/ajax/pagelef?query=%82F,%2F,%2F,%2F,%2F,%2F,%2F,%2F,%2F,%2F,%	404 NotFound % 404 NotFound 404 NotFound	95 ms 95 ms 96 ms 90 ms 500 ms 97 ms 105 ms 106 ms 91 ms 734 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,519 bytes 1,173 bytes 996 bytes 1,182 bytes	579,562 bytes 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes 588,443 bytes 0 bytes 72 bytes 580,176 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:34 PM 713 1/8/19 12:17:34 PM 714 1/8/19 12:17:34 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 700 1/8/19 12:17:37 PM 700 1/8/19 12:17:37 PM	1/8/19 12:17:35 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM	GET GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelef/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelef/query=%2Fetc%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.	404 NotFound % 404 NotFound 404 NotFound	95 ms 92 ms 96 ms 90 ms 500 ms 97 ms 105 ms 106 ms 91 ms 734 ms 79 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,173 bytes 996 bytes 1,173 bytes 1,173 bytes	579,562 pt/ss 579,562 pt/ss 72 bytes 580,498 bytes 583,252 bytes 579,694 bytes 588,443 bytes 0 bytes 580,176 bytes 0 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 711 1/8/19 12:17:35 PM 713 1/8/19 12:17:35 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:37 PM 720 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM	1/8/19 12:17:35 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM	GET GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelet/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagelet/query=%5Cajax https://www.facebook.com/ajax/pagelet/query=%5Cajax https://www.facebook.com/ajax/pagelet/query=%EN%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.	404 NotFound % 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound % 200 OK 404 NotFound 404 NotFound	95 ms 92 ms 96 ms 90 ms 500 ms 97 ms 105 ms 106 ms 91 ms 734 ms 79 ms 90 ms	1,172 bytes 1,380 bytes 995 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,173 bytes 996 bytes 1,173 bytes 996 bytes	579,562 bytes 579,562 bytes 580,498 bytes 583,262 bytes 578,694 bytes 578,694 bytes 588,443 bytes 0 bytes 72 bytes 72 bytes 72 bytes 72 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 713 1/8/19 12:17:34 PM 714 1/8/19 12:17:35 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 719 1/8/19 12:17:37 PM 720 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM 722 1/8/19 <t< td=""><td>1/8/19 12:17:35 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM</td><td>GET GET GET GET GET GET GET GET GET GET</td><td>https://www.facebook.com/ajax/pagelef/generic.php?query=%2Fet%2Fpasswd https://www.facebook.com/ajax/pagelef?query=%2Fs%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.</td><td>404 NotFound %</td><td>95 ms 95 ms 96 ms 96 ms 500 ms 500 ms 97 ms 106 ms 91 ms 734 ms 79 ms 90 ms 111 ms</td><td>1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,173 bytes 1,173 bytes 1,173 bytes 1,173 bytes 1,172 bytes 1,172 bytes</td><td>579,562 Dytes 579,562 Dytes 72 bytes 589,498 bytes 579,694 bytes 579,694 bytes 588,443 bytes 0 bytes 72 bytes 580,176 bytes 0 bytes 72 bytes 579,800 bytes</td><td></td></t<>	1/8/19 12:17:35 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM	GET GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagelef/generic.php?query=%2Fet%2Fpasswd https://www.facebook.com/ajax/pagelef?query=%2Fs%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.	404 NotFound %	95 ms 95 ms 96 ms 96 ms 500 ms 500 ms 97 ms 106 ms 91 ms 734 ms 79 ms 90 ms 111 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,173 bytes 1,173 bytes 1,173 bytes 1,173 bytes 1,172 bytes 1,172 bytes	579,562 Dytes 579,562 Dytes 72 bytes 589,498 bytes 579,694 bytes 579,694 bytes 588,443 bytes 0 bytes 72 bytes 580,176 bytes 0 bytes 72 bytes 579,800 bytes		
708 1/8/19 12:17:34 PM 709 1/8/19 12:17:34 PM 710 1/8/19 12:17:34 PM 711 1/8/19 12:17:34 PM 712 1/8/19 12:17:34 PM 713 1/8/19 12:17:34 PM 714 1/8/19 12:17:34 PM 715 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 716 1/8/19 12:17:35 PM 717 1/8/19 12:17:35 PM 718 1/8/19 12:17:35 PM 719 1/8/19 12:17:35 PM 719 1/8/19 12:17:37 PM 720 1/8/19 12:17:37 PM 721 1/8/19 12:17:37 PM 723 1/8/19 12:17:37 PM 723 1/8/19 12:17:37 PM	1/8/19 12:17:35 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM 1/8/19 12:17:37 PM	GET GET GET GET GET GET GET GET GET GET	https://www.facebook.com/ajax/pagele/generic.php?query=%2Fetc%2Fpasswd https://www.facebook.com/ajax/pagele?query=%5Cajax https://www.facebook.com/ajax/pagele?query=%5Cajax https://www.facebook.com/ajax/pagele?query=%5Cajax https://www.facebook.com/ajax/pagele?query=%5Cajax https://www.facebook.com/ajax/pagele?query=%5Cajax https://www.facebook.com/ajax/pagele?query=%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.	404 NotFound % 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound 404 NotFound % 200 OK 404 NotFound % 200 OK 404 NotFound 404 NotFound 404 NotFound 404 NotFound	95 ms 95 ms 96 ms 96 ms 500 ms 500 ms 105 ms 106 ms 734 ms 734 ms 79 ms 90 ms 111 ms 81 ms	1,172 bytes 1,380 bytes 996 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,172 bytes 1,173 bytes 996 bytes 1,173 bytes 996 bytes 1,173 bytes 996 bytes 1,172 bytes	579,562 bytes 579,562 bytes 580,498 bytes 588,262 bytes 579,694 bytes 588,443 bytes 0 bytes 580,176 bytes 0 bytes 72 bytes 579,800 bytes 72 bytes		

