## **Privacy pitfalls for your** web application



#### Agenda

- Introduction
- Information leakage
  - Hashed email (Gravatar)
  - Third party profile integration (Facebook Login)
  - Metadata in documents (Image, Keybase)
  - Search features (SonarSource, WordPress)
  - GraphQL / REST data binding
  - Side-channel attacks (Outlook, GMail)
- Conclusion

#### What is OSINT?

#### **Open-Source Intelligence**

"Collection and analysis of data gathered from open sources to produce actionable intelligence"

In this context, it is unrelated to Open-Source

Open-source refer to online publications, discussion groups and social media.

Your web application could become an "open-source".

#### Information asymmetry

- Lots of documentation for attackers
  - Techniques
  - Tools
  - Shared leaks
- No clear documentation for application developers for defence

F Doxing	Tutorials   RaidForums × +			∨ – □ X
$\rightarrow$	C 🏠 🗎 https:// <b>raidforums.com</b> /Forum-Doxing-Tutorials			🖈 💼 Incognito (2) 🚦
ه	How To Dox Anyone - IP / Phone Number Dox Method (Pages: 1 2 3 4 158 ) by  Vnti ③ December 20, 2019 at 04:46 AM	1,892	120,719	26 minutes ago Last Post: stormblessed13
ې	GUIDE TO DOX ANY YOUTUBER IN THE WORLD (Pages: 1 2 3 4 23 ) by mahadev () February 28, 2021 at 04:49 AM	270	27,464	31 minutes ago Last Post: martinmatte
ه	"P1" BEST DOXING TUTORIAL GET (FULL NAME, ADDRESS, EMAIL, PHONE NUMBER,) (Pages: 1 2 3 4 167) by azbe ③ September 20, 2019 at 05:10 PM	1,995	137,151	32 minutes ago Last Post: stormblessed13
ه	→ Best Dork Collection → (Pages: 1 2 3 4 22) by tronsec007 ③ September 27, 2021 at 08:57 AM	254	19,078	2 hours ago Last Post: terracottaboy
ه	Data breach tools + downloads (4 tools, 400+ breaches) (Pages: 1 2 3 4 71 ) by j4kx ③ April 04, 2021 at 04:35 AM	847	68,305	2 hours ago Last Post: mustark
ه	DOXING WITH JUST AN EMAIL (Pages: 1 2 3 4 90 ) by ☆ Vnti ③ March 21, 2020 at 12:30 AM	1,073	77,970	3 hours ago Last Post: vvared
ه	DOXING and ANONYMITY EBOOK PDF(s) FILE (Pages: 1 2 3 4 20 ) by <b>* iLoveNutella</b> ③ April 06, 2021 at 09:27 AM	233	26,587	3 hours ago Last Post: vvared
ى	DOXING DORK LIST (Pages: 1 2 3 4 13)	145	14,408	4 hours ago Last Post: Benjx

#### Leaks and emails

In this presentation, most of metadata leakage are going to either:

 Disclose emails, name, organization, physical address, social network connection

#### Why email privacy is important?

- The reality of password leaks
- Account correlation
- Privacy law:
  - GDPR (EU)
  - CCPA (California)
  - Loi sur la Protection des Renseignements Peronnels (Québec) \*



Source:

\* Coming soon: https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1

### **Gravatar URLs**

#### Gravatar

Gravatar is a service for providing globally unique avatars.



## 14 Comments Example of Gravatar integration

Thanks for info. I was wondering how I can buy some plugins that have been bugging mw such as wp bakery

★ Liked by <u>2 people</u>

#### Tex Feb 1st at 9:52 am

This is all great features. Has made my turned all of my websites into native apps. I love it. I won't have to pay dev fees to publish on Ios or Droid. Connecting my site to jetpack was a great experience for me. Thanks again for making development more easy.

