Pentestwerk

Pentest-Bericht

Kundenportal und REST-API der Musterwerk AG

Musterbericht. Firma, Systeme, Adressen und Befunde sind erfunden.

Dokument

PW-2026-MUSTER-CH-01

Version

1.0 vom 24.11.2026

Testzeitraum

16. bis 18. November 2026, 3 Testtage

Testtiefe

Grey Box

Durchgeführt von

Pentestwerk, Prüfer mit CISA

Vertraulichkeit

Vertraulich, nur für den Auftraggeber

Dokumentinformationen

Auftraggeber	Musterwerk AG (fiktiv), IT-Leitung
Auftragnehmer	Pentestwerk, eine Marke der Stratdata GmbH
Prüfer	Penetrationstester und IT-Sicherheitsauditor (CISA, CompTIA SecurityX); im echten Bericht mit Namen
Grundlage	Schriftliche Beauftragung vom 9.11.2026 mit Zielsystemen, Testfenster und Notfallkontakt; Vertrag zur Auftragsbearbeitung nach Art. 9 DSG
Verteiler	IT-Leitung, Leitung Entwicklung, CISO

1. Zusammenfassung für die Geschäftsleitung

> **Prüfstatus:** Alle vereinbarten Zielsysteme wurden vollständig getestet. Wie vereinbart nicht Teil des Tests: Lasttests, Social Engineering, die Geschäftslogik der Bestellabläufe (dafür ist ein separater Source-Code-Test nötig). Offen ist der Retest nach deiner Behebung.

Wir haben das Kundenportal, die REST-API, das Backoffice und die von aussen erreichbaren Server der Musterwerk AG drei Tage lang aus Sicht eines Angreifers geprüft, mit Testkonten für drei Rollen. Dabei haben wir zehn Schwachstellen gefunden: eine kritische, zwei hohe, vier mittlere und drei niedrige.

Die kritische Schwachstelle PW-01 hätte es jedem im Internet erlaubt, den Portal-Server zu übernehmen. Wir haben sie am ersten Testtag gemeldet, deine IT hat sie am selben Tag geschlossen. Die zwei hohen Befunde betreffen die API: Ein angemeldeter Kunde kann Daten anderer Kunden lesen und ändern (PW-02) und sich selbst Administratorrechte geben (PW-03). Beide Fehler haben dieselbe Ursache: Die Rechte werden in der Oberfläche durchgesetzt, aber nicht auf dem Server.

Gut gelöst sind die Abwehr von SQL-Injection, der Datei-Upload, das Zurücksetzen von Passwörtern und der CSRF-Schutz. Die Liste aller Prüfungen ohne Befund steht in Kapitel 4.

10 Befunde nach Schweregrad (CVSS 4.0)



Kritisch 1 Hoch 2 Mittel 4 Niedrig 3

Die drei wichtigsten Massnahmen

1. Rechte in der API bei jedem Zugriff auf dem Server prüfen: Objekt gehört zur eigenen Firma (PW-02), Rolle darf die Funktion nutzen (PW-03).
2. Prüfen, ob PW-01 und PW-02 vor dem Test ausgenutzt wurden, und bei Bedarf mit der Datenschutzberatung die Meldepflicht nach Art. 24 DSG klären.
3. Ausgaben im Backoffice kodieren und Sitzungen beim Abmelden beenden (PW-07, PW-05).

Übersicht der Befunde

ID	Schwere-grad	CVSS	Befund	Status
PW-01	Kritisch	9.3	Verwaltungsoberfläche des Anwendungsservers aus dem Internet erreichbar, Standardzugang aktiv	behoben (16.11.)
PW-02	Hoch	8.6	Fremde Kundenkonten über geänderte Kundennummer abrufbar und änderbar	offen
PW-03	Hoch	7.1	Rolle «Einkauf» kann über die API Administratoren der eigenen Firma anlegen	offen
PW-04	Mittel	6.9	Anmeldung ohne Begrenzung der Versuche, Benutzerkonten erkennbar	offen
PW-05	Mittel	6.0	Sitzung bleibt nach dem Abmelden gültig	offen
PW-06	Mittel	5.3	Veraltete JavaScript-Bibliothek mit bekannten Schwachstellen	offen
PW-07	Mittel	5.1	Gespeichertes Cross-Site-Scripting im Feld «Lieferhinweis»	offen
PW-08	Niedrig	2.3	Sicherheitsheader fehlen (Content-Security-Policy, HSTS)	offen
PW-09	Niedrig	2.3	Mailserver erlaubt noch TLS 1.0 und TLS 1.1	offen
PW-10	Niedrig	2.1	Portal lässt sich in fremde Seiten einbetten (Clickjacking)	offen

