



TRUSTED THIRD PARTY

CYBER-SECURITY TEST CENTER

Gerichtstaugliches Pentesting nach ASVS

Dr.tech Wolfgang Prentner . IT-Ziviltechniker . staatlich beeidet . Gerichtssachverständiger

Dominik Rieder, MSc . IT-Ziviltechniker . staatl. beeidet

Do. 6. Mai 2021. Webinar . Online Präsentation



Prentner

Rieder

Wolfgang Prentner

Informatiker . IT-Ziviltechniker .
Gerichtssachverständiger

Dominik Rieder

Informatiker . IT-Ziviltechniker

Unabhängig.

**Planen.
Prüfen.**

Nur sicher mit dem Siegel.
Ihre ZiviltechnikerInnen.



Inhalt

1. Ausgangssituation
2. Der IT-Ziviltechniker
- 3. Gerichtstauglichkeit - Pentesting nach ASVS**
4. Der CYBERBELT
 1. Cyber-Sicherheit Prüfung nach ASVS
 2. Cyber-Sicherheit Gutachten
 3. Cyber-Sicherheit Zertifikat
5. Zusammenfassung



Ausgangssituation

Ausgangssituation - Auftraggeber

Was braucht das Unternehmen?
(GF/Vorstand)

Sicherheit

Ausgangssituation - PenTester

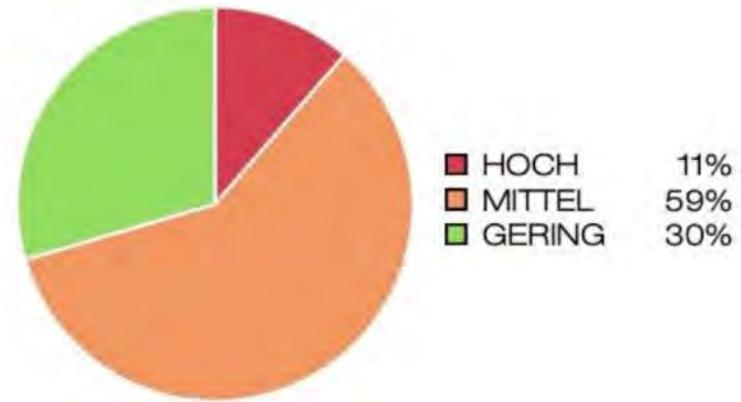
Was übernehmen PenTester?

