

CYBERBELT

Zertifizierte Cyber-Sicherheit

>>Technologien und Infrastrukturen . staatl. befugt und beeidet

Prüfen schützt.

IT-Ziviltechniker

Techniker . Informatiker . staatl. befugt und
beeidet

Vorsitzender der Fachgruppe IT .
Ziviltechnikerkammer

Hör-Bücher

Cyber-Sicherheit woher und warum . Krypto AG . CH / Steuer-CD . AT/CH



Hegemonie - Vorherrschaft



Amerika first



Eliten Demokratie und Neo Liberalismus, 2018
Wahl-Oligarchie ökonomischer
und politischer Eliten

Heimspiel

Standort neu: Campus V . Dornbirn
seit Sept. 2022

SEIT 1998



IHRE **PRÜFSTELLE** FÜR MEHR
CYBER-SICHERHEIT
UND **DATENSCHUTZ**

Wolfgang Prentner

- Mechaniker . Hohenems
 - HTL . Dornbirn
 - TU . Informatik . Wien
 - TU . Promotion . CyberSecurity Bereich . Wien
-
- Informatiker
 - IT-Ziviltechniker
 - Gerichtssachverständiger
-
- ZTP.digital ZT-GmbH . Geschäftsführer und Gründer
 - Standorte: Wien . Dornbirn . NÖ



Unabhängigkeit.

IT-Ziviltechniker



Fachgruppe der IT-Zivilingenieure



Sprechen wir die
selbe Sprache?

Quiz Instagram

Wir verlosen 3 Paper-Watches

LOGARITMOS

$\log 1000 =$

$\log 100 =$

$\log 1 =$

$\log 0,1 =$

$\log 0,001 =$

@profmarcelotavares

Aulas particulares

profmarcelotavares

Logik

What is the Output?

```
#include<stdio.h>
int main(){
    int a = 97;
    char *ptr;
    ptr = (char *)&a;
    printf("%c ",*ptr);
    return 0;
}
```

C

What will be the Output?

```
>>> f=lambda x:bool(x%2)
>>> print(f(20), f(21))
```

Options:

1. Error
2. False False
3. True False
4. False True

Python

Zertifizierte

Cyber-Security

Technologie

Resilienz Test Center

Offensive Security

E-Spionage
Social Hacking
Pentesting
Forensik
Notfall-Team
Red Team Operations
Code Analysen

Sicherheitsüberprüfung mit **Zertifikat**



Kunden-Projekte sprechen lassen.

Vorarlberg und Schweiz



...