2. Umfang und Vorgehen

Zielsysteme	portal.musterwerk.example (Kundenportal), api.musterwerk.example/v2 (REST-API), backoffice.musterwerk.example, Server 192.0.2.10 bis 192.0.2.12
Testkonten	«Einkauf» und «Administrator Kunde» der Testfirma 10471, «Sachbearbeitung» im Backoffice
Ausgeschlossen	Lasttests, Social Engineering, Zahlungsdienstleister, Geschäftslogik der Bestellabläufe
Testfenster	Montag bis Freitag, 8 bis 18 Uhr, Produktion; Notfallkontakt: IT-Leitung
Methodik	PTES; OWASP WSTG 4.2, OWASP Top 10:2025, OWASP API Security Top 10 (2023)
Bewertung	CVSS 4.0, Basiswert. Kritisch 9.0 bis 10.0, Hoch 7.0 bis 8.9, Mittel 4.0 bis 6.9, Niedrig 0.1 bis 3.9 (Skala von FIRST)

Alle Tests liefen manuell, unterstützt durch Werkzeuge. Jeder Befund ist mit einem Nachweis belegt. Personendaten sind im Bericht geschwärzt; Testdaten haben wir nach dem Test zurückgesetzt oder gelöscht.

3. Befunde im Detail

PW-01 Verwaltungsoberfläche des Anwendungsservers aus dem Internet erreichbar, Standardzugang aktiv

Schweregrad	Kritisch 9.3
Betroffen	192.0.2.10, Port 8443 (Server des Kundenportals)
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`
Status	Sofort gemeldet am 16.11.2026, 14:20 Uhr. Port seit 16.11.2026, 16:05 Uhr gesperrt, beim Nachsehen am 18.11.2026 bestätigt.

Beschreibung

Auf Port 8443 des Portal-Servers antwortet die Verwaltungsoberfläche des Anwendungsservers. Die Oberfläche ist ohne Einschränkung aus dem Internet erreichbar. Die Anmeldung gelang mit dem Zugang, den der Hersteller im Handbuch als Standard angibt.

Nachweis

Erreichbarkeit von aussen

```
$ nmap -Pn -sV -p 8443 192.0.2.10
PORT     STATE SERVICE  VERSION
8443/tcp open  ssl/http [Anwendungsserver, Version geschwärzt]
```

Anmeldung mit Standardzugang

```
GET /verwaltung/ HTTP/1.1
Host: 192.0.2.10:8443
Authorization: Basic [Standardzugang laut Handbuch, geschwärzt]

HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8

<title>Anwendungsverwaltung</title> … Anwendung hochladen … Anwendung starten
…
```

Auswirkung

Wer die Oberfläche kennt, kann eigene Anwendungen hochladen und auf dem Server ausführen. Damit liegen das Portal, seine Datenbankverbindung und alle Kundendaten offen. Wir haben das nicht ausgenutzt, sondern den Fund sofort dem Notfallkontakt gemeldet.

Empfehlung

Verwaltungsoberfläche aus dem Internet entfernen oder nur über VPN erreichbar machen. Standardzugang löschen, eigene Konten mit starkem Passwort und zweitem Faktor anlegen. Prüfen, ob der Zugang vor dem Test schon genutzt wurde (Protokolle der Verwaltungsoberfläche, Liste der installierten Anwendungen).

Referenzen: CWE-1392 Use of Default Credentials; OWASP Top 10:2025 A02 Security Misconfiguration

---

PW-02 Fremde Kundenkonten über geänderte Kundennummer abrufbar und änderbar

Schweregrad	Hoch 8.6
Betroffen	api.musterwerk.example, /api/v2/kunden/{kundennummer}
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N`
Status	Offen

Beschreibung

Die API prüft nur, ob ein gültiges Anmeldetoken vorliegt, nicht aber, ob die angefragte Kundennummer zur eigenen Firma gehört. Die Kundennummern sind fortlaufend. Mit dem Testkonto der Firma 10471 liessen sich Stammdaten der Firma 10482 lesen und ändern.

