

ERGEBNISBERICHT PENETRATIONSTEST

VERSION 1.0 | 27.02.2025

Abschlussbericht für Firma Soundso
Musterstraße 23
123456 Musterstadt

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden

Autoren
Max Mustertester

INHALTSVERZEICHNIS

1. DISCLAIMER.....	4
2. Zusammenfassung.....	5
2.1. Prüfung der Systeme über das Internet	5
2.2. Prüfung Webanwendung über das Internet	7
3. Allgemeines.....	9
3.1. Schwachstellenbewertung	9
3.2. Darstellung	10
4. Prüfung der Systeme über das Internet.....	11
4.1. Beschreibung der Vorgehensweise und des Ziels	11
4.2. Projektverlauf und Ergebnisdarstellung	14
4.2.1. Übersicht der Schwachstellen	14
S_01 Verwundbare phpMyAdmin-Version im Einsatz	14
S_02 Verwundbare Apache2-Version im Einsatz.....	16
S_03 Denial-of-Service durch DHE-Schlüsselaustausch (D(HE)ater-Angriff)	18
S_04 Verwundbares Transportverschlüsselungsprotokoll im Einsatz.....	21
4.2.2. Sicherheitshinweise.....	23
H_01 Nicht BSI-konforme Cipher Suites/ Verschlüsselungsprotokolle im Einsatz.....	23
H_02 Nicht BSI-konforme SSH-Verschlüsselungsprotokolle im Einsatz.....	24
4.2.3. Übersicht der geprüften IP-Adressen	25
5. Prüfung Webanwendung über das Internet	26
5.1. Beschreibung der Vorgehensweise und des Ziels	26
5.2. Projektverlauf und Ergebnisdarstellung	30
5.2.1. Übersicht der Schwachstellen	30
W_01 Cross-Site-Request-Forgery-Angriffe (CSRF) möglich	30
W_02 Brute-Force-Angriff auf Login-Maske möglich.....	34
W_03 Bearbeiten von Kundenaufträgen mit Rolle „Personal“ möglich	37
W_04 Unsichere Kommunikation	41
5.2.2. Zuordnung der Schwachstellen zu den OWASP Top 10.....	44
5.2.3. Ergebnisse der Überprüfung des Reichtmodells	44
H_03 Unzureichende Passwortrichtlinie	45
H_04 Unsichere Content-Security-Policy im Einsatz.....	45
6. Anhang A: Versionen und Verzeichnisse	47
6.1. Versionshistorie	47

6.2.	Abbildungsverzeichnis	47
6.3.	Tabellenverzeichnis	48
7.	Anhang B: Ermittlung des Sicherheitsniveaus	49
7.1.	Ermittlung Sicherheitsniveau systembasierter Penetrationstest	49
7.2.	Ermittlung Sicherheitsniveau Webanwendungspenetrationstest	50

1. DISCLAIMER

Der vorliegende Ergebnisbericht bildet einen **exemplarischen Ergebnisbericht** ab, der um kundenspezifische Inhalte gekürzt wurde. Damit stellt dieser Bericht einen nicht vollumfänglichen Bericht dar und kann je nach Anforderungsprofil auch inhaltlich vom angebotenen Projekt abweichen. Weitere Abweichungen können durch kundenspezifische Anpassungen der Informationstiefe entstehen.

In einem realen Ergebnisbericht werden in einem zusätzlichen Anhang dieses Berichts alle Reports der genutzten Tools übergeben, ebenso wie eine Gesamtliste aller Systeme inklusive deren Schwachstellen und offenen Ports.

Wir legen großen Wert darauf, die Schwachstellenbeschreibungen **in den Kontext des Kunden** und des System- bzw. Anwendungszweckes zu setzen. Da diese Beschreibungen selbstverständlich Ableitungen zum jeweiligen Kunden enthalten würden, konnten diese in den Beispielbericht nicht aufgenommen werden.

Dieses Dokument ist ausschließlich zur Verwendung im Kontext der Anfrage gedacht und darf daher nicht an Dritte weitergegeben werden.

2. ZUSAMMENFASSUNG

2.1. Prüfung der Systeme über das Internet

Im Zeitraum vom 10. bis zum 21. Februar 2025 wurde ein Netzsegment des Kunden einer Sicherheitsprüfung in Form eines technischen Penetrationstests unterzogen. Ziel der Prüfung war die Identifikation von Schwachstellen über das Netzwerk auf Systemebene.

Im Fokus der Prüfungen stand das Netzwerksegment XXX.XXX.XXX.0/24.

Die Prüfung fand über das Internet statt. Bei den geprüften Adressen handelt es sich um Adressen, die in einer Testumgebung verwendet werden.

Insgesamt lässt sich der getesteten Gesamtumgebung ein niedriges Sicherheitsniveau attestieren, da ein System mit einem kritischen Sicherheitsniveau, sowie zwei Systeme mit einem niedrigen Sicherheitsniveau identifiziert wurden.

Tabelle 1: Statistik: Sicherheitsniveau pro geprüfter IP-Adresse Prüfung der Systeme über das Internet

Anzahl Prüfobjekte		Anzahl Adressen m. Sicherheitsniveau					Gesamtbewertung Sicherheitsniveau
Gesamt	Erreichbar	Kritisch	Niedrig	Mittel	Hoch	Sehr hoch	
254	10	1	2	1	1	5	Niedrig

Im Rahmen der Untersuchung konnten vier Schwachstellen identifiziert werden. Diese werden nachfolgend nach dem *Schweregrad der Schwachstelle* absteigend sortiert aufgelistet. Eine genaue Zuordnung der Schwachstellen zu den geprüften Adressen erfolgt im Kapitel 4.2.3. und das daraus resultierende Sicherheitsniveau einer Adresse wird im Anhang B (siehe Kapitel 7.1.) erläutert.

Kritisch S_01 Verwundbare phpMyAdmin-Version im Einsatz

Während der Prüfungen wurde die Verwendung der phpMyAdmin-Version 4.9.5 festgestellt. Für diese Version sind Schwachstellen bekannt, die Angreifern ermöglichen, schadhafter Code in die Datenbank einzuführen und so unbefugten Zugriff auf oder die Manipulation sensibler Daten zu ermöglichen.

Hoch S_02 Verwundbare Apache2-Version im Einsatz

Es wurde ein Webserver identifiziert, der eine verwundbare Version von Apache2 verwendet. Für diese Version sind Schwachstellen bekannt, die es Angreifern ermöglichen, Autorisierungsregeln zu umgehen und unerlaubt auf Inhalte zuzugreifen.

Mittel S_03 Denial-of-Service durch DHE-Schlüsselaustausch (D(HE)ater-Angriff)

Bei mehreren Adressen werden kryptographische Mechanismen (Cipher Suites) angeboten, die ausgenutzt werden können, um einen Denial-of-Service-Angriff durchzuführen. Da diese Art von Angriffen nicht im Rahmen der Prüfung lag, wurde nicht versucht, diesen Umstand auszunutzen. Daher kann nicht abschließend eingeschätzt werden, ob die betroffenen Adressen tatsächlich

verwundbar sind. Dennoch wird diese Schwachstelle aufgeführt, da die Möglichkeit für einen Denial-of-Service-Angriff gegeben ist.

Niedrig S_04 Verwundbares Transportverschlüsselungsprotokoll im Einsatz

Bei der Prüfung wurden mehrere Dienste (u. a. Webserver) identifiziert, die verschlüsselt über das TLS-Protokoll kommunizieren. Diese Dienste bieten Verschlüsselungsmöglichkeiten an, die nicht dem Stand der Technik (nach Technischer Richtlinie 02102 des Bundesamts für Sicherheit in der Informationstechnik¹) entsprechen und für die teilweise Angriffe bekannt sind, die die Verschlüsselung aushebeln können.

Weiterhin wurden Sicherheitshinweise identifiziert, von denen kein direktes Risiko ausgeht und die somit auch keine direkte Schwachstelle darstellen. Durch die Beseitigung dieser Sicherheitshinweise lässt sich jedoch das Sicherheitsniveau der betroffenen Dienste erhöhen. Informationen zu den identifizierten Sicherheitshinweisen befinden sich in Kapitel 4.2.2.

Eine detaillierte Beschreibung des angewandten Verfahrens findet sich in Kapitel 4.1.

¹

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2>

2.2. Prüfung Webanwendung über das Internet

Im Zeitraum vom 10. bis zum 21. Februar 2025 wurden die unter <https://www.beispiel-kunde.de> erreichbare Webanwendung des Kunden einer Sicherheitsüberprüfung in Form eines technischen Penetrationstests auf Anwendungsebene unterzogen. Ziel der Prüfung war die Identifikation von technischen Schwachstellen in der Anwendung.

Die Prüfung fand über das Internet statt. Die Anwendung wurde in einer Testumgebung geprüft.

Insgesamt lässt sich der Gesamtumgebung ein mittleres Sicherheitsniveau attestieren, da eine Schwachstelle mit hohem Schweregrad, sowie eine Schwachstelle mit einem mittleren Schweregrad identifiziert werden konnte.

Tabelle 2: Statistik: Identifizierte Schwachstellen Penetrationstest Soundso

Gesamtanzahl		Anzahl Schwachstellen (Schweregrad)				Gesamtbewertung Sicherheitsniveau
Schwachstellen	Sicherheits-hinweise	Kritisch	Hoch	Mittel	Niedrig	
3	2	0	1	1	1	Mittel

Im Rahmen der Untersuchung konnten 3 Schwachstellen identifiziert werden. Diese werden nachfolgend nach dem *Schweregrad der Schwachstelle* absteigend sortiert aufgelistet. Das resultierende Sicherheitsniveau der Anwendung wird im Anhang B (siehe Kapitel 7.2. erläutert.

Hoch W_01 Cross-Site-Request-Forgery-Angriffe (CSRF) möglich

Die Schwachstelle wird dadurch verursacht, dass die Webanwendung nicht überprüft, von welcher Quelle Anfragen gesendet werden und auch Anfragen bearbeitet, die von anderen Websites abgeschickt werden. Angreifer können hierdurch beispielsweise Schad-Websites erstellen, die die Daten des Benutzers verändern oder Aktionen im Namen des Benutzers ausführen (z. B. neue User anlegen, Passwort ändern), sodass Angreifer hierüber potentiell auch Benutzerkonten übernehmen können. Damit dieser Angriff durchführbar ist, muss der angegriffene Benutzer in die Anwendung eingeloggt sein und eine speziell präparierte Schad-Websites des Angreifers aufrufen.

Mittel W_02 Brute-Force-Angriff auf Login-Maske möglich

Die Webanwendung bietet keinen Schutz vor Brute-Force-Angriffen. Bei den Prüfungen wurde im Zeitraum weniger Sekunden 25-mal ein falsches Passwort angegeben. Nach diesen fehlerhaften Versuchen war eine Anmeldung mit dem validen Passwort möglich. Es erfolgte keine Benachrichtigung des Benutzers über die fehlgeschlagenen Anmeldeversuche. Ein Angreifer wäre somit in der Lage, durch Ausprobieren von Benutzernamen und Passwörter Kombinationen, das richtige Passwort zu erraten und so Zugang zum Account zu erhalten

Niedrig W_03 Bearbeiten von Kundenaufträgen mit Rolle „Personal“ möglich

Die Webanwendung ermöglicht es Benutzern mit der Rolle „Personal“, durch das Senden manipulierten Serveranfragen die Details beliebiger Kundenaufträge zu verändern, sofern die Auftragsnummer bekannt ist. Ein Angreifer mit Zugriff auf ein Benutzerkonto der Rolle „Personal“

kann auf diese Weise das Rechtemodell der Anwendung umgehen und sensible Daten manipulieren

Niedrig W_04 Unsichere Kommunikation

In der Webanwendung werden die Daten auf unsichere Art und Weise übertragen. Die Daten werden unverschlüsselt und ohne Integritätsschutz übertragen. Somit können alle übertragenen Informationen, wie zum Beispiel Zugangsdaten von Angreifern mitgelesen und manipuliert werden.