★ Liked by <u>2 people</u>

Tony Feb 2nd at 4:20 pm

I feel it would be useful if all paid plans had access to at least some free or paid plug-ins

★ Liked by <u>4 people</u>

#### **Gravatar URLs**

MD5("**philippe@confoo.ca**") => 06b856f7ee1266fbf86eaa018f5b0906

https://secure.gravatar.com/avatar/

06b856f7ee1266fbf86eaa018f5b0906?s=96&d=identicon&r=G

- 06b856f7ee1266fbf86eaa018f5b0906 : email hash
- s=96 : image size
- d=identicon : default image if profile is not found
- r=G : Rating (May contains profanity, violence, nudity or drugs)

### Sites using Gravatar

#### • WordPress blogs

Organization	Number of Users	Alexa Rank
newsfeed.time.com	186	1524th
vimeo.com/blog	177	170th
blog.ted.com	120	1291st
blog.etsy.com	2570	76th
techcrunch.com	57	1754th
wired.com	1052	1525th
devblogs.microsoft.com	1000+	21st
gblogs.cisco.com	123	824th
godaddy.com/garage	1430	172nd
books.disney.com	14	4436th

- StackOverflow
- SuperUser
- AskUbuntu
- Gitlab
- Bitbucket
- SonarSource

#### **Wordpress Users**

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u>	tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp — _ X							
wordpress.httpwn.com/wp-json/wp × +								
↔ ∀ ⊕	🛈 wordpress.httpwn.com/wp-json/wp/v2/users 💟 🏠 🛞 🗊 🐚 🖆							
JSON Raw Data	JSON Raw Data Headers							
Save Copy	♥ Filter JSON							
∞0:								
id:	1							
name:	"superadmin"							
url:								
description:								
link:	"http://wordpress.httpwn.com/author/superadmin/"							
slug:	"superadmin"							
▼avatar_urls:								
₹24:	"http://0.gravatar.com/avatar/6e2b22791df03c1290687b2807f52afd?s=24&d=mm&r=g"							
₹48:	"http://0.gravatar.com/avatar/6e2b22791df03c1290687b2807f52afd?s=48&d=mm&r=g"							
<b>▼</b> 96:	"http://0.gravatar.com/avatar/6e2b22791df03c1290687b2807f52afd?s=96&d=mm&r=g"							
meta:								
<pre>Turks:</pre>								
▼self:								
∞0:								
href:	"http://wordpress.httpwn.com/wp-json/wp/v2/users/1"							
▼ collection:								
∞0:								
href:	"http://wordpress.httpwn.com/wp-ison/wp/v2/users"							

#### The risk

- When an URL is exposed, you should considered that the hash email can be reversed. 60%+ of all registered account were
- The risk need to be evaluated based on the information attached to the users.
  - Is the user anonymity important?
  - Could the metadata affect the user elsewhere?
  - IP / Geolocation : Located individual, Targeted Phishing
  - Company name : Target attack to employee of a specific company
  - Phone number, email: Building clients list (spam list)

More info : https://www.gosecure.net/blog/2021/03/02/emails-disclosure-on-wordpress/

#### **Credential Stuffing**

An adversary tries known username/password combinations against different systems, applications, or services to gain additional authenticated access.



#### Recommendations

- Avoid using Gravatar if user anonymity is important
  - If the avatar are not shown publicly, the risk is much lower.
- Download the image server-side rather than pointing to Gravatar service
- Implement/Integrate a second factor for authentication

## **Login with Facebook**

(Also applies to other SSO)

#### Login with Facebook & Graph API

When integrating Login with Facebook feature, it is possible to obtain the email, the full name and a profile image.

The profile image comes in the form an URL.

https://graph.facebook.com/XYZ/picture https://graph.facebook.com/XYZ/picture?height=256&width=256



