secuvera
Cybersicherheit. Nachhaltig.

ERGEBNISBERICHT PENETRATIONSTEST

VERSION 1.0 | 01.01.2100

Abschlussbericht für Firma Soundso
Musterstraße 23
123456 Musterstadt

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden

Autoren
Max Mustertester

INHALTSVERZEICHNIS

1. DISCLAIMER ... 3
2. Zusammenfassung ... 4
   2.1. Prüfung der Systeme über das Internet ... 4
   2.2. Prüfung Webanwendung über das Internet ... 6
3. Allgemeines ... 8
   3.1. Common Vulnerability Scoring System ... 8
   3.2. Darstellung ... 8
4. Prüfung der Systeme über das Internet ... 10
   4.1. Beschreibung der Vorgehensweise und des Ziels ... 10
   4.2. Projektverlauf und Ergebnisdarstellung ... 12
      4.2.1. Übersicht der Schwachstellen ... 12
      4.2.2. Sicherheitshinweise ... 17
      4.2.3. Übersicht der geprüften IP-Adressen ... 19
5. Prüfung Webanwendung über das Internet ... 20
   5.1. Beschreibung der Vorgehensweise und des Ziels ... 20
   5.2. Projektverlauf und Ergebnisdarstellung ... 23
      5.2.1. Übersicht der Schwachstellen ... 23
      5.2.2. Zuordnung der Schwachstellen zur OWASP Top 10 ... 30
      5.2.3. Ergebnisse der Überprüfung des Rechtemodells ... 31
      5.2.4. Sicherheitshinweise ... 31
         H_01 Zu lange Sitzungsdauer ... 31
         H_02 Fehlende HTTP-Security-Kopfzeilen (Header) ... 32
6. Anhang A: Versionen und Verzeichnisse ... 36
   6.1. Versionshistorie ... 36
   6.2. Abbildungsverzeichnis ... 36
   6.3. Tabellenverzeichnis ... 36
7. Anhang B: Ermittlung des Sicherheitsniveaus ... 38
   7.1. Ermittlung Sicherheitsniveau Prüfung der Systeme ... 38
   7.2. Ermittlung Sicherheitsniveau Webanwendungspenetrationstest ... 38

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 2. bis zum 24. August 2022 wurde ein Penetrationstest auf Systeme des Beispiel-Kunden (im Folgenden „Kunde“ genannt) durchgeführt. Ziel der Prüfungen war die Identifikation von Schwachstellen auf den Systemen.

Alle Prüfungen wurden über das Internet aus Sicht eines externen Angreifers ohne Kenntnisse der Aufgaben der Systeme oder des Aufbaus der Infrastruktur durchgeführt.

Das Prüfziel während des Penetrationstests waren die IP-Adressen des Netzes XXX.XXX.XXX.0/24

Um das Ziel zu erreichen, wurden die Adressen auf erreichbare Dienste auf allen 65.535 Ports TCP und aufgrund des sonst sehr hohen Zeitaufwands auf den „Common Ports“ UDP geprüft. Identifizierte Dienste wurden im Anschluss auf bekannte Schwächen abgetastet.

Sofern ein Dienst die Verschlüsselung von Daten auf dem Transportweg anbot, wurde die angetroffene Konfiguration mit den Empfehlungen der Technischen Richtlinie TR-02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgeglichen. Die Prüfungen erfolgten weitestgehend unter Zuhilfenahme von Werkzeugen, deren Ergebnisse durch den Prüfer ausgewertet und hinsichtlich Relevanz für den Kunden bewertet wurden.

Im Rahmen der Untersuchung konnten vier Schwachstellen und zwei Sicherheitshinweise identifiziert werden.

Eine Schwachstelle mit mittlerem Schweregrad lässt sich darauf zurückführen, dass Dienste bereitgestellt werden, die Secure Client-Initiated Renegotiation anbieten. Hierdurch kann durch den Client ein erneutes Aushandeln der für die verschlüsselte Kommunikation notwendigen Parameter beantragt werden („Secure Client-Initiated Renegotiation“). Dieser Vorgang beansprucht aufseiten des Servers bemerkbar Ressourcen, sodass hierüber ein Angriff möglich ist, der die Verfügbarkeit des Systems stark negativ beeinflussen kann (Denial-of-Service).

Als Schwachstelle mit niedrigem Schweregrad wurde bewertet, dass veraltete TLS-Protokollversionen (TLS 1.0 und TLS 1.1) angeboten werden. Diese sind gegenüber einer Vielzahl von Angriffen verwundbar und sollten nicht mehr eingesetzt werden.

Des Weiteren wurde eine veraltete Version des Mailservers „Microsoft Exchange“ identifiziert, für die mehrere Schwachstellen öffentlich bekannt sind. Durch die Schwachstellen ist es Angreifern unter anderem möglich, Schadcode auf dem System auszuführen („Remote Code Execution“). Dies wurde als Schwachstelle mit kritischem Schweregrad bewertet.

Es wurden mehrere Dienste (FTP, HTTP) identifiziert, die Daten auf unsichere Art und Weise übertragen. Die Daten werden unverschlüsselt und ohne Integritätsschutz übertragen. Somit können alle übertragenen Informationen, wie zum Beispiel Zugangs- oder persönliche Nutzerdaten von Angreifern mitgelesen und manipuliert werden. Hieraus resultiert eine Schwachstelle mit mittlerem Schweregrad.

Weiterhin wurden die folgenden beiden 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.

Bei der Prüfung wurden Dienste auf mehreren Adressen identifiziert, die verschlüsselt über das SSH- und 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 Informationstechnik[1]) entsprechen. Für diese Dienste wurden für TLS und SSH je ein Sicherheitshinweis gegeben.

Tabelle 1: Statistik identifizierter Schwachstellen Prüfung der Systeme

Gesamtanzahl Prüfobjekte	255
Anzahl der erreichbaren Prüfobjekte	66
Anzahl Systeme Sicherheitsniveau „Kritisch“	1
Anzahl Systeme Sicherheitsniveau „Niedrig“	9
Anzahl Systeme Sicherheitsniveau „Mittel“	14
Anzahl Systeme Sicherheitsniveau „Hoch“	5
Anzahl Systeme Sicherheitsniveau „Sehr hoch“	37
Gesamtbewertung Sicherheitsniveau	Mittel

Insgesamt lässt sich der getesteten Gesamtumgebung nur ein mittleres Sicherheitsniveau attestieren, da ein System mit einem kritischen Sicherheitsniveau, sowie 9 Systeme mit einem niedrigen Sicherheitsniveau identifiziert wurden.

[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 2. bis zum 24. August 2022 wurde die Webanwendung „Beispiel-Webanwendung“ des Kunden einer Sicherheitsüberprüfung in Form eines Penetrationstests unterzogen. Ziel des Penetrationstests war die Identifikation von technischen Schwachstellen.

Die Anwendung wurde zunächst mittels des automatisierten Scanwerkzeugs „Burp Suite Pro“ geprüft und die Ergebnisse manuell verifiziert. Weiterhin wurden manuelle Prüfungen durchgeführt um Schwächen der Anwendung identifizierten zu können.

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

Im Rahmen der Untersuchung konnten fünf Schwachstellen und zwei Sicherheitshinweise identifiziert werden.

Eine Schwachstelle mit hohem Schweregrad lässt sich darauf zurückführen, dass es während der Prüfungen möglich war, dass angemeldete Benutzer auf beliebige PDF-Dokumente zugreifen können. Hierfür werden jedoch die ID-Nummer und der Dokumenttitel benötigt. Durch die Anwendung erfolgt keine Prüfung, ob ein in der Anwendung angemeldeter Benutzer berechtigt ist, ein Dokument zu öffnen.

Als Schwachstelle mit mittlerem Schweregrad wurde bewertet, dass die Session-ID `JSESSIONID` beim Aufruf der Startseite generiert wird und selbst nach Kontextänderungen, z. B. vom anonymen zum angemeldeten Benutzer, unverändert bleibt. Lediglich nach dem Abmelden eines Benutzers ändert sich die Session-ID. Diese Tatsache begünstigt sogenannte Session-ID-Fixation-Angriffe. Sofern ein Angreifer die Session-ID kennt oder für ein Opfer vorbestimmen kann, ist es ihm möglich, Aktionen im Kontext eines Benutzers durchzuführen.