Verantwortung für Cyber-Sicherheit und Haftung

Report Ergebnis

USA

Hohes Risiko	5
Mittleres Risiko	26
Geringes Risiko	13



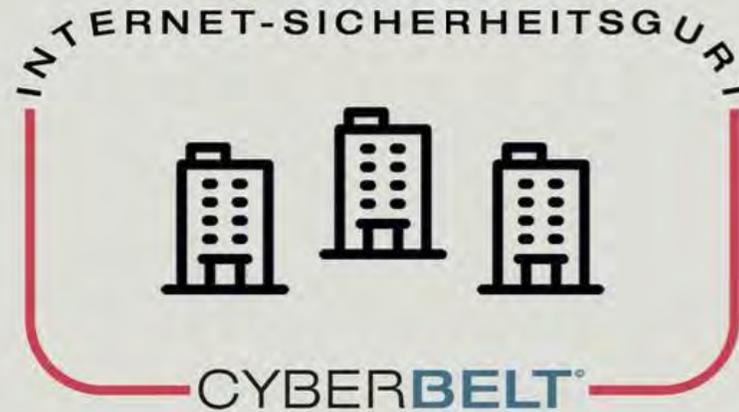
HERAUSFORDERUNGEN



PROBLEME



LÖSUNG



DAS PLUS



IT-Prüf- und Überwachungsstelle

Systeme . Software . Projekte . Datenschutz . IT-Kosten



Der IT-Ziviltechniker

Video >>

Wie werde ich
IT-Ziviltechniker?
mit staatlicher Befugnis



IT-Ziviltechniker



Behörden

IT-Ziviltechniker
seit 1860

staatlich befugt und beeidigt



Wirtschaft



Fachgruppe der IT-Zivilingenieure

Nicht erlaubte Tätigkeiten



Keine
kommerzielle
Entwicklung von
Software



Keine
kommerzieller
Verkauf von
Hardware oder
Software



Keine
kommerzieller
Betrieb eines
Rechenzentrums



Gerichtstauglichkeit

Pentesting nach ASVS

Schwächen von PenTest Report im Allgemeinen

- PenTesting mehr eine Kunst als Engineering
- Zu wenig „Drehbuch“
- Zu wenig „Formalismus“
- Zu wenig „Substanz“
- Zu wenig „Struktur“
- Zu wenig „Nachvollziehbarkeit“
- Zu wenig „rechtlich abgesichert“

Schaden durch Cyber-Angriff

1. Vorfall mit erheblichem Schaden (materiell und/oder immateriell)
2. Anlassfall zumeist durch Anzeige
3. Privatgutachten (Report/Befund/Gutachten) vom Pentester
4. Privatgutachten von der Gegenpartei
5. Gerichtsgutachten vom bestellten "Gerichtsgutachter"

Sachverständige

- Sachverständige/Sachverstand
 - Sie gilt für alle Berufe/Personen, die eine besondere Sachkenntnis erfordern, gleichgültig, ob sie selbständig oder unselbständig ausgeübt werden.
- Sachverständigenhaftung
 - nach dem ABGB ist keineswegs auf Personen beschränkt, die in die Sachverständigenliste eingetragen sind, um über Auftrag des Gerichts Gutachten in gerichtlichen Verfahren zu erstatten.

Rechtsgrundlagen: §§ 1295 ff, 1299 und 1300 ABGB

Haftung des Sachverständigen

- Haftung verschärft
- für typische Fähigkeiten eintreten
- objektiver Sorgfaltsmaßstab anzulegen
 - z.B. eine Ärzt:in für einen Behandlungsfehler
 - z.B. Techniker/Unternehmen/Steuerberater/Wirtschaftsprüfer: die Prüfberichte bzw. Gutachten im IT-Bereich erstellen
- Bereits leichte Fahrlässigkeit genügt.



Der CYBERBELT



CYBERBELT®

IHR INTERNET-SICHERHEITSGURT

cyberbelt.net

Sicherheits-Audit

Pentesting

Social Hacking

Red Team Operations

Code Analysen

mit **Zertifikat**



„Cyber Security Test Center (STC)“ Services

- CYBERBELT „Basic“ (80% Sicherheit)
 - Net- und App-Scan
 - Verwundbarkeitsanalysen (VA)
- Security Testing „Standard“ (92% Sicherheit)
 - Verwundbarkeitsanalysen (VA)
 - Pentesting (Black Box Testing)
- CYBERBELT „Premium“ (98% Sicherheit)
 - Cyber Security Testing: Premium
 - Verwundbarkeitsanalysen (VA)
 - Pentesting (Black Box Testing)
 - Code Review (White Box Testing)

Standards im „Cyber Security Testing“

- ÖNORM A7700: Sichere Webapplikationen
- BSI: Durchführungskonzept für Penetrationstests
- OWASP: Top 10 Web Application Security Risks
- OWASP: Application Security Verification Standard (ASVS)
-

