RANDORISEC

HACK-IT-N / 2019-12-10

RESTRICTED / TLP:WHITE

OWASP MOBILE SECURITY TESTING GUIDE

UN MOT SUR VOTRE SERVITEUR

- Davy Douhine (@ddouhine)
- Consultant en sécurité depuis 15 ans
- Assiste des institutions, des sociétés privées ainsi que le secteur de la défense dans la protection de leur système d'information
- Fondateur de RandoriSec, société spécialisée en sécurité offensive

AGENDA

- Quelques chiffres
- OWASP
- Le projet OWASP Mobile Security Testing
  - OWASP MASVS
  - OWASP MSTG
  - OWASP AppSec Checklist
- Exemples de vulnérabilités

AGENDA

- **Quelques chiffres**
- OWASP
  - Le projet OWASP Mobile Security Testing
    - OWASP MASVS
    - OWASP MSTG
    - OWASP AppSec Checklist
  - Exemples de vulnérabilités

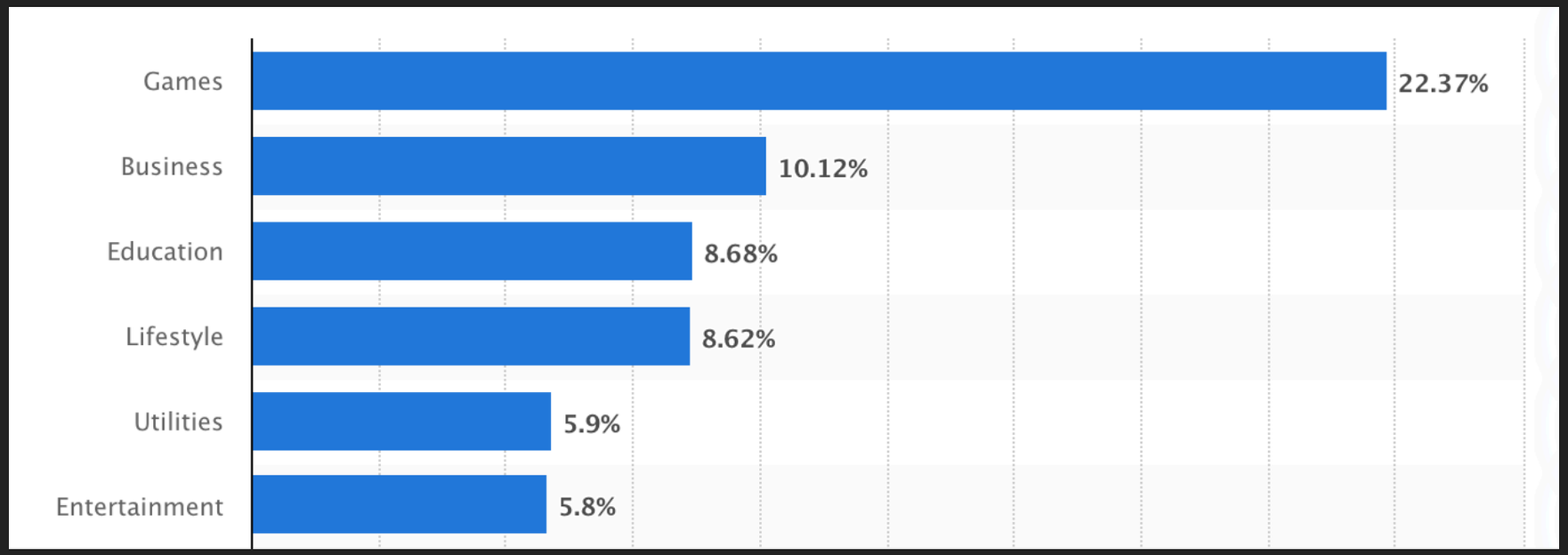
QUELQUES CHIFFRES: LA POPULATION

- En 2019:
  - 5,1 milliards d'utilisateurs de téléphones mobiles
  - 4,4 milliards d'utilisateurs de téléphones mobiles connectés à internet

QUELQUES CHIFFRES: LES APPLICATIONS

- En 2019:
  - 2,5 milliards d'applications disponibles sur le Google Play Store
  - 1,8 milliards d'applications disponibles sur l'Apple App Store

Catégories les plus populaires en novembre 2019 sur l'Apple App Store

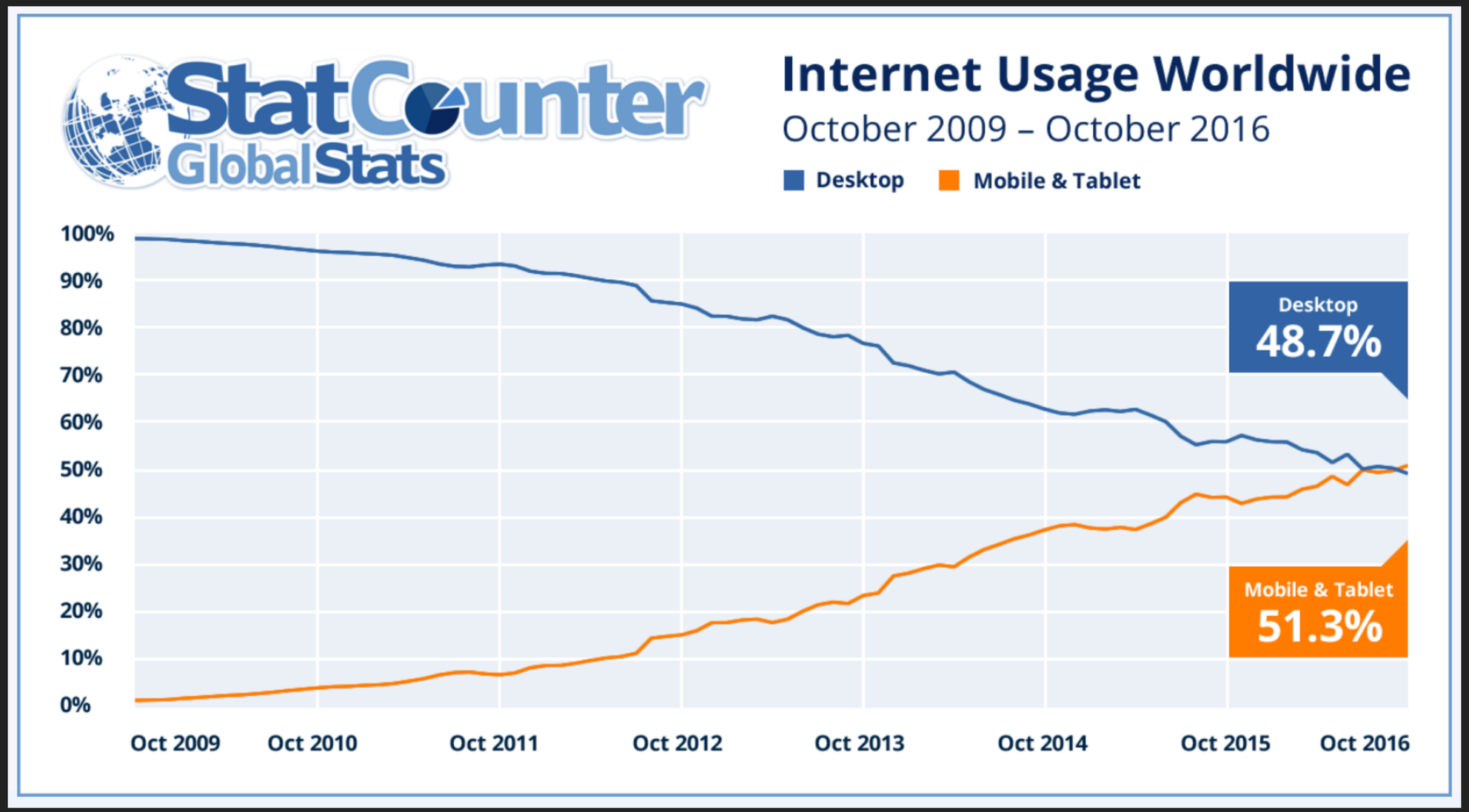


source: https://www.statista.com/statistics/270291/popular-categories-in-the-app-store/

QUELQUES CHIFFRES: LE TRAFIC

source: https://www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics

QUELQUES CHIFFRES: LA PROPORTION MOBILE/DESKTOP



source: https://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

AGENDA

- Quelques chiffres
- **OWASP**
  - Le projet OWASP Mobile Security Testing
    - OWASP MASVS
    - OWASP MSTG
    - OWASP AppSec Checklist
  - Exemples de vulnérabilités