Eine Schwachstelle mit mittlerem Schweregrad lässt sich darauf zurückführen, dass die Webanwendung JavaScript-Bibliotheken von Drittanbietern einsetzt, die gegenüber bekannten Schwächen verwundbar sind. Durch das Ausnutzen der Schwachstellen ist ein Angreifer in der Lage, Cross-Site-Scripting-Angriffe durchzuführen, wodurch sich z. B. eigener (Schad-)Code in Anfragen platzieren ließe, der dann im Browser von potentiellen Opfern zur Ausführung kommt.

Eine weitere Schwachstellen mit mittlerem Schweregrad ist dadurch bedingt, dass es möglich ist, schadhaften JavaScript-Code in die Anwendung einzuschleusen (Cross-Site Scripting), der wiederum im Browser der Benutzer ausgeführt wird. Hierdurch könnten Angreifer beispielsweise Zugriff auf Zugangsdaten erhalten. Der Schadcode kann persistent eingefügt werden, sodass automatisch alle Benutzer angegriffen werden, die die Unterseite aufrufen, in der der Schadcode eingefügt wurde.

Mit einem niedrigen Schweregrad wurde bewertet, dass ein Benutzer, der sein Passwort vergessen hat, sich über die Passwort-vergessen-Funktion ein neues Passwort per Mail senden lassen kann. Wird in das Eingabefeld der Passwort-vergessen-Funktion ein Benutzername eingetragen, so gibt die Anwendung Rückmeldung darüber, ob an den Benutzer eine E-Mail versendet wurde oder ob es sich um einen der Anwendung unbekannten Benutzer handelt. Einem Angreifer ist es so möglich, mit geringem Aufwand und ausreichend Zeit in einem Brute-Force-Angriff gültige E-Mail-Adressen beziehungsweise Benutzerkonten zu erraten.

Weiterhin wurden die folgenden zwei 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.

Ein Sicherheitshinweis resultiert aus einer zu langen Sitzungsdauer bei Inaktivität. Wenn ein Nutzer in beispielsweise einem Internetcafé vergisst sich abzumelden, kann auch nach Stunden noch auf die aktive Sitzung zugegriffen werden, da diese nicht automatisch nach gewisser Zeit invalidiert wird.

Um das Sicherheitsniveau nachhaltig zu steigern können durch die Anwendung auch zusätzliche HTTP-Kopfzeilen gesetzt werden, um weitere, in Browser eingebaute Schutzmechanismen besser zu nutzen. Die aus Prüfersicht nutzbaren HTTP-Kopfzeilen wurde im Rahmen eines Sicherheitshinweises zusammengefasst.

Tabelle 2: Statistik identifizierter Schwachstellen Webanwendungsprüfung

Anzahl identifizierter Schwachstellen mit kritischem Schweregrad	0
Anzahl identifizierter Schwachstellen mit hohem Schweregrad	1
Anzahl identifizierter Schwachstellen mit mittlerem Schweregrad	3
Anzahl identifizierter Schwachstellen mit geringem Schweregrad	1
Gesamtanzahl identifizierter Schwachstellen	5
Gesamtanzahl identifizierter Sicherheitshinweise	2
Gesamtbewertung Sicherheitsniveau	Niedrig

Insgesamt lässt sich der Gesamtumgebung nur ein niedriges Sicherheitsniveau attestieren, da eine Schwachstelle mit hohem Schweregrad identifiziert werden konnte.

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. Common Vulnerability Scoring System

Zur Ermittlung des Schweregrads von Schwachstellen wird das Common Vulnerability Scoring System (CVSS) 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 in allen Ebenen der IT getroffen werden, um nachhaltige Resilienz zu erzielen. So werden z. B. Empfehlungen des BSI für Kryptografie herangezogen und Abweichungen aufgezeigt, auch wenn keine direkt ausnutzbaren Schwachstellen aus den Abweichungen resultieren. Der CVSS-Score solcher Feststellungen ist üblicherweise „None".

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 Fasle 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.

[2] https://www.first.org/cvss/

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

- S_ Schwachstellen bei Systemprüfungen und
- 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. Diese werden 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 2. bis zum 24. August 2022 wurde ein Penetrationstest auf Systeme des Kunden durchgeführt. Ziel der Prüfungen war die Identifikation von Schwachstellen auf den Systemen.

Die Prüfungen der Adressen wurden vollständig mit dem eigens entwickelten Framework „tajanas" durchgeführt. Tajanas basiert auf den etablierten Werkzeugen „nmap"[3] für Portscans, „testssl"[4] für die Überprüfung der Verschlüsselung der Daten auf dem Transportweg mittels TLS sowie „OpenVAS"[5] 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 eine Verschlüsselung der Daten auf dem Transportweg anbieten, so wurde ein Abgleich der vorherrschenden Konfiguration mit den Empfehlungen der Technischen Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (BSI-TR-02102[6]) vorgenommen.

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

Wie vorab festgelegt, wurden keine Angriffe durchgeführt, die einen Denial-of-Service zum Ziel haben.[7]

In vielen Linuxdistributionen 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.

---

[3] https://nmap.org/

[4] https://testssl.sh/

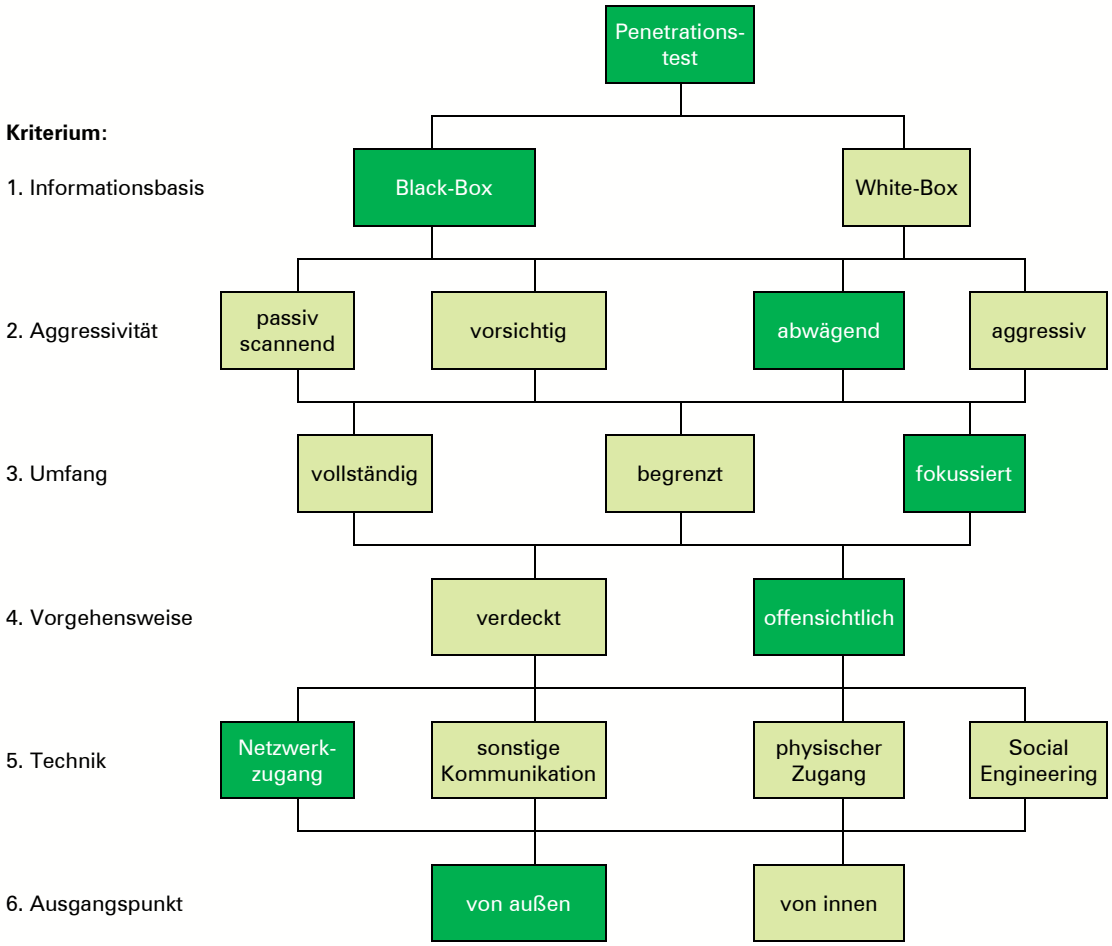
[5] http://www.openvas.org/index-de.html

[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

[7] Da die Prüfwerkzeuge in der Identifikation entsprechender Schwachstellen ohne einen DoS auszuführen sehr fehlerhaft sind, werden potentiell unzuverlässige Ergebnisse nicht aufgeführt.