Weiterhin wurden Sicherheitshinweise identifiziert, von denen kein direktes Risiko ausgeht und die somit auch keine direkte Schwachstelle darstellen. Durch die Beseitigung dieser Sicherheitshinweise lässt sich jedoch das Sicherheitsniveau der Anwendung erhöhen. Informationen zu den identifizierten Sicherheitshinweisen befinden sich in Kapitel 5.2.3.

Eine detaillierte Beschreibung des angewandten Verfahrens findet sich in Kapitel 5.1.

3. ALLGEMEINES

Allgemeine Informationen zur Struktur des Ergebnisberichts erfolgen in diesem Kapitel. Die Ergebnisse der Prüfung werden entsprechend der Projektschritte in eigenen Kapiteln dargestellt.

Sämtliche Ergebnisse sind nur für die zum Zeitpunkt der Prüfung jeweils eingesetzte Konfiguration gültig. Nach der Prüfung neu veröffentlichte oder durch Änderungen an den Systemen und Anwendungen eingebrachte Schwachstellen können nicht vorab erkannt werden. Rückschlüsse auf die zukünftige Robustheit können daher nur bedingt vom vorliegenden Ergebnis abgeleitet werden. Sofern größere Änderungen erfolgen, kann eine Nachprüfung sinnvoll sein.

Die Tests wurden mit einem durch den Projektrahmen definierten Aufwand durchgeführt. Durch die Vorgehensweise ist sichergestellt, dass innerhalb dieses Zeitfensters eine möglichst hohe Testabdeckung erreicht wird. Eine vollständige Testabdeckung ist durch die Art der Prüfungen und die naturgemäß limitierte Zeitvorgabe nicht möglich.

3.1. Schwachstellenbewertung

Zur Ermittlung des Schweregrads von Schwachstellen wird das Common Vulnerability Scoring System (CVSS) in Version 4 verwendet.² CVSS ist der Industriestandard zur Bewertung von Schwachstellen und wurde von der Organisation FIRST (Forum of Incident Response and Security Teams) entwickelt.

In der IT-Sicherheit hat sich der „Defense-in-Depth“-Ansatz durchgesetzt. Dies bedeutet, dass alle wirtschaftlich sinnvollen Maßnahmen auf allen Ebenen der IT getroffen werden, um nachhaltige Resilienz zu erzielen. So werden z. B. Empfehlungen des BSI für Kryptographie herangezogen und Abweichungen aufgezeigt, auch wenn keine direkt ausnutzbaren Schwachstellen aus den Abweichungen resultieren.

Die Basis-Bewertung („Base Score“) gibt den Schweregrad dieser Schwachstelle an und bezieht sich auf die durchgeführten Testfälle und das Verhalten der Testgegenstände. Eine Beachtung des vollständigen Kontextes innerhalb der Kundenumgebung kann im Rahmen von Penetrationstests nur eingeschränkt erfolgen. Die Bewertung stellt somit keine abschließende Risikobewertung nach gängigen Normen (bspw. ISO 27005) dar. Die Berechnung der Basis-Bewertung wird durch den Prüfer für alle selbstständig identifizierten Schwachstellen vorgenommen.

Häufig ergeben sich auch Schwachstellen durch die Verwendung von (veralteter) Software mit öffentlich bekannten Schwachstellen. Hier ist meist nur bekannt, dass die Version verwundbar ist, jedoch sind sehr häufig keine Details über die genaue Art der Schwachstelle, ihre Ausnutzbarkeit und ihre genauen Auswirkungen öffentlich bekannt.

In diesen Fällen kann durch den Prüfer keine manuelle Bewertung durchgeführt werden, da die Informationslage dies nicht zulässt und es in diesen Fällen auch nicht zielführend wäre, die notwendige Schwachstellenforschung im Rahmen des Kundenprojekts durchzuführen. Stattdessen referenzieren wir hier Angaben aus vertrauenswürdigen Schwachstellendatenbanken oder direkt vom Hersteller der betroffenen Software.

Bitte beachten Sie, dass bei einer solchen Referenzierung möglicherweise Bewertungen herangezogen werden müssen, die mit einer älteren CVSS-Version berechnet wurden. Gerade bei lange bekannten Schwachstellen oder besonders alten Versionen werden die CVSS-Bewertungen in den Schwachstellenmeldungen der Hersteller bzw. der Schwachstellendatenbanken häufig nicht auf die jeweils neueste CVSS-Version aktualisiert.

² <https://www.first.org/cvss/>

Für eine Risikobewertung und -behandlung durch den Kunden wird für jede Schwachstellenbewertung die entsprechende Vektorenzeichenkette (Vector-String) angegeben. Eine Anpassung an den jeweiligen Anwendungskontext kann durch den Kunden bspw. mit den CVSS Environmental Metrics erfolgen.

3.2. Darstellung

Das Ziel der Sicherheitsüberprüfung sowie die Vorgehensweise zum Erreichen des definierten Ziels sind für die Prüfungen in eigenen Kapiteln beschrieben. Dies erlaubt eine nachvollziehbare Arbeitsweise und ein Verständnis für die beschriebenen Testergebnisse.

Sämtliche Ergebnisreports der eingesetzten Werkzeuge zur automatisierten Erkennung von Schwachstellen werden zusammen mit diesem Ergebnisbericht übergeben. Alle Ergebnisse der Werkzeuge wurden manuell verifiziert und bewertet. Sofern ein Ergebnis aus den Reports nicht in diesen Ergebnisbericht überführt wurde, handelt es sich hierbei um ein False Positive bzw. ist das Ergebnis für das Ziel nicht relevant.

Um eine schnelle Auffindbarkeit der identifizierten Schwachstellen zu gewährleisten, wird für jede Schwachstelle eine eindeutige Kennung genutzt. Jede Schwachstelle wird zunächst allgemein beschrieben und die möglichen Auswirkungen benannt. Anschließend erfolgen eine individuelle Schweregradbewertung und eine Handlungsempfehlung zur Behebung der Schwachstelle.

Wir bemühen uns stets, möglichst deutsche Begrifflichkeiten zu verwenden, sofern die englischen Begriffe nicht zu sehr auch im deutschen Sprachraum verbreitet sind. Ggf. stehen geprägte Anglizismen in Klammern. Dies erleichtert die Lesbarkeit sowohl Lesern, die ein entsprechendes Hintergrundwissen mitbringen, als auch Lesern, die bisher kein Spezialwissen aufbauen konnten.

Zur besseren Übersicht sind alle verwendeten Begriffserläuterungen auf unserer Homepage unter <https://www.secuvera.de/download/penetrationstest-glossar/> zu finden und werden daher im Fließtext nicht beschrieben. Sollte eine Erläuterung fehlen, bitten wir Sie um eine kurze Nachricht.

Zur besseren Referenzierung werden Schwachstellen jeweils mit im Dokument fortlaufendem und damit eindeutigem Index versehen. Nachfolgend wird die Nomenklatur beschrieben:

- S_ Schwachstellen bei Systemprüfungen,
- W_ Schwachstellen bei Webanwendungsprüfungen.

Während der Prüfung werden möglicherweise Sicherheitsprobleme identifiziert, die nicht klar als Schwachstelle zu bewerten sind, etwa weil von ihnen kein direktes Risiko ausgeht oder es sich nur um Abweichungen von gängigen Sicherheitsstandards bzw. Best-Practices handelt. Der CVSS-Score solcher Feststellungen ist üblicherweise „None“, sie werden im Bericht als Sicherheitshinweise dokumentiert und mit der folgenden Nomenklatur beschrieben:

- H_ Sicherheitshinweis bei einem Penetrationstest.

Da von Sicherheitshinweisen kein direktes Risiko ausgeht, werden diese bei der Ermittlung von Sicherheitsniveaus nicht beachtet.

4. PRÜFUNG DER SYSTEME ÜBER DAS INTERNET

4.1. Beschreibung der Vorgehensweise und des Ziels

Im Zeitraum vom 10. bis zum 21. Februar 2025 wurde ein Netzsegment des Kunden einer Sicherheitsprüfung in Form eines technischen Penetrationstests unterzogen. Ziel der Prüfung war die Identifikation von Schwachstellen auf Systemebene.

Hierfür wurden durch den Kunden die folgenden Adressen des Netzsegmentes übergeben:

Tabelle 3: Auflistung geprüfetes Netzwerksegment

Netzwerksegment (CIDR)	Anzahl geprüfter Host-adressen ³	Erste Hostadresse	Letzte Hostadresse
XXX.XXX.XXX.0/24	254	XXX.XXX.XXX.1	XXX.XXX.XXX.254

Die Prüfungen fanden über das Internet statt. Bei den geprüften Systemen handelt es sich um Systeme, die in einer Testumgebung stehen.

Prüfungen auf erreichbare Dienste, Verschlüsselungseigenschaften und bekannte Schwachstellen

Die Prüfungen der Adressen wurden vollständig mit dem eigens entwickelten Framework „tajanas“ durchgeführt. Tajanas basiert auf den etablierten Werkzeugen „nmap“⁴ für Portscans, „testssl“⁵ für die Überprüfung der Verschlüsselung der Daten auf dem Transportweg mittels TLS sowie „OpenVAS“⁶ für die Schwachstellenanalyse. Im Framework tajanas werden die Werkzeuge intelligent miteinander verknüpft und die Ergebnisse in einheitlichen Berichten aufbereitet dargestellt.

Jede Adresse wurde dabei auf allen 65.535 Ports TCP und aufgrund des sonst sehr hohen Zeitaufwands auf den „Common Ports“ UDP überprüft. Ebenso wurde in diesem Rahmen versucht, durch Fingerprinting die Versionen der Dienste und Betriebssysteme zu erkennen.

Hierbei wurden die Dienste und Systeme so weit als möglich bezüglich folgender Eigenschaften erkannt:

- eingesetztes Betriebssystem,
- Name der Anwendungssoftware,
- Version der Anwendungssoftware.

Wurden Dienste identifiziert, die Daten auf einem geschützten Transportweg übertrugen, so wurden die angebotenen Transportverschlüsselungsprotokolle und Cipher Suites mit den Empfehlungen der Technischen Richtlinie TR-02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgeglichen.

Für die Bewertung der Ausnutzbarkeit von Schwachstellen, die als Folge einer fehlerhaften TLS-Konfiguration auftreten, wird die Annahme getroffen, dass aktuelle Clients eingesetzt werden. Als

³ Netzwerk- und Broadcast-Adressen werden nicht geprüft

⁴ <https://nmap.org/>

⁵ <https://testssl.sh/>

⁶ <http://www.openvas.org/index-de.html>

aktuelle Clients werden solche bezeichnet, bei denen alle Sicherheitsupdates (insbesondere von Browsern und TLS-Libraries), die weiter als ein Jahr zurückliegen, installiert sind.

Im Anschluss wurden die erreichbaren Dienste einer Analyse auf bekannte Schwachstellen unterzogen.