# Can image be linked back to a Facebook profile? (1/4)



# Can image be linked back to a Facebook profile? (2/4)

G Facebook × +

			← → C ☆ 🔒 https://www.faceb	https://www.facebook.com/					Ŕ	lê ☆ ■				
			Q Search Facebook		60	<b>₽</b> ₽₽	<b>1</b>	G	Philippe					
			1					5		-				
	onsole Elements	Recorder 👗	Sources Network	Performance	Memory	y Appl	ication	Security	Ligł	nthouse				
		▼ <div d<="" td=""><td>lass="q9uorilb 19j0dł</td><td>ne7 pzggbiyp</td><td>du4w351b</td><td>"&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></div>	lass="q9uorilb 19j0dł	ne7 pzggbiyp	du4w351b	">								
		▼ <svg< td=""><td>g aria-label="</td><td>class=</td><td>"pzggbiyp</td><td>" data-v:</td><td>isualcom</td><td>pletion=</td><td>="ignore</td><td>-dynamic" ı</td><td>role="img"</td><td>style="heig</td><td>nt: 168px;</td><td>width: 1</td></svg<>	g aria-label="	class=	"pzggbiyp	" data-v:	isualcom	pletion=	="ignore	-dynamic" ı	role="img"	style="heig	nt: 168px;	width: 1
		">												
		► <m< td=""><td>ask id="jsc_c_p"&gt;</td></m<> <td>ask&gt;</td> <td></td>	ask id="jsc_c_p">	ask>										
		▼ <g< td=""><td>mask="url(#jsc_c_p)"</td><td>&gt;</td><td></td><td></td><td></td><td>nant i n</td><td></td><td></td><td></td><td></td><td></td><td></td></g<>	mask="url(#jsc_c_p)"	>				nant i n						
***			<1mage x="0" y="0" he	1ght="100%" ~200/236326/	preserve# 48_vvz1_1	AspectRat	10="XM1	dYM1d SI wCecAd0n	lice" wid	1th="100%"  foEbsM20+1	xlink:href	=" <u>https://so</u> w010&ce=623/	Adea = +v1	<u>-"heigh</u>
			<pre>px: width: 168px:"&gt;</pre> //p200 px: width: 168px:">//p200	image> == \$0	<u>+oyyz1-1.</u> 0	. XX&011-08	7 AT 250	WCECAUON	INTESCIC	<u>TPENSH20U1</u>		<u>yeroaue-6234</u>	<u>044F9</u> Styl	v v
			<circle 84'<="" class="mlgo0d&lt;/td&gt;&lt;td&gt;h0 georvekb&lt;/td&gt;&lt;td&gt;s6kb5r3f'&lt;/td&gt;&lt;td&gt;' cx=" td=""><td>' cv="84</td><td>" r="84"</td><td><pre>&gt;</pre></td><td>le&gt;</td><td></td><td></td><td></td><td>3</td></circle>	' cv="84	" r="84"	<pre>&gt;</pre>	le>				3			
		</td <td>g&gt;</td> <td>Ŭ</td> <td></td> <td></td> <td>-</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	g>	Ŭ			-							
		<td>/g&gt;</td> <td></td>	/g>											
		<div< td=""><td>/ <mark>class="i09qt</mark>zwb n7fi</td><td>ilqx3 b5wmif</td><td>dl hzruof</td><td>5a pmk7j</td><td>nqg j9is</td><td>spegn kr5</td><td>520xx4 c</td><td>5ndavph art</td><td>tlomkt ot9</td><td>fgl3s rnr61a</td><td>n3 s45kf17</td><td>9 emlxlay</td></div<>	/ <mark>class="i09qt</mark> zwb n7fi	ilqx3 b5wmif	dl hzruof	5a pmk7j	nqg j9is	spegn kr5	520xx4 c	5ndavph art	tlomkt ot9	fgl3s rnr61a	n3 s45kf17	9 emlxlay
		p75v	v spb7xbtv" data-visua	lcompletion	="ignore"	>								
		<td>&gt;</td> <td></td>	>											
			lla Cault Zanu Juliana a 23 - du		والمركز مراجع والمحاصر	1								
		<ul> <li><ul> <li><ul></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul>	"prnynomw wkznzczi dy "i83agy80 psu0ly52 mp	cxazoy niyri mpiglə əbl60	nctz∵×/di Swa£ tma14	LV> 1saa ruv3	los d av	16+0/0 6	icfkmk3	dtiQuQuA r	vziof1z"\	(div) Flow		
		<pre>&gt; <div class="&lt;/pre"></div></pre>	"aublyx3c ew1m30ut dw	xdBoue cyml	bt9a izvtu	17xg eiaS	Sua2n dk	w9rofs d	1+19v0u4	t9ro7vwc n	vziof1z h	74gav3"> <td>tive</td> <td></td>	tive	
			qubitise cuimbout un	Auguate Tymzi	5056 12000	ind cloc	auzir ak	101013 U		corproduce in	y210/12 //.	// - Bd) 5 /	1107	

# Can image be linked back to a Facebook profile? (3/4)

- Both URL will return the same picture byte for byte
  - Public profile : http://scontent-yyz1-1.xx.fbcdn.net/v/...
  - Graph API (FB Login): https://graph.facebook.com/XYZ/picture



# Can image be linked back to a Facebook profile? (3/4)

In order to correlate the profile picture from the Facebook Graph API to the one from public profile, the attacker needs to **crawl multiples profiles** and keep either a signature from the image or the FBMD code from the image.