Wir folgen dem Deming Kreis in OWSAP/ASVS



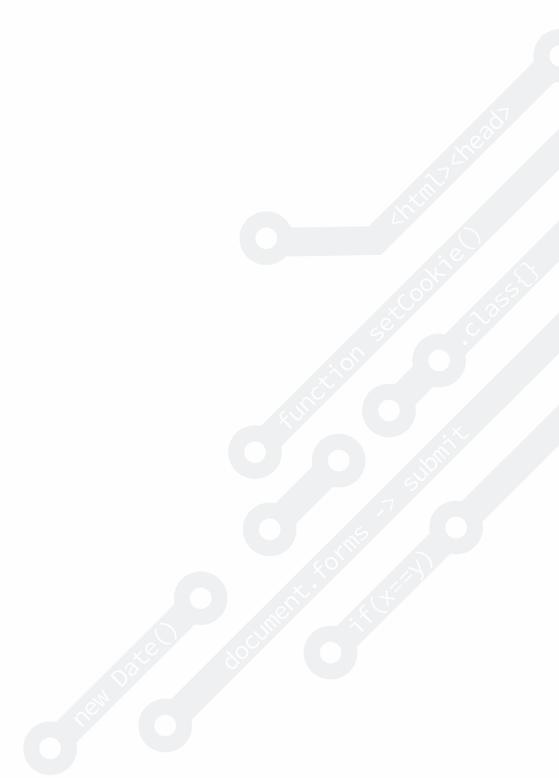
Technischer Teil



Cyber-Sicherheit Prüfung

nach Application Security Verification
Standard (ASVS)

ztp.digital



ASVS Verifikationsstufen (Levels)

Der **Application Security Verification Standard** definiert drei Stufen der Sicherheitsverifikation, wobei jede Stufe an Tiefe zunimmt.

- **Stufe 1** ist für **geringe Sicherheitsanforderungen** gedacht und lässt sich mittels Pentests prüfen.
- **Stufe 2** ist für Anwendungen, die **sensible Daten** enthalten und diese schützen müssen. Das ist die empfohlene Stufe für die meisten Anwendungen.
- **Stufe 3** ist für die **kritischsten Anwendungen**, z. B. solche, die hochwertige Transaktionen durchführen, sensible medizinische Daten enthalten oder aus anderen Gründen ein Höchstmaß an Vertrauen erfordern.

[<https://raw.githubusercontent.com/OWASP/ASVS/v4.0.2/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.2-de.pdf>]

ASVS Verifikationsbereiche

- V1. Architektur, Design und Bedrohungsmodellierung
- V2. Authentifizierung
- V3. Session-Management
- V4. Zugriffssteuerung
- V5. Eingabepfung
- V6. Kryptographische Komponenten
- V7. Fehlerbehandlung und Protokollierung
- V8. Datenschutz
- V9. Kommunikation
- V10. Verhinderung von böartigem Code
- V11. Geschäftslogik
- V12. Dateien und Ressourcen
- V13. API und Web Services
- V14. Konfiguration

ASVS Verifikationsstufen – Beispiel V2: Authentifizierung

ID	Beschreibung	L1	L2	L3
2.1.1	Prüfen Sie, dass Benutzerpasswörter mindestens 12 Zeichen lang sind, nachdem zusammenhängende Leerzeichen gekürzt wurden. (C6)	✓	✓	✓
2.1.2	Prüfen Sie, dass Passwörter mit 64 oder mehr Zeichen erlaubt sind, jedoch nicht mehr als 128 Zeichen. (C6)	✓	✓	✓
2.1.3	Prüfen Sie, dass Passwörter nicht gekürzt werden. Mehrere aufeinanderfolgende Leerzeichen können zu einem zusammengefasst werden. (C6)	✓	✓	✓
2.1.4	Prüfen Sie, ob alle druckbaren Unicode-Zeichen, auch Leerzeichen oder Emojis, in Passwörtern zulässig sind.	✓	✓	✓
2.1.5	Prüfen Sie, dass Benutzer ihr Passwort ändern können.	✓	✓	✓
2.1.6	Prüfen Sie, dass die Passwortänderungsfunktion das bisherige sowie das neue Kennwort des Benutzers erfordert.	✓	✓	✓
...				
2.2.5	Prüfen Sie, dass der CSP und die nutzende Anwendung über zweiseitig authentifiziertes TLS kommunizieren.			✓
2.2.6	Prüfen Sie, dass Authentifikationsdaten nicht wiedereingespielt werden können. Dies kann z.B. mit One Time Password (OTP) Generatoren, Chipkarten o.ä. verhindert werden.			✓
...				
2.3.2	Prüfen Sie, dass die Registrierung und die Verwendung von vom Teilnehmer bereitgestellten Authentifizierungsgeräten unterstützt werden, wie z. B. U2F- oder FIDO-Token.		✓	✓
2.3.3	Prüfen Sie, dass die Anweisungen zur Erneuerung zeitgebundener Authentifikatoren rechtzeitig gesendet werden.		✓	✓