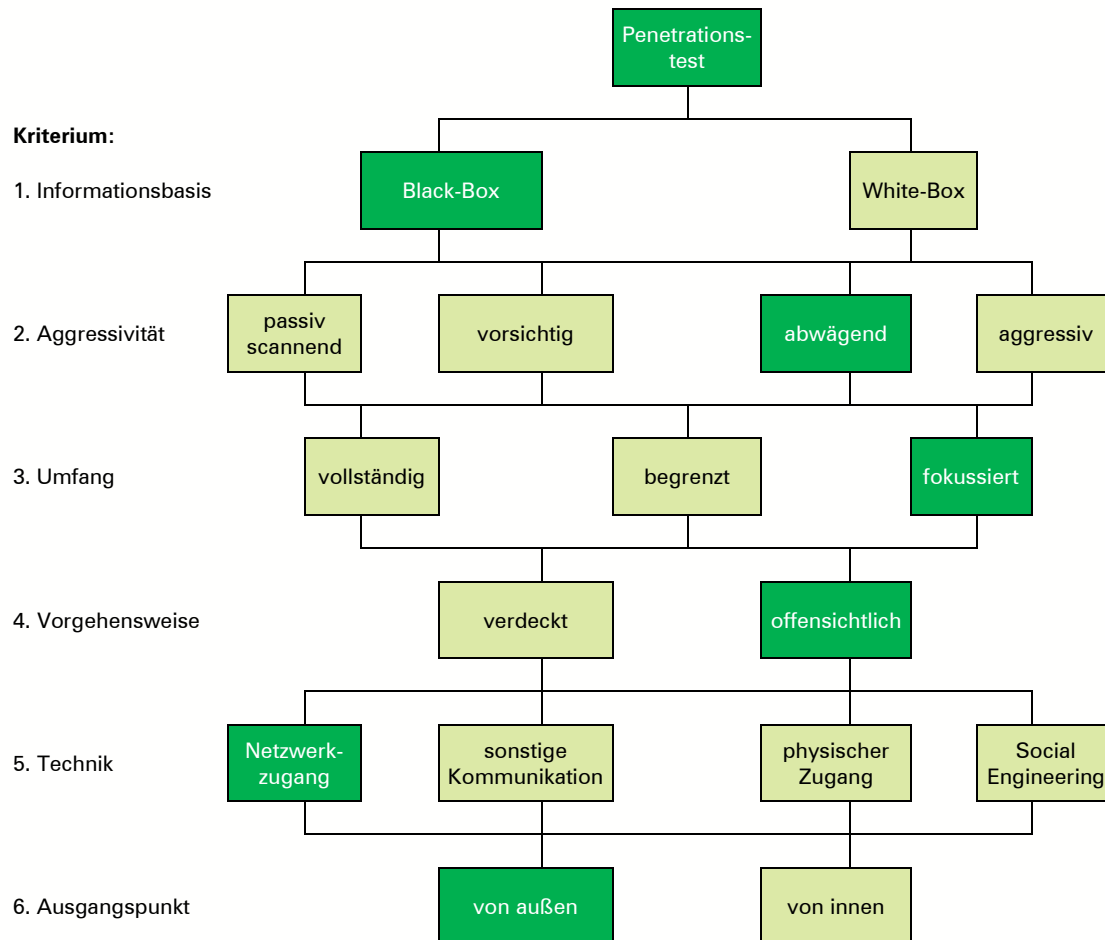
Prüfung auf Standardkennungen

Sofern SSH-Serverdienste erkannt wurden, wurden automatisch Standardbenutzerkennungen überprüft. Für Webanwendungen ist dies aufgrund der Individualität der Implementierung – auch von Standardsoftware – nur mit zusätzlichem Aufwand möglich. Dies war nicht Bestandteil des Auftrags, weshalb diese Prüfungen nicht durchgeführt wurden.

In vielen Linux-Distributionen werden Softwarepakete nicht aktuell gehalten. Behebungen von Schwachstellen werden neben Verbesserungen jedoch auch in den Paketen innerhalb der gleichen Versionsnummer behoben. Im Rahmen dieses Penetrationstests wurden möglicherweise veraltete Versionen festgestellt. Es ist von außen jedoch leider nicht bzw. nur mit Ausnutzung der möglicherweise vorhandenen Schwachstellen möglich, festzustellen, ob entweder eine veraltete Version mit Schwachstellen vorliegt oder eine Version mit Backports ohne Schwachstelle installiert ist. Daher sind alle Versionen mit möglichen Schwachstellen aufgeführt. Sie können uns gerne eine Liste der Systeme und Schwachstellen zur Verfügung stellen, auf denen Backports installiert sind. Wir aktualisieren gerne den Ergebnisbericht entsprechend.

Für den Penetrationstest wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“⁷ zugrunde gelegt:

Abbildung 1: Vorgehensweise nach BSI-Studie Prüfung Systeme über das Internet



⁷ <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.html>

4.2. Projektverlauf und Ergebnisdarstellung

Das Projekt konnte wie vorab geplant und in der Vorgehensweise beschrieben durchgeführt werden.

4.2.1. Übersicht der Schwachstellen

Zur besseren Lesbarkeit werden die Schwachstellen in diesem Kapitel beschrieben. Die Zuordnung zwischen den Schwachstellen und den konkreten IP-Adressen erfolgt in einem separaten Unterkapitel.

S_01

Verwundbare phpMyAdmin-Version im Einsatz

Beschreibung	Während der Prüfung wurde die Verwendung einer verwundbaren Version von phpMyAdmin (Version 4.9.4 wurde identifiziert) festgestellt., Für diese Version sind Schwachstellen bekannt.Auswirkung Durch das Ausnutzen der bekannten Schwachstellen ist ein Angreifer in der Lage, z. B. SQL injection-Angriffe durchzuführen (CVE-2020-26935).
Hinweis	Die Feststellung der Versionsnummer beruht auf Bannerinformationen aus der Serverantwort und den Analyseergebnissen der verwendeten Werkzeuge. Es wurde nicht versucht, die für diese Versionsnummer bekannten Schwachstellen auszunutzen. Da Bannerinformationen und Werkzeugergebnisse fehlerbehaftet sein können (z. B. durch die absichtliche Angabe einer falschen Versionsnummer), sollte überprüft werden, ob tatsächlich diese Version verwendet wird. Des Weiteren ist es möglich, dass das System bereits gegen bekannte Schwachstellen gepatcht wurde (Backporting), auch dies sollte durch den Kunden verifiziert werden.
Empfehlung	Aktualisierung der eingesetzten Software auf eine vom Hersteller unterstützte Version. Um der Schwachstelle nachhaltig zu begegnen, sollte das Vorgehen zum Patch- und Änderungsmanagement angepasst werden. Zur langfristigen Behebung der Schwachstelle sollte regelmäßig überprüft werden, ob die Software noch aktiv unterstützt wird und frühzeitig eine Migration auf eine neue Version geprüft werden. Um über Sicherheitsprobleme informiert zu werden, sollten die entsprechenden Mailinglisten abonniert werden.
Referenzen	https://www.cvedetails.com/vulnerability-list/vendor_id-784/product_id-1341/version_id-100425/Phpmyadmin-Phpmyadmin-3.3.7.html https://www.cvedetails.com/vulnerability-list/vendor_id-784/product_id-1341/version_id-205320/Phpmyadmin-Phpmyadmin-4.6.4.html
Schweregrad	Critical

Tabelle 4: Bewertung des Schweregrades Schwachstelle S_01

Schwachstellenbewertung entlang CVSS v3.1		
Referenz	https://nvd.nist.gov/vuln/detail/CVE-2020-26935	
Base Score	9,8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	
Temporal Score		
Metrik	Bewertung	Begründung der Wertewahl
Exploit Code Maturity (E)	Functional	Ein funktionaler Exploit ist öffentlich verfügbar.
Remediation Level (RL)	Official Fix	Der Hersteller hat eine aktualisierte Version zur Verfügung gestellt, in der die Schwachstelle behoben ist.
Report Confidence (RC)	Confirmed	Die Existenz der Schwachstelle wurde durch den Hersteller bestätigt.
Temporal Score	9,1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

S_02

Verwundbare Apache2-Version im Einsatz

Beschreibung	Es wurde ein Webserver identifiziert, der eine verwundbare Version von Apache2 (Version 2.4.41 wurde identifiziert) einsetzte. Für diese Apache-Version sind Schwachstellen bekannt.
Auswirkung	Der Webserver ist durch spezielle manipulierte Anfragen verwundbar. Nach Ausführen des Angriffs könnten Angreifer Autorisierungsregeln umgehen und unerlaubt auf Inhalte zugreifen (HTTP Request Smuggling, CVE-2023-25690).
Hinweis	Die Feststellung der Versionsnummer beruht auf Bannerinformationen aus der Serverantwort und den Analyseergebnissen der verwendeten Werkzeuge. Es wurde nicht versucht, die für diese Versionsnummer bekannten Schwachstellen auszunutzen. Da Bannerinformationen und Werkzeugergebnisse fehlerbehaftet sein können (z. B. durch die absichtliche Angabe einer falschen Versionsnummer), sollte überprüft werden, ob tatsächlich diese Version verwendet wird. Des Weiteren ist es möglich, dass das System bereits gegen bekannte Schwachstellen gepatcht wurde (Backporting), auch dies sollte durch den Kunden verifiziert werden. Da die Schwachstelle aus einer verwundbaren Softwareversion resultiert, beziehen wir uns bei der Bewertung des Schweregrads auf Aussagen des Herstellers oder aus verlässlichen Schwachstellendatenbanken.
Empfehlung	Aktualisierung der eingesetzten Software auf eine vom Hersteller unterstützte Version. Um der Schwachstelle nachhaltig zu begegnen, sollte das Vorgehen zum Patch- und Änderungsmanagement angepasst werden. Zur langfristigen Behebung der Schwachstelle sollte regelmäßig überprüft werden, ob die Software noch aktiv unterstützt wird, und frühzeitig eine Migration auf eine neue Version geprüft werden. Um über Sicherheitsprobleme informiert zu werden, sollten die entsprechenden Mailinglisten abonniert werden.
Referenzen	https://httpd.apache.org/security/vulnerabilities_24.html https://nvd.nist.gov/vuln/detail/CVE-2023-25690
Schweregrad	High

Tabelle 5: Bewertung des Schweregrades Schwachstelle S_02

Schwachstellenbewertung entlang CVSS v3.1		
Referenz	https://httpd.apache.org/security/vulnerabilities_24.html	
Base Score	9,8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	
Temporal Score		
Metrik	Bewertung	Begründung der Wertewahl
Exploit Code Maturity (E)	Proof-of-Concept	Ein Proof-of-Concept-Exploit-Code ist verfügbar, der jedoch an die Kundenumgebung angepasst werden muss.