Kundenstimmen

Vorarlberg und Schweiz



Doppelmayr



Rotes Kreuz VBG



V.Milch



VLKH



Variosystems . CH

Top 5 österreichweit

Raiffeisen
Software



REWE
GROUP

 cyberDOC

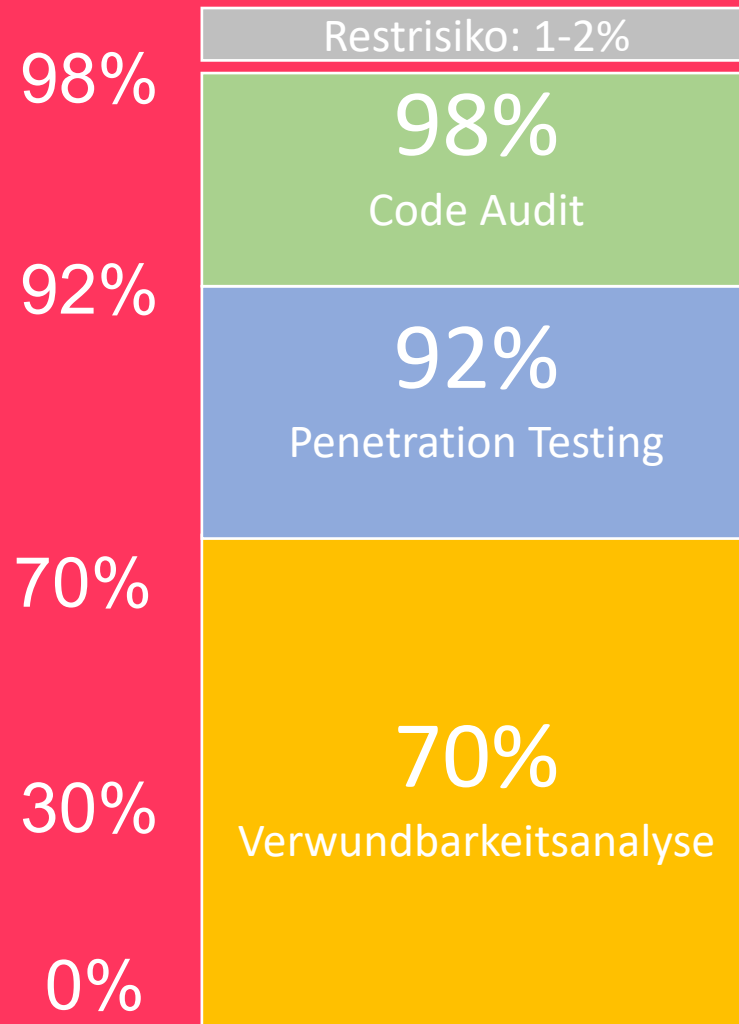
 WIENER LINIEN

voestalpine

 BÖHLER

Prüfung

Technologie und Infrastruktur: Zusagen/Gewährleistung (Garantie)



Normen, Standards und anderweitige Grundlagen

>> Technologie

- Stand der Technik
- Web-Applikationen
 - OWSAP: Top 10 Risks
 - **OWASP: ASVS - Application Security Verification Standard**
 - ÖNORM: A 7700
 - BSI: Leitfaden zur Entwicklung sicherer Webanwendungen
 - ISO 25010
- Infrastrukturen
 - Best Practice (BSI)
 - Industrie-Werkzeuge mit Eigen-Entwicklung (CyBelt ScanReporter)
- Infrastrukturen IT/OT (Management-Systeme)
- ISO 27000
- IEC 62443 (NIS-G)
- Cyber-Trust Gütesiegel (ISO 27000 light Zulieferer)