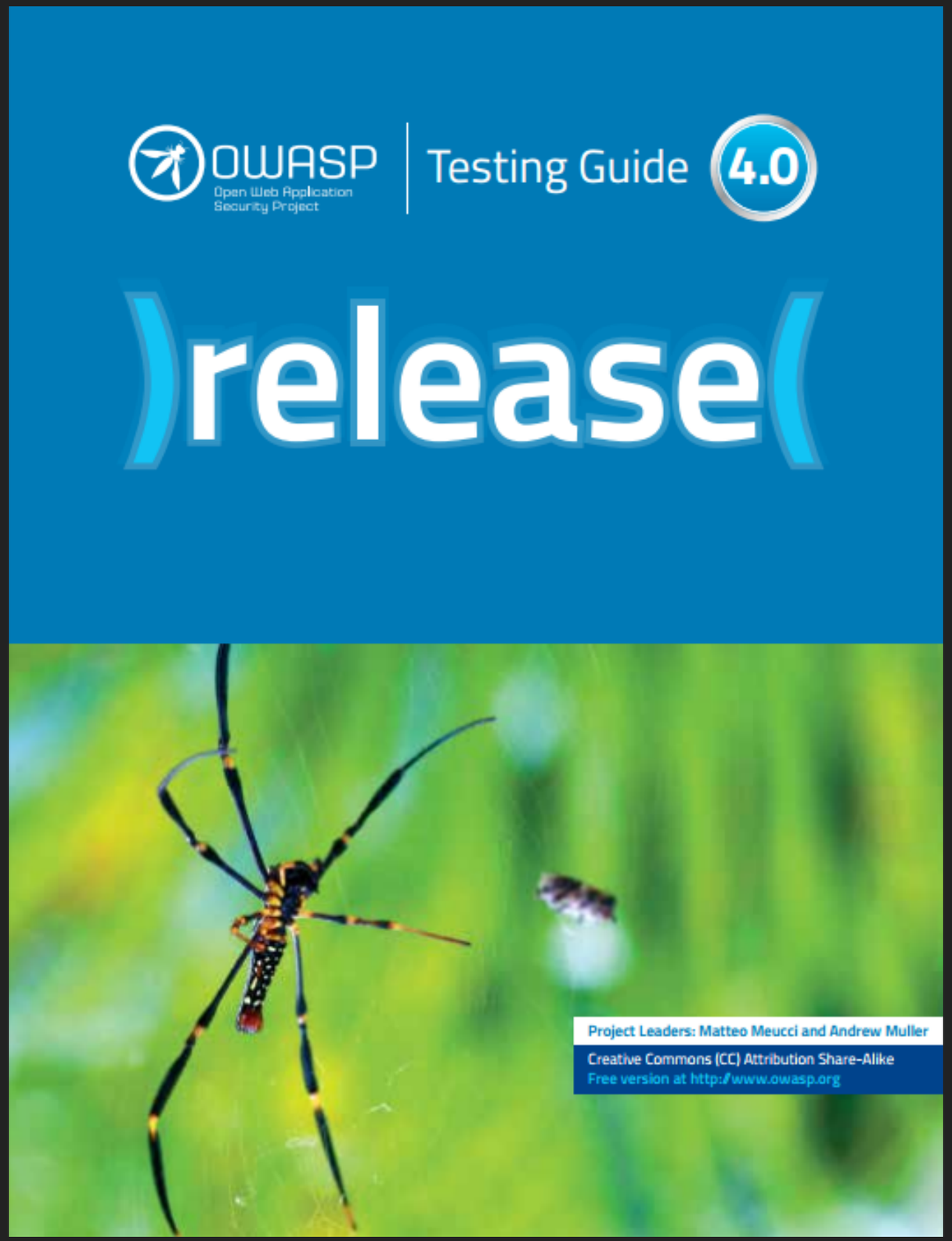
OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

- Association a but non lucratif
- Objectif: améliorer la sécurité des logiciels
- Communauté de 45 000 personnes
- Outils: ZAP, Juice Shop, Dependency Check, iGoat, DVIA
- Documentations: TOP10, Testing Guide, Secure Coding Practises
- Conférences

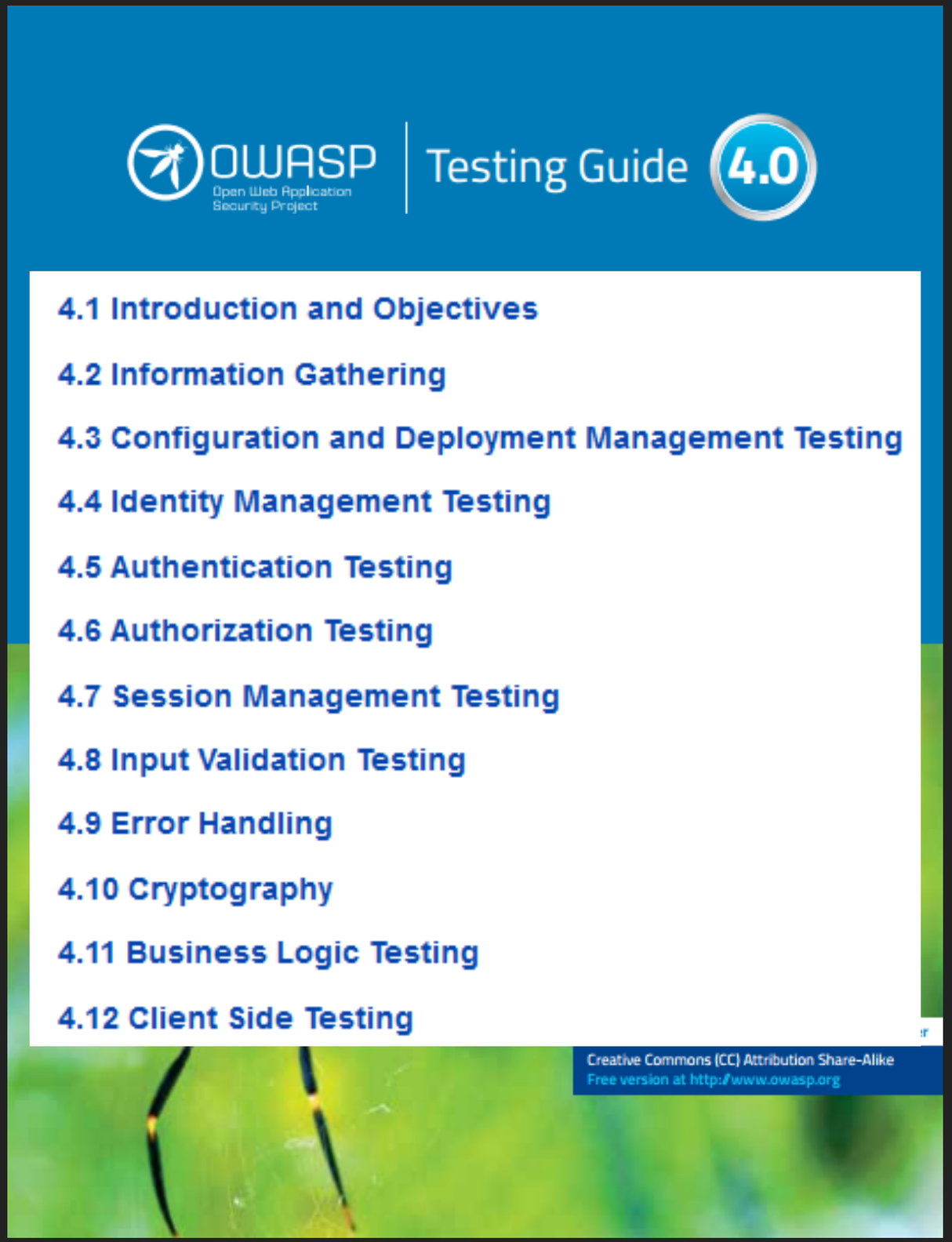
OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

OWASP (OPEN WEB APPLICATION SECURITY PROJECT)



OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

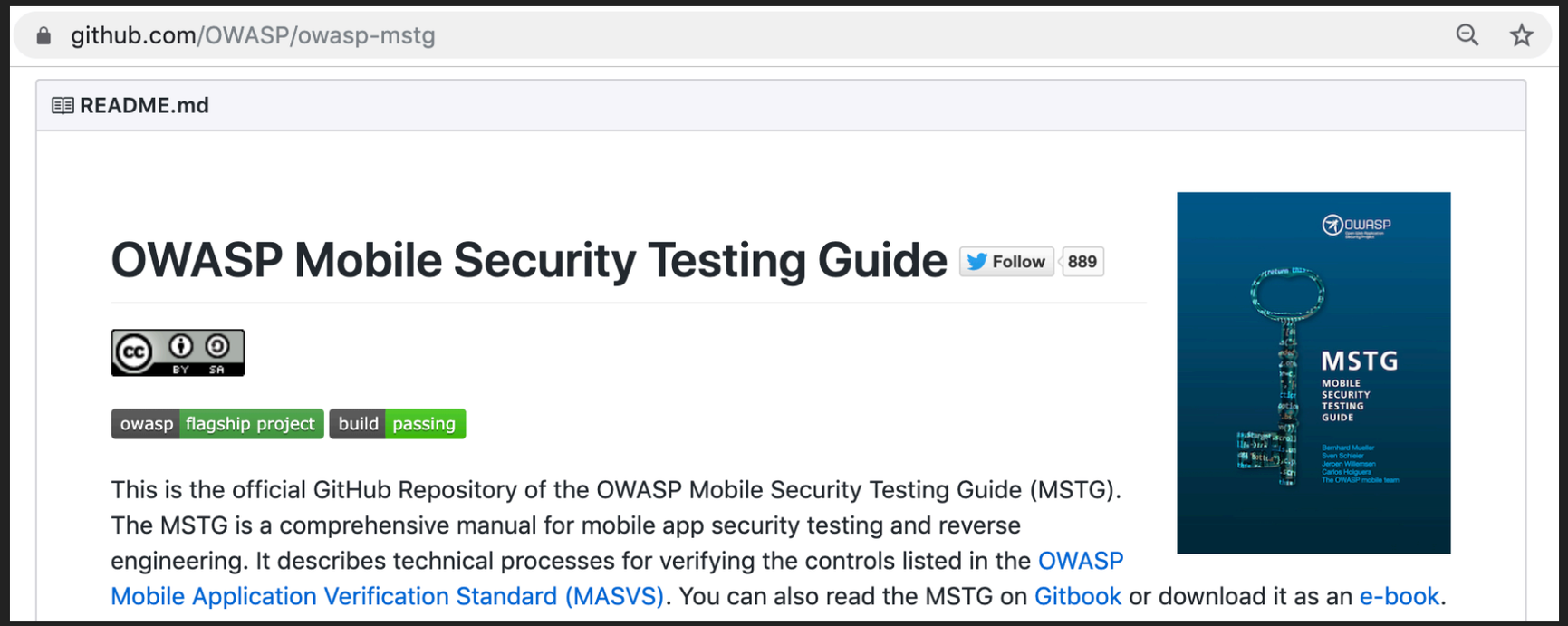


Web != Mobile

AGENDA

- Quelques chiffres
- OWASP
- **Le projet OWASP Mobile Security Testing**
  - OWASP MASVS
  - OWASP MSTG
  - OWASP AppSec Checklist
- Exemples de vulnérabilités

MOBILE SECURITY TESTING: LE PROJET

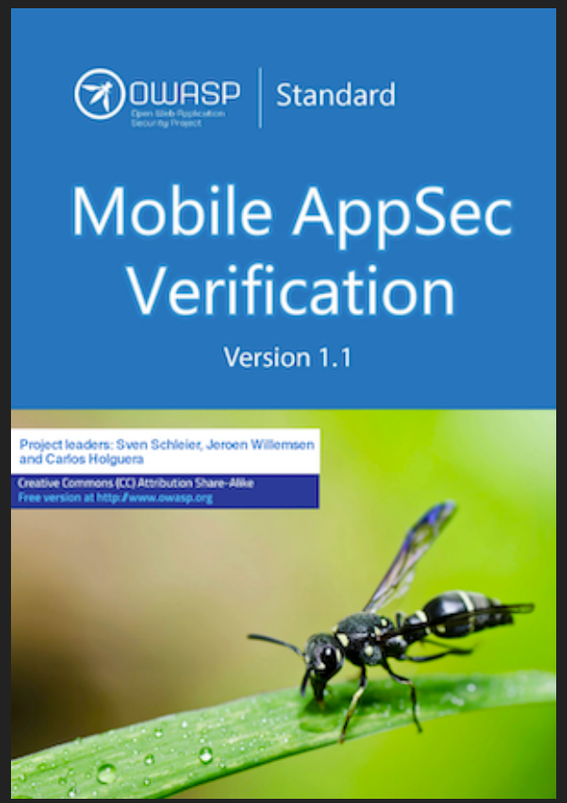


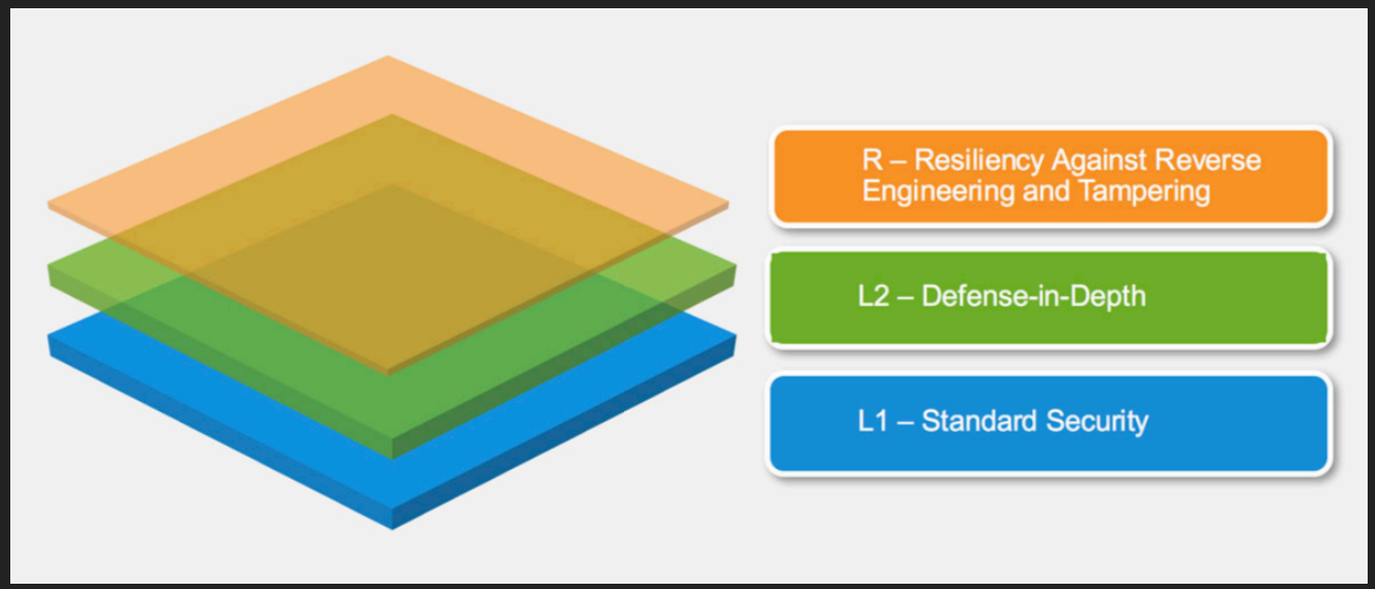
- Projet initié en 2015:
  - 1 standard + 1 guide + 1 checklist
- Sortie de la première version de la checklist en 2017
- Sortie de la v1.0 du standard en janvier 2018
- Sortie de la première beta du guide en juin 2018

AGENDA

- Quelques chiffres
- OWASP
- Le projet OWASP Mobile Security Testing
  - **OWASP MASVS**
  - OWASP MSTG
  - OWASP AppSec Checklist
- Exemples de vulnérabilités

MOBILE APPSEC VERIFICATION STANDARD





- Le standard défini trois niveaux de sécurité :
  - L1: Sécurité standard
  - L2: Défense en profondeur
  - R: Résistance à la rétro-ingénierie et à la modification