Schwachstellenbewertung entlang CVSS v3.1		
Referenz	https://httpd.apache.org/security/vulnerabilities_24.html	
Base Score	9,8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	
Temporal Score		
Metrik	Bewertung	Begründung der Wertewahl
Remediation Level (RL)	Official Fix	Der Hersteller hat eine aktualisierte Version zur Verfügung gestellt, in der die Schwachstelle behoben ist.
Report Confidence (RC)	Confirmed	Die Existenz der Schwachstelle wurde durch den Hersteller bestätigt.
Temporal Score	8,8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

S_03

Denial-of-Service durch DHE-Schlüsselaustausch (D(HE)ater-Angriff)

Beschreibung	Es wurde eine abgesicherte Kommunikation festgestellt, bei der Cipher Suites angeboten werden, die den Schlüsselaustauschmechanismus „Diffie-Hellman Ephemeral“ (kurz „DHE“) verwenden.
Auswirkung	Die Verwendung des DHE-Schlüsselaustausches kann für Denial-of-Service-Angriffe missbraucht werden, indem Angreifer den Schlüsselaustausch bewusst falsch durchführen, was zur Folge hat, dass der Server unentwegt neue Schlüssel berechnet. Da die Schlüsselberechnung viel Rechenleistung beansprucht, ist es hierüber gegebenenfalls möglich, den Server auszulasten und seine Erreichbarkeit damit negativ zu beeinflussen. Dieser Angriff ist als „D(HE)ater“ bekannt (siehe Referenzen).
Beispiel	Der Serverdienst bietet die folgenden TLS-Cipher-Suites mit DHE-Schlüsselaustausch an: • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 Der Serverdienst bietet die folgenden Verschlüsselungsalgorithmen für den SSH-Schlüsselaustausch mit DHE an: • diffie-hellman-group14-sha256 • diffie-hellman-group14-sha256 • diffie-hellman-group18-sha512 • diffie-hellman-group-exchange-sha256
Hinweis	Es wurde nicht versucht, diese Schwäche auszunutzen, da Denial-of-Service-Angriffe nach Absprache nicht durchzuführen waren. Es kann daher nicht abschließend eingeschätzt werden, ob die Dienste tatsächlich verwundbar sind.
Empfehlung	Es sollte überprüft werden, ob die betroffenen Dienste tatsächlich verwundbar sind. Die Verwendung der im Hinweis genannten Cipher Suites sollte deaktiviert werden, sodass nur noch Cipher Suites mit dem ECDHE-Schlüsselaustausch (EC = „Elliptic Curve“) angeboten werden. Dieser Schlüsselaustausch ist zum aktuellen Zeitpunkt nicht verwundbar, da hier deutlich kürzere Schlüssellängen verwendet werden können als bei einem DHE-Schlüsselaustausch ohne elliptische Kurven. Durch die Verwendung von kürzeren Schlüssellängen beim ECDHE-Schlüsselaustausch verringert sich die benötigte Rechenleistung, was die Auswirkungen des Angriffs stark einschränkt.
Referenzen	https://github.com/Balasys/dheater
Schweregrad	Medium

Tabelle 6: Bewertung des Schweregrades Schwachstelle S_03

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	Low	Der Angreifer muss keine messbaren Maßnahmen ergreifen, um vorhandene sicherheitserhöhende Vorkehrungen aktiv zu umgehen oder zu überwinden, damit er die Schwachstelle ausnutzen kann.
Attack Requirements (AT)	None	Zum Ausnutzen der Schwachstelle müssen keine besonderen Anforderungen an die Konfiguration des Prüfgegenstandes erfüllt sein.
Privileges Required (PR)	None	Vor dem Ausnutzen der Schwachstelle benötigt ein Angreifer keine Authentifizierung am Prüfgegenstand.
User Interaction (UI)	None	Die Schwachstelle kann unabhängig von anderen Benutzern ausgenutzt werden.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Vertraulichkeit der Daten.
Integrity Impact (VI)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Integrität der Daten.
Availability Impact (VA)	Low	Durch Ausnutzen der Schwachstelle kann ein Angreifer die Verfügbarkeit des Prüfgegenstands einschränken, der Angriff ermöglicht jedoch keine vollständige oder langfristige Einschränkung der Verfügbarkeit.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.
Integrity Impact (SI)		
Availability Impact (SA)		

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
CVSS-B	6,9 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	

S_04

Verwundbares Transportverschlüsselungsprotokoll im Einsatz

Beschreibung	Bei der eingesetzten Transportverschlüsselung werden die verwundbaren Protokoll-versionen TLS 1.0/TLS 1.1 angeboten. Diese sind gegenüber einer Vielzahl von Angriffen verwundbar und sollten nicht mehr eingesetzt werden.
Auswirkung	Für die eingesetzten Protokollversionen sind mehrere Angriffe bekannt, mit denen es möglich ist, verschlüsselte Daten im Klartext auszulesen.
Empfehlung	Anpassung der Serverkonfiguration, sodass durch das System nur die aktuell empfohlenen Protokolle (TLS 1.2 und TLS 1.3) angeboten werden. Möglicherweise sind Clients im Einsatz, die die Empfehlungen des BSI nicht anwenden können. Dies ist vor allem bei Geräten der Fall, die nicht auf einem aktuellen Softwarestand gehalten werden, oder Hardware-Komponenten, für die das Gleiche gilt. Durch eine Änderung der Konfiguration würde dann keine Verbindung mehr zustande kommen können. Entsprechende Prüfungen sind vor der Produktivsetzung daher notwendig.
Referenzen	https://www.secuvera.de/blog/blogserie-zur-tls-konfiguration-technische-richtlinie-tr-02102-2-des-bsi/ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2 PDF „Konformitätsprüfung der Transportverschlüsselung“ (als Anhang zu diesem Dokument)
Schweregrad	Low

Tabelle 7: Bewertung des Schweregrades Schwachstelle S_04

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	Low	Der Angreifer muss keine messbaren Maßnahmen ergreifen, um vorhandene sicherheitserhöhende Vorkehrungen aktiv zu umgehen oder zu überwinden, damit er die Schwachstelle ausnutzen kann.
Attack Requirements (AT)	Present	Zum Ausnutzen der Schwachstelle muss der Angreifer sich in einem Machine-in-the-Middle-Szenario befinden.
Privileges Required (PR)	None	Vor dem Ausnutzen der Schwachstelle benötigt ein Angreifer keine Authentifizierung an der Anwendung.

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
User Interaction (UI)	Passive	Das Opfer muss Daten mit der Anwendung austauschen.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	Low	Durch Ausnutzen der Schwachstelle kann ein Angreifer sensible Daten einsehen, den Umfang der Daten jedoch nicht selbst bestimmen.
Integrity Impact (VI)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Integrität der Daten.
Availability Impact (VA)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der Anwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.
Integrity Impact (SI)		
Availability Impact (SA)		
CVSS-B	2.3 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

4.2.2. Sicherheitshinweise

Im Laufe der Prüfung fielen einige Probleme auf, die nicht klar als Schwachstelle klassifiziert werden können. Die Beseitigung dieser Probleme kann jedoch das allgemeine Sicherheitsniveau der Systeme zusätzlich erhöhen.

H_01 Nicht BSI-konforme Cipher Suites/ Verschlüsselungsprotokolle im Einsatz

Beschreibung	Es werden Cipher Suites für die verschlüsselte Kommunikation angeboten, die nicht konform zur Technischen Richtlinie TR-02102-02 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS)“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sind.
Auswirkung	In dieser Richtlinie wird empfohlen, nur die Verschlüsselungsprotokolle TLS 1.2 bzw. TLS 1.3 und die darin als sicher geltenden Cipher Suites zu nutzen. Eine Auflistung aller empfohlenen Cipher Suites findet sich in der TR in Kapitel 3.3.4 für TLS 1.2 und im Kapitel 3.4.4 für TLS 1.3. Die in dieser Richtlinie gegebenen Empfehlungen für die Verwendung von TLS werden durch die durchgeführte „Konformitätsprüfung der Transportverschlüsselung“ reflektiert. Dabei konnten Cipher Suites identifiziert werden, die aktuell nach dieser Technischen Richtlinie nicht mehr empfohlen werden.
Empfehlung	Anpassung der TLS-Konfiguration, sodass durch den Web- oder Application-Server nur die in der Richtlinie empfohlenen Protokolle und Cipher Suites angeboten werden. Möglicherweise sind Clients im Einsatz, die die Empfehlungen des BSI nicht anwenden können. Dies ist vor allem bei Geräten der Fall, die nicht auf einem aktuellen Softwarestand gehalten werden, oder Hardwarekomponenten, für die das Gleiche gilt. Durch eine Änderung der Konfiguration würde dann keine Verbindung mehr zustande kommen können. Entsprechende Prüfungen sind vor der Produktivsetzung daher notwendig.
Referenzen	https://www.secuvera.de/blog/blogserie-zur-tls-konfiguration-technische-richtlinie-tr-02102-2-des-bsi/ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2 PDF „Konformitätsprüfung der Transportverschlüsselung“ (als Anhang zu diesem Dokument)

H_02

Nicht BSI-konforme SSH-Verschlüsselungsprotokolle im Einsatz

Beschreibung	Die Konfigurationsanalyse des identifizierten Secure-Shell-Serverdienstes (SSH) ergab, dass kryptografische Verfahren für die verschlüsselte Kommunikation angeboten werden, die nicht konform zur Technischen Richtlinie TR-02102-04 „Kryptographische Verfahren: Teil 4 – Verwendung von Secure Shell (SSH)“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sind.
Auswirkung	In dieser Richtlinie wird empfohlen, nur das Verschlüsselungsprotokoll SSH Protokollversion 2 zu verwenden. Ferner werden Empfehlungen zu den einzusetzenden kryptografischen Verfahren und Schlüssellängen ausgesprochen. Die in dieser Richtlinie gegebenen Empfehlungen für die Verwendung von SSH werden durch die durchgeführte „Konformitätsprüfung der Transportverschlüsselung“ reflektiert. Dabei konnten Protokolle identifiziert werden, die aktuell nach dieser Technischen Richtlinie nicht mehr empfohlen werden.
Empfehlung	Anpassung der Serverkonfiguration, sodass durch den SSH-Server nur das in der Richtlinie empfohlene Protokoll bzw. nur die in der Richtlinie empfohlenen kryptografischen Verfahren und Schlüssellängen angeboten werden. Möglicherweise sind Clients im Einsatz, die die Empfehlungen des BSI nicht anwenden können. Dies ist vor allem bei Geräten der Fall, die nicht auf einem aktuellen Softwarestand gehalten werden. Durch eine Änderung der Konfiguration könnte dann keine Verbindung mehr aufgebaut werden. Entsprechende Prüfungen sind daher vor der Produktivsetzung notwendig.
Referenzen	https://www.secuvera.de/blog/ssh-server-konfiguration-technische-richtlinie-tr-02102-4-des-bsi/ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4

4.2.3. Übersicht der geprüften IP-Adressen

In diesem Abschnitt werden die einzelnen IP-Adressen, die geprüft wurden, und die dabei gefundenen Schwachstellen aufgeführt.

Hinweis zur Erreichbarkeit eines Systems: Eine IP-Adresse wird auch dann als erreichbar klassifiziert, wenn kein Dienst auf einem Port aktiv war, aber dennoch Antwortpakete von der entsprechenden Adresse erhalten wurden.

Hinweis zur folgenden Tabelle: In einem echten Ergebnisbericht sind in der folgenden Tabelle selbstverständlich alle Systeme aufgeführt. Um den Beispiel-Ergebnisbericht jedoch nicht in die Länge zu ziehen, wird die Tabelle hier lediglich angedeutet. Um den Kunden eine Weiterarbeit mit den Ergebnissen zu erleichtern, erhalten Sie diese natürlich auch im Excel-Format.