V2: Authentifizierung

The screenshot displays a web application's login interface. The form includes the following elements:

- Input field for email: `rieder@ztp.at`
- Input field for password: masked with dots
- Checkbox: `Remember me for 7 days` (unchecked)
- Link: `Forgot password?`
- Button: `Log In`
- Language selector: `English`

The browser's developer tools show the following network request details:

```
Request to https://datenraum.ztp.at:443 [10.0.3.11]
Forward Drop Intercept is on Action Open Browser
Pretty Raw in Actions
1 POST /accounts/Login/?next=/ HTTP/1.1
2 Host: datenraum.ztp.at
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-GB,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://datenraum.ztp.at/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 139
10 Origin: https://datenraum.ztp.at
11 Connection: close
12 Cookie: sfcstoken=ncrUbyZ2iJrBtybNF9v3nvQ8rn7GNC5FRWxt9yskCIeA9kfs9j; sessionId=a8ijxpma10lmf2j0btf8e
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=v6qs79gBIhsyRbXCh0zftBwOGFe4f2cZqVpK1KAJbYMKp2k&login=rieder%40ztp.at&password=&next=%2F
```

V3: Session-Management

Request

```
1 POST /accounts/login/?next=/ HTTP/1.1
2 Host: datenraum.ztp.at
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
  Firefox/88.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-GB,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://datenraum.ztp.at/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 139
10 Origin: https://datenraum.ztp.at
11 Connection: close
12 Cookie: sfcsrcftoken=
  nCrUbY2ZiJrBtYbNF9v3nvQ8rn7GNC5rFWXnt9yskCIeA9kf59jG6pe
  a8ijxpma10lmf2j0bt8seltv
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=
  v8qs79gBIhsyRBbXChozftBw0GFe4f2cZqWvpkP1KaJbYMkp2HccYnZ
  rieder%40ztp.at&password=
  &next=%2F
```

Response

```
1 HTTP/1.1 302 Found
2 Server: nginx
3 Date: Wed, 28 Apr 2021 13:37:53 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 0
6 Connection: close
7 Location: /
8 Expires: Wed, 28 Apr 2021 13:37:53 GMT
9 Cache-Control: max-age=0, no-cache, no-store, must-revalidate
10 Vary: Accept-Language, Cookie
11 Content-Language: en
12 Set-Cookie: sessionId=44o6kuf1wkzgoY3omtvrbbE
13 Strict-Transport-Security: max-age=31536000; includeSubDomains
14 X-XSS-Protection: 1; mode=block
15 X-Frame-Options: SAMEORIGIN
16 Content-Security-Policy: default-src 'none'; script-src http://seafiler.com/ ht
17 Referrer-Policy: strict-origin
18
19
```

V5: Eingabeprüfung

The screenshot displays the ZTP web interface with an 'Add User' modal form open. The form contains the following fields:

- Email: te<script>st@ztp.at
- Name(optional):
- Password: [masked]
- Password again: [masked]

Buttons for 'Cancel' and 'Submit' are visible at the bottom right of the modal.

