



Projektstudium Pen-testing

MORITZ RUPP, DEAN BASIC, LUKAS HEINZELMANN, MARIUS HALD

Inhalt

Aufgabenstellung

Ablauf

Zielgerät

Szenario

Vorgehen Pentest

Findings

Report schreiben

Präsentation bei der SySS

Penetrationstest - Aufgabenstellung

1

ANWENDUNG / PEN
TEST AUF EIN REALES
PRODUKT / SYSTEM

2

ERSTELLUNG EINES
REPORTS

3

VORSTELLUNG DER
ERGEBNISSE

4

UMSETZUNG VON
PROJEKTMANAGEMENT
KONZEPTEN

Ablauf



Vorstellung des Gerätes

- ▶ Smart-home Zentrale
- ▶ Heimautomatisierung
- ▶ Steuereinheit für smarte Geräte

Heizung, Rolläden, Türen, Fenster,
Beleuchtung

- ▶ Bietet Weboberfläche





Raspberry 3 Verbaut

Szenario



Weboberfläche

► Login-oberfläche

POWNERD

HomeMatic

homematic 

Anmelden

Admin

guest

user

Bitte geben Sie Ihren
Benutzernamen ein.

Bitte geben Sie Ihr Passwort
ein.

Anmelden

Vorgehen Pentest

- ▶ Phase 1 Interaktionen vor dem Test
- ▶ Phase 2 Informationsbeschaffung
- ▶ Phase 3 Bedrohungsmodellierung
- ▶ Phase 4 Analyse der Sicherheitsanfälligkeit
- ▶ Phase 5 Auswertung
- ▶ Phase 6 Nach der Auswertung
- ▶ Phase 7 Berichterstattung

Beispiel findings

Login hat kein
cooldown

- Brute-force
möglich

Standart
credentials
(admin:admin)

Session stealing

Replay attacke

Session stealing

- ▶ Session-id wird bei jeder Anmeldung angelegt
- ▶ Nach Abmeldung für 300 sekunden gültig
- ▶ Kommt man an die Session-id, wird man angemeldeter User

🔖 ⚠️ Nicht sicher | 141.87.29.101/pages/index.htm?sid=@d13GTmEAxf@

Weitere findings

- ▶ Remote code execution
- ▶ Nur auf alter Version möglich
- ▶ SSH brute force
- ▶ Cross-side scripting
- ▶ Fehlende HTTP-Security header
- ▶ Etc.

Report schreiben

- ▶ Alle findings zusammenfassen
- ▶ Risikobewertung einführen
- ▶ Findings dementsprechend einordnen
- ▶ Empfehlungen definieren
- ▶ Zusammenfassung

Präsentation bei SySS

- ▶ Einem Auftrag-abnahme-gespräch nachempfunden
- ▶ Vorgehensweise
- ▶ Zusammenfassung
- ▶ Empfehlung
- ▶ Antworten auf Fragen

The background consists of numerous overlapping, slightly crumpled teal-colored rectangular papers. Each paper has a large, dark teal question mark printed on it. In the top right corner, there is a solid red rectangle.

Noch fragen?