IP-Adresse	Erreichbarkeit	Schwachstellen / Sicherheitshinweise	Schweregrad Schwachstelle	Port	Sicherheitsniveau Adresse
XXX.XXX.XXX.4	erreichbar	S_03 Denial-of-Service durch DHE-Schlüsselaustausch (D(HE)ater-Angriff)	Medium	443/tcp	Kritisch
		S_01 Verwundbare phpMyAdmin-Version im Einsatz	Critical		
		H_01 Nicht BSI-konforme Cipher Suites/ Verschlüsselungsprotokolle im Einsatz	Hinweis		
XXX.XXX.XXX.5	erreichbar	S_02 Verwundbare Apache2-Version im Einsatz	High	443/tcp	Niedrig
		H_02 Nicht BSI-konforme SSH-Verschlüsselungsprotokolle im Einsatz	Hinweis	22/tcp	
XXX.XXX.XXX.70	erreichbar	S_04 Verwundbares Transportverschlüsselungsprotokoll im Einsatz	Low	443/tcp	Niedrig
		S_02 Verwundbare Apache2-Version im Einsatz	High		
XXX.XXX.XXX.71	erreichbar	S_04 Verwundbares Transportverschlüsselungsprotokoll im Einsatz	Low	443/tcp	Mittel
		S_03 Denial-of-Service durch DHE-Schlüsselaustausch (D(HE)ater-Angriff)	Medium		
XXX.XXX.XXX.72	erreichbar	S_04 Verwundbares Transportverschlüsselungsprotokoll im Einsatz	Low	443/tcp	Hoch
		H_01 Nicht BSI-konforme Cipher Suites/ Verschlüsselungsprotokolle im Einsatz	Hinweis		
		H_02 Nicht BSI-konforme SSH-Verschlüsselungsprotokolle im Einsatz		22/tcp	

5. PRÜFUNG WEBANWENDUNG ÜBER DAS INTERNET

5.1. Beschreibung der Vorgehensweise und des Ziels

Im Zeitraum vom 10. bis zum 21. Februar 2025 wurde die unter <https://www.beispiel-kunde.de> erreichbare Webanwendung des Kunden einer Sicherheitsüberprüfung in Form eines technischen Penetrationstests auf Anwendungsebene unterzogen. Ziel der Prüfung war die Identifikation von technischen Schwachstellen in der Anwendung sowie das bestehende Rechte- und Rollenmodell.

Die Prüfung fand über das Internet statt. Die Anwendung wurde in einer Testumgebung geprüft.

Die Webanwendung wurde zunächst mittels automatisierter Scanwerkzeuge abgetastet. Verwendet wurde hierfür das Werkzeug „Burp Suite Pro“⁸. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. False Positives möglichst ausschließen zu können. Die Tests wurden durch manuelle Methoden ergänzt, um prinzipbedingte Schwächen des toolgestützten Tests auszugleichen.

Die Anwendung wird derzeit nicht von einer Webanwendungsfirewall (WAF) geschützt. Daher wird direkt die Sicherheit der Anwendung und nicht die Sicherheit der Gesamtumgebung überprüft.

Die Tests wurden als Black-Box-Tests durchgeführt, das heißt, dass die Tester bis auf die Adresse und Anmeldedaten der Webanwendung keine weiteren Informationen zum technischen Aufbau oder der Implementierung erhalten haben.

Weitere Randbedingungen

Für die Durchführung von Massenprüfungen mit automatisierten Werkzeugen wurde durch den Kunden vor Beginn der Prüfungen Anti-Automatisierungs-Schutzmechanismen (CAPTCHA) deaktiviert. Deren Wirksamkeit wurde im Testverlauf nach vorheriger Abstimmung mit dem Kunden und Reaktivierung überprüft.

Prüfziele

Auffinden technischer Schwachstellen in den Funktionen der Anwendung

In diesem Teilschritt wurden alle Funktionen der Anwendung überprüft, die aus den im Folgenden definierten Rollen heraus aufrufbar sind:

- anonymer Benutzer ohne Benutzerkonto,
- angemeldeter Benutzer aus der Gruppe „Personal“,
- angemeldeter Benutzer aus der Gruppe „Marketing“.

Die Anwendung bietet eine Anmeldemaske an. Um zu verifizieren, ob die Anmeldemaske einen Brute-Force-Schutz besitzt, wurden vom Kunden zur Verfügung gestellte Anmeldedaten verwendet.

⁸ <https://www.portswigger.net>

Auffinden von Schwachstellen in der Umsetzung des Rollen- und Rechtemodells

In diesem Schritt wurde geprüft, ob eine horizontale oder vertikale Rechteausweitung möglich ist. Eine horizontale Rechteausweitung liegt z. B. vor, wenn innerhalb einer Berechtigungsstufe Unberechtigte auf Daten eines anderen Nutzers gleicher Berechtigungsstufe zugreifen können. Eine vertikale Rechteausweitung ist z. B. dann erreicht, wenn ein Nutzer Funktionen aufrufen oder Daten einsehen kann, zu denen nur andere Berechtigungsstufen – z. B. ein höher privilegierter Nutzer – zugelassen sind.

Der Kunde übergab die Zugangsdaten für die folgenden Benutzerzugänge:

Tabelle 8: Übergebene / Erstellte Benutzerzugänge Prüfung B

Benutzername	Gruppe
user1	Personal
user2	Marketing

Ein Ziel des anschließenden Penetrationstests war es, dieses Rechtemodell zu verifizieren und ggf. Verstöße gegen das Rechtemodell aufzudecken.

Tabelle 9: Der Prüfung zugrunde gelegtes Berechtigungsmodell

Berechtigung	Anonymer Benutzer	Personal	Marketing
Kontoeinstellungen ändern	nein	nur eigene	nur eigene
Mitarbeitende anzeigen	nein	ja	ja
Mitarbeiter:in hinzufügen	nein	ja	nein
Mitarbeiter:in bearbeiten	nein	ja	Nein
Kundenaufträge anzeigen	nein	nein	ja
Kundenauftrag hinzufügen	nein	nein	ja
Kundenauftrag bearbeiten	nein	nein	ja

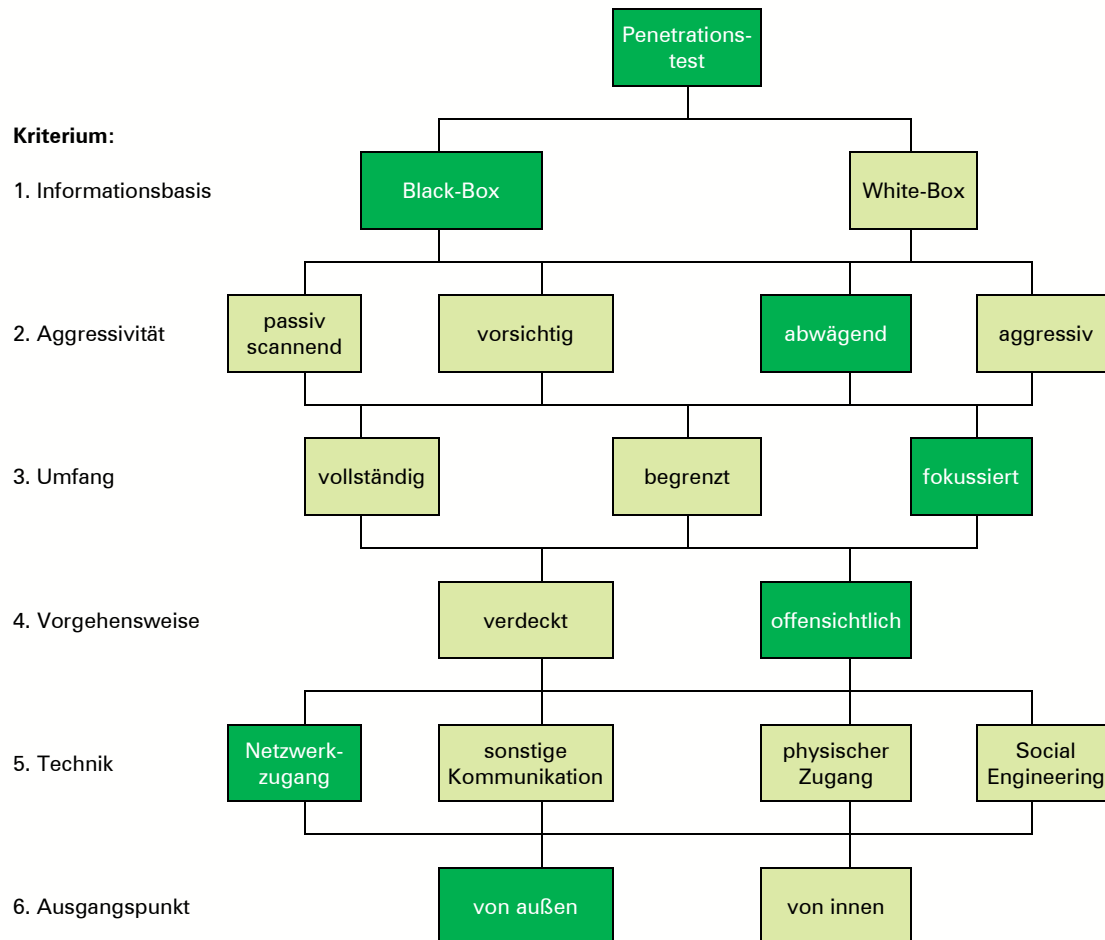
Um eine gleichbleibende Güte der Tests und eine hohe Qualität der Prüfungen zu gewährleisten, wurde als Testgrundlage der OWASP Testing Guide in Version 4 genutzt. Auf Basis dieses Testing Guides und aufgrund von Erfahrungen aus vergangenen Penetrationstests wurde ein speziell auf die Besonderheiten der jeweiligen Anwendung angepasster Testplan erstellt. Damit können alle technisch prüfbaren Inhalte der zum Zeitpunkt der Prüfung aktuellen OWASP Top 10 abgedeckt werden. Sofern Schwächen identifiziert werden, deren Risiko einem OWASP-Top-10-Risiko zugeordnet werden kann, wird dieses entsprechend in der Beschreibung der Schwachstelle referenziert.

Zusätzlich wurden weitere Analysen durchgeführt, die über die in den OWASP Top 10 benannten Risiken hinausgehen und durch den Testplan vorgegeben sind. Diese primär manuellen Untersuchungen dienen zur Prüfung der Anwendungslogik, indem dort gezielt Fehler provoziert und ausgenutzt werden sollen.

Die Webanwendung wurde in der Version 12.4 geprüft. Die Information konnte unterhalb des Logins abgelesen werden.

Für den Penetrationstest wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“⁹ zugrunde gelegt:

Abbildung 2: Vorgehensweise nach BSI-Studie Prüfung B



5.2. Projektverlauf und Ergebnisdarstellung

Das Projekt konnte wie vorab geplant und in der Vorgehensweise beschrieben durchgeführt werden.

5.2.1. Übersicht der Schwachstellen

W_01

Cross-Site-Request-Forgery-Angriffe (CSRF) möglich

Beschreibung

Die Webanwendung ist anfällig für Cross-Site-Request-Forgery-Angriffe (CSRF). Dabei ruft ein Anwender eine durch einen Angreifer präparierte Seite auf. In dieser präparierten Seite ist ein vom Angreifer präparierter Aufruf auf die verwundbare Anwendung enthalten.

Während der Prüfung wurden folgende Funktionen als angreifbar identifiziert:

Tabelle 10: Durch CSRF angreifbare Funktionen

Pfad	Funktion
www.beispiel-kunde.de/account	Passwort ändern, Benutzer anlegen
www.beispiel-kunde.de/users	Mitarbeiter:in bearbeiten Mitarbeiter:in löschen

Auswirkung

Durch einen CSRF-Angriff werden Aktionen innerhalb der verwundbaren Anwendung durch einen Angreifer ausgelöst, die dann im Rechtekontext eines angemeldeten Benutzers ausgeführt werden.