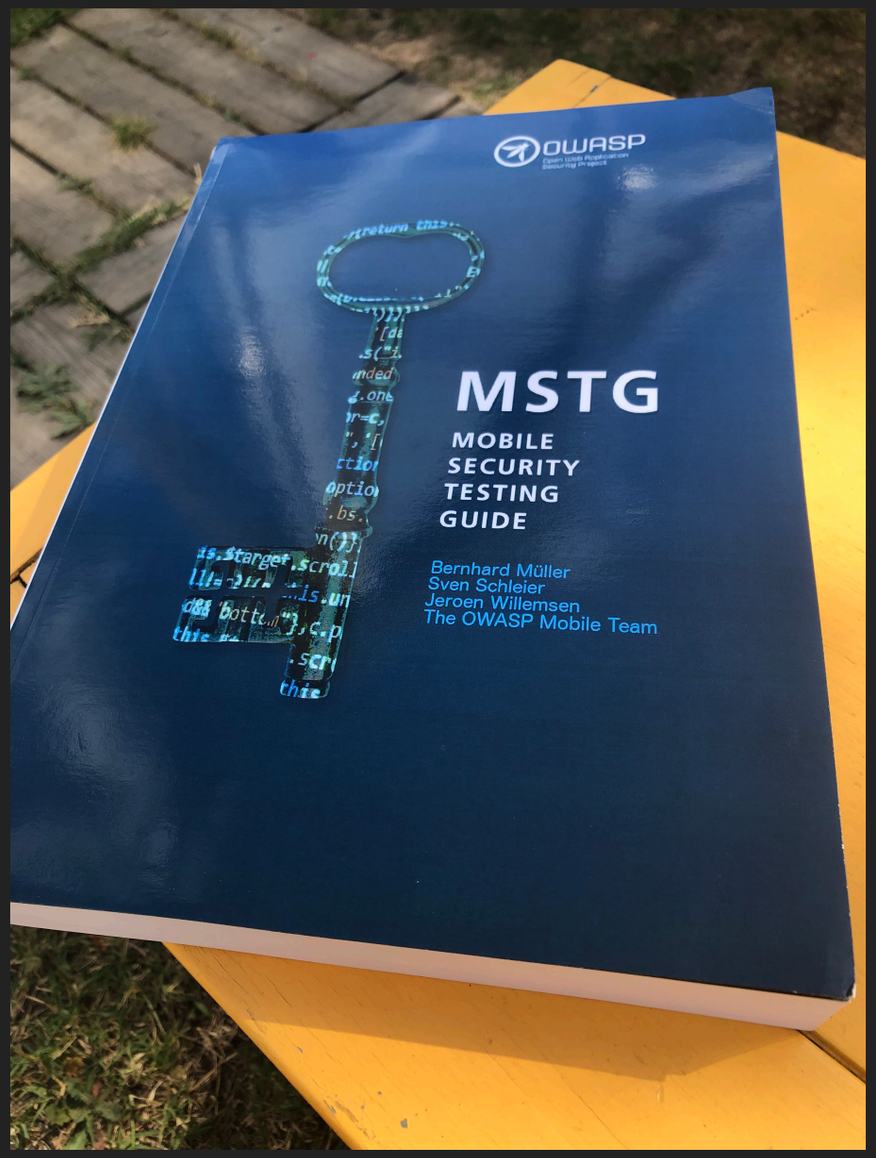
MOBILE APPSEC VERIFICATION STANDARD

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

AGENDA

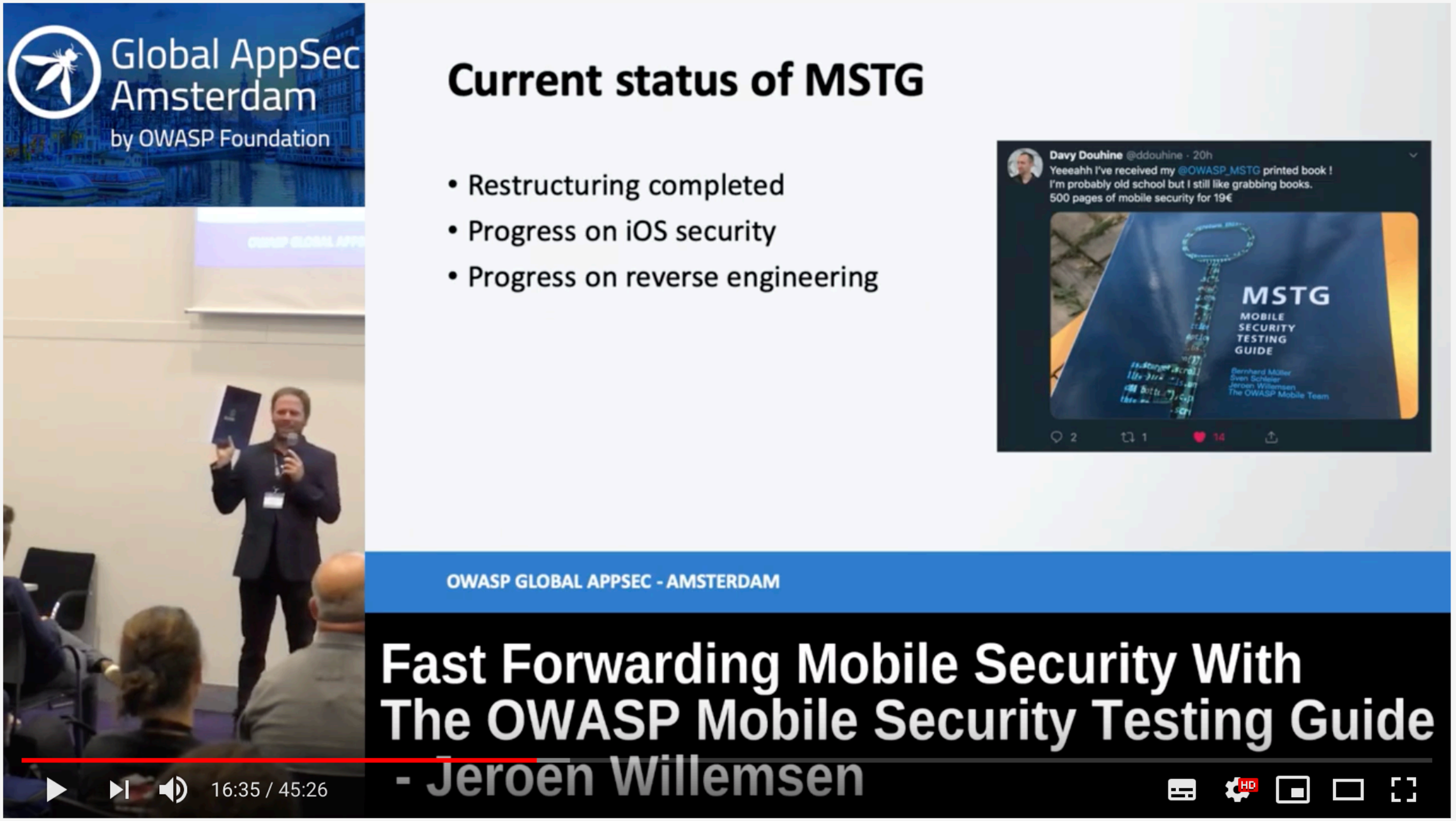
- Quelques chiffres
- OWASP
  - Le projet OWASP Mobile Security Testing
    - OWASP MASVS
    - **OWASP MSTG**
    - OWASP AppSec Checklist
  - Exemples de vulnérabilités

MOBILE SECURITY TESTING: LE GUIDE



- 3 grandes parties : une section générale, une section Android, une section iOS
- + 500 pages

MOBILE SECURITY TESTING: LE GUIDE



AGENDA

- Quelques chiffres
- OWASP
- Le projet OWASP Mobile Security Testing
  - OWASP MASVS
  - OWASP MSTG
  - **OWASP AppSec Checklist**
- Exemples de vulnérabilités

MOBILE APPSEC CHECKLIST

Mobile Application Security Requirements - iOS

ID	Detailed Verification Requirement	Level 1	Level 2	Status	Testing Procedure(s)
V1	**Architecture, design and threat modelling**				
1.1	All app components are identified and known to be needed.	✓	✓		-
1.2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	✓	✓		-
1.3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	✓	✓		-
1.4	Data considered sensitive in the context of the mobile app is clearly identified.	✓	✓		-
1.5	All app components are defined in terms of the business functions and/or security functions they provide.		✓	N/A	-
1.6	A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.		✓	N/A	-
1.7	All security controls have a centralized implementation.		✓	N/A	-
1.8	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	N/A	-
1.9	A mechanism for enforcing updates of the mobile app exists.		✓	N/A	-
1.10	Security is addressed within all parts of the software development lifecycle.		✓	N/A	-
V2	**Data Storage and Privacy**				
2.1	System credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.	✓	✓		Testing For Sensitive Data in Local Data Storage
2.2	No sensitive data should be stored outside of the app container or system credential storage facilities.				Testing For Sensitive Data in Local Data Storage
2.3	No sensitive data is written to application logs.	✓	✓		Testing For Sensitive Data in Logs
2.4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.	✓	✓		Testing Whether Sensitive Data Is Sent To Third Parties
2.5	The keyboard cache is disabled on text inputs that process sensitive data.	✓	✓		Testing Whether the Keyboard Cache Is Disabled for Text Input Fields
2.6	No sensitive data is exposed via IPC mechanisms.	✓	✓		Testing Whether Sensitive Data Is Exposed via IPC Mechanisms
2.7	No sensitive data, such as passwords or pins, is exposed through the user interface.	✓	✓		Testing for Sensitive Data Disclosure Through the User Interface
2.8	No sensitive data is included in backups generated by the mobile operating system.		✓	N/A	Testing for Sensitive Data in Backups
2.9	The app removes sensitive data from views when backgrounded.		✓	N/A	Testing for Sensitive Information in Auto-Generated Screenshots
2.10	The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.		✓	N/A	Testing for Sensitive Data in Memory
2.11	The app enforces a minimum device-access-security policy, such as requiring the user to set a device passcode.		✓	N/A	Testing Local Authentication
2.12	The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.		✓	N/A	Testing user education
V3	**Cryptography**				
3.1	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	✓	✓		Verifying Key Management