Nachweis

Lesen fremder Stammdaten

```
GET /api/v2/kunden/10482 HTTP/1.1
Host: api.musterwerk.example
Authorization: Bearer [Token Testkonto «Einkauf», Kunde 10471]

HTTP/1.1 200 OK
Content-Type: application/json

{"kundennummer":10482,"firma":"[geschwärzt]","ansprechpartner":"[geschwärzt]",
 "lieferadresse":{"strasse":"[geschwärzt]","ort":"
[geschwärzt]"},"zahlungsziel":30}
```

Ändern der fremden Lieferadresse (danach sofort zurückgesetzt)

```
PUT /api/v2/kunden/10482/lieferadresse HTTP/1.1
Host: api.musterwerk.example
Authorization: Bearer [Token Testkonto «Einkauf», Kunde 10471]
Content-Type: application/json

{"strasse":"Teststrasse 1","plz":"0000","ort":"Testort"}

HTTP/1.1 204 No Content
```

Auswirkung

Jeder angemeldete Kunde kann die Stammdaten aller anderen Kunden lesen und ändern, darunter Ansprechpersonen und Lieferadressen. Ein Angreifer könnte Lieferungen umleiten. Betroffen sind Personendaten. Kläre mit deiner Datenschutzberatung, ob eine Meldung an den EDÖB nach Art. 24 DSG nötig ist, falls die Lücke vor dem Test genutzt wurde.

Empfehlung

Bei jedem Zugriff serverseitig prüfen, ob das Objekt zur Firma des angemeldeten Kontos gehört. Diese Prüfung zentral umsetzen, nicht in jedem Endpunkt einzeln. Für alle Endpunkte mit Objekt-IDs automatische Tests mit zwei Firmenkonten ergänzen. Zugriffsprotokolle der API auf auffällige Abrufe fremder Kundennummern auswerten.

Referenzen: CWE-639 Authorization Bypass Through User-Controlled Key; OWASP API Security Top 10 2023 API1 Broken Object Level Authorization; OWASP Top 10:2025 A01 Broken Access Control

---

PW-03 Rolle «Einkauf» kann über die API Administratoren der eigenen

Firma anlegen

Schweregrad	Hoch 7.1
Betroffen	api.musterwerk.example, POST /api/v2/firma/benutzer
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N`
Status	Offen

Beschreibung

In der Weboberfläche sieht die Rolle «Einkauf» keine Benutzerverwaltung. Die API nimmt den Aufruf zum Anlegen von Benutzern trotzdem an, auch mit der Rolle «Administrator». Die Rechte werden also nur in der Oberfläche ausgeblendet, nicht auf dem Server geprüft.

Nachweis

Neues Administratorkonto mit dem Konto «Einkauf»

```
POST /api/v2/firma/benutzer HTTP/1.1
Host: api.musterwerk.example
Authorization: Bearer [Token Testkonto «Einkauf»]
Content-Type: application/json

{"email":"pw-test-admin@musterwerk.example","rolle":"administrator"}

HTTP/1.1 201 Created
{"id":5531,"rolle":"administrator"}
```

Auswirkung

Jede Person mit Einkaufsrechten kann sich selbst oder Dritten Administratorrechte für das Firmenkonto geben, Bestellungen freigeben und Benutzer sperren. Das Testkonto 5531 haben wir nach dem Nachweis gelöscht.

Empfehlung

Rollen und Rechte für jede Funktion auf dem Server prüfen. Eine Rechtematrix je Rolle festlegen und als automatischen Test hinterlegen. Bestehende Konten auf unerwartete Administratoren prüfen.

Referenzen: CWE-285 Improper Authorization; OWASP API Security Top 10 2023 API5 Broken Function Level Authorization; OWASP Top 10:2025 A01 Broken Access Control

PW-04 Anmeldung ohne Begrenzung der Versuche, Benutzerkonten erkennbar

Schweregrad	Mittel 6.9
Betroffen	portal.musterwerk.example/anmelden
CVSS 4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
Status	Offen

Beschreibung

Wir haben 500 Anmeldeversuche mit falschem Passwort in vier Minuten an das eigene Testkonto geschickt. Es gab keine Sperre und keine Verzögerung. Die Fehlermeldung lautet je nach Fall «Benutzer unbekannt» oder «Passwort falsch». So lässt sich prüfen, welche E-Mail-Adressen ein Konto haben.

Nachweis

Unterschiedliche Antworten

```
POST /anmelden  email=gibt-es-nicht@musterwerk.example  ->  «Benutzer
unbekannt»
POST /anmelden  email=[Testkonto]                       ->  «Passwort
falsch»
```

Keine Begrenzung

```
500 Versuche in 4 Minuten, alle mit HTTP 200 und gleicher Antwortzeit,
kein Captcha, keine Kontosperre, keine Benachrichtigung an das Konto
```

Auswirkung

Angreifer können gültige Kundenkonten sammeln und dann geleakte oder einfache Passwörter durchprobieren. Konten ohne zweiten Faktor sind dadurch gefährdet.

