secuvera
Cybersicherheit. Nachhaltig.

SICHERHEITSANALYSE IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

VERSION 1.4 | 31.10.2024

Gutachten im Auftrag der Bundesrechtsanwaltskammer – Körperschaft des öffentlichen Rechts
Littenstraße 9
10179 Berlin

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden

INHALTSVERZEICHNIS

1. ZUSAMMENFASSUNG

1.1. Zielsetzung

Die IAM-Lösung (BRAK Identity and Access Management bzw. BRAK-IAM) nutzt für die Identifizierung und Authentisierung von Nutzer:innen aus unterschiedlichen Teilnehmerkreisen unterschiedliche Anteile und Protokolle. Im Kern besteht die Lösung basierend auf dem BRAK Identity Provider (IdP), der innerhalb des BRAK-IAM die zentrale Komponente für Authentifizierung von Nutzeranfragen bildet. Der BRAK-IdP ist eine für die BRAK konfigurierte Instanz der Open-Source-Software Keycloak.

Der BRAK Identity Provider stellt eine Reihe von Services für die Authentifizierung von beA-Benutzern und Keycloak-Clients bereit. Die Endpunkte für diese Services sind teilweise im Internet zugänglich und können von außen angesprochen werden.

Für eine erfolgreiche Authentifizierung und Ausstellung eines Access Tokens ist entweder ein gültiges PKI-Zertifikat mit einem privaten Schlüssel (Benutzer) oder Clientname/Passwort (Keycloak-Clients) notwendig.

Die Architektur setzt auf unterschiedliche Kommunikations- und Authentisierungswege. Es sind weitere Systeme und Identitäts-Objekte einbezogen.

Die Prüfung der eingesetzten Lösung soll sowohl für die jeweiligen Authentisierungsabschnitte erfolgen als auch die Ergebnisse vor dem Hintergrund der Gesamtlösung bewerten. Die Prüfung ist unterteilt in zwei Schritte: eine dokumentbasierte Sicherheitsanalyse in Form einer Architekturanalyse und einer technischen Sicherheitsanalyse in der Form eines Penetrationstests. Ziel der Prüfungen ist es, die Belastbarkeit der Implementierung zu prüfen und mögliche Schwachstellen zu identifizieren, die ggf. über eine Justierung der Parameter zu einer Verbesserung der Lösung führen können.

Die folgenden Prüfgegenstände werden hierbei im Rahmen der Prüfung adressiert bzw. über geeignete Fragestellungen einbezogen:

- Implementierung des Identity Providers (BRAK-IdP) unter Zuhilfenahme des Frameworks „Keycloak“,
- Sicherheit von Protokollen und Schnittstellen, die für die einzelnen Abschnitte genutzt werden (REST, SOAP).

Die Ergebnisse und die Vorgehensweisen der einzelnen Prüfschritte werden in den folgenden Unterkapiteln kurz zusammengefasst. Eine detaillierte Beschreibung aller Prüfschritte erfolgt in den Folgekapiteln.

1.2. Ergebnisse der Prüfung

1.2.1. Analyse

Um die Implementierung des zentralen Identitäts- und Zugriffsmanagements (Identity and Access Management (IAM)) auf der Basis „Keycloak“ des Kunden zu betrachten, wurde im Zeitraum vom 19. Februar bis einschließlich 22. Mai 2024 eine Architekturanalyse durchgeführt. Ziel derer war die Identifikation von Verbesserungspotential zur Steigerung des Sicherheitsniveaus der Implementierung.

Hierfür wurde durch den Prüfer ein Fragenkatalog vorbereitet, der sich am Lebenszyklusmodell von IT-Systemen orientiert und Prüffragen aus gängigen Kriterienwerken, den Härtungsanweisungen des Herstellers sowie der langjährigen Prüferfahrung der secuvera enthält.

Mithilfe durch den Kunden übermittelter Dokumentation wurden die Fragen durch den Prüfer vorab beantwortet. Offengebliebene Fragestellungen wurden vorab des Interviews über ein JIRA-Ticket an den Dienstleister des Kunden übermittelt.