- Liste des tests à valider pour atteindre un niveau du standard MASVS
- Classés par section (ex: Architecture, etc., Stockage des données et respect de la vie privée, Cryptographie)

AGENDA

- Quelques chiffres
- OWASP
- Le projet OWASP Mobile Security Testing
  - OWASP MASVS
  - OWASP MSTG
  - OWASP AppSec Checklist
- **Exemples de vulnérabilités**

EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

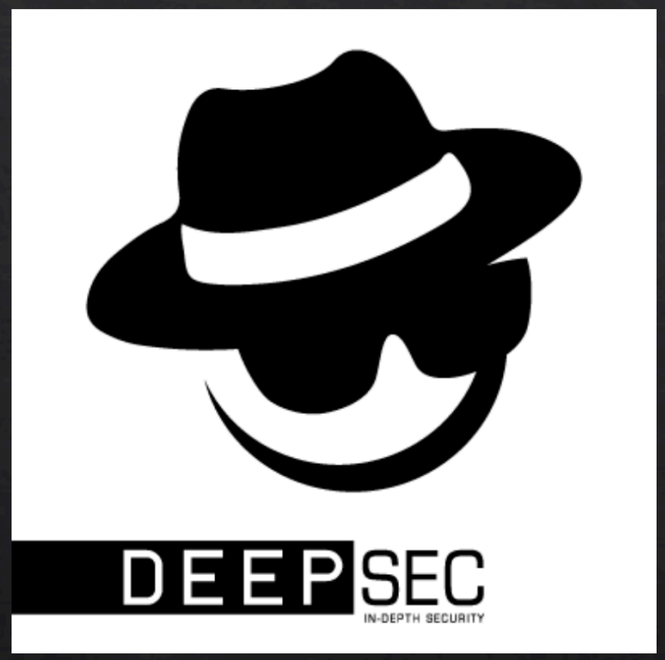
EXAMPLES DE VULNERABILITES

- **V1 Architecture, design and threat modelling**
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

V1 ARCHITECTURE, DESIGN AND THREAT MODELLING

- Pas de tests techniques
- Revue papier / interview
- Conception et architecture de l'application
- Tous les composants sont-ils bien référencés / utiles ?
- Mécanismes de sécurité implémentés
  - Y a t'il des mises à jour ?
  - Les contrôles de sécurité sont-ils effectués server-side ?

- Mécanismes de sécurité implémentés
  - **Les contrôles de sécurité sont-ils effectués server-side ?**



Abusing Google Play Billing for fun and unlimited credits!

Guillaume Lopes - @Guillaume_Lopes

source: https://www.randorisec.fr/publications/DeepSec2019-Abusing_Google_Play_Billing_for_fun_and_unlimited_credits.pdf

EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- **V2 Data Storage and Privacy**
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

V2 DATA STORAGE AND PRIVACY

- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - Journalisées (Logcat / NSlog) ?
  - Mises en cache (dictionnaire clavier, navigation) ?
  - Stockées en dehors du conteneur de l'application ?
  - Stockées en clair ?
  - Envoyées à des tiers ?
  - Stockées par les outils de sauvegarde (ex: iTunes) ?

- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - **Journalisées (Logcat / NSlog) ?**

```
10-15 14:13:20.972 4511-4565/com.[redacted] D/OkHttp: --> POST https://[redacted]
10-15 14:13:20.972 4511-4565/com.[redacted] D/OkHttp: Content-Type: application/x-www-form-urlencoded
10-15 14:13:20.972 4511-4565/com.[redacted] D/OkHttp: Content-Length: 103
10-15 14:13:20.972 4511-4565/com.[redacted] D/OkHttp: [redacted]password=password123&devi
10-15 14:13:20.972 4511-4565/com.[redacted] D/OkHttp: --> END POST (103-byte body)
10-15 14:13:21.038 4511-4536/com.[redacted] W/EGL_emulation: eglSurfaceAttrib not implemented
10-15 14:13:21.038 4511-4536/com.[redacted] W/OpenGLRenderer: Failed to set EGL_SWAP_BEHAVIOR on surface 0xdc4f4780,
```

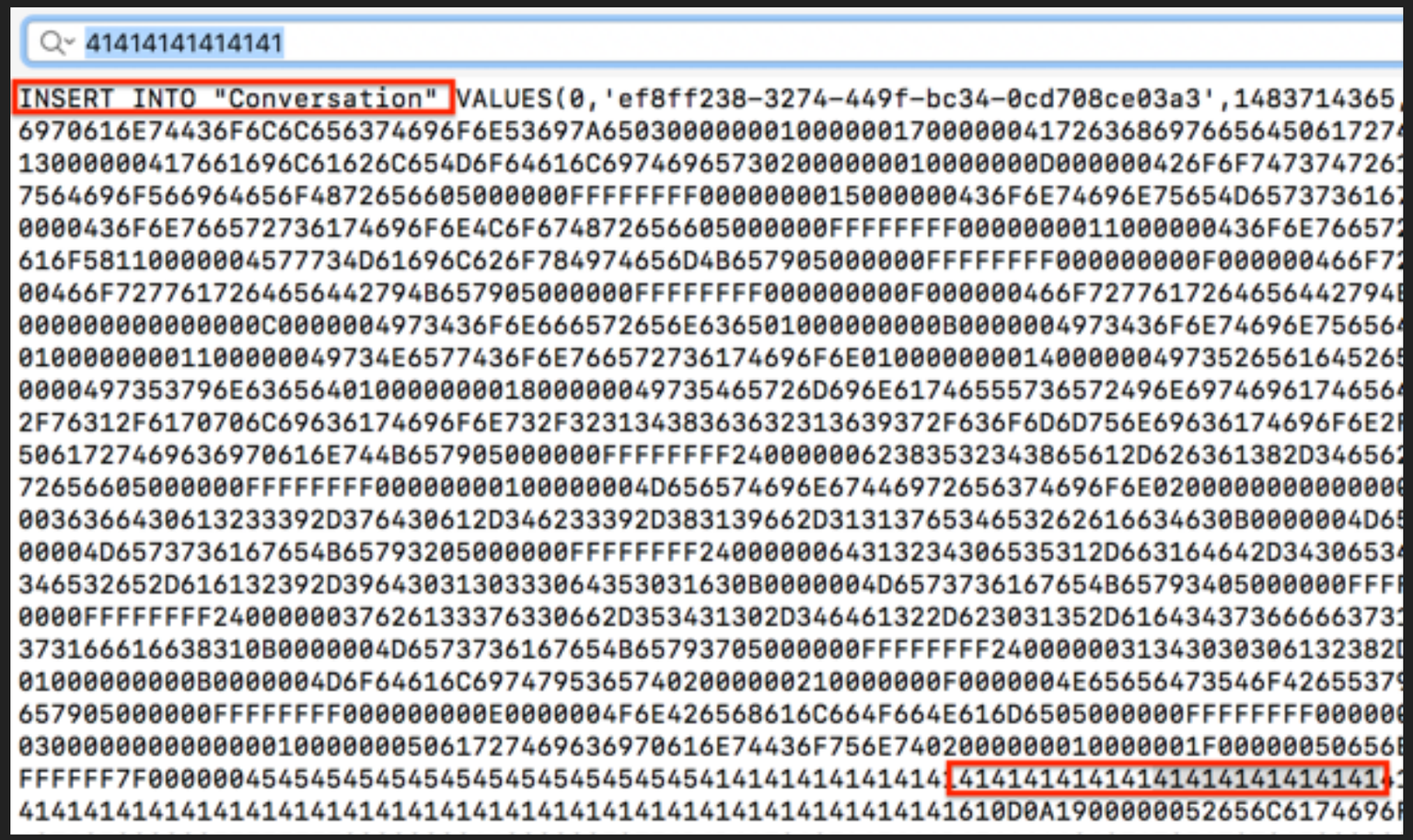
- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - **Mises en cache (dictionnaire clavier, navigation) ?**