- Using a free tool provided by OWASP called "Zap"
- Finds / crawls all URLs and calls being used by application during each step of a process
- Look for exposed information including cookies, tokens, login credentials, infrastructure info, etc.

High Level Security Lifecycle



٠

- Corporate Owners
- CISO, Compliance Officer, **General Counsel**
- Security Architecture
- SOC

- Emulate attacker/black hat • reconnaissance scanning and pen • testing
 - Monitor the darknet for chatter about attacks, data dumps
- Monitor and log for anomalous behavior Constant vulnerability testing using latest signatures
- Security test/code review new releases, • regression test existing software/code services/web/data stores/ apps/containers
- Harden devices/services
- Constant training/updating

- Periodic live testing of IR plan
- Security Posture Assessments
- Red Team/ Blue Team exercises
- Third party audits, internal audits
- Third party testing via bug bounty

Securing Databases

- Generally, two types of databases Structured and Unstructured (No-SQL)
 - No-SQL does not contain default audit trails and built-in security
 - Encrypting storage may cause unacceptable latency, but an organization can encrypt tiers based upon last access date, age of data, and other qualifiers
- Best practice No-SQL is a combination of the following:
 - Strong multi-factor authentication and authorization
 - Strong perimeter network and isolation
 - Change default ports
 - Segmentation of access rights (gateways)
 - Time-based access controls
 - Disallow concurrent access
 - Input and extract validation
 - Audit or log all plugin access (trusted and untrusted), server logs, and control access to logs
 - Replication and data segmentation, key structures
 - Strong encryption where possible

Securing Web Apps

- OWASP (Open Web Application Security Project)
 - Globally recognized non-profit for cloud security best practices and standards
 - Industry standard:
 - Test for the Top 10 Security Risks for Cloud based applications
 - Open source vulnerability scanning software
 - Security software assurance maturity model
 - Open source tools and resources testing tools, best practice code
 - Accepted as the standard for web-based applications for most organizations
- OWASP critical threats and penetration testing methods
 - Cross Site Scripting (XSS)
 - Enables attackers to inject client-side scripts, bypass access controls such as the same-origin policy, steal visible tokens and cookies
 - Cross Site Request Forgery (XSRF)
 - Broken Access Control

Authentication, Access Tokens, and Hacking Tokens

• Matt Strebe

- Over 29 years of experience in the field of cyber security, database design and security, secure network protocols, and cryptography
- CEO of Connetic IT Services & CeNRG cloud hosting
- Has served as an expert witness in several data breach cases
- Author of numerous books and publications, including Network Security Foundations & Firewalls 24x7
- Inventor, "No Transfer" (NOTX) patented device authentication protocol
- CV provided for the Court and counsel

Authentication

- Logging in
 - Access to Private Resources
 - Access Control Lists
- Sessions and Web Sessions
 - Website simultaneous access to multiple resources in a distributed web application
 - Authentication and Authorization are different matters
 - Here, it appears authentication is the issue, not encryption
 - Large scale web applications typically use access tokens to solve distributed access control issues

Access Tokens

- Access Token
 - An access token is an object encapsulating the security identity of a process such as a web session. A token is used to make security decisions and to store tamper-proof information about some system entity. An access token is generated by by the logon service when a user logs on to the system
 - Bearer instrument example: court access keycards
 - Can contain anything the developer wants
 - Access Token could be limited to a single purpose (master key v. bathroom key)
- Types of Tokens
 - User Access Token (short-term, long-term)
 - App Access Token
 - Refresh Token
- For Facebook
 - Here, it appears the token Facebook associated with the "View As" function gave the hacker the same access as the original user (e.g., keycard)

How Tokens are Transacted and Used

- Token portability (and theftability)
 - They are protected
 - On Web servers by encryption at rest
 - In transit over the Internet by encryption in flight
 - On Web browsers by encryption at rest
 - They are not necessarily protected in the running web browser
- Developers must be careful when sending Access Tokens to the web browser client, such that it applies only to that user
 - For developer, a conscious trade-off between security and ease-of-use
 - Expedited access requires constant vigilance upon implementation
 - Access token should never be exposed to any other users in a running browser