In einem mehrteiligen Interview mit verantwortlichen Ansprechpartnern des Dienstleisters des Kunden wurden die offengebliebenen Fragestellungen gemeinsam mit dem Prüfer erörtert und, wo nötig, Einsicht in die aktuelle Konfiguration genommen.

Im Nachgang wurden die gefundenen Antworten durch den Prüfer ausgewertet und Verbesserungspotential – sofern vorhanden – in Form von Verbesserungsempfehlungen abgeleitet.

Am 20. September 2024 fand eine Verifizierung der Behebung identifizierter Befunde und Anmerkungen statt, soweit dies möglich gewesen war. Das Ergebnis wurde um die neuen Erkenntnisse entsprechend aktualisiert.

Bei der Prüfung konnten ein Befund sowie eine Anmerkung identifiziert werden.

Tabelle 1: Statistik: Identifizierte Befunde der Analyse

Gesamtanzahl		**Anzahl Befunde (Schweregrad)**			
Befunde	**Anmerkungen**	**Kritisch**	**Hoch**	**Mittel**	**Niedrig**
1	1	0	0	0	1

Niedrig B_01 Protokollierung und Auswertung von Sicherheitsereignissen verbessern

Durch eine noch nicht erfolgte konfigurative Änderung des Reverse-Proxys ist derzeit noch die Account-Management-Konsole für eingeloggte Benutzer aufrufbar. Innerhalb der Konsole ist ein angemeldeter Benutzer in der Lage, seine persönlichen Daten im Keycloak zu ändern (SAFE-ID). Des Weiteren werden auf den Unterseiten interne Informationen wie z. B. die interne IP-Adresse eines Loadbalancers angezeigt.

Es wurden Anmerkungen identifiziert, von denen kein direktes Risiko ausgeht und die somit auch kein Befund darstellen. Durch die Beseitigung dieser Anmerkungen lässt sich jedoch das Sicherheitsniveau des Prüfgegenstands erhöhen. Informationen zu den identifizierten Sicherheitshinweisen befinden sich in Kapitel 5.2.2.5.

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

1.2.2. Technischer Penetrationstest

Vor der Prüfungsdurchführung wurden die Vorgehensweise sowie die Prüfungsgegenstände im Rahmen einer Auftaktbesprechung behandelt.

Im Zeitraum vom 22. bis einschließlich 28. August 2024 wurden die extern über das Internet erreichbaren Anteile des Identitätsanbieters (Identity Provider, IDP) mithilfe von insgesamt zwei beA-Anwendungsbestandteilen (Weblogin, Login über Webschnittstelle (KSW)) einer Sicherheitsüberprüfung in der Form eines technischen Penetrationstests über das Internet unterzogen. Das Ziel der Prüfungen war die Identifikation von Schwachstellen auf Anwendungsebene in den Komponenten des IDP.

Am 20. September 2024 fand eine Verifizierung der Behebung identifizierter Schwachstellen statt. Das Ergebnis wurde um die neuen Erkenntnisse entsprechend aktualisiert.

Es wurden IDP-Funktionen der Anwendungsbestandteile überprüft, die aus den im Folgenden definierten Rollen heraus aufrufbar sind:

- Benutzer mit Login-Berechtigung beA und
- Anonym.

Die Webanwendungen wurden zunächst ohne gültige Benutzerdaten, d. h. aus der Sicht eines anonymen Angreifers, überprüft. Durch den Kunden wurden zudem drei X.509-Zertifikate zur Authentifizierung gegenüber dem IDP übermittelt: zwei für das beA und eines für die KSW-Schnittstelle.

Die Tests wurden als White-Box-Tests durchgeführt, das heißt, dass die Tester zusätzlich zu Adresse und Anmeldedaten der Webanwendungen noch weitere Informationen zum technischen Aufbau und der Implementierung erhalten haben.

Für die Prüfungen wurden einzelne dem IDP vorgelagerte Schutzmechanismen (Web Application Firewall, WAF) selektiv für die IP-Adressen der Prüfer deaktiviert. Sofern Schwächen identifiziert werden konnten, wurden diese im Anschluss einer selektiven Nachprüfung mit aktivierten Schutzmechanismen unterzogen, um eine Aussage über etwaig vorhandene risikominimierende Einwirkungen der Sicherheitsmechanismen auf identifizierte Schwächen treffen zu können.