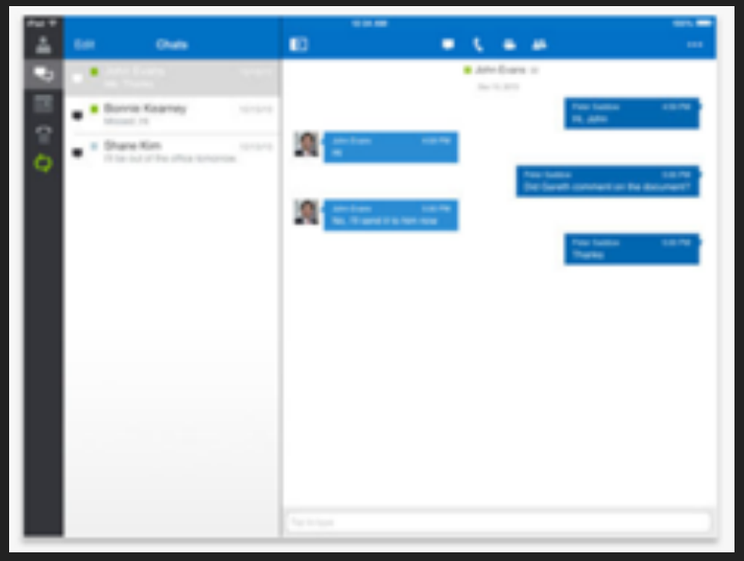

```
funk4it:/var/mobile/Library/Keyboard root# strings en-dynamic.lm/dynamic-lexicon.dat | grep "Frappes\|string2grepp"
b{FrappesClavierMisesEnCache
bzstring2grepp
```

- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - **Stockées en clair ?**

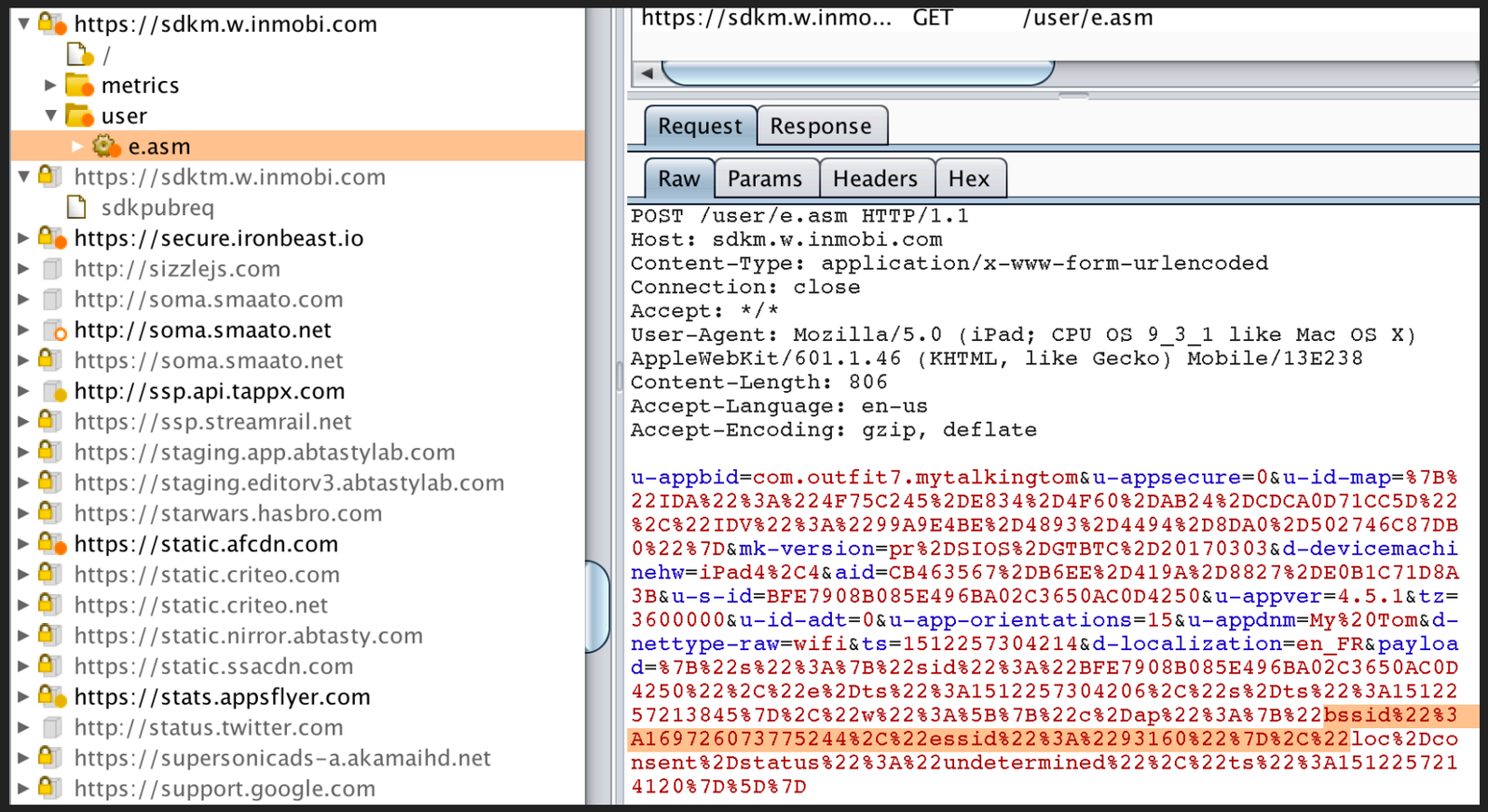
```
ZaEbWWlQaG9uZSA2cwAIABsAI                    CUAKwArgDlAOcA6wDtAQABAgEJAQsBDwERARcBGQEdAR8BMwE1AAAA
nse_type":"code","client_id":"api-gateway","username":"                    ","password":"p3nT4st_",
f713da4-6930-47d7-8174-0b7dd9a8c5f1","login_context":{"                    66411395287-6715115"}}^@
```

- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - **Stockées en clair ?**





- Les données sensibles (identifiants, clés crypto, données personnelles) sont-elles:
  - **Envoyées à des tiers ?**



EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- **V3 Cryptography**
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

- Les bonnes pratiques en matière de cryptographie sont-elles respectées ?
  - L’application n’utilise pas de clé codée en dur
  - L’application n'utilise pas d’algorithme de chiffrement obsolète ou “fait maison”
  - Une clé cryptographique par fonction
  - Générateur de nombres aléatoires à l’état de l’art

- Les bonnes pratiques en matière de cryptographie sont-elles respectées ?
  - **L'application n'utilise pas de clé codée en dur**

Fraunhofer SIT team [SIK]

Title:

Hardcoded Master Key in LastPass Password Manager

The used cryptographic keys are hardcoded in the following obfuscated application class (LPCommon):

```
public abstract class LPCommon {
//first part of the key
protected static String aA = "ldT52Fjsnjdn4390";
//second part of the key
protected static String aB = "89y23489h989fFFF";
```

Both strings concatenated build the encryption key (`ldT52Fjsnjdn439089y23489h989fFFF`) for the stored master password or PIN in the shared preferences file `LPandroid.xml`.

Therefore, decrypting the password is trivial, once an attacker gains access to the shard preference file he can decrypt the stored master password or the PIN.

