

# **Telekom - BROKEN W3B CHALLENGE 2.0**

## **Penetrationstest - Bericht**

von Andreas Zinkl

# Inhaltsangabe

1. Übersicht der Schwachstellen
2. Risikobewertung
3. Informationsgewinnung
4. Eindringen in das System
5. Fazit und Handlungsempfehlungen
6. Anhang (Ermittelte Flags)

# 1. Übersicht der Schwachstellen (1)

- Preisgabe von internen Informationen auf der Webseite unter der Adresse <http://80.158.6.18:80>
  - Kommentar im Quelltext enthalten
    - Information über User-Datenbank (Verwendung einer NoSQL-Datenbank)
    - Ein Mitarbeiter heißt „Mark“
- Verwendung von veralteter Software und schlechten Authentifizierungsmethoden
  - Apache httpd Service – Version 2.4.18
  - Apache .htaccess Authentifizierung (Port 8888)
  - HTTP-Post Request mit Authentifizierungsinformationen (Port 80)

# 1. Übersicht der Schwachstellen (2)

- Unzureichende Validierung von Benutzereingaben
  - Datei-Uploads unter <http://160.44.192.138/> von Fotos können Schadcode enthalten
  - Keine Validierung der Anmeldeinformationen unter <http://80.158.6.18/> führt zu einer NoSQL-Injection Schwachstelle
- Keine Verwendung von HTTPS bei allen verfügbaren Diensten
- Local-File-Intrusion (LFI) Schwachstelle
  - URL: [http://80.158.6.18:8881/grabfile.php?key={user\\_key}&download=../../../../etc/passwd](http://80.158.6.18:8881/grabfile.php?key={user_key}&download=../../../../etc/passwd)

## 2. Risikobewertung

Bewertungsskala:  
0 = kein Risiko  
1-2 = geringes Risiko  
3-4 = mittleres Risiko  
5-6 = hohes Risiko  
7 = sehr hohes Risiko

Nr.	Schwachstelle	Eintrittswahrscheinlichkeit	Schadensrisiko	Gesamtrisiko
1.	Kommentare in den Website-Quellcodes über die interne Infrastruktur	3	3	3
2.	Verwendung der Standard-“.htaccess“ Authentifizierung von Apache	4	4	4
3.	Veraltete Service Version (z.B. Apache)	5	6	6
4.	Unzureichende Validierung beim Upload von Bildern	5	6	6
5.	Keine bzw. unzureichende Validierung der Eingaben – NoSQL Injection	7	7	7
6.	Keine Verwendung von HTTPS	7	7	7
7.	Local-File-Intrusion (LFI) Schwachstelle	7	7	7

# 3. Informationsgewinnung (1)

- Durch Port-Scanning (Software *nmap*) der Adresse <http://80.158.6.18> ermittelte Services
  - HTTP Services (Port 80 und Port 8888)
    - Port 80: NodeJS / ExpressJS Server
      - → Vermutung zur Verwendung von MongoDB liegt nahe
    - Port 8888: Apache Server *httpd* (Version 2.4.18)
- Ermittlung der DB-Schwachstelle
  - Kommentare in der Webseite informieren zur Verwendung einer NoSQL-Datenbank
  - In der Datenbank hinterlegte Nutzer können durch NoSQL-Injection ermittelt werden
    - User, Guest, Admin

# 3. Informationsgewinnung (2)

- Ermittlung der Authentifizierungsdaten ({User:Hash}) für das Dashboard auf Port 8888 über die LFI-Schwachstelle
  - TSSFinal:\$apr1\$PMI4Sd50\$Hi6cxWYqgbOh/.VIKppt1
- Ermittlung der User im System durch LFI-Schwachstelle
  - LFI-Schwachstelle ermöglicht Zugriff zu z.B. /etc/passwd

# 4. Eindringen in das System

- Schritt 1: Upload eines Fotos (PNG-Format) mit angehängtem PHP-Schadcode
  - Verwendung von Metasploit zur Erstellung einer PHP-Meterpreter-Reverse-TCP Payload
- Schritt 2: Starten eines „Port-Listeners“ der auf eingehende TCP-Verbindung wartet
  - Verwendung von Metasploit (exploit/multi/handler)
- Schritt 3: Verwendung der LFI-Schwachstelle zum Ausführen des hinterlegten PHP-Schadcodes
- Schritt 4: Zugriff auf das System über eine Meterpreter-Shell

# 5. Fazit und Handlungsempfehlungen

- Aktueller Status zur Sicherheit: **Extrem unsicher**
- Schwerwiegende Schwachstellen ermöglichen einen raschen Zugang in das System
- Handlungsempfehlung:
  - Updates der Services (Apache)
  - Keine Verwendung von Standard-Authentifizierungsmechanismen wie .htaccess
  - Prüfen von zulässigen Eingaben
    - NoSQL-Injection vermeiden
    - LFI – Schwachstelle vermeiden
  - Verwendung aktueller Sicherheitsstandards durch Anwendung des HTTPS-Protokolls

# 6. Anhang: Ermittelte Flags

- Ermittelte Flags:
  - Flag 1: TSEC{5f39e90d93baad53fd7288e8a6fa9586}
  - Flag 2: TSEC{24c2dc999e66bba7c356b91334a25308}
  - Flag 3: TSEC{aa791a74d55bbd786833b6e490dd6677}
  - Flag 4: TSEC{1d55c399453b885892ea51820b460c40}
  - Flag 5: Finales Flag ist unbekannt (Pfad im System: /home/flagmaster/final\_step/flag.txt)
    - Dieses konnte nicht ermittelt werden.
    - Hierbei stellte das „main“-Executable ein Hindernis dar, da das Passwort nicht ermittelt werden konnte
    - Benutzer „adm1n“ konnte mit Hilfe des verfügbaren *gdb* durch debuggen ermittelt werden

# Vielen Dank für Ihre Aufmerksamkeit!

Noch Fragen?

- Kontakt:
  - Andreas Zinkl
  - Email: [andreas.zinkl@st.oth-regensburg.de](mailto:andreas.zinkl@st.oth-regensburg.de)
  - Twitter: [@zinklandi](https://twitter.com/zinklandi)