Insgesamt kann den überprüften Bestandteilen zum Zeitpunkt der Dokumentationserstellung ein sehr hohes Sicherheitsniveau attestiert werden, da nach der Verifikation keine Schwachstellen identifiziert werden konnten.

Tabelle 2: Statistik: Identifizierte Schwachstellen Penetrationstest BRAK-IdP

Gesamtanzahl		**Anzahl Schwachstellen (Schweregrad)**				**Gesamtbewertung Sicherheitsniveau**
Schwachstellen	**Anmerkungen**	**Kritisch**	**Hoch**	**Mittel**	**Niedrig**	
0	4	0	0	0	0	Sehr hoch

Im Rahmen der initialen Untersuchung konnten zwei Schwachstellen identifiziert werden, die jedoch bereits als behoben verifiziert werden konnten. Diese werden nachfolgend nach dem *Schweregrad der Schwachstelle*absteigend sortiert aufgelistet. Das resultierende Sicherheitsniveau der Anwendung wird im Anhang C (siehe Kapitel 9.) erläutert.

Mittel W_01 Account-Management-Konsole noch aktiv (A_02, behoben)

Durch eine fehlende konfigurative Änderung des Reverse-Proxys war die Account-Management-Konsole für eingeloggte Benutzer aufrufbar. Innerhalb der Konsole war ein angemeldeter Benutzer in der Lage, seine persönlichen Daten im Keycloak zu ändern (SAFE-ID).

Mittel W_02 Keycloak-Metriken öffentlich einsehbar (behoben)

Ebenfalls durch eine fehlende konfigurative Änderung des Reverse-Proxys waren Health-Check der Datenbank sowie die Metriken vom IDP über die entsprechenden Pfade öffentlich erreichbar. Ein Angreifer ohne Authentisierung war bis zur Änderung der Konfiguration in der Lage, Informationen

über den IDP auszulesen, um diese ggf. für die Präzisierung weiterer Angriffe zu verwenden. Die Informationen ließen sich durch das Prüfpersonal jedoch nicht für weitere Angriffe verwenden.

Weiterhin wurden Sicherheitshinweise in Form von Anmerkungen 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 6.2.2.5.

Eine detaillierte Beschreibung des angewandten Verfahrens findet sich in Kapitel 6.1.

1.3. Resümee und Empfehlung

Die Analyse brachte zunächst für den Prüfenden zum Vorschein, dass bereits einiges für das Erreichen bzw. Aufrechterhalten eines hohen Sicherheitsniveaus beim Einsatz und Betrieb eines neuen Identitätsanbieters unternommen wurde. Entlang dem Lebenszyklusmodell von IT-Systemen zeigte sich nur im Abschnitt „Notfallvorsorge“ im Rahmen der Protokollierung Potential zur Steigerung des Sicherheitsniveaus. Weiterhin konnten Verbesserungen identifiziert werden, die im Projektverlauf durch die Beteiligten umgesetzt wurden, sodass die Umsetzung auch verifiziert werden konnte. Zum einen wurden nicht benötigte, aber noch aktivierte Elemente (z. B. Account Management Console) der eingesetzten Software identifiziert und konfigurativ deaktiviert. Zum anderen wurde nicht verwendete Funktionalität (z. B. Token Audience) identifiziert, die ggf. einen Sicherheitsgewinn für die Robustheit des IDP darstellen kann.

Das Ziel war es, dass bis zu einem technischen Test zumindest die nicht benötigten Elemente deaktiviert werden, um die Wirksamkeit mit den technischen Prüfungen bestätigen zu können. Im Rahmen einer Verifikation der Behebung identifizierter Schwachstellen mit geringem zeitlichem Abstand zu den Prüfungen konnte festgestellt werden, dass das Ziel als erreicht gilt.

Es wird weiterhin empfohlen, die Anmerkungsempfehlungen kurz- bis mittelfristig umzusetzen. Die Übersichtstabellen zu den Befunden bzw. Schwachstellen finden sich in den Kapiteln 5.2.1 und 6.2.1.