source: https://team-sik.org/sik-2016-022/

EXAMPLES DE VULNERABILITES

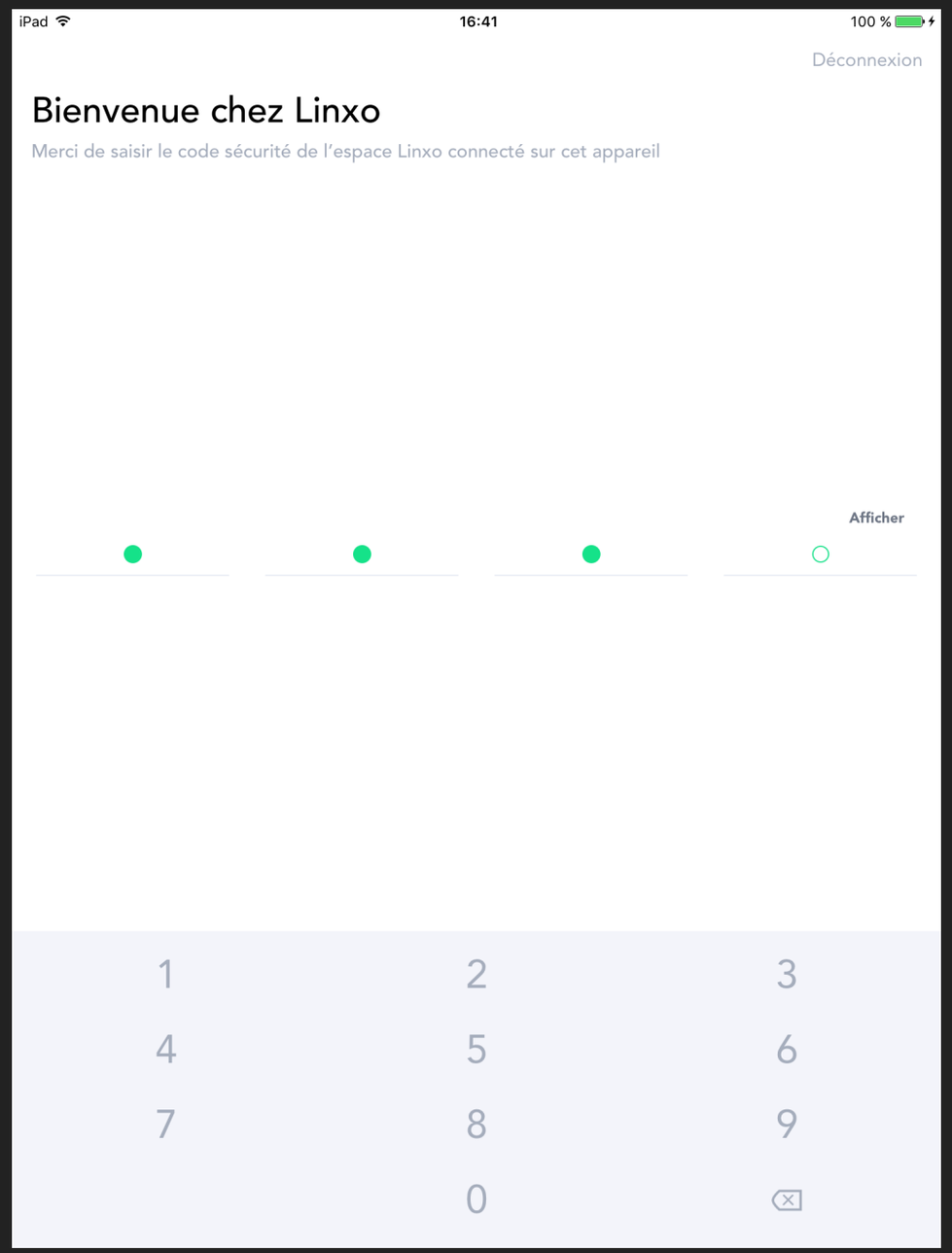
- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- **V4 Authentication and Session Management**
- V5 Network Communication
- V6 Platform Interaction
- V7 Code Quality and Build Settings

- Gestion de l'authentification
  - Authentification effectuée server-side ?
  - Protection contre les attaques de type brute-force ?
    - Politique des mots de passe ?
- Gestion des sessions:
  - Durée de vie raisonnable ?
  - Entropie suffisante pour les jetons ?

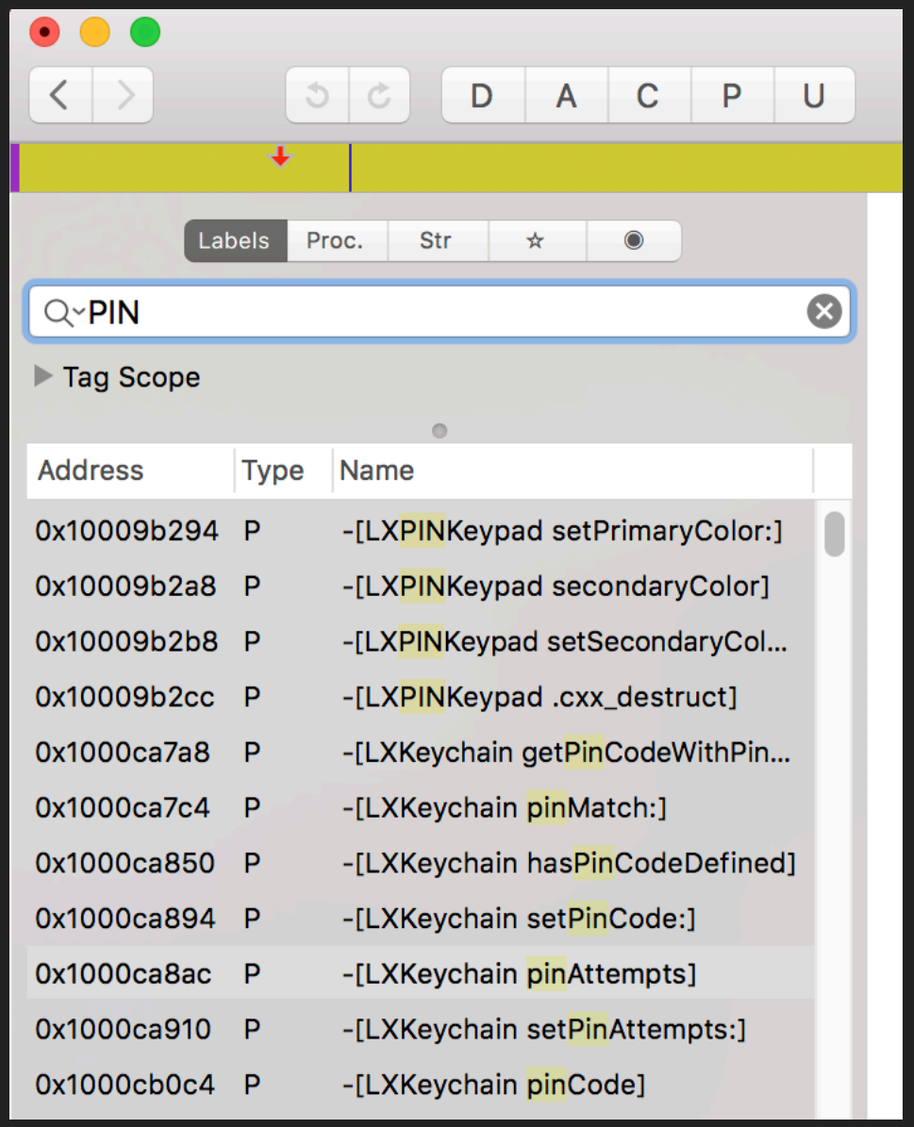
- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**

- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**

- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**



- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**



- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**

```
(0x15c6d6e20)  -[LXKeychain pinMatch:]
pinMatch: 7777
0x1005bd2dc Linxo!0x5112dc
0x1004d4740 Linxo!0x428740
0x1004d31c4 Linxo!0x4271c4
0x1004d3d88 Linxo!0x427d88
0x1004d4054 Linxo!0x428054
0x1005bce90 Linxo!0x510e90
0x1004d41fc Linxo!0x4281fc
0x10049224c Linxo!0x3e624c
0x1005853cc Linxo!0x4d93cc
0x100587080 Linxo!0x4db080
0x10049145c Linxo!0x3e545c
0x10048f7b8 Linxo!0x3e37b8
0x18796e3d8 UIKit!-[UICollectionView _selectItemAtIndexPath:animated:scrollPosition:notifyDelegate:]
0x18796dd1c UIKit!-[UICollectionView touchesEnded:withEvent:]
0x1878db30c UIKit!forwardTouchMethod
0x1879290a0 UIKit!-[UIResponder touchesEnded:withEvent:]
RET: 0x1
```

- Gestion de l'authentification:
  - **Authentification effectuée server-side ?**

```
/**
 * Called synchronously when about to return from -[LXKeychain pinMatch:].
 *
 * See onEnter for details.
 *
 * @this {object} - Object allowing you to access state stored in onEnter.
 * @param {function} log - Call this function with a string to be presented to the user.
 * @param {NativePointer} retval - Return value represented as a NativePointer object.
 * @param {object} state - Object allowing you to keep state across function calls.
 */
onLeave: function (log, retval, state) {
console.log("Function [LXKeychain pinMatch:]] originally returned:"+ retval);
retval.replace(1);
console.log("Changing the return value to:"+retval);
}
}
```

```
Function [LXKeychain pinMatch:]] originally returned:0x1
Changing the return value to:0x1
           /* TID 0xc07 */
  4004 ms  -[LXKeychain pinMatch:0x15f4ef4e0]
Function [LXKeychain pinMatch:]] originally returned:0x0
Changing the return value to:0x1
 17799 ms  -[LXKeychain pinMatch:0x15f2f2d40]
```