Für den Penetrationstest wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“[8] zugrunde gelegt:

Abbildung 1: Vorgehensweise nach BSI-Studie



[8] https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.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 Secure Client-Initiated Renegotiation möglich

Beschreibung	Es werden Dienste bereitgestellt, die Secure Client-Initiated Renegotiation anbieten. Bei einer TLS-Renegotiation werden bestehende TLS-Verbindungsparameter neu ausgehandelt. Im Falle von Secure Renegotiation sind dabei serverseitig deutlich mehr Ressourcen als beim Client notwendig. Ist es dem Client in der Verbindung erlaubt, diese Secure Renegotiation selbst anzustoßen, so kann dies für einen Denial-of-Service-Angriff ausgenutzt werden.
Auswirkung	Durch wiederholtes Anfordern einer Secure Renegotiation kann ein Angreifer das Ziel unter große Last stellen, wodurch die Verfügbarkeit des Systems beeinträchtigt wird.
Empfehlung	Secure Renegotiation sollte nur vom Server und nicht vom Client initiierbar sein. Wenn möglich sollte TLS-Renegotiation allgemein deaktiviert werden.
Referenzen	https://blog.qualys.com/product-tech/2011/10/31/tls-renegotiation-and-denial-of-service-attacks „Tajanas Report [IP-Adresse].pdf“, wobei [IP-Adresse] die Adresse der geprüften Systeme darstellt (als Dateianhang zu diesem Dokument)
Schweregrad	Medium

Tabelle 3: Schweregrad Schwachstelle S_01

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung**
Attack Vector (AV)	Network	Weil der Dienst über ein Netzwerk erreichbar ist.
Attack Complexity (AC)	Low	Weil ein erfolgreicher Angriff keine besonderen Rahmenbedingungen voraussetzt.
Privileges Required (PR)	None	Weil der Angriff ohne Authentifizierung erfolgen kann.
User Interaction (UI)	None	Weil der Angriff unabhängig von anderen Benutzern durchgeführt werden kann.
Scope (S)	Unchanged	Weil der Autorisierungsbereich der Dienstes nicht verlassen wird.
Confidentiality Impact (C)	None	Weil der Angriff keine Auswirkung auf die Vertraulichkeit der Daten hat.

Integrity Impact (I)	None	Weil der Angriff keine Auswirkung auf die Integrität der Daten hat.
Availability Impact (A)	Low	Weil ein Angreifer das System durch den Angriff unter hohe Last stellen kann und damit zeitweise die Verfügbarkeit des Systems betroffen ist.
Score	Medium	5,3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

S_02 Veraltetes Transportverschlüsselungsprotokoll im Einsatz

Beschreibung

Bei der eingesetzten Transportverschlüsselung werden die veralteten Protokollversionen TLS 1.0 und 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 den Web- oder Application-Server 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

„Tajanas Report [IP-Adresse].pdf“, wobei [IP-Adresse] die Adresse der geprüften Systeme darstellt (als Dateianhang zu diesem Dokument)

Schweregrad

Low

Tabelle 4: Schweregrad Schwachstelle S_02

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Weil der Dienst über ein Netzwerk erreichbar ist.
Attack Complexity (AC)	High	Weil ein erfolgreicher Angriff eine Man-in-the-Middle-Position voraussetzt.
Privileges Required (PR)	None	Weil ein erfolgreicher Angriff keine Authentifizierung erfordert.

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
User Interaction (UI)	Required	Weil ein Opfer Daten mit dem betroffenen Dienst austauschen muss.
Scope (S)	Unchanged	Weil nur die Anwendung selbst betroffen ist.
Confidentiality Impact (C)	Low	Weil der Angreifer Einsicht in vertrauliche Daten erhalten, den Umfang der Daten aber selbst nicht kontrollieren kann.
Integrity Impact (I)	None	Weil das Mitlesen von Daten keine Auswirkungen auf die Datenintegrität hat.
Availability Impact (A)	None	Weil der Angriff keine Auswirkungen auf die Verfügbarkeit der Daten oder des Dienstes hat.
Score	Low	3,1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)

S_03 Verwundbarer Microsoft Exchange Server im Einsatz

Beschreibung

Es wurde die Verwendung des Servers „Microsoft Exchange“ in der Version 8.5 identifiziert. Für diese Version sind Schwachstellen öffentlich bekannt.

Auswirkung

Für die verwendete Version sind unter anderem folgende Schwachstellen bekannt:

- Angreifer können Schadcode auf dem Server ausführen (Remote Code Execution, bekannte Schwachstelle: CVE-2022-23277). Hierüber können Angreifer Zugriff auf sensible Daten erhalten und die Verfügbarkeit des Servers erheblich negativ beeinflussen.
- Angreifer mit Zugriff auf ein Benutzerkonto auf dem Server können Adminrechte erhalten (Privilege Escalation, bekannte Schwachstelle: CVE-2022-21978). Hierüber können Angreifer Zugriff auf sensible Daten erhalten und die Verfügbarkeit des Servers erheblich negativ beeinflussen.

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.

Über die genannten Schwachstellen sind nur wenige Informationen öffentlich bekannt. Bei der Schweregrad wurden daher offizielle Aussagen des Herstellers Microsoft (siehe Referenzen) zur Bewertung herangezogen.

Empfehlung

Der eingesetzte Microsoft Exchange Server sollte auf die aktuellste Version aktualisiert werden. Zur langfristigen Behebung der Schwachstelle sollte ein

Prozess etabliert werden, der dafür sorgt, dass regelmäßig überprüft wird, ob durch den Hersteller neue (Sicherheits-)Updates zur Verfügung gestellt werden, und wenn ja, dass diese eingespielt werden.

Um über Sicherheitsprobleme informiert zu werden, sollten die entsprechenden Mailinglisten abonniert werden.

Referenzen

https://support.microsoft.com/de-de/topic/hinweise-zum-sicherheitsupdate-f%C3%BCr-microsoft-exchange-server-2016-und-2019-10-mai-2022-kb5014261-cd5ecb59-a0eb-47ef-ae35-f62b13c8b817

https://support.microsoft.com/en-gb/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-and-2016-march-8-2022-kb5012698-440c5421-dc0e-448f-93ef-4e686c18f7c3

Schweregrad Kritisch (bewertet wurde CVE-2022-23277)

Tabelle 5: Schweregrad Schwachstelle S_03

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Da der Server über das Internet erreichbar ist.
Attack Complexity (AC)	Low	Da keine speziellen Vorbedingungen für einen Angriff gelten.
Privileges Required (PR)	Low	Da einfache Benutzerrechte für einen Angriff notwendig sind.
User Interaction (UI)	None	Da keine Benutzerinteraktion notwendig ist.
Scope (S)	Changed	Da durch die Schwachstelle Code auf dem System zur Ausführung gebracht werden und somit der Autorisierungs-bereich des Exchange Servers verlassen werden kann.
Confidentiality Impact (C)	High	Da Angreifer Schadcode ausführen und darüber gezielten Zugriff auf sensible Daten erhalten können.
Integrity Impact (I)	High	Da Angreifer Schadcode ausführen und darüber gezielten Zugriff auf sensible Daten erhalten können.
Availability Impact (A)	High	Da Angreifer Schadcode ausführen und damit die Erreichbarkeit des Servers fortwährend negativ beeinflussen können.
Score	Kritisch	9,9 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

S_04 Unsichere Kommunikation

Beschreibung

Die Kommunikation mit mehreren Diensten ist über unsichere Kanäle möglich (Details siehe Beispiele). Jegliche bei der Nutzung der Webanwendung übertragenen Informationen, wie zum Beispiel Zugangsdaten, werden unverschlüsselt und ohne Integritätsschutz übertragen.

Auswirkung

Ein Angreifer in einem Man-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

Es wurden die folgenden unsicheren Protokolle bzw. Dienste identifiziert:

Tabelle 6: Identifizierte unsichere Kommunikationsmöglichkeiten

Dienst	Adresse mit Port	Problembeschreibung
FTP	{IP-Adresse}, 21/tcp	Übertragene Daten (Benutzerlogin, Datenübertragung über FTP) werden unsicher übertragen und können von Angreifern mitgelesen sowie modifiziert werden.
HTTP	{IP-Adresse}, 6303/tcp, {IP-Adresse}, 8801/tcp, {IP-Adresse}, 8801/tcp	Auf diesen Adressen werden Web-anwendungen über das unsichere HTTP-Protokoll angeboten. Es kann nicht eingeschätzt werden, welchen Verwendungszweck die Anwendungen haben, es liegt jedoch immer eine Loginmaske vor. Die dort eingege-benen Logindaten sowie alle Anwendungsdaten werden unsicher übertragen.