#### Metadata in documents

#### Example #1: Metadata in Image

Potential information

- Geolocation
- Image path
- Software version



#### Example #2: Keybase

		為 https://keybase.io/_/api/1.0/user/ 🗙	+	~	-		×
		← → C ☆ 🔒 https://keybase	e.io/_/api/1.0/user/lookup.json?usernam 년	2 \$		* 🌒	:
<ul> <li>kroyhunt (Troy Hunt)   Keybase × +</li> <li>← → C △ ● https://keybase.io/troyhunt</li> <li>Search Keybase</li> </ul>		<pre>{"status":{"code":0,"name":"OK"},"th {"username":"troyhunt","ctime":14538 ast_id_change":1642059595,"username_ d57eb7a","eldest_seqno":1},"profile" Hunt","location":"Australia","bio":" buttlope</pre>	<pre>iem":[{"id":"5b1e99759dd653ea52eb577310f i12159,"mtime":1565618750,"id_version":5 cased":"troyhunt","status":0,"salt":"fa ':{"mtime":null,"full_name":"Troy 'Pluralsight author. Microsoft Regional , ccennolog, and the cloud cerestor of</pre>	59019"," 55,"trac c9ffbe47 Director	basics k_vers 3c2ef5	": ion":7, 830a295⁄ №P for	"1 e6
<image/> Image: Arrow of the constraint	<ul> <li>5 devices</li> <li>troyhunt tweet</li> <li>troyhunt gist</li> <li>troyhunt post</li> <li>troyhunt profile</li> <li>havelbeenpwned.com</li> <li>asafaweb.com thtps</li> <li>troyhunt.com dns</li> <li>troyhunt*keybase.io</li> <li>121CEyDDEewZfp7mpFLc</li> </ul>	<pre>Pwned."},"public_keys":{"all_bundles OpenPGP v2.0.49\nComment: https://keybase.io/crypto\n\nxsFNBFa DXWUzFwf2nT9JMEkmqY3du+P73j2kWzWYaCt theairdC3/isqqicQBJpBP3/t38xb\n89rhB JeAclSaz2W5wC3Cj2lAPmb5vpIROgbLCHQ6Q +7efRH6xVBmluf4x+FDR0NIhlcfCI7t\nHzJ n6RSwxCZ7FXGUMP5kKfyutkCsBv+HWbV+eKb C449mV9prIHRXJ10gqtPeIvw3DcoPQ9d2\n7 E\ntJn/ORKqW3kwgOLVoA+UEQRx7HeJz0Q5a GhvdG1haWwuY29tPsLBdAQTAQoAHgUCVqdq\ H73\nrFTeviGB07gUegUdbfWnvCMpa9X7HHK +Runh1KCirpihoPY8g5+U4114551TL7 +CBhh\ns86bkKq2XBU5gt xTX q22 mVKA t/fwjwCtt3fyZsteQ0sj+ Nw2 ww37th/ A8TtHfS\n217h/rzH0Q5n ravLtmLtn67N HY1MGJ+fqCcB27uQbpDc+ H8Trt01 2004 eu8HvhqEU\n92+CVP8r19BQ1v20CZSV9x61G 4rmkCLj7uuE4s7ATQRWp2okAQgAw9/F4xYA0 F6xv1Vfw33p\nzGy3fi1zqUXyKAQsN/PAyuX rkt1Q/3LYkS0kkhlvcAKRdolUE+UTWaoC/mk Ve0xJ5Rg/PBNS\nWKk8iSqyOI9hvU0saAEmj BgBCgAPBQJWp2okBQkPCZwAAhsMASkJEAHjT 1NmYdpzZeI1SNZI\nJwSUly+44PeuCnz5Yzf I1zGF/Of0vY+TroD+TSIHK1qjnTbw9NrNte6 d5onrSwLGRHj4tJy9\nbzz5f5CIibhrM3nRW 7eKeZ++vkqMaUAomhi8r3s3LDuU6TdhbBufk L7z7/PnPRgL4nUjPExi\no7H5C7783RT4mB0 