- Gestion de l'authentification:
- **Protection contre les attaques de type brute-force ?**
  - Rarement le cas sur les applications rencontrées

- Gestion de l'authentification:
  - **Politique des mots de passe ?**
    - Rarement le cas sur les applications rencontrées

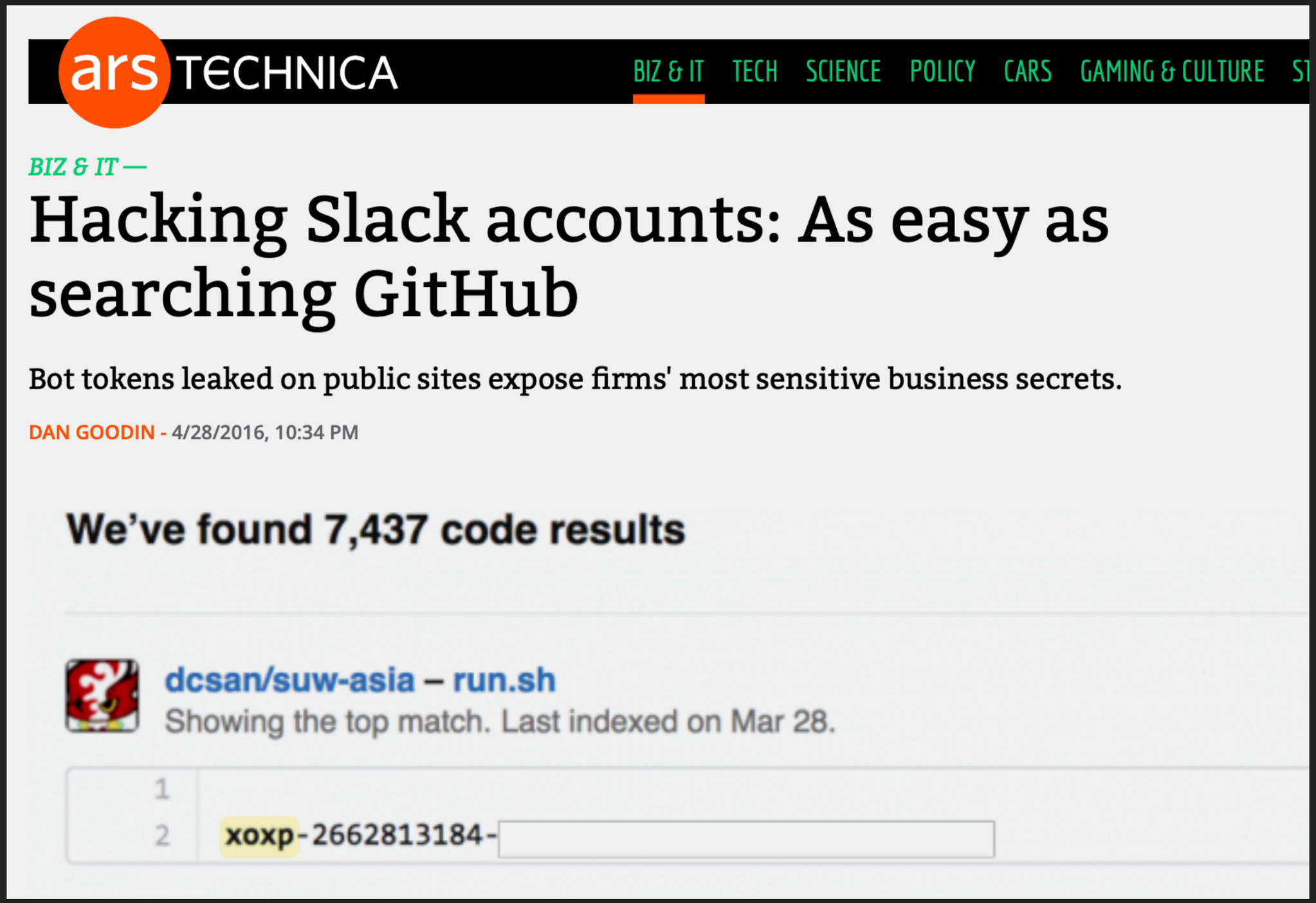
- Gestion des sessions:
  - **Durée de vie raisonnable ?**
    - Plus de 1 an pour Slack

[redacted] closed the report and changed the status to **Informative**. Nov 16th (5 months ago)

Thank you for your report.

At this time, we are choosing to keep the functionality here as it is, however we do thank you for submitting your report. I'm going to close your report as "Informative".

Thanks, and good luck with your future bug hunting.



source:https://arstechnica.com/information-technology/2016/04/hacking-slack-accounts-as-easy-as-searching-github/

EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- **V5 Network Communication**
- V6 Platform Interaction
- V7 Code Quality and Build Settings

- Mécanismes en place pour assurer la confidentialité et l'intégrité des communications:
  - Canal de communication chiffré ?
  - Algorithmes / configuration à l'état de l'art ?
  - Vérification de la chaine de certification ?
  - Certificate pinning (L2) ?

- Mécanismes en place pour assurer la confidentialité et l'intégrité des communications:
  - **Canal de communication chiffré ?**

```
MinimumOSVersion = "9.0";
NSAppTransportSecurity =     {
    NSAllowsArbitraryLoads = 1;
};
UIDeviceFamily =     (
    1,
    2
);
```

- Mécanismes en place pour assurer la confidentialité et l'intégrité des communications:
  - **Vérification de la chaine de certification ?**

3169	https://sync.bankin.com	GET	/v2/banks?client_id=f8d39787dbdd491bb11924891241c97c&client_secret=HzUGKTc7JV...	✓	200	79682
3168	https://sync.bankin.com	POST	/v2/authenticate?client_id=f8d39787dbdd491bb11924891241c97c&client_secret=HzUG...	✓	200	924
3167	https://sync.bankin.com	POST	/v2/authenticate?client_id=f8d39787dbdd491bb11924891241c97c&client_secret=HzUG...	✓	401	702
3166	https://sync.bankin.com	POST	/v2/authenticate?client_id=f8d39787dbdd491bb11924891241c97c&client_secret=HzUG...	✓	401	714

Request | Response

Raw | Params | Headers | Hex

```
POST
/v2/authenticate?client_id=f8d39787dbdd491bb11924891241c97c&client_secret=HzUGKTc7JVY7yys7IGi67jJBkzfoT4bNUIIk2odAmDDlHjaHoPSL05FnXSuAqp1q
&email=ddouhine%40gmail.com&password=[redacted] HTTP/1.1
Host: sync.bankin.com
User-Agent: iphone-3.9.9-10.3.2-iPhone5,2-standard-fr
Bankin-Version: 2018-06-15
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: fr
Cookie: __cfduid=daa5e7c35cf188e8f94e3e9ce53e6ea151540978708
Content-Length: 0
Connection: close
Bankin-Device: CBABB0AE-2505-4E9A-ACE0-2090AC9D9F10
```

EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- **V6 Platform Interaction**
- V7 Code Quality and Build Settings

- Mécanismes permettant d'interagir avec l'application:
  - Permissions de l'application
  - Fonctionnalités de l'application exposées ? (via un schéma d'URL spécifique - spotify: ou via IPC)
- Configuration des WebViews:
  - JavaScript désactivé ?
  - Support restreint des schéma d'URL (éviter file: et tel:)

- Mécanismes permettant d'interagir avec l'application:
  - **Permissions de l'application**
    - Android Camera app trop permissive

Checkmarx

Products Services Solutions Partners Company Resources

How Attackers Could Hijack Your Android Camera to Spy on You

Nov 19, 2019 by Erez Yalon

source: https://www.checkmarx.com/blog/how-attackers-could-hijack-your-android-camera

CNN BUSINESS

UNHACKABLE

Hackers could be using your Android camera to spy on you

By Jordan Valinsky, CNN Business

Updated 1640 GMT (0040 HKT) November 20, 2019

source: https://edition.cnn.com/2019/11/20/tech/google-android-camera-hijack-trnd/index.html

EXAMPLES DE VULNERABILITES

- V1 Architecture, design and threat modelling
- V2 Data Storage and Privacy
- V3 Cryptography
- V4 Authentication and Session Management
- V5 Network Communication
- V6 Platform Interaction
- **V7 Code Quality and Build Settings**

V7 CODE QUALITY AND BUILD SETTINGS

- Les bonnes pratiques liées au développement sont-elles respectées ?
  - Mode release (et non pas mode dev / debug)
  - Code de déboggage supprimé
  - Pas de journalisation de messages de debug
  - Symboles supprimés des binaires
  - Pas de vulnérabilités connues sur les bibliothèques externes

QUESTIONS ?

@ddouhine