Below the modal, the Burp Suite interface shows an HTTP history entry for a GET request to `/api/v2.1/admin/users/rieder%40zt...` with a status of 200. The request details are as follows:

```
Request
Pretty Raw \n Actions
1 POST /api/v2.1/admin/users/ HTTP/1.1
2 Host: datenraum.ztp.at
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-GB,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://datenraum.ztp.at/
8 X-CSRFToken: nCrUbyZ2iJrBtYbNF9v3nvQ8rn7GNCSrFWXnt9yskCIeA9kf59jG6peBj
9 Content-Type: multipart/form-data; boundary=-----342981171427449305752591636855
10 Content-Length: 425
11 Origin: https://datenraum.ztp.at
12 Connection: close
13 Cookie: sfcsrftoken=nCrUbyZ2iJrBtYbNF9v3nvQ8rn7GNCSrFWXnt9yskCIeA9kf5; sessionid=44a6kuf1wkzgoY3omtvrbb9;
14
15
16 Content-Disposition: form-data; name="email"
17
18 te<script>st@ztp.at
19
20 Content-Disposition: form-data; name="name"
21
```

The response details are as follows:

```
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 400 Bad Request
2 Server: nginx
3 Date: Wed, 28 Apr 2021 13:41:13 GMT
4 Content-Type: application/json
5 Content-Length: 30
6 Connection: close
7 Allow: GET, POST, HEAD, OPTIONS
8 Vary: Accept-Language, Cookie
9 Content-Language: en
10 Strict-Transport-Security: max-age=31536000; includeSubDomains
11 X-XSS-Protection: 1; mode=block
12 X-Frame-Options: SAMEORIGIN
13 Content-Security-Policy: default-src 'none'; script-src http://seafiler.com/
14 Referrer-Policy: strict-origin
15
16 {
17   "error_msg": "email invalid."
18 }
```



V9: Kommunikation

```
Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): final
NPN/SPDY   h2, http/1.1 (advertised)
ALPN/HTTP2 |2, http/1.1 (offered)

Testing cipher categories

NULL ciphers (no encryption)          not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)         not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) not offered (OK)
Triple DES Ciphers / IDEA             not offered
Obsolete CBC ciphers (AES, ARIA etc.) not offered
Strong encryption (AEAD ciphers)      offered (OK)

Testing robust (perfect) forward secrecy. (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4

PFS is offered (OK)
TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-CHACHA20-POLY1305 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256

Elliptic curves offered:
DH group offered:
prime256v1 secp384r1 secp521r1 X25519 X448
ffdhe2048

Testing server preferences

Has server cipher order? no (NOT OK)
Negotiated protocol     TLSv1.3
Negotiated cipher       TLS_AES_256_GCM_SHA384, 256 bit ECDH (X25519) (limited sense as client will pick)
Negotiated cipher per proto (limited sense as client will pick)
ECDHE-RSA-AES256-GCM-SHA384: TLSv1.2
TLS_AES_128_GCM_SHA256: TLSv1.3
No further cipher order check has been done as order is determined by the client
```

V13: API und Web Services

The screenshot displays the 'Request' and 'Response' sections of a web browser's developer tools. The 'Request' section shows a GET request to an API endpoint with various headers and cookies. The 'Response' section shows a JSON response with file metadata.

Request

```
1 GET /api/v2.1/repos/35aa3bdd-b2b6-41c7-a2a8-.../dir/?p=%2F&with_thumbnail=true HTTP/1.1
2 Host: datenraum.ztp.at
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-GB,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://datenraum.ztp.at/
8 X-CSRFToken: nCrUbYZ2iJrBtYbNF9v3nvQ8rn7GNC5rRWXnt9yskCIeA9kf59
9 Connection: close
10 Cookie: sfcsrftoken=nCrUbYZ2iJrBtYbNF9v3nvQ8rn7GNC5rRWXnt9yskCIeA9kf59jG6p...; sessionId=h218jusvsv23becylgockrne
11
12
```