1.4. Abgrenzung

Die Prüfungsanteile bezogen sich auf die bestehende Implementierung und die dafür eingesetzte Lösungsarchitektur. Die Hintergründe und die Art der verwendeten Attribute für die Identifizierung und Authentisierung wurden nicht hinterfragt, da diese für die notwendige Kontinuität und den Übergang von vorigen Lösungen erforderlich sind.

Die Prüfungsanteile stellen keine Ergebnisse bereit, die auf eine vordefinierte Konformität abzielen. Auch wenn einschlägige Quellen und Kriterienwerke im Hintergrund für die Prüfung berücksichtigt wurden, so besteht dennoch keine unabhängige und konkret auf die Objekte bezogene Anforderungszusammenstellung, die eine Maßzahl für das Sicherheitsniveau ergeben würde.

2. ALLGEMEINES

In diesem Kapitel wird beschrieben, wie die Darstellung von Befunden und Schwachstellen in den folgenden Kapiteln erfolgt und wie die Einordnung in die Risikostufen durchgeführt wurde.

2.1. Unterscheidung zwischen Befund und Schwachstelle

Zur einfacheren Unterscheidung zwischen Ergebnissen der Architekturanalyse und der externen technischen Prüfung wird nachfolgend zwischen Befunden und Schwachstellen unterschieden.

Als „Befund" werden hierbei die Ergebnisse der Architekturanalyse bezeichnet. Als „Schwachstelle" gelten die Ergebnisse der externen technischen Prüfung im Rahmen eines Penetrationstests.

Zur besseren Referenzierung werden Befunde und Schwachstellen jeweils mit im Dokument fortlaufendem und damit eindeutigem Index versehen. Hierbei wird die nachfolgende Nomenklatur verwendet:

- B_ Befund aus Dokumentenprüfung, Umsetzungsprüfung, Audit oder Konfigurationsprüfung,
- W_ Schwachstelle aus technischer Prüfung,
- OOS-W_ Schwachstelle aus technischer Prüfung, die sich jedoch außerhalb des Prüffokus befindet (Out-of-Scope-Schwachstellen) und
- A_ Befund oder Schwachstelle der Kategorie Anmerkung.

2.2. Befund

2.2.1. Darstellungsform

Folgende Darstellungsform wurde für die identifizierten Befunde gewählt.

B_01	***Titel***
Beschreibung	*Beschreibung des gefundenen Befundes*
Auswirkung	*Nennung der möglichen Auswirkungen*
Beispiel	*[Optional] Nennung von Beispielen*
Hinweis	*[Optional] Nennung von Hinweisen*
Empfehlung	*Eine Empfehlung, was getan werden muss, damit der Befund langfristig behoben wird.*
Referenzen	*[Optional] Nennung von Referenzen*
Schweregrad	Niedrig Mittel Hoch Kritisch
Begründung	*[Optional] Nennung einer Begründung*
Behebungsstatus	*Dokumentation des Stands der Behebung*

Befunde der Kategorien „Anmerkung" und „Verbesserung" werden wegen der geringen Priorität nur überblicksartig dargestellt.

2.2.2. Schweregradbewertung

Die Schweregradbewertung von Befunden wird auf Grundlage der möglichen Folgen in folgenden Kategorien vorgenommen.

- Verbesserung:
  Der Befund erhöht das Sicherheitsniveau im Vergleich zum vorherigen Niveau. Eventuell ist jedoch noch eine zusätzliche Dokumentation im Sicherheitsregelwerk nötig.

- Anmerkung:
  Die Behebung würde das Sicherheitsniveau nicht erhöhen, dient jedoch zur Verbesserung der Darstellung oder Verständlichkeit der Dokumentation. Die Umsetzung wird angeraten, ist jedoch nicht dringend umzusetzen.
- Niedrig:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in geringem Umfang bedeuten, dient jedoch mehr der Verbesserung der Verständlichkeit der Dokumentation. Die Umsetzung ist langfristig anzugehen.
- Mittel:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in deutlichem Umfang bedeuten. Die Umsetzung ist mittelfristig anzugehen.
- Hoch:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in erheblichem Umfang bedeuten. Die Umsetzung ist kurzfristig anzugehen.
- Kritisch:
  Der Befund steht einem Betrieb entgegen. Die Umsetzung ist vor einem (Weiter-)Betrieb anzugehen.