Empfehlung

Einheitliche Fehlermeldung für beide Fälle. Anmeldeversuche je Konto und je Quelle begrenzen und schrittweise verzögern. Zweiten Faktor zumindest für Administratoren anbieten. Fehlgeschlagene Anmeldungen überwachen.

Referenzen: CWE-307 Improper Restriction of Excessive Authentication Attempts; CWE-204 Observable Response Discrepancy; OWASP Top 10:2025 A07 Authentication Failures

PW-05 Sitzung bleibt nach dem Abmelden gültig

Schweregrad	Mittel 6.0
Betroffen	portal.musterwerk.example, Sitzungscookie
CVSS 4.0	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N
Status	Offen

Beschreibung

Beim Abmelden löscht das Portal nur das Cookie im Browser. Auf dem Server bleibt die Sitzung 24 Stunden gültig. Mit dem zuvor kopierten Cookie war das Kundenkonto nach dem Abmelden weiter nutzbar.

Nachweis

Wiederverwendung nach dem Abmelden

```
POST /abmelden            -> 302 /anmelden (Cookie im Browser gelöscht)
GET /konto  Cookie: sitzung=[alter Wert]

HTTP/1.1 200 OK  … Willkommen, [Testkonto] …
```

Auswirkung

Wer an ein Sitzungscookie kommt, etwa an einem gemeinsam genutzten Rechner oder über eine Schwachstelle wie PW-07, behält den Zugang auch dann, wenn sich die Person abmeldet.

Empfehlung

Sitzung beim Abmelden auf dem Server beenden. Sitzungen nach einer festgelegten Zeit ohne Aktivität beenden, zum Beispiel nach 30 Minuten. Bei Passwortänderung alle Sitzungen des Kontos beenden.

Referenzen: CWE-613 Insufficient Session Expiration; OWASP Top 10:2025 A07 Authentication Failures

PW-06 Veraltete JavaScript-Bibliothek mit bekannten Schwachstellen

Schweregrad	Mittel 5.3
Betroffen	portal.musterwerk.example/assets/js/vendor/jquery-3.4.1.min.js
CVSS 4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
Status	Offen

Beschreibung

Das Portal lädt jQuery 3.4.1. Für diese Version sind zwei Schwachstellen veröffentlicht, die Cross-Site-Scripting ermöglichen, wenn HTML aus fremden Quellen an bestimmte jQuery-Funktionen übergeben wird. Eine ausnutzbare Stelle haben wir im Portal nicht gefunden.

Nachweis

Version

```
GET /assets/js/vendor/jquery-3.4.1.min.js

/*! jQuery v3.4.1 | (c) JS Foundation and other contributors |
jquery.org/license */
```

Auswirkung

Das Risiko hängt davon ab, wie der eigene Code jQuery verwendet. Neue Funktionen könnten die Lücke unbemerkt ausnutzbar machen.

Empfehlung

jQuery auf die aktuelle Version aktualisieren. Ein Verzeichnis aller Fremdbibliotheken führen (zum Beispiel als SBOM) und regelmässig gegen bekannte Schwachstellen prüfen.

Referenzen: CVE-2020-11022, CVE-2020-11023 (behoben in jQuery 3.5.0); CWE-1395 Dependency on Vulnerable Third-Party Component; OWASP Top 10:2025 A03 Software Supply Chain Failures

PW-07 Gespeichertes Cross-Site-Scripting im Feld «Lieferhinweis»

Schweregrad	Mittel 5.1
Betroffen	portal.musterwerk.example/bestellung, Anzeige im Backoffice /backoffice/bestellungen
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N`
Status	Offen

Beschreibung

Kunden können zu einer Bestellung einen Lieferhinweis eingeben. Das Portal speichert den Text ungefiltert. In der Bestellansicht des Backoffice wird er ohne Kodierung ausgegeben. Ein Skript im Hinweis lief beim Öffnen der Bestellung im Konto der Sachbearbeitung.

