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

ZTP IT-PRÜFSTELLE

V1.0 . 03.05.2021 Wien

Wolfgang Prentner

Informatiker . IT-Ziviltechniker .
Gerichtssachverständiger

Dominik Rieder

Informatiker . IT-Ziviltechniker

Inhalt

1 Ausgangssituation

Ausgangssituation - Auftraggeber

Was braucht das Unternehmen?

(GF/Vorstand)

Sicherheit

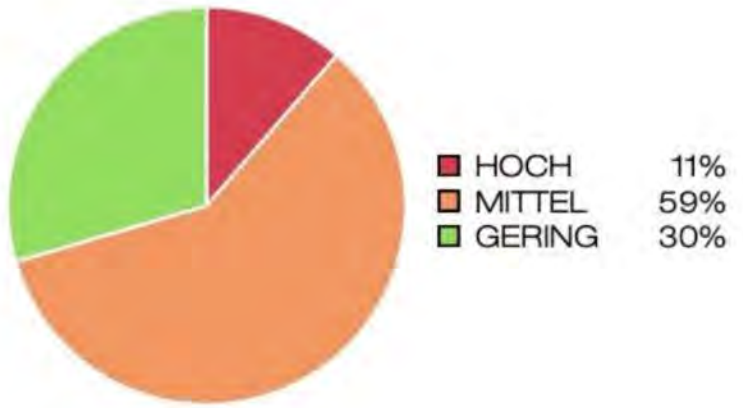
Ausgangssituation - PenTester

Was übernehmen PenTester?

Verantwortung für Cyber-Sicherheit und Haftung

Report Ergebnis

USA	
Hohes Risiko	5
Mittleres Risiko	26
Geringes Risiko	13



HERAUSFORDERUNGEN

- Ordentl. Kaufmann
- Techn. Gesetze
- Techn. Governance
- Techn. Compliance
- Techn. Standards

PROBLEME

- Cybercrime
- IT-Mitarbeiter
- IT-Dienstleister

LÖSUNG

INTERNET-SICHERHEITSGURT

CYBERBELT®

IT-Prüf- und Überwachungsstelle

Systeme . Software . Projekte . Datenschutz . IT-Kosten

DAS PLUS

- Haftung
- ... mit Brief und Siegel
- Zertifikat

ZTP IT-PRÜFSTELLE

Der IT-Ziviltechniker

Video >>

Wie werde ich

IT-Ziviltechniker?

mit staatlicher Befugnis

IT-Ziviltechniker

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

Quelle: https://www.oesterreich.gv.at/themen/dokumente_und_recht/zivilrecht/Sachverst%C3%A4ndigenhaftung.html

Haftung des Sachverständigen

- Haftung **verschärft**
- **für typische Fähigkeiten** einstehen
- **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