Konkret kann ein Angreifer durch das Ausnutzen der oben angegebenen Funktion „Passwort ändern“ oder „Benutzer Anmeldung“ einen CSRF-Angriff durchführen. Dabei sendet der Angreifer eine präparierte Anfrage, die im Namen eines angemeldeten Benutzers ausgeführt wird. Dies geschieht oft durch das Einbinden eines schädlichen Links oder Skripts auf einer externen Webseite, die der Benutzer unwissentlich besucht. Dadurch kann der Angreifer ohne direkten Zugriff auf das Konto vertrauliche Aktionen wie Passwortänderungen oder unbefugte Anmeldungen auslösen.

Beispiel:

Hierfür müssen Links zur Anwendung oder eine ganze Webseite präpariert werden. Ein potentielles Opfer muss dazu gebracht werden, auf einen präparierten Link zu klicken oder eine präparierte Webseite zu öffnen, während das Opfer gleichzeitig in der Webanwendung angemeldet ist.

`https://www.beispiel-kunde.de/login`

Das Demo-Skript wurde mit dem folgenden Skript ausgeführt:

```
<html>

  <!-- CSRF PoC - generated by Burp Suite Professional and
edit by Secuvera -->

  <body>

    <form action="https://www.beispiel-kunde.de/account "
method="POST">

      <input          type="hidden"          name="newpass"
value="password1337" />

      <input          type="hidden"          name="confnewpass"
value="password1337" />      <input type="submit"
value="Submit request" />

    </form>

    <script>

      history.pushState('', '', '/');

      document.forms[0].submit();

    </script>

  </body>

</html>
```

Wenn Sie der Folgenden Anleitung folgen, können Sie die Schwachstell selbst ausführen.

1. In die Webanwendung einloggen.
2. Speichern Sie das oben geschrieben Script in einer .html Datei.
3. Führen Sie diese Datei aus (im selben Browser).
4. Drücken Sie auf `Submit request`
5. Dadurch wurde das Passwort des angemeldeten Users auf das Passwort `password1337` geändert.

OWASP Top 10

2021 A07 – Identification and Authentication Failures

Empfehlung

Um CSRF-Angriffe zu verhindern, müssen vielschichtige Techniken verwendet werden, u. a. empfiehlt sich die Verwendung des „SameSite“-Merkmals beim Session Cookie und die Verwendung von sogenannten „CSRF-Tokens“. CSRF-

Tokens sind zufällige Zeichenketten, die vom Server erstellt und für Benutzer nicht sichtbar in die Seite integriert werden. Beim Ausführen einer Funktion wird das Token mitgesendet und vom Server überprüft. Die Funktion wird nur dann ausgeführt, wenn es sich um ein gültiges Token handelt. Da die Tokens zufällig gewählt werden, ist es Angreifern nicht möglich, diese vorherzusagen. Detaillierte Beschreibungen von wichtigen Gegenmaßnahmen finden Sie in der verlinkten Referenz.

Referenzen https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Schweregrad **High**

Tabelle 11: Bewertung des Schweregrades Schwachstelle W_01

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	Low	Der Angreifer muss keine messbaren Maßnahmen ergreifen, um vorhandene eingebaute sicherheitserhöhende Vorkehrungen aktiv zu umgehen oder zu überwinden, damit er die Schwachstelle ausnutzen kann.
Attack Requirements (AT)	Present	Der Benutzer muss im selben Browser auf der Internetseite eingeloggt sein und eine aktive Session haben.
Privileges Required (PR)	Low	Der Angreifer benötigt Zugangsdaten, um die Parameter für das Skript herauszufinden.
User Interaction (UI)	Active	Das Opfer muss auf einen vom Angreifer präparierten Link klicken.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	High	Durch das Ändern des Passworts kann der Angreifer alle Daten des Nutzers einsehen und bearbeiten
Integrity Impact (VI)	High	Der Angreifer könnte alle Dinge diese das Opfer ausführen kann im Namen des Opfers ausführen.
Availability Impact (VA)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der Webanwendung.

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.
Integrity Impact (SI)		
Availability Impact (SA)		
CVSS-B	7,3	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N

W_02

Brute-Force-Angriff auf Login-Maske möglich

Beschreibung

Die Webanwendung bietet keinen Schutz vor Brute-Force-Angriffen.

Bei den Prüfungen wurde im Zeitraum weniger Sekunden 25-mal ein falsches Passwort angegeben. Nach diesen fehlerhaften Versuchen war eine Anmeldung mit dem validen Passwort möglich. Es erfolgte keine Benachrichtigung des Benutzers über die fehlgeschlagenen Anmeldeversuche.

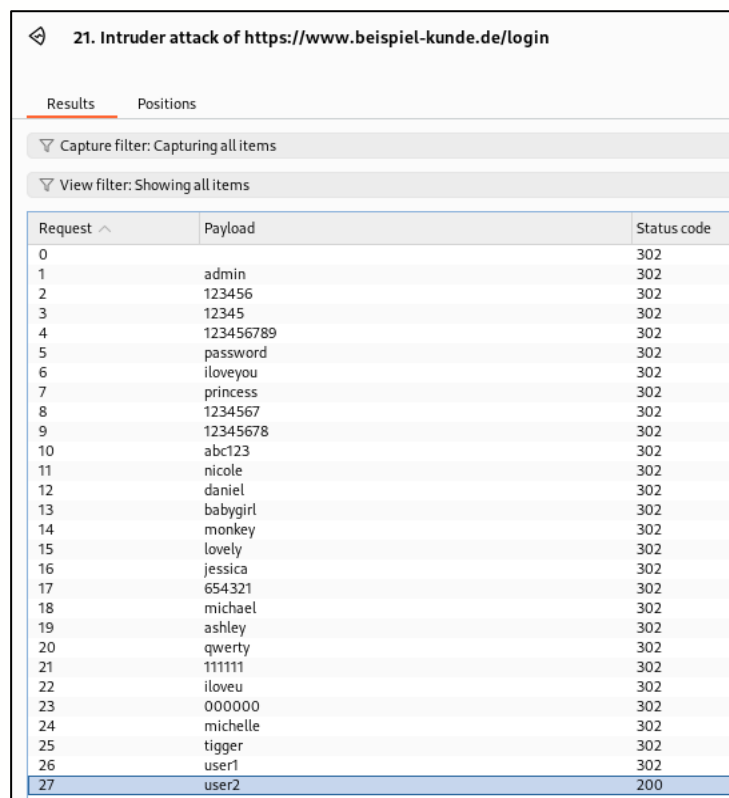
Auswirkung

Ein Angreifer wäre in der Lage, zu einem bekannten Benutzernamen das Passwort durch Ausprobieren zu erraten und somit Zugang zu dessen Account zu erhalten.

Beispiel

Die Anmeldemaske war unter folgender URL erreichbar: <https://www.beispiel-kunde.de/login>. Für die Verifikation der Schwachstelle kam die Funktion „Intruder“ des Werkzeugs Burp Suite Professional zum Einsatz. Diese wurde so konfiguriert, dass 25 Anmeldeversuche mit bekannt schwachen Passwörtern ausprobiert wurden, bevor die Anmeldung mit dem zum Nutzer `user1` gehörenden, korrekten Passwort erfolgte. Die folgende Abbildung zeigt, dass die Anwendung trotz der vorherigen Fehlschläge mit dem Status `200 OK` antwortete und die Anmeldung gelang. Die abgebildeten Antwortzeiten zeigen auch, dass keine serverseitige Drosselung erfolgte.

Abbildung 3: Brute-Force-Angriff auf Login-Maske mit Burp Intruder



Request ^	Payload	Status code
0		302
1	admin	302
2	123456	302
3	12345	302
4	123456789	302
5	password	302
6	iloveyou	302
7	princess	302
8	1234567	302
9	12345678	302
10	abc123	302
11	nicole	302
12	daniel	302
13	babygirl	302
14	monkey	302
15	lovely	302
16	jessica	302
17	654321	302
18	michael	302
19	ashley	302
20	qwerty	302
21	111111	302
22	iloveu	302
23	000000	302
24	michelle	302
25	tigger	302
26	user1	302
27	user2	200

OWASP Top 10

2021 A07 – Identification and Authentication Failures

Empfehlung

Das wiederholte Aufrufen der Login-Funktion sollte begrenzt werden. Beispielsweise wäre der Einsatz von sogenannten Teergruben (zunehmende Verlangsamung der verarbeiteten Anfragen mit steigender Anzahl von fehlerhaften Versuchen), eine generelle Limitierung der Anfragen pro Zeiteinheit (Rate-

Limiting) oder eine IP-Sperre der Angriffs-IP empfehlenswert. Auch wäre es denkbar, Accounts nach mehreren fehlgeschlagenen Versuchen (z. B. zehn Versuche) temporär zu sperren. Welche Maßnahme am geeignetsten ist, muss für jede Anwendung individuell abgewogen werden.

Zusätzlich zu den genannten Maßnahmen werden häufig CAPTCHAs verwendet. Diese können die vorher genannten Maßnahmen nicht ersetzen, sondern nur ergänzen, da CAPTCHAs mithilfe von KI-Werkzeugen häufig lösbar sind. Zudem wird die Nutzbarkeit der Anwendung durch deren Einsatz negativ beeinflusst. Aus diesen Gründen sind CAPTCHAs aus unserer Sicht nur eingeschränkt empfehlenswert.

Referenzen https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Schweregrad **Medium**

Tabelle 12: Bewertung des Schweregrades Schwachstelle W_01

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	Low	Zum Ausnutzen der Schwachstelle sind keine besonderen Rahmenbedingungen erforderlich, und ein Angriff ist daher beliebig wiederholbar.
Attack Requirements (AT)	None	Ein erfolgreicher Angriff hängt nicht von einem besonderen Ausführungszustand des Systems ab; der Angreifer kann damit rechnen, die Schwachstelle immer zu erreichen.
Privileges Required (PR)	None	Vor dem Ausnutzen der Schwachstelle benötigt ein Angreifer keine Authentifizierung an der Werbanwendung.
User Interaction (UI)	None	Die Schwachstelle kann unabhängig von anderen Benutzern ausgenutzt werden.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	Low	Durch Ausnutzen der Schwachstelle kann ein Angreifer das Passwort einzelner Anwender in Erfahrung bringen. Ob der Angriff tatsächlich Erfolg hat, kann der Angreifer jedoch nicht selbst bestimmen, da dies von dem individuell gewählten Passwort abhängig ist.