Hinweis: In einem realen Ergebnisbericht würden an dieser Stelle Screenshots zur besseren Nachvollziehbarkeit dargestellt werden.

Empfehlung

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

Konkret sollten die folgenden Vorkehrungen getroffen werden:

- Statt FTP sollten die sicheren Varianten FTPS (FTP über SSL/TLS) oder SFTP (FTP über SSH) verwendet und sicher konfiguriert werden.
- Statt HTTP sollte die sichere Variante HTTPS verwendet und sicher konfiguriert werden.

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

Medium

Tabelle 7: Schweregrad Schwachstelle S_04

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Weil der Dienst über das Internet erreichbar ist.
Attack Complexity (AC)	High	Weil der Angreifer sich in einer Man-in-the-Middle-Position befinden muss.
Privileges Required (PR)	None	Weil der Angreifer keine Berechtigungen oder Zugangsdaten benötigt.
User Interaction (UI)	Required	Weil ein legitimer Nutzer Daten an den Dienst übertragen muss, damit der Angreifer diese mitlesen kann.
Scope (S)	Unchanged	Weil durch den Angriff lediglich der Dienst selbst betroffen ist.
Confidentiality Impact (C)	Low	Da der Angreifer gegebenenfalls Zugriff auf sensible Daten erhalten, deren Umfang jedoch nicht kontrollieren kann.
Integrity Impact (I)	Low	Der Angreifer kann die übertragenen Daten abfangen und verändern und somit die Integrität der Anwendung bzw. des Dienstes beeinträchtigen. Der Angreifer hat dabei jedoch keine Kontrolle darüber, welche Daten übertragen und somit manipuliert werden können.
Availability Impact (A)	None	Der Angriff hat keine Auswirkung auf die Verfügbarkeit der Anwendung oder des Dienstes.
Score	Medium	4,2 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A: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 Transportverschlüs-

selung“ 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

„Tajanas Report [IP-Adresse].pdf“, wobei [IP-Adresse] die Adresse der geprüften Systeme darstellt (als Dateianhang zu diesem Dokument)

H_02 Nicht BSI-konforme SSH-Konfigurationen 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

„Tajanas Report [IP-Adresse].pdf“, wobei [IP-Adresse] die Adresse der geprüften Systeme darstellt (als Dateianhang zu diesem Dokument)

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, wir die Tabelle hier lediglich angedeutet. Um den Kunden eine Weiterarbeit mit den Ergebnissen zu erleichtern, erhalten Sie diese natürlich auch im Excel-Format.

Systeme	Erreichbarkeit	Schwachstellen	Schweregrad	Port	Sicherheits-niveau System
XXX.XXX.XXX.4	erreichbar	S_01 Secure Client-Initiated Renegotiation möglich	Medium	25/tcp	Mittel
XXX.XXX.XXX.5	erreichbar	S_02 Veraltetes Transportverschlüsselungsprotokoll im Einsatz	Low	443/tcp	Hoch
XXX.XXX.XXX.69	erreichbar	S_01 Secure Client-Initiated Renegotiation möglich	Medium	443/tcp	Kritisch
		S_02 Veraltetes Transportverschlüs-selungsprotokoll im Einsatz	Low		
		S_03 Verwundbarer Microsoft Exchange Server im Einsatz	Critical		
XXX.XXX.XXX.71	erreichbar	H_01 Nicht BSI-konforme Cipher Suites/Verschlüsselungsprotokolle im Einsatz	-	443/tcp	Sehr hoch
		H_02 Nicht BSI-konforme SSH-Konfigurationen im Einsatz	-	22/tcp	

5. PRÜFUNG WEBANWENDUNG ÜBER DAS INTERNET

5.1. Beschreibung der Vorgehensweise und des Ziels

Im Zeitraum vom 2. bis zum 24. August 2022 wurde die Webanwendung „Beispiel-Webanwendung“ des Kunden einer Sicherheitsüberprüfung in Form eines Penetrationstests unterzogen. Ziel des Penetrationstests war die Identifikation von technischen Schwachstellen.

Die Anwendung wurde in der Abnahmeumgebung geprüft und war erreichbar unter der URL https://www.beispiel-kunde.de.

Die Anwendung wurde zunächst mittels automatisierter Scanwerkzeuge abgetastet. Verwendet wurde hierfür das Werkzeug „Burp Suite Pro“[9]. 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. Zur Überprüfung von SQL-Schwachstellen wurde das Open-Source-Tool „sqlmap“[10] genutzt.

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.

Die Webanwendung wurde sowohl als anonymer Benutzer ohne Zugangsdaten als auch als registrierter Benutzer mit Zugangsdaten geprüft.

Der Kunde übergab die Zugangsdaten für die folgenden Benutzerzugänge:

- testbenutzer1@beispiel-kunde.de,
- testbenutzer2@beispiel-kunde.de,
- testbenutzer3@beispiel-kunde.de,
- testbenutzer4@beispiel-kunde.de,
- testbenutzer5@beispiel-kunde.de,

Um einen Überblick über die Berechtigungen der einzelnen Benutzer zu erhalten, wurde die Anwendung mit den übergebenen Benutzern durch den Prüfer verwendet und die aktuelle Ist-Situation der verfügbaren Funktionen pro Benutzer aus Sicht des Prüfers erfasst.

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

Für die Überprüfung des Rechtemodells wurde durch den Prüfer zunächst eine Tabelle mit den Funktionen pro Benutzer erstellt. Hierbei wurden vier Funktionen mit Einschränkungen der Berechtigungen durch die Anwendung identifiziert.

Für die Überprüfung des Rechtemodells wurde durch den Prüfer zunächst eine Tabelle mit den Funktionen pro Benutzer erstellt. Hierbei wurden vier Funktionen mit Einschränkungen der Berechtigungen durch die Anwendung identifiziert.

[9] https://www.portswigger.net

[10] https://sqlmap.org

Tabelle 8: Übersicht der Funktionen

Funktion	Beschreibung
Meldungen	Der Benutzer kann Daten (Meldungen) hochladen, den Meldungsverlauf ansehen und ältere Meldungen löschen.
Postfach	Der Benutzer kann Benachrichtigungen anzeigen lassen und Bestätigungen über angeforderte Dokumente abrufen.

Für die Prüfung dieser Funktionen wurden drei unterschiedliche Benutzerzugänge mit unterschiedlichen Berechtigungen verwendet:

- testbenutzer1: hat nur Zugriff auf seine eigenen Daten,
- testbenutzer2: hat nur Zugriff auf seine eigenen Daten,
- testbenutzer3: hat Zugriff auf die Daten von testbenutzer2.

Tabelle 9: Übersicht des Berechtigungsmodells

Besitzer	Funktion	Zugriff durch Benutzer		
		Testbenutzer1	Testbenutzer2	Testbenutzer3
Testbenutzer2	Meldungen	Ja	Nein	Nein
	Postfach	Ja	Nein	Nein
Testbenutzer3	Meldungen	Nein	Ja	Ja
	Postfach	Nein	Ja	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 TOP10 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.