02120vixFpFjjHvCNJ0rUXGIIGgGbWonwVQi</pre>	<pre>;":["BEGIN PGP PUBLIC KEY BLOCK inaiQBEAD5V+EOGjsDogCyso9LK90jioLoHZJCdY: :bSE0VNq00HnnVf06j71ZLdazG\nFIDJY0Xr0iuZ: Dy4WNqrB0X/46C0evsRpdV2xw+uh5vQdHHZxP6J/ )Fd2nedCiFtD3/N1RuPzNMxm58MY\nj6mih5JqbT: IddPS+NrCK2JAj2MYI5Wv2ZnQkqe6faJF5ejj6Bd: &gt;tLhbZFXda0t9vqBMqVJpv5cBEQVZK\n34WdBYoar /LH+FIV+zqU+/08r4oanklbCBSjX77148HnmBAOy /ufjjPuUFbtJ/RhW9SABDLcBQARAQAB\nzSBUcm nJAIbAwMLCQcDFQoIAh4BAheAAxYCAQIZAQAKCR/ QCyJmvBGHIoGGQ99r4AS4tvX15qyccH7x\nSYSb Nov64045RkhVdg40.sxd12lax/dmaoj42713k 4635E MxnupJnsc\nKvcdnASIS24wyiCp\n+p (MF\ tVS0 8izszrn40gvA7 62265+00g) Zeu HroHLNHA6y 000 av20.cmvc37 62 200 neK/4QyGKUL0/NG042X242.cmvc37 62 22 wneK/4QyGKUL0/NG042X242.cmvc37 62 22 wneK/4QyGKUL0/NG042X242.cmvc37 62 23 wneK/4QyGKUL0/NG042X242.cmvc37 62 24 wneK/4QyGKUL0/NG042X242.cmvc37 62 24 wneK/4QyGKUL0/NG042X242.cmvc37 62 24 wneK/4QyGKUL0/NG042X242.cmvc37 62 25 wnz/v11xRbf8nq/Twm6qf1xRZINEM2PLeW be DaeaK+QK\nkky8RWHRwzyQXfsi/wpb/HJ9T14qs (887rgcBzQjTB5IWXmjudZNyZAEEcmS3btuhYiJ+ cZkLnLyWYO\nr9D21rv2aeBJGqjtINHf3o3Lm/1m jILGeXSCyIB4ewYhMJgdIrYTyZdQsvzfEqVFX26 IZPmnZvawF0g\nBBkBCgAGBQJWp2okAAoJEOkP1+ fyI64VGK5zZqwOjnNdzqa4xSw9pdqmh9WxpJE24S 5JZb0gwtNGOcaV\n5NQWDQxgSsOVOszUKDuN6Jzz, vbny0DOAkpPGnEY5bLodZSBF9X11UodkEmgOuuTA kr0bnzs8crMYQg/\nbPRj9M+SZ581KUKBLubhXX 0Hcd0W8CLt2WJ0PesGRT6Ko+/CaUmzKquR3ojf5A iWZDvJLIMbNTSYd47i\nNB1b7ToLUdWUPGKMyGjc</pre>	<pre>\nVersi itVqAY21 idHSwr1L \54QotJZ L1GXaDP6 ZuFdr+xq JV2ewxFZ 3ewTRBV JSIEh1bn \B402T5p vJMUxK/H Js4aE0E0 rdYL2UFS Jsb2LDuC LNFDZHOd 5+VsVU6f (njvY1V3 Fguq6CYw E0\nSUsz jUQGXW8a /hby\nk5 zpn/wQCp 75GmrH\n yh03Mgu+ w1YE17iI J/NTabRK Djwv4K+e fEPNFKSt</pre>	on: Ke zyfnw7 ØbkJtB sAPqAL OyEMgH h3dTCh vXYfpc xqjtW1 QgPHRy 2b2uSE qEdWNh t2MPkf z5rIPv rGZQxi Kecqsy FMsvHg pgmcAr N9Yloi u8Lv+p XLgba+ AfWwAR MIAIgg U9TrlU 4XhLGi \npCbC 05j/Et	ybase TuRT\n8 IM3c62il CG04+d\r c1Q/011 EQXQ4kql KyDS+vg vAiqIQD b3lodW5 EADr1Bx 5Sd5VTo 3h7DwUil d9B+k4vl yEFX6vZ b+F3ysA aJre1Bs wiRr6bt QrkJfkel e0312N8 RmHW53n AQABwsK 5CeVMbb Ms5Gdof J6jJ17J 8kSmqw8 Qt71pj8 lbe0HiMW ItYUu9w	pn kN nD rM E US 20 0 5K rt De k 15 fX LH XY D/ VQ EB Fd 7 7 I 5 5 F 1 uS 2 1 0 0 5K rt De k 15 fX LH XY D/ VQ 5 2 0 1 2 1 0 2 5 1 2 1 2 1 2 0 2 5 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2