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Integrity Impact (VI)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Integrität der Daten.
Availability Impact (VA)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der Webanwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.
Integrity Impact (SI)		
Availability Impact (SA)		
CVSS-B	6,9 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	

W_03

Bearbeiten von Kundenaufträgen mit Rolle „Personal“ möglich

Beschreibung	Die Anwendung bietet eine „Auftrag bearbeiten“-Funktion, die es Benutzern mit der Rolle „Marketing“ ermöglicht, die Details von Kundenaufträgen zu bearbeiten. Bei der Prüfung wurde jedoch festgestellt, dass der zugehörige HTTP-Request auch dann von der Anwendung akzeptiert wird, wenn er aus der Sitzung eines Benutzers mit der Rolle „Personal“ gesendet wird. Dies ermöglicht es auch unberechtigten Benutzern, die Details der Kundenaufträge zu verändern.
Auswirkung	Ein Angreifer, der Zugriff auf ein Benutzerkonto mit der Rolle „Personal“ hat, kann beliebige Kundenaufträge verändern oder löschen, wenn er die Auftragsnummer sowie die Struktur des entsprechenden HTTP-Requests kennt.
Beispiel	Zur Verifizierung der Schwachstelle wurde mit dem Benutzer <code>user2</code> ein neuer Kundenauftrag angelegt. Anschließend wurden die Details des Auftrags durch Aufrufen der Aktion „Auftrag bearbeiten“ verändert. Der zugehörige POST-Request wurde dabei mit der Interceptor-Funktion von Burp Suite Professional abgefangen.

Abbildung 4: Request der Funktion "Auftrag bearbeiten"

```
1 POST /orders.php HTTP/1.1
2 Host: beispiel-kunde.de
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: JSESSION=12989809af90
17 Connection: keep-alive
18 Content-Type: application/x-www-form-urlencoded
19 Content-Length: 17
20
21 action=order_edit&orderid=9a91be1724181ff188429aa411&service_name=Kampagnenstart+Q2&budget=1000&deadline=
  2025-05-01
```

Es wurde sich darauffolgend mit dem Benutzer `user1` eingeloggt und das Sitzungstoken `JSESSION` notiert. Dann wurde der zuvor abgefangene Request mit der Repeater-Funktion von Burp Suite Professional so verändert, dass statt des Sitzungstokens von `user2` nun das von `user1` gesendet wird. Zusätzlich wurden noch Auftragsdetails im Body des Requests verändert. Danach wurde der veränderte Request an die Anwendung gesendet.

Abbildung 5: Manipulation des Sitzungstokens und der Auftragsdetails im Request

```

1 POST /orders.php HTTP/1.1
2 Host: beispiel-kunde.de
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
9 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://localhost:3000/
16 Cookie: JSESSIONID=9833121000ee
17 Content-Type: application/x-www-form-urlencoded
18 Content-Length: 17
19 action=order_edit&orderid=9a91be1724181ff188429aa411&service_name=Pentest+Q2&budget=1&deadline=2025-02-01
20
21

```

Nach dem Senden dieses Requests waren die Details des betroffenen Kundenauftrags entsprechend verändert.

Abbildung 6: Veränderte Auftragsdaten in der Anwendung

Übersicht der Kundenbestellungen			
Home Bestellungen Kunden Kontakt			
Kunde	Status	Aktionen	
Acme Corp	Ausstehend	Details anzeigen Auftrag bearbeiten	
Bestell-ID	Service	Budget	Frist
1001	Pentest Q2	1 €	2025-02-01

Hinweis Da die ID des Auftrags eine zufällige 26 Zeichen lange Zeichenkette in base64-Kodierung ist, kann diese praktisch nicht erraten werden, sodass ein Angreifer Kenntnis über die ID haben muss, um den Angriff durchführen zu können. In der Bewertung der Schwachstelle wurde dieser Umstand berücksichtigt.

OWASP Top 10 2021 A01 – Broken Access Control

Empfehlung Die Anwendung sollte bei jedem Request zum Bearbeiten eines Auftrags überprüfen, ob der Benutzer die Berechtigung hat, auf den entsprechenden Kundenauftrag zu bearbeiten.

Referenzen https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Schweregrad **Low**

Tabelle 13: Bewertung des Schweregrades Schwachstelle W_03

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	High	Der Angreifer muss Kenntnis über die ID des Auftrags und die Struktur des POST-Requests erlangt haben.
Attack Requirements (AT)	None	Zum Ausnutzen der Schwachstelle müssen keine besonderen Anforderungen an die Konfiguration der Anwendung erfüllt sein.
Privileges Required (PR)	Low	Vor dem Ausnutzen der Schwachstelle muss sich ein Angreifer an der Anwendung als regulärer Benutzer mit der Rolle „Personal“ anmelden.
User Interaction (UI)	None	Die Schwachstelle kann unabhängig von anderen Benutzern ausgenutzt werden.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Vertraulichkeit der Daten.
Integrity Impact (VI)	Low	Durch Ausnutzen der Schwachstelle kann ein Angreifer sensible Daten verändern, den Umfang der Daten jedoch nicht selbst bestimmen.
Availability Impact (VA)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der Anwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.
Integrity Impact (SI)		

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Availability Impact (SA)		
CVSS-B	2,3 CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	

W_04

Unsichere Kommunikation

Beschreibung

Die Kommunikation mit der Webanwendung ist über einen unsicheren Kanal via HTTP möglich. Jegliche bei der Nutzung der Webanwendung übertragenen Informationen, wie zum Beispiel Zugangsdaten, werden unverschlüsselt und ohne Integritätsschutz übertragen.

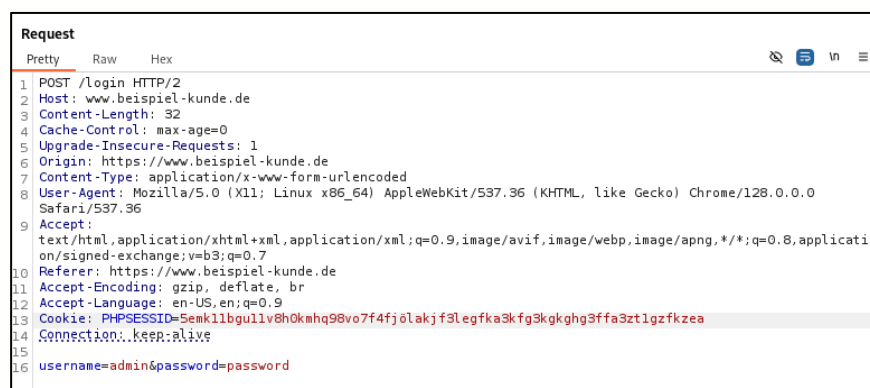
Auswirkung

Ein Angreifer in einem Machine-in-the-Middle-Szenario ist in der Lage, die an den Dienst übertragenen Daten mitzulesen, da diese im Klartext übertragen werden, sowie die übertragenen Daten uneingeschränkt zu manipulieren, da ihre Integrität nicht geschützt wird. Angreifer können somit gegebenenfalls Zugriff auf sensible Informationen erlangen und diese manipulieren.

Beispiel

In diesem Beispiel werden die Daten über einen POST-Request im Klartext übertragen, was ein Sicherheitsrisiko darstellt, da Dritte diese Informationen während der Übertragung abfangen könnten.

Abbildung 7: Klartext-Übertragung von Daten im POST-Request



```
Request
Pretty Raw Hex
1 POST /login HTTP/2
2 Host: www.beispiel-kunde.de
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: https://www.beispiel-kunde.de
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: https://www.beispiel-kunde.de
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=Semk11bgullv8h0kmhq98vo7f4fj6Lakjf3Legfka3kfg3kgkghg3ffa3zt1gzfkzea
14 Connection: keep-alive
15
16 username=admin&password=password
```

OWASP Top 10

2021 A02 – Cryptographic Failures

Empfehlung

Die Kommunikation mit dem Dienst sollte nur über eine kryptographisch abgesicherte Verbindung erfolgen. Daten sollten ausschließlich verschlüsselt übertragen werden und durch geeignete Mechanismen zum Integritätsschutz vor Manipulation abgesichert werden. Hierzu bietet sich im konkreten Fall die Verwendung von TLS an, Informationen zur sicheren Konfiguration gibt die Technische Richtlinie 02102 des Bundesamts für Sicherheit in der Informationstechnik (siehe Referenzen).

Referenzen

https://owasp.org/www-community/vulnerabilities/Insecure_Transport
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html>

Schweregrad

Low

Tabelle 14: Bewertung des Schweregrades Schwachstelle W_04

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Attack Vector (AV)	Network	Die Schwachstelle kann über ein Netzwerk ausgenutzt werden.
Attack Complexity (AC)	Low	Der Angreifer muss keine messbaren Maßnahmen ergreifen, um vorhandene sicherheitserhöhende Vorkehrungen aktiv zu umgehen oder zu überwinden, damit er die Schwachstelle ausnutzen kann.
Attack Requirements (AT)	Present	Zum Ausnutzen der Schwachstelle muss der Angreifer sich in einem Machine-in-the-Middle-Szenario befinden.
Privileges Required (PR)	None	Vor dem Ausnutzen der Schwachstelle benötigt ein Angreifer keine Authentifizierung an der Webanwendung.
User Interaction (UI)	Passive	Das Opfer muss Daten mit der Webanwendung austauschen.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	Low	Durch Ausnutzen der Schwachstelle kann ein Angreifer sensible Daten einsehen, den Umfang der Daten jedoch nicht selbst bestimmen.
Integrity Impact (VI)	Low	Durch Ausnutzen der Schwachstellen kann ein Angreifer sensible Daten verändern, den Umfang der Daten jedoch nicht selbst bestimmen.
Availability Impact (VA)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der Webanwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Das Ausnutzen der Schwachstelle hat keine Auswirkung auf nachgelagerte Systeme.

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	Bewertung	Begründung der Wertewahl
Integrity Impact (SI)		
Availability Impact (SA)		
CVSS-B	2,3 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N	

5.2.2. Zuordnung der Schwachstellen zu den OWASP Top 10

Im Folgenden wird das Ergebnis des Webanwendungspenetrationstests den in der Beschreibung der Vorgehensweise dargestellten OWASP-Top-10-Kategorien zugeordnet.

Tabelle 15: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-Top-10-Risiken

Risiko	Fail/Pass
2021 A01 – Broken Access Control	Pass
2021 A02 – Cryptographic Failures	Fail
2021 A03 – Injection	Fail
2021 A04 – Insecure Design	Pass
2021 A05 – Security Misconfiguration	Fail*
2021 A06 – Vulnerable and Outdated Components	Pass
2021 A07 – Identification and Authentication Failures	Fail*
2021 A08 – Software and Data Integrity Failures	Pass
2021 A09 – Security Logging and Monitoring Failures	Pass
2021 A10 – Server-Side Request Forgery	Pass

Legende: * Es existieren Sicherheitshinweis(e) zu dieser Kategorie, siehe entsprechendes Kapitel weiter unten.

5.2.3. Ergebnisse der Überprüfung des Rechtemodells

Bei den in der folgenden Tabelle rot markierten Spalten, konnte ein Ausbruch aus dem identifizierten Rechtemodell festgestellt werden. Einen Verweis, um welche Schwachstelle es sich bei dem Ausbruch handelt, finden Sie im Anschluss an

Berechtigung	Anonymer Benutzer	Personal	Marketing
Kontoeinstellungen ändern	nein	nur eigene	nur eigene
Mitarbeitende anzeigen	nein	ja	ja
Mitarbeiter:in hinzufügen	nein	ja	nein
Mitarbeiter:in bearbeiten	nein	ja	Nein
Kundenaufträge anzeigen	nein	nein	ja
Kundenauftrag hinzufügen	nein	nein	ja
Kundenauftrag bearbeiten	nein	nein ¹	ja

Identifizierte Schwachstellen:

¹ siehe Schwachstelle **W_03 Bearbeiten von Kundenaufträgen mit Rolle „Personal“** möglich

Im Laufe der Prüfung fielen einige Probleme auf, die nicht klar als Schwachstelle klassifiziert werden können. Die Beseitigung dieser Probleme kann jedoch das allgemeine Sicherheitsniveau der Anwendung zusätzlich erhöhen.