Nachweis

Eingabe als Kunde

```
Lieferhinweis: <img src=x onerror=alert(document.domain)>
```

Ausgabe im Backoffice

```
<td class="hinweis"><img src=x onerror=alert(document.domain)></td>

-> Meldung «backoffice.musterwerk.example» im Browser des Testkontos
«Sachbearbeitung»
```

Auswirkung

Ein Kunde könnte Skripte im Browser deiner Mitarbeitenden ausführen, etwa um Bestellungen im Namen der Sachbearbeitung zu ändern. Zusammen mit PW-05 könnte er eine Sitzung des Backoffice übernehmen.

Empfehlung

Alle Ausgaben passend zum Kontext kodieren (HTML, Attribut, JavaScript). Eingaben auf erwartete Zeichen prüfen. Im Backoffice eine Content-Security-Policy ohne Inline-Skripte setzen (siehe PW-08).

Referenzen: CWE-79 Improper Neutralization of Input During Web Page Generation; OWASP Top 10:2025 A05 Injection

PW-08 Sicherheitsheader fehlen (Content-Security-Policy, HSTS)

Schweregrad	Niedrig 2.3
Betroffen	portal.musterwerk.example, backoffice.musterwerk.example
CVSS 4.0	`CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N`
Status	Offen

Beschreibung

Portal und Backoffice senden weder eine Content-Security-Policy noch Strict-Transport-Security. Beide Header sind keine Lücke für sich, begrenzen aber die Folgen anderer Fehler.

Nachweis

Antwortkopf

```
HTTP/1.1 200 OK
Server: [geschwärzt]
Content-Type: text/html; charset=utf-8
Set-Cookie: sitzung=…; Path=/; HttpOnly; Secure
(kein Content-Security-Policy, kein Strict-Transport-Security)
```

Auswirkung

Ohne CSP wirken Fehler wie PW-07 stärker. Ohne HSTS kann ein Angreifer im selben Netz den ersten Aufruf über unverschlüsseltes HTTP abfangen.

Empfehlung

Strict-Transport-Security mit mindestens einem Jahr Gültigkeit setzen. Eine Content-Security-Policy einführen, zuerst im Berichtsmodus, dann verbindlich.

Referenzen: CWE-693 Protection Mechanism Failure; OWASP Top 10:2025 A02 Security Misconfiguration

---

PW-09 Mailserver erlaubt noch TLS 1.0 und TLS 1.1

Schweregrad	Niedrig 2.3
Betroffen	mail.musterwerk.example (192.0.2.12), Ports 25 und 587
CVSS 4.0	`CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N`
Status	Offen

Beschreibung

Der Mailserver akzeptiert bei STARTTLS neben TLS 1.2 und 1.3 auch die veralteten Versionen TLS 1.0 und 1.1. Die IETF hat TLS 1.0 und TLS 1.1 mit RFC 8996 im März 2021 offiziell abgekündigt.

Nachweis

Ausgehandelte Versionen

```
$ openssl s_client -starttls smtp -connect 192.0.2.12:587 -tls1
… Protocol  : TLSv1
$ openssl s_client -starttls smtp -connect 192.0.2.12:587 -tls1_1
… Protocol  : TLSv1.1
```

Auswirkung

Gering, solange beide Seiten TLS 1.2 oder 1.3 können. Veraltete Gegenstellen fallen aber auf schwache Verfahren zurück.

Empfehlung

TLS 1.0 und 1.1 abschalten. Danach Zustellung an wichtige Partner einmal prüfen.

Referenzen: CWE-327 Use of a Broken or Risky Cryptographic Algorithm; RFC 8996; OWASP Top 10:2025 A04 Cryptographic Failures

---

PW-10 Portal lässt sich in fremde Seiten einbetten (Clickjacking)

Schweregrad	Niedrig 2.1
Betroffen	portal.musterwerk.example
CVSS 4.0	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
Status	Offen

Beschreibung

Das Portal setzt weder X-Frame-Options noch die CSP-Anweisung frame-ancestors. Eine fremde Seite kann das Portal unsichtbar einbetten und Klicks darauf lenken.

Nachweis

Einbettung in eine Testseite

```
<iframe src="https://portal.musterwerk.example/bestellung"></iframe>

-> Portal wird im Rahmen geladen und ist bedienbar
```

Auswirkung

Ein Angreifer könnte angemeldete Kunden dazu bringen, unbemerkt Aktionen im Portal auszulösen, etwa eine Bestellung abzuschicken. Dafür braucht er die aktive Mitwirkung der Person.

Empfehlung

In der Content-Security-Policy frame-ancestors 'self' setzen, für ältere Browser zusätzlich X-Frame-Options: DENY.