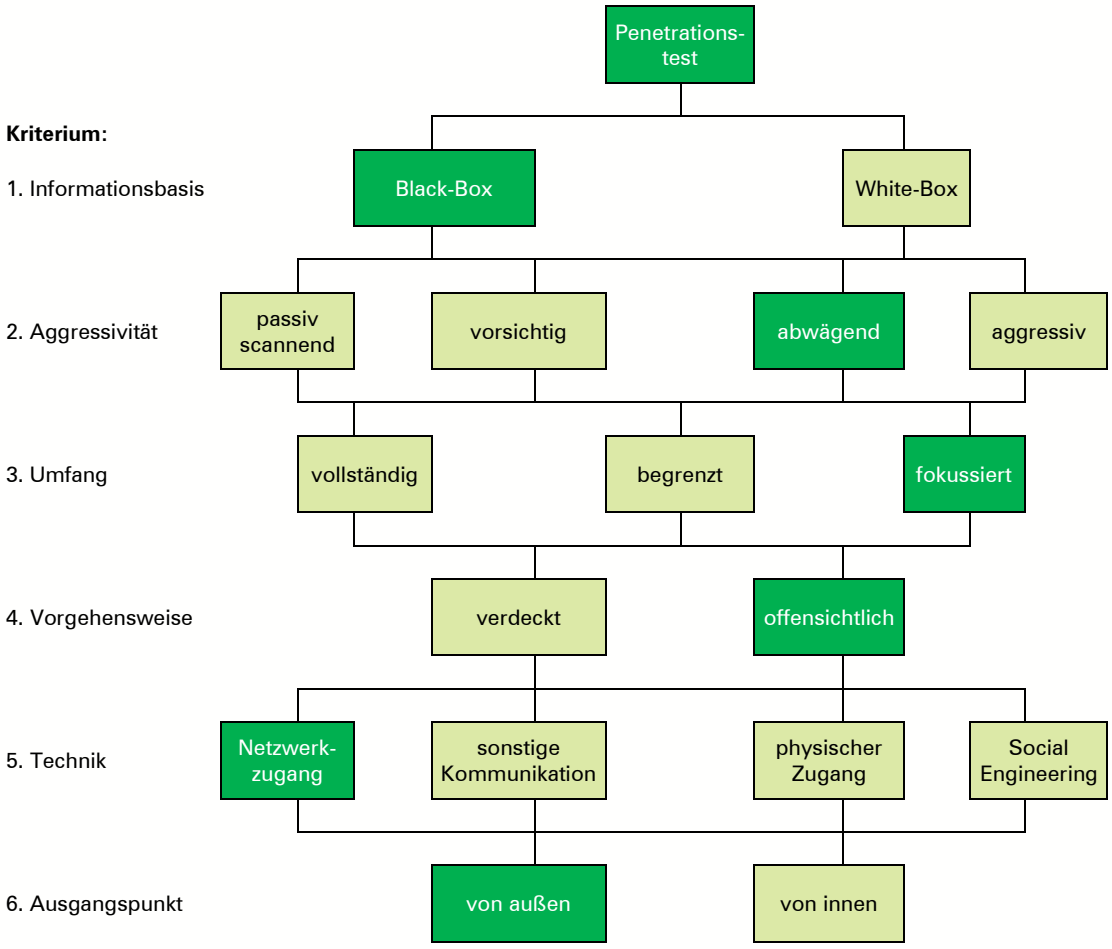
Zusätzlich wurden weitere Analysen durchgeführt, die über die in der OWASP Top 10 benannten Risiken hinausgehen und durch den Testplan vorgegeben sind. Diese primär manuellen Untersuchungen dienen zur Prüfung der Anwendungslogik, indem dort gezielt Fehler provoziert und ausgenutzt werden sollen.

Die Webanwendung wurde in der Version 7.3 geprüft.

Für den Penetrationstest wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“[11] zugrunde gelegt:

[11] https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.html

Abbildung 2: Vorgehensweise nach BSI-Studie Prüfung Webanwendung über das Internet



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 Verwundbare JavaScript-Bibliothek im Einsatz

Beschreibung

Durch die Webanwendung werden JavaScript-Bibliotheken von Drittanbietern eingesetzt. Es wurden veraltete Bibliotheken identifiziert, die gegenüber bekannten Schwächen verwundbar sind. Im Abschnitt „Beispiel“ werden die identifizierten Bibliotheken aufgeführt.

Auswirkung

Durch das Ausnutzen der Schwachstellen ist ein Angreifer in der Lage, Cross-Site-Scripting-Angriffe durchzuführen, wodurch sich z. B. eigener (Schad-)Code in Anfragen platzieren ließe, der dann im Browser von potentiellen Opfern zur Ausführung kommt.

Beispiel

Folgende Versionen wurden als veraltet erkannt:

Tabelle 10: Identifizierte, verwundbare Bibliotheken

Host / Pfad	Bibliothek	Version	Bekannte Schwachstelle(n)
/js/jquery-3.3.1.min.js	jQuery	3.3.1	CVE-2020-11022 CVE-2020-11023 CVE-2020-11358

Hinweis

Die Informationen basieren auf Versionsinformationen. Für einen erfolgreichen Angriff gelten Randbedingungen: Die verwundbare Funktion der Bibliothek muss durch die Anwendung verwendet werden. Dies wurde durch die Prüfer nicht verifiziert und sollte daher durch einen Entwickler untersucht werden. Ferner muss ein Opfer dazu gebracht werden, einen vom Angreifer präparierten Link anzuklicken.

Die Feststellung der Versionsnummer beruht auf Versionsangaben aus der Serverantwort und den Analyseergebnissen der verwendeten Werkzeuge Da Versionsinformationen 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.

OWASP Top 10

2021 A06 – Vulnerable and Outdated Components

Empfehlung

Aktualisieren der Bibliotheken auf die aktuellste Version. Sämtliche im Einsatz befindlichen Bibliotheken und Frameworks von Drittherstellern sollten in regelmäßigen Abständen bzw. zeitnah nach dem Bekanntwerden von Schwachstellen aktualisiert werden.

Um der Schwachstelle nachhaltig zu begegnen, sollte das Vorgehen zum Patch- und Änderungsmanagement angepasst werden. Verantwortliches Personal (z. B. Entwickler) sollte sich aktiv über das Bekanntwerden von Schwachstellen der im Einsatz befindlichen Bibliotheken und Frameworks informieren. Dies kann z. B. durch das Abonnieren von Mailinglisten (Announcements) oder Schwachstellen-

informationsdiensten geschehen. Patches sollten zeitnah auf Kompatibilität in der Testumgebung getestet und danach in eine Produktivumgebung ausgerollt werden.

Referenzen https://nvd.nist.gov/vuln/detail/CVE-2019-11358

Schweregrad Medium

Tabelle 11: Schweregrad Schwachstelle W_01

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Weil die Anwendung über das Internet erreichbar ist.
Attack Complexity (AC)	High	Da die verwundbare Komponente in der Bibliothek von der Webanwendung benutzt werden muss, damit die Schwachstelle ausnutzbar ist.
Privileges Required (PR)	Low	Da zum erfolgreichen Ausnutzen der Schwachstelle ein Standard Benutzerzugang benötigt werden.
User Interaction (UI)	Required	Da für einen erfolgreichen Angriff ein Opfer auf einen vom Angreifer präparierten Link klicken muss.
Scope (S)	Changed	Da der Schadcode im Browser eines Opfers zur Ausführung kommt und dadurch der Scope verlassen wird.
Confidentiality Impact (C)	Low	Da durch einen erfolgreichen Angriff sensible Daten an den Angreifer gelangen können, dieser aber Art und Umfang der Daten schwer vorhersagen bzw. kontrollieren kann.
Integrity Impact (I)	Low	Da durch einen erfolgreichen Angriff sensible Daten im Browser verändert dargestellt werden könnten, ein Angreifer aber Art und Umfang der Daten schwer vorhersagen bzw. kontrollieren kann.
Availability Impact (A)	None	Da das erfolgreiche Ausnutzen der Schwachstelle keine Auswirkungen auf die Verfügbarkeit der Anwendung bzw. der darin verarbeiteten Daten hat.
Score	Medium	4,4 (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N)

W_02 Erraten von Benutzerzugängen über die Passwort-vergessen-Funktion

Beschreibung	Wenn ein Benutzer sein Passwort vergessen hat, kann er sich über die Passwort-vergessen-Funktion ein neues Passwort per Mail senden lassen. Wird in das Eingabefeld der Passwort-vergessen-Funktion ein Benutzername eingetragen, so gibt die Anwendung Rückmeldung darüber, ob an den Benutzer eine E-Mail versendet wurde oder ob es sich um einen der Anwendung unbekannten Benutzer handelt.
Auswirkung	Einem Angreifer ist es möglich, mit geringem Aufwand und ausreichend Zeit in einem Brute-Force-Angriff gültige E-Mail-Adressen beziehungsweise Benutzerkonten zu erraten.
OWASP Top 10	2021 A05 - Security Misconfiguration
Empfehlung	Die Anwendung sollte keine Rückschlüsse darauf zulassen, ob eine E-Mail-Adresse registriert ist oder nicht. Dem Benutzer sollte eine einheitliche Meldung angezeigt werden.
Referenzen	https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet
Schweregrad	Low