KGtSeGxIRs3ATLvzCaD0T\nC/g/vwuqqqSnLoHxg7dV650Knuc70JuevbhEUSuJnvE7unU+quUhgjqcVhakvsKA\nRl79uadYY eleYKnuYfs9LVS4647+0l0iLKGU0mBWqCKbzng9iS/8qnsJgeXkacXM\ngxh+gsBhy4Ni60qShGBUsHqPlHna7eIIE07PfVXXH

#### Example #2: Keybase

PGP Key include:

- Header metadata (Versions + Comment)
- Key information
  - Algorithm
  - Issuer
  - Key value
  - ...
- User ID (Usually the user email)

Command Prompt
$C: \sum_{n \in \mathbb{N}} c_n = c_n c_n + c_n $
and: apmon: REGIN DOD DURITO VEV RIOCK
gpg, annor, beaden: Vension: Keybase OpenDGD v2 0 40
gpg. armon headen: Comment: https://keybase jo/crypto
gpg. almoi header. comment. https://keybase.io/clypto
nuhlic key nacket:
version 4 algo 1 created 1453812260 expires 0
nkev[0]: [4096 hits]
pkey[1]: [17 hits]
kevid: 01F34D93F69D9BDA
# off=528 ctb=cd_tag=13 hlen=2 nlen=32 new_cth
:user ID packet: "Troy Hunt <troyhunt@hotmail.com>"</troyhunt@hotmail.com>
# off=562 ctb=c2 tag=2 hlen=3 plen=304 new-ctb
signature packet: algo 1, keyid 01E34D93E69D9BDA:
version 4, created 1453812260, md5len 0, sigclass 0x13
digest algo 10, begin of digest e4 84
hashed subpkt 2 len 4 (sig created 2016-01-26)
hashed subpkt 27 len 1 (key flags: 03)
hashed subpkt 11 len 2 (pref-sym-algos: 9 7)
hashed subpkt 21 len 2 (pref-hash-algos: 10 8)
hashed subpkt 30 len 1 (features: 01)
hashed subpkt 23 len 1 (keyserver preferences: 80)
hashed subpkt 22 len 2 (pref-zip-algos: 2 1)
hashed subpkt 25 len 1 (primary user ID)
subpkt 16 len 8 (issuer key ID 01E34D93E69D9BDA)

#### Recommendations

- Identify documents or files that are likely to contain metadata
- Strip metadata from images upon upload
  - Unless your service is a cloud hosting provider

### **Search features**

#### **Search features**

Private information **might not be shown** on your application but, could **be queried** through search features.



#### Example #1 SonarQube / SonarCloud

#### % GET api/users/search since 3.6



Get a list of active users.

The following fields are only returned when user has Administer System permission or for logged-in in user :

- 'email'
- 'externalIdentity'
- 'externalProvider'
- 'groups'
- 'lastConnectionDate'
- 'tokensCount'

	sonarcloud.io/api/users/search?q=p × +								
$\leftarrow$	$\rightarrow$	С	6		E	htt	tps:// <b>sonarcloud</b>	d.io/api/users/searc	l ?q=philippe.arteau@gmail.com
JSON	Rav	v Data	He	aders					
Save	Сору	Collap	se All	Expand All	🗑 Filter	JSON			
💌 pagi	ing:								
р	ageInd	ex:	1						
р	ageSiz	e:	50						
t	otal:		1						
vusers:									
▼ 0:									
	logi	n:	"h3xs	tream@githu	b"				
	name	:	"Phil	ippe Arteau					

#### Example #2 : WordPress users endpoint





### **REST Data binding**

@Entity
public class UserEntity {

@Id
private Long id;
private String username;
private String fullName;
private String address;
private String ip;

@Controller
public class UsersController {

}

[...]

@RequestMapping("/users")
public UserEntity getU(@RequestParam("id") String id) {
 return ...

[...]