Sicherheits-Audit

Pentesting

Social Hacking
Red Team Operations

Code Analysen

mit **Zertifikat**

CYBERBELT®

IHR INTERNET-SICHERHEITSGURT

cyberbelt.net

ZTP

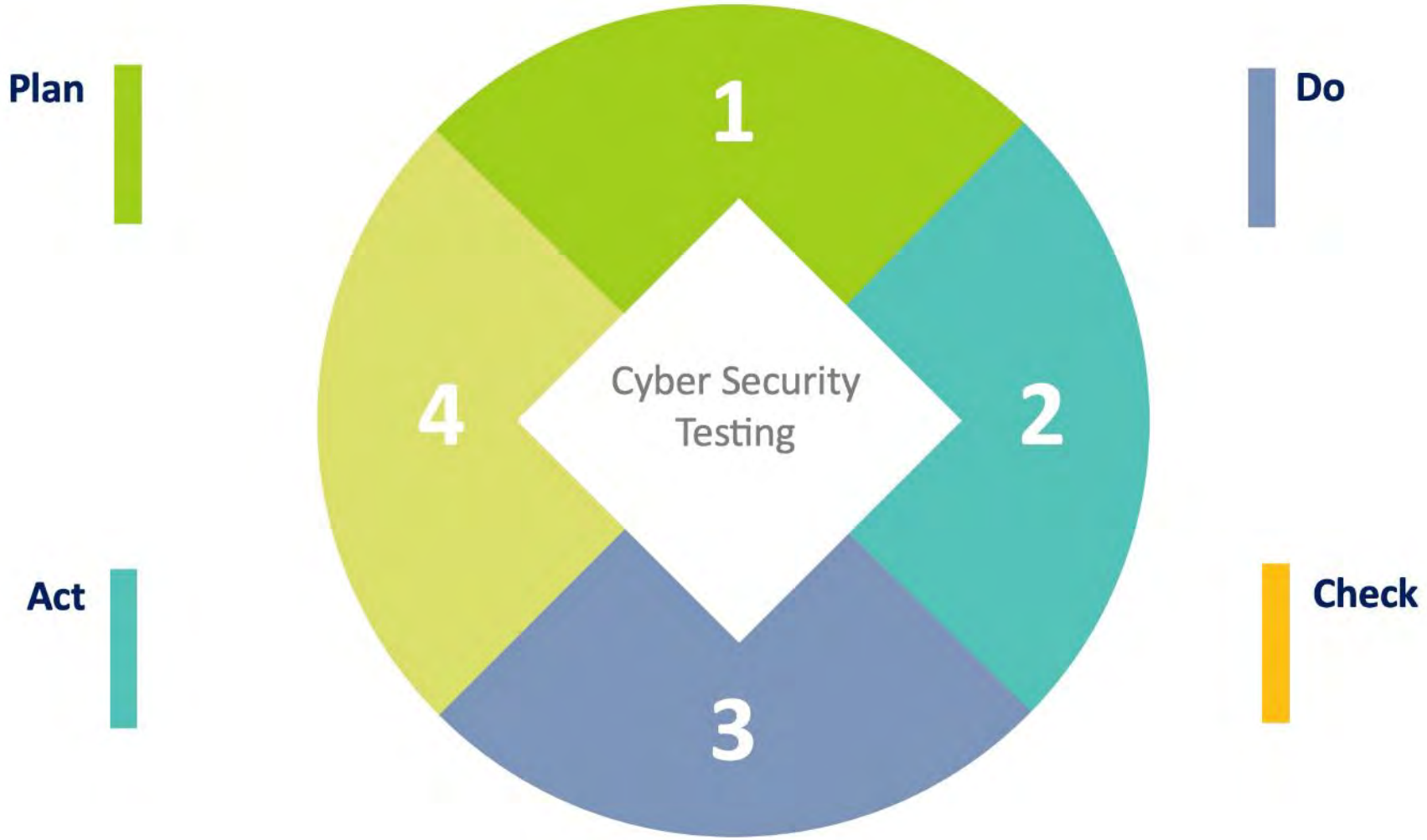
„Cyber Security Test Center (STC)“ Services

- 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)

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]