Tabelle 12: Schweregrad Schwachstelle W_02

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Die Schwachstelle ist aus dem Internet ausnutzbar.
Attack Complexity (AC)	High	Durch den hohen zeitlichen Aufwand und das automatisieren des Angriffs ist fachwissen Notwendig.
Privileges Required (PR)	None	Es werden keine besonderen Rechte benötigt.
User Interaction (UI)	None	Es wird keine Benutzerinteraktion benötigt.
Scope (S)	Unchanged	Durch das Ausnutzen der Schwachstelle erlangt der Angreifer keine Kontrolle über das System.
Confidentiality Impact (C)	Low	Durch das Ausnutzen der Schwachstelle kann der Angreifer Rückschlüsse auf Benutzerkonten treffen.
Integrity Impact (I)	None	Die Integrität der Informationen ist nicht betroffen.
Availability Impact (A)	None	Die Verfügbarkeit des Dienstes und der Informationen ist nicht gefährdet.
Score	Low	3,7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

W_03 Fehlerhaftes Sessionmanagement

Beschreibung	Die Session-ID `JSESSIONID` wird beim Aufruf der Startseite generiert und bleibt selbst nach Kontextänderungen, z. B. vom anonymen zum angemeldeten

	Benutzer, unverändert. Lediglich nach dem Abmelden eines Benutzers ändert sich die Session-ID.
Auswirkung	Diese Tatsache begünstigt sogenannte Session-ID-Fixation-Angriffe. Sofern ein Angreifer die Session-ID kennt oder für ein Opfer vorbestimmen kann, ist es ihm möglich, Aktionen im Kontext eines Benutzers durchzuführen.
Beispiel	Der Angreifer öffnet die Startseite bzw. Anmeldeseite an einem von mehreren Personen genutzten Rechner. Dabei kopiert er sich die erzeugte Session-ID. Anschließend meldet sich ein Benutzer an der Anwendung unter Verwendung desselben Computers an. Da sich die Session-ID nicht verändert, kann der Angreifer selbst an einem anderen Rechner dieselbe Session-ID verwenden, um im Kontext des angemeldeten Benutzers Aktionen auszuführen.
Hinweis	Bei der Abmeldung wird die Session-ID ungültig und es wird eine neue Session-ID erzeugt. Damit könnte der Angreifer nach der Abmeldung des Benutzers dessen Session nicht weiterverwenden.
OWASP Top 10	2021 A01 – Broken Access Control
Empfehlung	Nach einer Kontextänderung wie einer erfolgreichen Anmeldung oder Abmeldung eines Benutzers sollte das Session-Token neu generiert werden. Das alte Session-Token sollte damit seine Gültigkeit verlieren.
Referenzen	https://www.owasp.org/index.php/Session_fixation
Schweregrad	Medium

Tabelle 13: Schweregrad Schwachstelle W_03

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Die Session-ID kann erraten werden und über das Internet ausgenutzt werden.
Attack Complexity (AC)	High	Der Angreifer muss in der Lage sein, eine eigene Session durch den Benutzer authentisieren zu lassen oder die Session zu erraten. Dies erfordert technisches Fachwissen.
Privileges Required (PR)	None	Der Angreifer benötigt keine besonderen Rechte zur Ausnutzung der Schwachstelle.
User Interaction (UI)	Required	Der Benutzer muss sich bereits authentisiert haben, bzw. eine durch den Angreifer übermittelte Session authentisieren.
Scope (S)	Unchanged	Der Angreifer erhält keine Kontrolle über das System.
Confidentiality Impact (C)	High	Der Angreifer erhält lesenden Zugriff auf Daten des Benutzers
Integrity Impact (I)	High	Der Angreifer kann Aktionen im Kontext des Benutzers ausführen und Daten verändern.
Availability Impact (A)	None	Ziel eines solchen Angriffs ist es in der Regel nicht, die Verfügbarkeit zu stören.

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Score	Medium	6,8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)

W_04 Unautorisierter Download von PDF-Dateien

Beschreibung

Jeder registrierte Benutzer verfügt über ein Postfach. Auf dieses wird mittels einer eindeutigen ID-Nummer *idn* zugegriffen. Alle Nachrichten in diesem Postfach sind als PDF-Dateien verfügbar, die über eindeutige Dokumenttitel referenziert werden.

Durch die Anwendung erfolgt keine Prüfung, ob ein in der Anwendung angemeldeter Benutzer berechtigt ist, ein Dokument zu öffnen.

Auswirkung

Ein angemeldeter Benutzer ist in der Lage, beliebige Dokumente aus beliebigen Postfächern zu öffnen. Hierfür muss der Benutzer jedoch die ID-Nummer `idn` und den Dokumenttitel kennen.

Da die Dokumenttitel und ID-Nummer einer festgelegten Struktur entsprechen, wird davon ausgegangen, dass es einem angemeldeten Benutzer leicht möglich ist, Dokumenttitel und Betriebskontennummern zu erraten oder durch Brute-Force-Angriffe herauszufinden.

Beispiel

Im Postfach des Benutzers `testbenutzer1@beispiel-kunde.de` liegt eine Bestätigung über eine Datenänderung. Diese Bestätigung kann über die URL https://abnahme.webapps.beispiel-kunde.de/css-webapp/javax.faces.resource/dynamiccontent.properties.sbo?ln=primefaces&v=6.1&pfdrid=8f9636f9a174f27707f2b7f98992bbc2&pfdrt=sc&idn=testbenutzer1&dokumentenTitel=Daten%C3%A4nderung+09.11.2017+13%3A12%3A43

Diese URL kann auch von einem anderen angemeldeten Benutzer aufgerufen und das PDF angezeigt werden. Während der Prüfungen wurde hierfür das Benutzerkonto des Benutzers `testbenutzer2@beispiel-kunde.de` verwendet. Nachdem dieser sich in der Webanwendung angemeldet hatte, war es ihm ebenfalls möglich, das PDF-Dokument des Benutzers `testbenutzer1@beispiel-kunde.de` anzuzeigen.

OWASP Top 10

2021 A01 – Broken Access Control

Empfehlung

Es sollte ein Mechanismus implementiert werden, der bei jedem Dokumentzugriff prüft, ob der Benutzer autorisiert ist, das Dokument zu öffnen. Es sollte verhindert werden, dass nicht autorisierte Benutzer Dokumente öffnen und anzeigen können.

Referenzen

https://www.owasp.org/index.php/Category:Access_Control

Schweregrad

High

Tabelle 14: Schweregrad Schwachstelle W_04

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Die Schwachstelle ist über das Internet ausnutzbar.
Attack Complexity (AC)	Low	Es sind keine besonderen fachlichen Kompetenzen nötig um die Schwachstelle auszunutzen.
Privileges Required (PR)	None	Jeder angemeldete Nutzer kann die Schwachstelle ausnutzen.
User Interaction (UI)	None	Es ist keine Benutzerinteraktion notwendig.
Scope (S)	Unchanged	Durch das Ausnutzen der Schwachstelle bekommt der Angreifer keine Kontrolle über andere Geräte.
Confidentiality Impact (C)	High	Jede beliebige Nachricht kann ausgelesen werden.
Integrity Impact (I)	None	Die Integrität der Nachricht wird nicht beeinträchtigt.
Availability Impact (A)	None	Die Verfügbarkeit der nachrichten wird nicht beeinträchtigt.
Score	High	7,5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

W_05 Persistentes Cross-Site Scripting (XSS)

Beschreibung

An die Webanwendung übermittelte Benutzereingaben werden nur unzureichend auf schädliche Inhalte gefiltert. Die Benutzereingaben werden unverändert in den Datensatz der Anwendung gespeichert und beim Aufruf der Seite ausgeführt.

Folgende Skripte und Parameter wurden während der Prüfung als angreifbar identifiziert:

Tabelle 15: Auflistung der verwundbaren Skripte und Parameter persistentes XSS

Endpunkt	Parameter
`/api/{…}`	`Name`

In realen Kundenprojekten werden in dieser Tabelle alle identifizierten verwundbaren Aufrufe dokumentiert. Da es sich hier um einen Beispiel-Ergebnisbericht handelt, wird die Darstellung lediglich skizziert.