More info: https://graphql.org/learn/introspection/

#### GraphQL

```
GraphiQL
                        Prettify
                                   Merge
                History
1 v query{
                                    "data": {
 2
     persons {
 З
                                       "persons": [
     name,
4
      address
                                          \leftrightarrow },
 5
 6
                                           "name": "Josh",
 7
                                           "address": "1878 Smith Road"
                                         },
                                           "name": "Simon",
                                           "address": "402 Mesa Drive"
                                         j,
                                           "name": "Audun",
                                           "address": "2867 Rivendell Drive"
                                         3,
                                           "name": "Truls",
                                           "address": "4765 Star Trek Drive"
                                         },
                                           "name": "Maria",
                                           "address": "284 White Avenue"
                                         },
```

#### Recommendations

- Avoid binding of persistence class directly to endpoints
  - Prefer separate data class
- Audit public classes for unexpected private or sensitive information
  - Address, IP, password, third-party account disclosure (FB, Google, Github), ...
- Look for search API that could be queried with private information
- Reconsider complete users enumeration as REST/GraphQL endpoint?

#### **Side-channel attacks**

#### **Side-channel attacks**

- A side-channel attack is any attack based on **information gained from the implementation**.
- Another channel can provide an extra source of information.
- Channel usually refer to
  - Timing information
  - Power consumption
  - Electromagnetic leaks
  - Sound
- Here I'll be referring to different systems or protocols.

#### « Side-channel » leaks

Get information on specific user using a private PII.

The attacker will succeed by **sending a user identifier** and **receiving details on another channel** about this user.



#### Example #1: Web Mail Client

1. The attacker imports spoofed emails through either SMTP. (Some provider allow pull from external mailbox in POP3 or IMAP)

2. The attacker view the crafted email through the web interface to see if the identify were enriched with additional information. (Full name, organisation, ...)



#### Example #1: Web Mail Client (Outlook)

К	kmitnick@mitnicksecurity.com	$ \rightarrow $ $ \cdots $
	K kmitnick@mitnickse	Kevin Mitnick 2nd
PA	Send email 🖵 🛄 … View LinkedIn profile for kmitnick@mitnicksecurity.	The World's Most Famous Hacker   CEO   Author   Professional Speak           Henderson, Nevada • 500+ connections
	Contact >	
	kmitnick@mitnicksecurity.com	Overview Contact Email Files LinkedIn
	Show more	Highlights
	in LinkedIn >	26 mutual connections You and Kevin Mitnick both know Tanya Janca, Madhu Akula, and 24 others
	26 mutual connections	
	Experience	Experience
	CEO and Chief 'White Hat' Hacker Mitnick Security Consulting	CEO and Chief 'White Hat' Hacker Mitnick Security Consulting Jan 2003 – Present
	Show LinkedIn profile	Worldwide

#### **Example #2: Git repository**

1. The attacker imports commit with spoof emails.

2. The attacker view the commits through the web interface to see if the identify were enriched with additional information. (username, full name, organisation)



### Conclusion

#### Recommendations

On your next threat modelling...

- Identify API that could **return** sensitive information.
- Identify API that could be **queried** with sensitive information
- Identify third party integrations (ie: Facebook Login, Google Account, Gravatar, etc.)
- See if the risks matter for your application and context

In your code...

• Avoid security by obscurity (base64, unsalted hash)

#### **Forewarned is forearmed**

Users that are aware of those leakage are more likely to take precautions.

Examples:

- Knowing that your FB account will be linked to multiple websites, avoid publishing sentive information such as your address, affiliations or even full name.
- Create separate account to avoid identity correlation. (Creating multiples Gravatar/Github/Bitbucket account rather than one.)



## **Questions?**

- parteau@gosecure.ca
- @GoSecure\_Inc
- @h3xStream

https://www.gosecure.net/blog

### References

#### Blogs/tools on similar topics

- Gravatar risk assessment on Wordpress.com/Gravatar.com
  - <u>https://blog.h3xstream.com/2021/03/emails-disclosure-on-wordpress.html</u>
- Hardening tests for Wordpress related to Gravatar
  - <u>https://blog.h3xstream.com/2021/03/6-ways-to-enumerate-wordpress-users.html</u>
- LinkedIn deanonymization example
  - <a href="https://blog.h3xstream.com/2021/04/deanonymizing-linkedin-users.html">https://blog.h3xstream.com/2021/04/deanonymizing-linkedin-users.html</a>
- Ghunt: Google account investigation tool
  - <u>https://github.com/mxrch/GHunt</u>

#### Privacy acts around the world

- GDPR (EU)
  - <u>https://gdpr-info.eu/art-5-gdpr/</u>
- CCPA (California)
  - <u>https://oag.ca.gov/privacy/ccpa</u>
- Loi sur la Protection des Renseignements Peronnels (Québec)
  - <u>https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1</u>