Referenzen: CWE-1021 Improper Restriction of Rendered UI Layers or Frames; OWASP Top 10:2025 A02 Security Misconfiguration

4. Geprüft ohne Befund

SQL-Injection	Suche, Filter, Sortierung und alle API-Parameter: keine Injektion möglich, Abfragen sind parametrisiert.
Datei-Upload	Anhänge zu Bestellungen: Dateityp, Grösse und Ablageort werden serverseitig geprüft; Skripte wurden nicht ausgeführt.
Passwort zurücksetzen	Link ist einmalig gültig und läuft nach 30 Minuten ab; keine Kontoübernahme möglich.
CSRF	Formulare und zustandsändernde API-Aufrufe verlangen ein gültiges Token.
Trennung zwischen Kundenfirmen in der Weboberfläche	In der Oberfläche selbst kein Zugriff auf fremde Firmen; betroffen ist nur die API (PW-02).
TLS am Portal	Nur TLS 1.2 und 1.3, aktuelle Zertifikatskette.
Offene Dateien und Verzeichnisse	Keine Sicherungsdateien, kein .git-Verzeichnis, keine Verzeichnisauflistung gefunden.
Externe Angriffsfläche	Auf 192.0.2.10 bis 192.0.2.12 nur die erwarteten Dienste (443, 25, 587) und der Port aus PW-01.

5. Massnahmenplan

Frist	Befund	Massnahme	Aufwand	Zuständig	Stand
Sofort	PW-01	Verwaltungsoberfläche sperren, Standardzugang löschen, Protokolle prüfen	gering	Betrieb	erledigt am 16.11.
Sofort	PW-02	Objektprüfung in der API, Zugriffe auswerten	mittel	Entwicklung	offen
Sofort	PW-03	Rollenprüfung je Funktion auf dem Server	mittel	Entwicklung	offen
30 Tage	PW-07	Ausgaben im Backoffice kodieren	gering	Entwicklung	offen
30 Tage	PW-04	Begrenzung der Anmeldeversuche, einheitliche Meldung	gering	Entwicklung	offen
30 Tage	PW-05	Sitzung beim Abmelden serverseitig beenden	gering	Entwicklung	offen
90 Tage	PW-06	jQuery aktualisieren, Bibliotheken inventarisieren	gering	Entwicklung	offen
90 Tage	PW-08, PW-10	CSP mit frame-ancestors und HSTS setzen	mittel	Entwicklung	offen

Frist	Befund	Massnahme	Auf-wand	Zu-ständig	Stand
90 Tage	PW-09	TLS 1.0 und 1.1 am Mailserver abschalten	ge-ring	Be-trieb	offen

Nach der Behebung prüfen wir die Befunde im Retest erneut (ab CHF 800) und ergänzen diesen Bericht um den Status jedes Befunds.

Anhang A: Testprotokoll

16.11.2026, 08:45	Freigabe und Testfenster mit IT-Leitung bestätigt, Testkonten erhalten
16.11.2026	Externe Angriffsfläche 192.0.2.10 bis 192.0.2.12, TLS, Portal ohne Anmeldung
16.11.2026, 14:20	PW-01 telefonisch und per Mail an den Notfallkontakt gemeldet
16.11.2026, 16:05	Rückmeldung der IT: Port 8443 von aussen gesperrt
17.11.2026	Portal mit den Rollen «Einkauf» und «Administrator Kunde», REST-API v2
18.11.2026	Backoffice mit der Rolle «Sachbearbeitung», Sitzungen, Nachsehen PW-01
18.11.2026, 17:10	Testende, Testkonto 5531 gelöscht, geänderte Lieferadresse zurückgesetzt
24.11.2026	Bericht Version 1.0 übergeben
26.11.2026	Ergebnisbesprechung mit Entwicklung und IT-Leitung

Anhang B: Begriffe

CVSS
Common Vulnerability Scoring System, ein offener Standard von FIRST zur Bewertung der Schwere von Schwachstellen auf einer Skala von 0 bis 10.

Grey Box
Test mit Testkonten und grobem Wissen über das System, aber ohne Quellcode.

IDOR / BOLA
Zugriff auf fremde Objekte, indem man eine Kennung in der Anfrage ändert, weil der Server die Berechtigung nicht prüft.

Cross-Site-Scripting (XSS)

Fremder Skriptcode, der im Browser anderer Nutzer ausgeführt wird.

Clickjacking

Eine fremde Seite bettet die Anwendung unsichtbar ein und lenkt Klicks darauf.