Auswirkung	Ein Angreifer kann schädliche Inhalte wie beispielsweise JavaScript-Code in die Anwendung einschleusen, die im Browser der Benutzer zur Ausführung kommen. Die schädlichen Inhalte werden dabei dauerhaft innerhalb der Anwendung gespeichert. Dies kann beispielsweise dazu ausgenutzt werden, um sensible Daten einzelner Benutzer zu erlangen oder Informationen innerhalb der Anwendung zu manipulieren.
Beispiel	Wenn Sie der folgenden Anleitung folgen, führen Sie einen persistenten XSS-Angriff durch: 1. Anmelden an der Anwendung als ein Benutzer. 2. Navigieren in das Menü {xxx} und klicken auf das Plus-Icon, um ein neues Element zu erstellen. 3. Verwundbar ist der Name des erstellten Elements, dieser wird direkt in die Darstellung der Anwendung übernommen. So ist jeder der aufgelisteten Einträge verwundbar. 4. Wird beispielsweise ein neuer Ordner erstellt, kann dieser mit dem folgenden JavaSkript Code benannt werden: `<script>alert('xss im Ordnernamen');</script>` Hinweis: In einem realen Ergebnisbericht folgen hier Screenshots. Da es sich hier um einen exemplarischen Bericht handelt, wurde an die Darstellung von Screenshots verzichtet.
Hinweis	Aufgrund der Vielzahl von Übergabeparametern sind die als Beispiele benannten Skripte und Parameter lediglich zur besseren Nachvollziehbarkeit aufgeführt. Die Beispiele bilden keine vollständige Liste des Auftretens der Schwachstelle ab.
OWASP Top 10	2021 A03 – Injection
Empfehlung	Zur vollständigen Behebung der Schwachstelle sollte sichergestellt werden, dass eine Prüfung sämtlicher an die Webanwendung übergebenen Parameter z. B. mittels Allowlists durchgeführt und zusätzlich Sonderzeichen bei der Rückgabe in den HTML-Code gefiltert bzw. durch korrektes Encoding für den Zielkontext unschädlich gemacht werden.
Referenzen	https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
Schweregrad	Medium

Tabelle 16: Schweregrad Schwachstelle W_05

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Vector (AV)	Network	Weil die Anwendung über ein Netzwerk erreichbar ist.
Attack Complexity (AC)	Low	Weil keine speziellen Voraussetzungen für einen erfolgreichen Angriff gelten.

Schwachstellenbewertung entlang CVSS v3.1 (Base Score)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Privileges Required (PR)	Low	Der Angreifer benötigt mindestens Benutzerberechtigungen in der betroffenen Anwendung um die Schwachstelle auszunutzen.
User Interaction (UI)	None	Da ein Benutzer zufällig an die Stelle in der Anwendung navigieren kann, wo der Schadcode dann automatisch ausgeführt wird.
Scope (S)	Changed	Die Schwachstelle betrifft die Webanwendung, die Ausführung des JavaScript-Codes findet jedoch im Browser des Nutzers statt.
Confidentiality Impact (C)	Low	Der Angreifer kann gegebenenfalls sensible Daten einzelner Nutzer erlangen.
Integrity Impact (I)	Low	Der Angreifer kann gegebenenfalls die Darstellung der Daten in der Anwendung manipulieren.
Availability Impact (A)	None	Der Angriff beeinträchtigt nicht die Verfügbarkeit der Daten der Webanwendung.
Score	Medium	6,4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

5.2.2. Zuordnung der Schwachstellen zur OWASP Top 10

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

Tabelle 17: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-Top-10-Risiken

Risiko	Fail/Pass
2021 A01 – Broken Access Control	Fail
2021 A02 – Cryptographic Failures	Pass
2021 A03 – Injection	Fail
2021 A04 – Insecure Design	Pass
2021 A05 – Security Misconfiguration	Fail*
2021 A06 – Vulnerable and Outdated Components	Fail
2021 A07 – Identification and Authentication Failures	Pass

Risiko	Fail/Pass
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 sowie mit einer Zahl versehenen Spalten, konnte ein Ausbruch aus dem identifizierten Rechtemodell festgestellt werden.

Tabelle 18: Übersicht der Ergebnisse der Prüfung des Rechtemodells

Besitzer	Funktion	Zugriff durch Benutzer		
		Testbenutzer1	Testbenutzer2	Testbenutzer3
Testbenutzer2	Meldungen	Ja	Nein	Nein
	Postfach	Ja	Ja	Ja
Testbenutzer3	Meldungen	Nein	Ja	Ja
	Postfach	Ja	Ja	Ja

5.2.4. 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 Anwendung zusätzlich erhöhen.

H_01 Zu lange Sitzungsdauer

Beschreibung: Innerhalb der Anwendung erstellte Sitzungen bleiben auch nach mehreren Stunden Inaktivität intakt. Während der Prüfung konnte die Sitzung auch nach zwei Stunden und 30 Minuten Inaktivität weiterverwendet werden. Während einer Berater Sitzung blieb die Sitzung auch über Nacht aktiv.

Auswirkung: Ein unbedarfter Nutzer könnte durch eingegebene Daten an öffentlichen Systemen, wie in Internet-Cafés oder an gemeinsam genutzten Arbeitsplätzen, eine Sitzung innerhalb der Anwendung erstellen. Wenn der Nutzer vergisst sich abzumelden, kann auch nach Stunden noch auf die aktive Sitzung zugegriffen werden. Daher ist es mittlerweile übliche Praxis, diese automatisch bei Inaktivität zu invalidieren und den Nutzer abzumelden.

OWASP Top 10: 2021 A05 – Security Misconfiguration

Empfehlung: Die OWASP-Foundation empfiehlt bei Inaktivität die Sitzung nach 15-30 Minuten zu invalidieren.

Die Gültigkeit sollte mittels `Expires` oder `Max-Age` auf einen angemessenen Zeitraum beschränkt werden, bspw. die durchschnittliche Verwendungsdauer der Anwendung durch einen legitimen Benutzer.

Referenzen https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#session-expiration

H_02 Fehlende HTTP-Security-Kopfzeilen (Header)

Beschreibung Die Anwendung bzw. deren Webserver setzt in der Antwort einige Header nicht, die (zusätzlichen) Schutz vor Angriffen bieten würden, da diese Sicherheitsmechanismen in Browsern aktivieren.

Es wurde festgestellt, dass die Anwendung HTTP Strict Transport Security nicht umsetzt.

Auswirkung Allgemein führt das Fehlen dieser Header dazu, dass die entsprechenden Sicherheitsmechanismen nicht aktiviert werden. Dies erhöht die Wahrscheinlichkeit für erfolgreiche Angriffe.

Bei HSTS wird der Browser angewiesen, nach der ersten Verwendung der Anwendung diese fortan nur noch per gesicherten Kanal (HTTPS) anzusprechen (Trust On First Use – TOFU). Weiterhin wird durch den Browser die Genehmigung von Ausnahmen bei fehlerhafter Zertifikatsprüfung verweigert. So werden auch Man-in-the-Middle-Angriffe erschwert.

Durch den Einsatz einer Content-Security-Policy (CSP) kann durch die Anwendung die Nutzung von Ressourcen (wie z. B. JavaScript oder andere, teilweise Aktive Inhalte) in Browsern reglementiert werden. Ferner kann das Einbetten der Webseite in andere Seiten unterbunden werden. So kann das Einbinden fremder Ressourcen oder das Ausführen von eingeschleustem Script-Code durch eine restriktive CSP unterbunden werden, sodass der Browser diese nicht nachlädt oder ausführt.

Beispiel: Mittels des Tools „cURL“ können die Antwort-kopfzeilen des Servers ausgelesen werde. Die folgende Schrittabfolge beschreibt diesen Vorgang.

1. Öffnen eines neuen cmd.exe Fensters durch betätigen der Tasten „Win+R“ und dann eintragen von cmd.exe.
2. Eintragen des folgenden Befehls. Die Parameter „-s“ und „-D-“ deaktivieren zusätzliche unnötige Ausgaben des Tools (-s) und zeigen die gewollten Antwort-Kopfzeilen an (-D-):
   ```
   curl -s -D- "{ADRESSE DER WEBANWENDUNG}"
   ```
3. Absenden des Befehls.

Nun können alle verwendeten Antwort-Kopfzeilen ausgelesen werden.