Cyber-Sicherheit

Gutachten und Zertifikat

GUTACHTEN
AUDITS UND PRÜFBERICHTE

Ziviltechnikergutachten

nach Application Security Verification Standard . ASVS Version 4.0.1

■ Lfd.Nr.: 59 ■ Version 1.0 ■ Final ■ freigegeben ■ vertraulich

Wien, am 10. Februar 2021



Inhaltsverzeichnis

Teil 1: Allgemeines 5

1. Einleitung 6

2. Auftragnehmer 6

3. Auftraggeber 6

4. Prüfauftrag 6

4.1. Penetrationstest-Audit („Black Box Auditing“) 6

4.2. Quelltext-Audit („White Box Auditing“) 7

4.3. Infrastruktur-Audit 8

5. Beurteilungsgegenstand 8

6. Abgrenzung des Prüfungsumfangs 9

6.1. [REDACTED] 9

6.2. [REDACTED] 9

6.3. [REDACTED] 10

6.4. Funktionales Testen 10

7. Vorgehensmodell 10

7.1. Bewertungsmodell und Nomenklatur 10

7.2. Qualitätssicherung mittels „Ziviltechniker Peer-Review“ 10

8. Sonstiges 11

8.1. Haftungsbeschränkung 11

8.2. Abkürzungen und Begriffsdefinitionen 11

8.3. Standards, Normen und anderweitige Grundlagen 12

8.4. Zusammenarbeit 12

Teil 2: Ziviltechnikergutachten 13

9. Allgemeines 14

9.1. Grundlagen aus Standards und Normen 14

10. Bewertung von [REDACTED] 15

10.1. Prüfung: Architektur, Design und Threat Modeling 15

10.2. Prüfung: Authentifizierung 15

10.3. Prüfung: Sitzungsverwaltung 15

10.4. Prüfung: Zugriffskontrolle 15



10.5.	Prüfung: Datenvalidierung	16
10.6.	Prüfung: Kryptographie	16
10.7.	Prüfung: Fehlerbehandlung	16
10.8.	Prüfung: Datenschutz	17
10.9.	Prüfung: Sichere Kommunikation	17
10.10.	Prüfung: Böartiger Code	17
10.11.	Prüfung: Business-Logik	17
10.12.	Prüfung: Dateien und sonstige Ressourcen	18
10.13.	Prüfung: APIs und Webservices	18
10.14.	Prüfung: Konfiguration	18
11.	Zusammenfassung	19
11.1.	Ausblick	19
Teil 3: Befund		20
12.	Prüfungsdetails	21
12.1.	Penetrationstest-Audit	21
12.2.	Quelltext-Audit	21
12.3.	Infrastrukturaudit	22
13.	Prüfungsergebnis	22
13.1.	Architektur, Design und Threat Modeling (V1)	22
13.2.	Authentifizierung (V2)	23
13.3.	Sitzungsverwaltung (V3)	27
13.4.	Zugriffskontrolle (V4)	29
13.5.	Datenvalidierung (V5)	30
13.6.	Kryptographie (V6)	34
13.7.	Fehlerbehandlung (V7)	34
13.8.	Datenschutz (V8)	35
13.9.	Sichere Kommunikation (V9)	36
13.10.	Böartiger Code (V10)	37
13.11.	Business-Logik (V11)	37
13.12.	Dateien und sonstige Ressourcen (V12)	38
13.13.	APIs und Webservices (V13)	40

13.14.	Konfiguration (V14)	41
14.	Prüfberichte	44
14.1.	Penetrationstest-Audit	44
14.2.	Quelltext-Audit	55
14.3.	Infrastruktur-Audit	88
Teil 4: Anhang		396
15.	Systemblatt	397
16.	Sammel-Hashwerte	398
16.1.	Einzel-Hashwerte	399
17.	Permission to Attack	401
18.	Protokoll zur Erstellung der Infrastruktur-Audit Policy	403
19.	Literaturverzeichnis	408

Abbildungsverzeichnis

Abbildung 1: Anmeldemaske von [REDACTED]	23
Abbildung 2: HTTP-Authorization-Header nach erfolgreicher Anmeldung	27
Abbildung 3: Keine Daten bei ungültigem Kontozugriff	34
Abbildung 4: Überblick über TLS-Einstellungen	36
Abbildung 5: Zugriff über Rest-API	40





Geschichten

1. Doktorat Uni.Prof. nervt (finger hans@uni.abc.ch)
2. Forschungs- und Entwicklungszeit: Spaß-Code in Applikation
3. Internet-Bank 1: Krypto-Algo falsch implementiert, aus 2000 (Algo RC4)
4. Internet-Banking 2: wird gehackt aus 2001 (Geschenke machen)
5. Glückspiel Anbieter: Zufallsgenerator aus (Zahlen erraten)
6. Weihnachtsgeschenke: iPhone und iPad
7. Elektronische Köder (unerlaubtes mitlesen von Dokumenten)
8. Dienstleister überwacht Vorstand (Fernwartung machen es möglich)
9. Spear-Phishing (Handy-TAN Transaktionsnummer)
10. Sex-Coins - jagt auf einen Hacker, weltweit (Wenn die Handschellen klicken)
11. Jagt auf einen Trojaner Emotet (Dienstleister klickt)
12. und nicht zu erzählend



Besten Dank
für die Zusammenarbeit!

Haben Sie noch Fragen?





Gesundheit für Ihre IT ■

ZTP.digital ZT-GmbH

T: +43 1 532 46 68 0

✉ office@ztp.digital

Wien . Niederösterreich . Vorarlberg

Prüfstelle für
Digitale Sicherheit

💻 www.ztp.digital

Austria . Europe



Prüfstelle für Digitale Sicherheit

ZTP.digital ZT-GmbH . IT-Ziviltechniker . Informatiker . staatlich befugt und beeidet