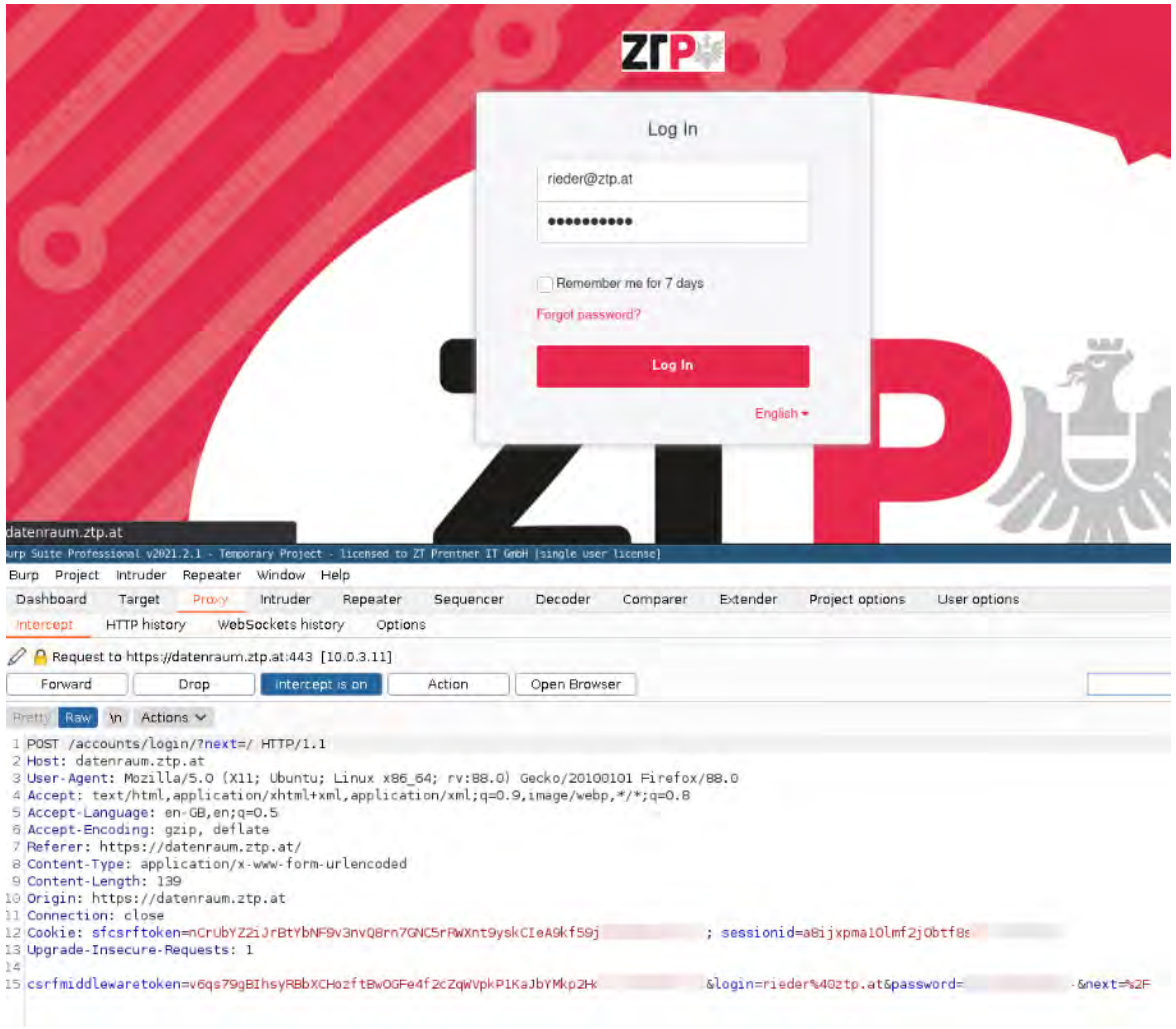
ASVS Verifikationsbereiche

- V1. Architektur, Design und Bedrohungsmodellierung
- V2. Authentifizierung
- V3. Session-Management
- V4. Zugriffssteuerung
- V5. Eingabeprüfung
- V6. Kryptographische Komponenten
- V7. Fehlerbehandlung und Protokollierung
- V8. Datenschutz
- V9. Kommunikation
- V10. Verhinderung von bösartigem 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 aufein-anderfolgende 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



V3: Session-Management

Request

Pretty | Raw | \n | Actions

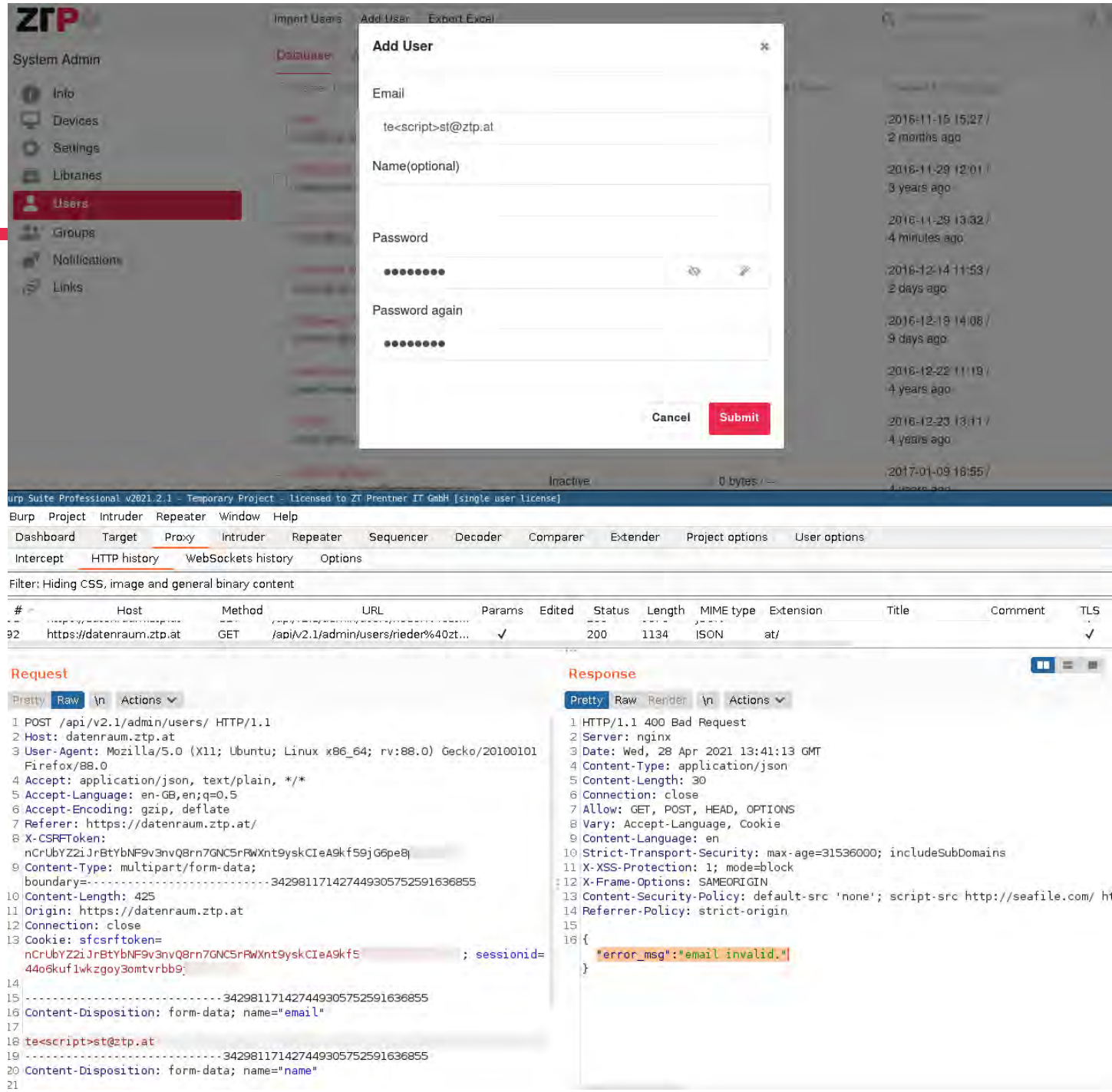
```
1 POST /accounts/login/?next=/ HTTP/1.1
2 Host: datenraum.ztp.at
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
  Firefox/88.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-GB,en;q=0.5
6 Accept-Encoding: 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: sfcsrftoken=
  nCrUbYZ2iJrBtYbNF9v3nvQ8rn7GNC5rRWXnt9yskCIeA9kf59jG6pe          ; sessionid=
  a8ijxpmal0lmf2j0btf8seltv
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=
  v6qs79gBIhsyRBbXCHozftBwOGFe4f2cZqWVpkP1KaJbYMkp2HccYnZ          &login=
  rieder%40ztp.at&password=              &next=%2F
```