2.3. Schwachstelle

2.3.1. Darstellungsform

Folgende Darstellungsform wurde für die identifizierten Schwachstellen gewählt.

[OOS-]W _01 *Titel*

Beschreibung	*Beschreibung der gefundenen Schwachstelle*
Auswirkung	*Nennung der möglichen Auswirkungen*
Beispiel	*[Optional] Nennung von Beispielen*
Hinweis	*[Optional] Nennung von Hinweisen*
OWASP Top 10	*[Optional bei Prüfungen auf Anwendungsebene] Referenzierung der Risikokategorie aus den Top-10-Risiken des Open Worldwide Application Security Projects.*
Empfehlung	*Eine Empfehlung, was getan werden muss, damit die Schwachstelle langfristig behoben wird.*
Referenzen	*[Optional] Nennung von Referenzen*
Schweregrad	Low Medium High Critical *Tabellarische Übersicht der gewählten Werte sowie einer Begründung, warum der Wert gewählt wurde, errechneter Zahlenwert (CVSS4 Vektor-String zur Rückverfolgung der Berechnung in der Bewertung[1] und zur Weiterberechnung durch den Kunden mit z. B. dem Environmental Score).*
Behebungsstatus	*Dokumentation des Stands der Behebung*

[1] Der Vektorstring kann in folgendes URL-Schema nach dem Raute-Symbol eingetragen werden, um das Berechnungswerkzeug der FIRST zu verwenden: https://www.first.org/cvss/calculator/4.0#<VEKTOR-STRING>

2.3.2. Bewertung des Schweregrads

Für Schwachstellen erfolgt eine Bewertung des Schweregrads nach dem Common Vulnerability Scoring System (CVSS).[2] CVSS ist der Industriestandard zur Bewertung von Schwachstellen und wurde von der Organisation FIRST (Forum of Incident Response and Security Teams) entwickelt. Aus diesem Schema ergibt sich die nachfolgende Kategorisierung, die in Tabelle 3 dargestellt ist.

Tabelle 3: Zuordnung der CVSS-Scores zu den Kategorien

CVSS-Score	CVSS-Bewertung	Zugeordnete Kategorie
0	None	Anmerkung
0,1 – 3,9	Low	Niedrig
4,0 – 6,9	Medium	Mittel
7,0 – 8,9	High	Hoch
9,0 – 10,0	Critical	Kritisch

2.4. Gemeinsame Anteile

Für die beiden Unterscheidungen „Befund“ und „Schwachstelle“ gelten allgemein einzelne Hinweise, die in den folgenden Unterkapiteln dargestellt werden.

2.4.1. Empfehlung

Eintragungen im Bereich der Empfehlung beschreiben beispielhafte Maßnahmen, die umgesetzt werden könnten, um den Befund oder die Schwachstelle zu beseitigen. Die Maßnahmen stellen lediglich mögliche Lösungen dar und sollen belegen, dass Befunde oder Schwachstellen beseitigt werden können. Die Notwendigkeit und Priorität der Schwachstellenbehebung hängt aber nur von der bereits beschriebenen Schweregradeinstufung ab.

2.4.2. Angaben zum Status der Behebung

Der Status der Behebung unter jedem Befund oder Schwachstelle gibt den Stand des Befundes oder der Schwachstelle zum Stichtag an und ob der Befund/die Schwachstelle durch den Gutachter verifiziert behoben wurde. Dabei gelten die nachfolgenden Definitionen:

- Nicht verifiziert/Nicht bearbeitet (-)
  Eine Bearbeitung der Schwachstelle oder des Befundes durch die Betreiberin liegt noch nicht vor oder es wurde noch kein erneuter Test/Begutachtung durch den Gutachter durchgeführt.
- Verifiziert: Schwachstelle/Befund behoben (J)
  Die festgestellte Schwachstelle oder der Befund konnte nicht mehr nachgewiesen werden bzw. eine adäquate Veränderung hat stattgefunden. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als vollständig behoben angesehen.