Response

```
10 Strict-Transport-Security: max-age=31536000, includeSubdomains
11 X-XSS-Protection: 1; mode=block
12 X-Frame-Options: SAMEORIGIN
13 Content-Security-Policy: default-src 'none'; script-src http://seafiler.com/
14 Referrer-Policy: strict-origin
15
16 {
  "user_perm": "rw",
  "dir_id": "78bf4eb37fb12c1e025d99d45f...",
  "dirent_list": [
    {
      "type": "file",
      "id": "c11e9e49ad69ee81fc26bc5729...",
      "name": "...",
      "mtime": 1615144151,
      "permission": "rw",
      "parent_dir": "/",
      "size": 6144,
      "modifier_email": "rieder@ztp.at",
      "modifier_name": "Dominik Rieder",
      "modifier_contact_email": "rieder@ztp.at",
      "starred": false
    }
  ]
}
```

Cyber-Sicherheit Gutachten und Zertifikat

ztp.digital



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: Bössartiger 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.	Bössartiger 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







Zusammenfassung

Zusammenfassung

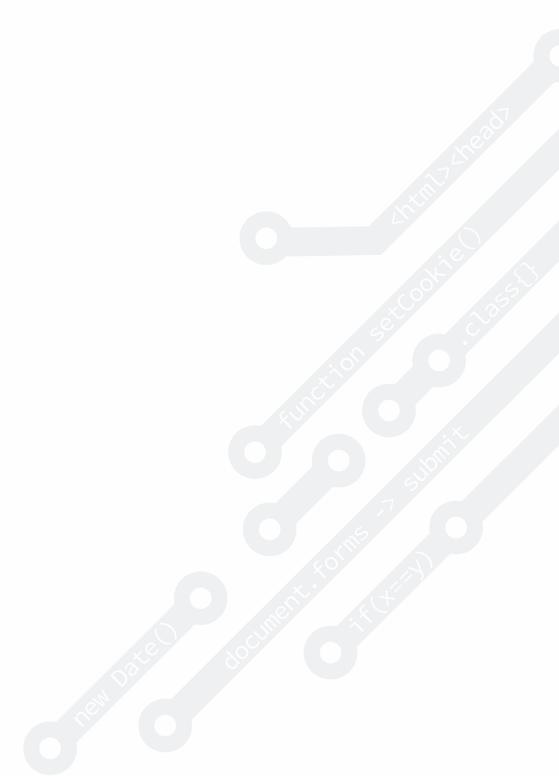
- Standard PenTest-Berichte sind wichtig, bei Auseinandersetzungen aber zumeist zu wenig nachvollziehbar, formal und qualitativ
- Datenschutz-Gutachten und Zertifizierung mit erhöhter Beweiskraft vor Behörden und Gerichten nur vom IT-Ziviltechniker (ZTG §4 Abs. 3, ZPO §292)
- Beilage auch zum Abschlussbericht des Wirtschaftsprüfer bestens geeignet
- Mehraufwand ist eine Frage der Kosten und der Berufsethik



QUALIFIZIERTE STELLE
GEMÄSS DER NIS-DIREKTIVE

**FÜR KRITISCHE
INFRASTRUKTUREN
IN EUROPA**

Sonstiges





**Wir übernehmen die Kontrolle
Ihrer Unternehmensnetzwerke und Daten!**

SOCIAL HACKING
Red Team Operations

ZfP 
IT-PRÜFSTELLE

CYBERBELT – Ihr Internet-Sicherheitsgurt

- CYBERBELT: Promo Video [>>](#)
- CYBERBELT: Information Video [>>](#)
- CYBERBELT: WebSite [>>](#)



Besten Dank
für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?





TRUSTED THIRD PARTY

**CYBER-SECURITY
TEST CENTER**

ZTP.digital ZT-GmbH

T: +43 1 532 46 68 0

✉ office@ztp.digital

Wien . Niederösterreich . Vorarlberg

Prüfstelle für
Digitale Sicherheit

F: +43 1 532 46 68 - 20

🌐 www.ztp.digital

Austria . Europe