Hinweis Folgende Kopfzeilen, die bei korrekter Konfiguration die Sicherheit der Webanwendung erhöhen, wurden nicht gesetzt:

Tabelle 19: Fehlende HTTP-Kopfzeilen zur Erhöhung der Sicherheit der Webanwendung

Header	Beschreibung	Vorgeschlagener Wert
Strict-Transport-Security	Mittels HTTP Strict Transport Security (HSTS) weist der Webserver den Browser an, zukünftig nur verschlüsselt über HTTPS mit ihm zu kommunizieren. Zudem wird durch die gängigen Browser fortan das Konfigurieren von Ausnahmen bei fehlerhafter Zertifikatsprüfung verweigert. Wird die Webanwendung mit HSTS-Header einmal aufgerufen, wird der Browser für die in Sekunden gesetzte Dauer alle Aufrufe nur noch verschlüsselt ausführen, selbst wenn der Nutzer „http://“ eingibt. Dies kann zudem für alle Subdomains erzwungen werden.	`Strict-Transport-Security: max-age=31536000 ; includeSubDomains`

X-Frame-Options	X-Frame-Options-Header verbessern den Schutz von Webanwendungen vor Clickjacking. Beim Clickjacking wird die Ziel-Anwendung über einen Frame in eine präparierte Webseite eingebunden und durch andere von einem Angreifer definierte Inhalte überlagert. Der Benutzer hat den Anschein, mit den sichtbaren Elementen im Vordergrund zu interagieren, löst aber Aktionen in der ihm nicht sichtbaren Anwendung im Hintergrund aus.
	X-Frame-Options-Header sind veraltet und in den meisten Browsern durch frame ancestor (siehe Content Security Policy) abgelöst. Es sollten beide Header parallel eingesetzt werden, da Browser die X-Frame-Options-Header ignorieren, wenn CSP frame ancestors implementiert sind.
		`X-Frame-Options: deny`
		oder
		`X-Frame-Options: sameorigin`
		oder
		`X-Frame-Options: allow-from: DOMAIN`

Header	Beschreibung	Vorgeschlagener Wert
X-Content-Type-Options	In einigen Fällen nutzen Browser die Funktion „Content Type Sniffing“, um zu erkennen, von welchem Typ die durch den Webserver übertragenen Antwortdaten sind. Content Type Sniffing wird in einigen Fällen auch dann durchgeführt, wenn der Content-Type-Header gesetzt ist. Um dies für „script“- und „style“-Typen zu verhindern und damit die Ausführung von möglicherweise bösartigem Script zu unterbinden, sollte der Content-Type-Options-Header mit dem Wert nosniff gesetzt werden.	`X-Content-Type-Options: nosniff`
Content-Security-Policy	Die Content-Security-Policy (CSP) umfasst mehrere Attribute zum Schutz der Webanwendung vor Angriffen wie z. B. Cross-Site-Scripting- oder Clickjacking-Angriffen. Über die Attribute können sehr differenziert Schutzmechanismen eingesetzt werden. Allerdings haben diese einen erheblichen Einfluss auf die Funktionsweise der Webanwendung. Der Einsatz von CSP-Attributen wird empfohlen, allerdings erfordert die Umsetzung eine sorgfältige Prüfung der Attribute und Parameter. Weitere Informationen finden sich in den Referenzen zu CSP. Das Attribut `frame-ancestors` unterbindet Clickjacking-Angriffe, in dem es festlegt, welche andere Webanwendung die Webanwendung - in welcher das Attribut angegeben ist - einbinden kann. Sofern die Webanwendung nicht eingebunden wird, sollte das Attribut `frame-ancestors: 'none'` verwendet werden. Andernfalls sollte `frame-ancestors <source>` mit Angabe der einbindenden Webanwendung verwendet werden. Es wird empfohlen `frame-ancestors` einzusetzen, da (im Gegensatz zu anderen CSP-Attributen) die Vorbedingungen zum Einsatz einfacher geprüft werden können.	`Content-Security-Policy: frame-ancestors 'none';` ODER `frame-ancestors <source>;`

Header	Beschreibung	Vorgeschlagener Wert
X-Permitted-Cross-Domain-Policies	Durch den Header können die gültigen Cross-Domain-Policies eingeschränkt werden. Dies geschieht üblicherweise durch die Datei `crossdomain.xml` im Wurzelverzeichnis der Domain. Sofern auf diese Datei jedoch kein Zugriff besteht, kann der dort gesetzte Wert mit dem Header beeinflusst und so beispielsweise der seitenübergreifende Zugriff vollständig unterbunden werden. Die Cross-Domain-Policy regelt, ob ein Webclient, wie beispielsweise Adobe Flash Player oder Adobe Acrobat, die Daten der Webanwendung im Kontext anderer Domains verarbeiten darf.	`X-Permitted-Cross-Domain-Policies: none`

OWASP Top 10 2021 A05 – Security Misconfiguration, 2021 A02 – Cryptographic Failures

Empfehlung Es wird empfohlen, die oben benannten HTTP-Security-Header entlang dem Defence-in-Depth-Ansatz nach einer Prüfung der Kompatibilität zur Anwendung einzusetzen, um das Sicherheitsniveau der Webanwendung weiter zu erhöhen.

Referenzen https://owasp.org/www-project-secure-headers/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

6. ANHANG A: VERSIONEN UND VERZEICHNISSE

6.1. Versionshistorie

Tabelle 20: Versionsverlauf des Ergebnisberichts

Version	Datum	Bearbeiter	Änderungen
0.9	XX.XX. 2022	Name, secuvera	Einpflegen der Änderungen aus dem Lektorat, Version zur Abstimmung mit dem Kunden
0.8	XX.XX.2022	Name, secuvera	Lektorat des Ergebnisberichts
0.7	XX.XX.2022	Name, secuvera	Abnahme der Änderungen aus dem Rücklauf
0.6	XX.XX.2022	Name, secuvera	Einpflegen der Änderungen aus der fachlichen Qualitätssicherung
0.5	XX.XX.2022	Name, secuvera	Fachliche Qualitätssicherung
0.4	XX.XX.2022	Name, secuvera	Letzte Änderungen, Version für die fachliche Qualitätssicherung

6.2. Abbildungsverzeichnis

Abbildung 1: Vorgehensweise nach BSI-Studie 11
Abbildung 2: Vorgehensweise nach BSI-Studie Prüfung Webanwendung über das Internet 22

6.3. Tabellenverzeichnis

Tabelle 1: Statistik identifizierter Schwachstellen Prüfung der Systeme 5
Tabelle 2: Statistik identifizierter Schwachstellen Webanwendungsprüfung 7
Tabelle 3: Schweregrad Schwachstelle S_01 12
Tabelle 4: Schweregrad Schwachstelle S_02 13
Tabelle 5: Schweregrad Schwachstelle S_03 15
Tabelle 6: Identifizierte unsichere Kommunikationsmöglichkeiten 16
Tabelle 7: Schweregrad Schwachstelle S_04 17
Tabelle 8: Übersicht der Funktionen 21
Tabelle 9: Übersicht des Berechtigungsmodells 21
Tabelle 10: Identifizierte, verwundbare Bibliotheken 23
Tabelle 11: Schweregrad Schwachstelle W_01 24
Tabelle 12: Schweregrad Schwachstelle W_02 25
Tabelle 13: Schweregrad Schwachstelle W_03 26
Tabelle 14: Schweregrad Schwachstelle W_04 28

Tabelle 15: Auflistung der verwundbaren Skripte und Parameter persistentes XSS 28
Tabelle 16: Schweregrad Schwachstelle W_05 29
Tabelle 17: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-Top-10-Risiken 30
Tabelle 18: Übersicht der Ergebnisse der Prüfung des Rechtemodells 31
Tabelle 19: Fehlende HTTP-Kopfzeilen zur Erhöhung der Sicherheit der Webanwendung 33
Tabelle 20: Versionsverlauf des Ergebnisberichts 36
Tabelle 21: Ermittlung des Sicherheitsniveaus bei systembasierten Penetrationstests 38
Tabelle 22: Ermittlung des Sicherheitsniveaus bei Webanwendungspenetrationstests 38

7. ANHANG B: ERMITTLUNG DES SICHERHEITSNIVEAUS

7.1. Ermittlung Sicherheitsniveau Prüfung der Systeme

Das Sicherheitsniveau pro System wird aus dem Schweregrad der auf diesem System identifizierten Schwachstellen berechnet. Bei der Berechnung des Gesamt-Sicherheitsniveaus wird das festgestellte Sicherheitsniveau der erreichbaren Systeme entsprechend anhand der folgenden Tabelle bestimmt.

Tabelle 21: 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 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 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 identifiziert wurde.
Kritisch	Wird gewählt, sofern mindestens eine Schwachstelle mit Schweregrad kritisch identifiziert wurde.	Wird gewählt, sofern auf mehr als 20% der erreichbaren Prüfziele ein niedriges Sicherheitsniveau identifiziert wurde.

7.2. Ermittlung Sicherheitsniveau Webanwendungspenetrationstest

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

Tabelle 22: 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.

Sicherheitsniveau	Kriterien für das Sicherheitsniveau einer Webanwendung
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.