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

- Verifiziert: Schwachstelle/Befund teilweise behoben (T)
  Eine Behandlung der Schwachstelle oder des Befundes hat stattgefunden, jedoch sind noch nicht alle Aspekte zum Stichtag behoben. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als teilweise behoben angesehen.
- Verifiziert: Schwachstelle/Befund nicht behoben (N)
  Eine Behandlung der Schwachstelle oder des Befundes hat stattgefunden, jedoch ist bei einer erneuten Begutachtung die Schwachstelle oder der Befund erneut aufgefallen oder die Behandlung wird als nicht ausreichend bewertet. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als nicht behoben angesehen.

3. PRÜFOBJEKTE/SYSTEMKOMPONENTEN

Die Komponenten, die bei der Identitäts- und Zugriffsverwaltung zum Einsatz kommen, wurden im Rahmen eines Prüfauftrags betrachtet und analysiert. Im Wesentlichen besteht die implementierte Authentisierungslösung aus zwei Hauptkomponenten: einem Identitätsprovider (Identity Provider, IDP bzw. BRAK-IdP) und einem Identitätsverwalter (Identity Manager, IDM bzw. BRAK-IdM). Beide Komponenten werden hochverfügbar in einer Cluster-Infrastruktur verteilt auf unterschiedlichen Rechenzentrumslokationen betrieben.

3.1. Identity Provider (BRAK-IdP, IDP)

Beim IDP wird die Open-Source-Lösung „Keycloak“ eingesetzt. Diese stellt Sicherheitsfunktionen wie eine Implementierung der Protokolle Open Authorization (OAuth) bzw. OpenID Connect (OIDC) sowie Security Assertion Markup Language (SAML) in Version 2 bereit. Im beA-Kontext wird Keycloak dafür verwendet, um Identitäten zu verwalten und Zugriffe zu steuern.

Im Rahmen des besonderen anwaltlichen Postfachs beA wird der IDP zum Zeitpunkt der Erstellung der Container über eine entsprechende Konfigurationsdatei (YAML) gesteuert, in der sowohl die Parametrisierung der Container als auch der Keycloak-Komponenten vorgenommen werden. Die Konfigurationsdatei wird über ein Code-Repository verwaltet, sodass Änderungen an den Dateien nachvollziehbar sind und nur durch Berechtigte erfolgen können.

Der IDP stellt einen Webservice-Port bereit und wird von unterschiedlichen Komponenten angesprochen.

3.2. Identity Manager (BRAK-IdM, IDM)

Unterstützt wird der IDP durch einen IDM. Der BRAK-IdM ist eine eigene Entwicklung und basiert auf unterschiedlichen Frameworks: Spring Boot mit Spring Security und JOOQ. Der IDM kann über eine SCIM-API angesprochen werden.

Mithilfe des IDM werden die Daten in einem Datenbankschema verwaltet. Das Datenbankschema basiert zum Zeitpunkt der Analyse auf dem Schema der bisher zur Identitätsverwaltung genutzten Software Governikus Autent.

4. AUTHENTISIERUNG

Die Authentisierung kann web- oder API-basiert erfolgen. Sie erfolgt dabei immer gegenüber dem Identitätsprovider (BRAK-IdP, IDP). Nachfolgend werden die unterschiedlichen Authentisierungsmethoden und deren Ablauf kurz zusammengefasst, um dem Leser die Möglichkeit zu geben, die Authentisierung nachzuvollziehen.

4.1. Webbasierte Authentisierung

Die webbasierte Authentisierung erfolgt standardmäßig über OpenID Connect (OIDC), kann aber auch über Security Assertion Markup Language (SAML) erfolgen. Bei OIDC wird der Authorization Code Grant Flow ohne Proof-Key for Code Exchange verwendet.

Alternativ kann eine Authentisierung auch via SAML erfolgen.

4.2. API-basierte Authentisierung

Wenn ein externer Service eines Fachverfahrens auf Services der BRAK zugreifen möchte, ist das webbasierte Verfahren aus dem vorherigen Kapitel nicht einsetzbar. Stattdessen wird eine zertifikatsbasierte Authentifizierung von Identitäten mit Challenge-Response-Verfahren (Challenge Response Authentication Mechanism, CRAM) verwendet. Nach erfolgreicher Durchführung des Verfahrens wird ein Authentifizierungstoken erstellt und zurückgeliefert.