Response

Pretty | Raw | Render | \n | Actions

```
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=44o6kuf1wkzgoy3omtvrbb          ; expires=Thu, 29-Apr-20
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://seafile.com/ ht
17 Referrer-Policy: strict-origin
18
19
```

V5: Eingabeprüfung



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 h2, 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:     prime256v1 secp384r1 secp521r1 X25519 X448
DH group offered:            ffdhe2048

Testing server preferences

Has server cipher order?     no (NOT ok)
Negotiated protocol          TLSv1.3
Negotiated cipher            TLS_AES_256_GCM_SHA384, 253 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

Request

Pretty | Raw | \n | Actions

```
1 GET /api/v2.1/repos/35aa3bdd-b2b6-41c7-a2a8-[redacted]/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[redacted]
9 Connection: close
10 Cookie: sfcsrftoken=
  nCrUbYZ2iJrBtYbNF9v3nvQ8rn7GNC5rRWXnt9yskCIeA9kf59jG6p[redacted]; sessionid=
  hz18jusvsv23becylgockrn[redacted]
11
12
```

Response

Pretty | Raw | Render | \n | Actions

```
11 X-XSS-Protection: 1; mode=block
12 X-Frame-Options: SAMEORIGIN
13 Content-Security-Policy: default-src 'none'; script-src http://seafile.com/ h
14 Referrer-Policy: strict-origin
15
16 {
    "user_perm":"rw",
    "dir_id":"78bf4eb37fb12c1e025d99d45f[redacted]",
    "dirent_list":[
      {
        "type":"file",
        "id":"c11e9e49ad69ee81fc26bc5729[redacted]",
        "name":"[redacted]",
        "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

Cyber-Sicherheit Auditing

GUTACHTEN
AUDITS UND PRÜFBERICHTE

Ziviltechnikergutachten

nach Application Security Verification Standard . ASVS Version 4.0.1

[redacted] ▪ Lfd.Nr.: 59 ▪ Version 1.0 ▪ Final ▪ freigegeben ▪ vertraulich

Wien, am 10. Februar 2021

ZTP

Inhaltsverzeichnis

ZTP

Abbildungsverzeichnis

ZERTIFIKATE

5 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


CYBER SICHERHEIT
ZTP
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
ZTP
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
Prüfstelle für
Digitale Sicherheit

T: +43 1 532 46 68 0
F: +43 1 532 46 68 - 20

✉ office@ztp.digital
💻 www.ztp.digital

Wien . Niederösterreich . Vorarlberg
Austria . Europe

ZTP
IT-PRÜFSTELLE