H_03 Unzureichende Passwortrichtlinie

Beschreibung	Die Webanwendung setzt keine Vorgaben an Passwörter um, sodass Anwender beliebig einfache Passwörter wählen können.
Auswirkung	Einem Angreifer ist es deutlich einfacher möglich, Passwörter von Benutzern zu erraten, wenn diese einfache Passwörter wählen sollten. Sollte ein Angreifer in den Besitz von gültigen Anmeldedaten kommen, so könnte er beliebige Dateien im Namen des Benutzers abrufen und verändern.
Beispiel	Es war möglich, im Prüfungszeitraum beispielsweise das Passwort „password“ für den Account „admin“ zu wählen.
OWASP Top 10	2021 A07 – Identification and Authentication Failures
Empfehlung	Es sollte eine passendere und restriktivere Passwortrichtlinie erstellt und technisch umgesetzt werden. Hierbei kann keine „allgemeingültige“ Richtlinie empfohlen werden, sondern es muss eine den behandelten Daten und damit dem nötigen Sicherheitsniveau entsprechende Richtlinie definiert werden. Orientierung bieten gängige Standards und Regelwerke. Unter „Referenzen“ werden Beispiele hierfür benannt.
Referenzen	Abschnitt 5.1.1 der NIST Special Publication 800-63B, https://pages.nist.gov/800-63-3/sp800-63b.html#sec5 ORP.4.A8 und ORP.4.A22 des IT-Grundschutz-Kompodiums, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT_Grundschutz_Kompodium_Edition2021.html?nn=128568 ORP.4.M22 der Umsetzungshinweise zum IT-Grundschutz-Kompodium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=1

H_04 Unsichere Content-Security-Policy im Einsatz

Beschreibung Während der Prüfung wurde die folgende Content-Security-Policy identifiziert:

Abbildung 8: Eingesetzte Content-Security-Policy

```
Content-Security-Policy: default-src 'self';script-src 'self'
'unsafe-inline' 'unsafe-eval';object-src 'self';style-src 'self'
'unsafe-inline';img-src 'self' data::media-src 'self';frame-src
'self';font-src 'self' data::connect-src 'self';frame-ancestors
'self';report-uri /WebResource.axd?cspReport=true
```

Folgende Konfigurationen wurden als unsicher identifiziert:

- **unsafe-inline:** erlaubt die Benutzung von Inline-Code wie z. B. Eventhandler-Attribute wie onclick und in <script>-Elementen notierter JavaScript-Code,

	• <code>unsafe-eval</code>: ermöglicht die Ausführung von Code, der in DOM-API-Funktionen wie <code>eval()</code> eingeschleust wird.
Auswirkung	Die eingesetzte Content-Security-Policy erlaubt es, willkürlichen in die Anwendung eingeschleusten JavaScript-Code zur Ausführung zu bringen.
Hinweis	Während der Prüfung konnten keine Cross-Site-Scripting-Schwachstellen identifiziert werden. Werden jedoch in Zukunft Cross-Site-Scripting-Schwachstellen identifiziert, wird deren Ausnutzung durch die aktuell eingesetzte Content-Security-Policy stark begünstigt. Da diese Schwachstelle lediglich Folgeangriffe erleichtern kann und selbst keine Auswirkungen auf angegriffene Nutzer oder Systeme hat, wird dies lediglich als Sicherheitshinweis aufgenommen.
OWASP Top 10	2021 A05 – Security Misconfiguration
Empfehlung	Aus der Content-Security-Policy sollten beide genannten Attribute entfernt werden. Sollte dies nicht praktikabel sein, sollten lediglich vertrauenswürdige JavaScript-Codeabschnitte erlaubt werden. Dies kann beispielsweise unter Verwendung von Datei-Hashes umgesetzt werden. Bei diesem Ansatz kann eine externe Datei in einem <code><script></code> -Element lediglich geladen und ausgeführt werden, wenn alle gültigen Hash-Werte in ihrem Integritätsattribut mit den zulässigen Werten im CSP-Header übereinstimmen. Die Integritätsfunktion für Subressourcen prüft zusätzlich, ob die heruntergeladene Datei den angegebenen Hash-Wert hat und somit nicht verändert wurde.
Referenzen	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src#allowlisting_external_scripts_using_hashes

6. ANHANG A: VERSIONEN UND VERZEICHNISSE

6.1. Versionshistorie

Tabelle 16: Versionsverlauf des Ergebnisberichts

Version	Datum	Bearbeiter	Änderungen
1.0	27.02.2025	Musterprüferin, secuvera	Finale Berichtsversion
0.9	27.02.2025	Musterprüferin, secuvera	Einpfelegen der Änderungen aus dem Lektorat, Version zur Abstimmung mit dem Kunden
0.8	27.02.2025	Musterlektor, secuvera	Lektorat des Ergebnisberichts
0.7	25.02.2025	Musterprüferin, secuvera	Abnahme der Änderungen aus dem Rücklauf
0.6	24.02.2025	Mustertester, secuvera	Einpfelegen der Änderungen aus der fachlichen Qualitätssicherung
0.5	24.02.2025	Musterprüferin, secuvera	Fachliche Qualitätssicherung
0.4	21.02.2025	Mustertester, secuvera	Letzte Änderungen, Version für die fachliche Qualitätssicherung
0.3	20.02.2025	Mustertester, secuvera	Zusammenfassung für das Management geschrieben
0.2	17.02.2025	Mustertester, secuvera	Prüfung Webanwendung über das Internet dokumentiert
0.1	10.02.2025	Mustertester, secuvera	Dokument initialisiert und Prüfung der Systeme über das Internet dokumentiert

6.2. Abbildungsverzeichnis

Abbildung 1: Vorgehensweise nach BSI-Studie Prüfung Systeme über das Internet	13
Abbildung 2: Vorgehensweise nach BSI-Studie Prüfung B	29
Abbildung 3: Brute-Force-Angriff auf Login-Maske mit Burp Intruder	34
Abbildung 4: Request der Funktion "Auftrag bearbeiten"	37
Abbildung 5: Manipulation des Sitzungstokens und der Auftragsdetails im Request	38

Abbildung 6: Veränderte Auftragsdaten in der Anwendung	38
Abbildung 7: Klartext-Übertragung von Daten im POST-Request	41
Abbildung 8: Eingesetzte Content-Security-Policy	45

6.3. Tabellenverzeichnis

Tabelle 1: Statistik: Sicherheitsniveau pro geprüfter IP-Adresse Prüfung der Systeme über das Internet	5
Tabelle 2: Statistik: Identifizierte Schwachstellen Penetrationstest Soundso	7
Tabelle 3: Auflistung geprüftes Netzwerksegment	11
Tabelle 4: Bewertung des Schweregrades Schwachstelle S_01	15
Tabelle 5: Bewertung des Schweregrades Schwachstelle S_02	16
Tabelle 6: Bewertung des Schweregrades Schwachstelle S_03	19
Tabelle 7: Bewertung des Schweregrades Schwachstelle S_04	21
Tabelle 8: Übergebene / Erstellte Benutzerzugänge Prüfung B	27
Tabelle 9: Der Prüfung zugrunde gelegtes Berechtigungsmodell	27
Tabelle 10: Durch CSRF angreifbare Funktionen	30
Tabelle 11: Bewertung des Schweregrades Schwachstelle W_01	32
Tabelle 12: Bewertung des Schweregrades Schwachstelle W_01	35
Tabelle 13: Bewertung des Schweregrades Schwachstelle W_03	38
Tabelle 14: Bewertung des Schweregrades Schwachstelle W_04	42
Tabelle 15: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-Top-10-Risiken	44
Tabelle 16: Versionsverlauf des Ergebnisberichts	47
Tabelle 17: Ermittlung des Sicherheitsniveaus bei systembasierten Penetrationstests	49
Tabelle 18: Ermittlung des Sicherheitsniveaus bei Webanwendungspenetrationstests	50

7. ANHANG B: ERMITTLUNG DES SICHERHEITSNIVEAUS

Hinweis: Da von Sicherheitshinweisen kein direktes Risiko ausgeht, werden diese bei der Ermittlung des Sicherheitsniveaus nicht beachtet.

7.1. Ermittlung Sicherheitsniveau systembasierter Penetrationstest

Das Sicherheitsniveau pro System wird aus dem Schweregrad der auf diesem System identifizierten Schwachstellen berechnet. Bei der Berechnung des Gesamtsicherheitsniveaus wird das festgestellte Sicherheitsniveau der erreichbaren Systeme anhand der folgenden Tabelle abgeleitet:

Tabelle 17: Ermittlung des Sicherheitsniveaus bei systembasierten Penetrationstests

Sicherheitsniveau	Kriterien für das Sicherheitsniveau eines Systems	Kriterien für die Gesamtbewertung Sicherheitsniveau
Sehr hoch	Wird gewählt, sofern keine Schwachstellen auf den Prüfzielen identifiziert wurden.	Wird gewählt, sofern alle erreichbaren Prüfziele ein sehr hohes Sicherheitsniveau aufweisen.
Hoch	Wird gewählt, sofern nur Schwachstellen mit Schweregrad Gering identifiziert wurden.	Wird gewählt, sofern auf höchstens 20 % der erreichbaren Prüfziele ein mittleres Sicherheitsniveau und auf keinem erreichbaren Prüfziel ein niedriges oder kritisches Sicherheitsniveau identifiziert wurde.
Mittel	Wird gewählt, sofern nur Schwachstellen mit Schweregrad Gering und Mittel identifiziert wurden.	Wird gewählt, sofern auf höchstens 20 % der Prüfziele ein niedriges Sicherheitsniveau und auf keinem erreichbaren Prüfziel ein kritisches Sicherheitsniveau identifiziert wurde.
Niedrig	Wird gewählt, sofern mindestens eine Schwachstelle mit Schweregrad Hoch identifiziert wurde.	Wird gewählt, sofern auf mehr als 20 % der erreichbaren Prüfziele ein niedriges Sicherheitsniveau oder auf höchstens 20 % der erreichbaren Prüfziele ein kritisches Sicherheitsniveau identifiziert wurde.
Kritisch	Wird gewählt, sofern mindestens eine Schwachstelle mit Kritisch identifiziert wurde.	Wird gewählt, sofern auf mehr als 20 % der erreichbaren Prüfziele ein kritisches Sicherheitsniveau identifiziert wurde.

7.2. Ermittlung Sicherheitsniveau Webanwendungspenetrationstest

Die Ermittlung des Sicherheitsniveaus einer geprüften Webanwendung wird abschließend anhand der folgenden Tabelle abgeleitet:

Tabelle 18: Ermittlung des Sicherheitsniveaus bei Webanwendungspenetrationstests

Sicherheitsniveau	Kriterien für das Sicherheitsniveau einer Webanwendung
Sehr hoch	Wird gewählt, sofern keine Schwachstellen auf den Prüfzielen identifiziert wurden.
Hoch	Wird gewählt, sofern nur Schwachstellen mit Schweregrad Gering identifiziert wurden.
Mittel	Wird gewählt, sofern nur Schwachstellen mit Schweregrad Gering und Mittel identifiziert wurden.
Niedrig	Wird gewählt, sofern mindestens eine Schwachstelle mit Schweregrad Hoch identifiziert wurde.
Kritisch	Wird gewählt, sofern mindestens eine Schwachstelle mit Schweregrad Kritisch identifiziert wurde.