Gafari File Edit	View History Bookmarks	Develop Window Help	U.S. \	Wed Dec 5 11:09	Q Matthew Strebe ⋮Ξ
		Open Page With User Agent	•		1 1
	Facebook I		•	ew posts	>>> +
f Search		Service Workers	•	me Create 💄	* 🕗 🔔 🚱 👻
	✓ Make Post	Experimental Features	►	Stories	(i) Archive . Settings
E Nows Food		Enter Responsive Design Mode	^	otories	Archive Voctaligs
Messenger	What's on your mind,	Show Snippet Editor Show Extension Builder			
⊵ Watch 🔹		Show Web Inspector	۲%۱		
m Marketplace	watch Party	Show JavaScript Console	C ℃ ℃		
Shortcuts		Show Page Source Show Page Resources	て第0 て第A		
		Start Timeline Recording Start Element Selection	T第①了 公第C		
		Empty Caches	Σ₩E		
▼ See More		Disable Images Disable Styles		See More	
Explore		Disable JavaScript			
5 Events 1		Disable Extensions		15 1 event invite	
Sroups		Disable Local File Restrictions			
Pages		Disable Cross-Origin Restrictions			
Memories 5		WebRTC	►		000
▼ See More		Allow JavaScript from Smart Searc	h Field		
2019 – Plaintiffs' Tutorial in 3:1	8-cv-05982-WHA (and all related ca	ses) 🗸			17

🔹 🗯 Sá	Ifari File Edit View History Bookmarks Develop Window Help		U.S. Wed Dec 5	11:08	QN	Aatthew Str	ebe ≔		
	Web Inspector — www.facebook.c	com							
	□	① 0 ▲ 0 ♀ Q~ Search							
뮴 Eler	nents 🕀 Network 🛱 Debugger 🗋 Resources 🕘 Timelines		Storage 🖾 Canvas 🔀) Console	도 Console + 63		
$\square \langle \rangle$	🚳 Cookies						CI		
Name 🗸	Value		Expires	Size	HTTP	Secure	Same		
xs	24%3AQMA9VyWXRhS1UA%3A2%3A1543440092%3A19988%3A2301	1	3/5/2019, 11:01:00 AM	53 B	~	~			
wd	1024x554	1	12/12/2018, 11:01:0	10 B		~			
spin	r.4601297_b.trunk_t.1544025657_s.1_v.2_	1	12/6/2018, 12:00:57	43 B	~	~			
sb	zQb_WzE1YQkpe362ekEO0Gmu	1	11/27/2020, 4:21:32	26 B	\checkmark	~			
presence	$EDvF3EtimeF1544025830 E userFA2507990199A2 E stateFDutF1544025830269 C E chFDp_5f507$	1	Session	96 B		~			
pl	n	1	2/26/2019, 4:21:32 PM	3 B	~	~			
fr	1atWP5pO0QRZj6zXn.AWUt4VWZu3XOS8RAfM6FzGsOmg4.Bb_wbN.0i.FwF.0.0.BcB_Y8.AWUi3LbI	1	3/5/2019, 11:01:00 AM	81 B	~	~			
dpr	2	1	12/12/2018, 11:03:5	4 B		~			
datr	zQb_Wwps8M_MoGNQdtPaXbw2	1	11/27/2020, 4:21:19	28 B	~	~			
c_user	507990199	1	3/5/2019, 11:01:00 AM	15 B		~			
2019 -	Plaintiffs' Tutorial in 3:18-cv-05982-WHA (and all related cases)						1		

<u>OAuth 2.0</u>

- OAuth 2.0 is an authorization protocol frequently used as an easier authentication protocol
 - Used by companies like Facebook
 - The access token supplants other authentication steps
 - Allows third-party marketers some benefits
 - For example: simple user experience to prevent "usage walls" and encourage adoption
 - Adoption of OAuth 2.0

OAuth 2.0 – Vulnerabilities

- But OAuth 2.0 presents a greater risk of the "bearer instrument" being misused
 - You don't have to decrypt or comprehend an Access Token to use it
 - When you find someone else's Access Token in a web session, you have whatever level of access that token permits within its expiration
 - Ease of coding, code re-use, complex application design, and lack of testing lead to mistakes and increased risks to users' PII

How Tokens Can Be Exploited

- Hackers determine that they can exploit a website to obtain another user's Access Token
- Hackers access the website as each user, access PII, then identify and steal other available Access Tokens
- And Repeat. Very quickly, hacker can obtain many millions of accounts' Access Tokens with automated scripts ("crawling")
- PII is taken and in possession of hackers and misused and/or sold

Preliminary Questions

- 1. How was the "View As" token developed, security and functionality tested, prior to release?
 - a) What process did Facebook use to test the "View As" feature prior to release?
 - b) Where else was/is the token used?
 - c) What Security Development (i.e. Secure SDLC) processes does Facebook use to test their software prior to release?
- 2. When did Facebook first detect the issue, and how?
- 3. When did Facebook identify the root cause of the issue, and how?
- 4. Any report done by Facebook or third-party?
- 5. How did Facebook determine the affected entities?
- 6. What steps did Facebook take to contain and remediate the issue?