Über einen Webservice-Endpunkt wird eine CRAM-Sitzung beim IDP erstellt. Die Challenge wird mit einem Nutzerzertifikat signiert und an den IDP zurück übergeben. Sofern die Signatur gültig war, wird die CRAM-Sitzung authentisiert, und es kann ein Zugriffstoken angefordert werden.

5. SICHERHEITSANALYSE

5.1. Beschreibung der Vorgehensweise und des Ziels

Um die Implementierung des zentralen Identitäts- und Zugriffsmanagements (Identity and Access Management (IAM)) auf der Basis „Keycloak“[3] des Kunden zu betrachten, wurde im Zeitraum vom 19. Februar bis einschließlich 22. Mai 2024 eine Architekturanalyse durchgeführt. Ziel derer war die Identifikation von Verbesserungspotential zur Steigerung des Sicherheitsniveaus der Implementierung.

Hierfür wurde durch den Prüfer ein Fragenkatalog vorbereitet, der sich am Lebenszyklusmodell von IT-Systemen mit den Phasen

- Planung und Konzeption,
- Inbetriebnahme,
- Betrieb,
- Notfallvorsorge und
- Aussonderung

orientiert und Prüffragen aus gängigen Kriterienwerken, wie z. B. dem Baustein „ORP.4: Identitäts- und Berechtigungsmanagement“[4] oder dem benutzerdefinierten Baustein „APP.bd.3 IAM Dienst Keycloak“[5] des IT-Grundschutz-Kompendiums, den Härtungsanweisungen des Herstellers[6] sowie der langjährigen Prüferfahrung der secuvera enthält.

Mithilfe durch den Kunden übermittelter Dokumentation wurden die Fragen durch den Prüfer vorab beantwortet. Dazu wurde durch den Kunden ein Zugang zur Wissensdatenbank der beA-Anwendung übergeben und eine Absprungseite eingerichtet, die Verweise zu den einzelnen Unterseiten mit den relevanten Informationen zum IAM und IDP enthalten. Dort waren wesentliche Rahmenparameter der Umgebung festgehalten.

Offengebliebene Fragestellungen wurden vorab des Interviews über ein Ticket-System an den Dienstleister des Kunden übermittelt.

In einem mehrteiligen, virtuellen Interview mit verantwortlichen Ansprechpartnern des Dienstleisters des Kunden wurden die offengebliebenen Fragestellungen gemeinsam mit dem Prüfer erörtert und, wo nötig, Einsicht in die aktuelle Konfiguration genommen.

Im Nachgang wurden die gefundenen Antworten durch den Prüfer ausgewertet und Verbesserungspotential – sofern vorhanden – in Form von Verbesserungsempfehlungen abgeleitet.

Die Fragestellungen und deren Beantwortung in den durchgeführten Workshops werden in einer Aufzeichnung geführt, die bewusst nicht Teil dieses Ergebnisberichts ist. Im Projektkontext liegen die Beantwortungen entlang der geprüften Aspekte vor.

---

[3] https://www.keycloak.org/

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2023.pdf?__blob=publicationFile&v=3#download=1

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/BS_IAM_Dienst_Keycloak.html?nn=943082

[6] https://www.keycloak.org/docs/latest/securing_apps/

5.2. Ergebnisdarstellung

Im Rahmen eines Workshops am 17. April 2024 wurden die Fragen zum IDM besprochen. Dabei wurde bereits eine Verbesserung identifiziert (siehe A_01). Des Weiteren wurden fünf Nachprüfungen durch den Dienstleister zu unterschiedlichen Themen wie z. B. die Absicherung gegenüber Clickjacking-Angriffen, unternommen. Da nicht alle offenen Fragen im zur Verfügung stehenden Zeitfenster beantwortet werden konnten, wurde ein Folgetermin angesetzt.

Im Rahmen des zweiten Workshops am 26. April 2024 wurden die restlichen Fragen zum IDM sowie die Fragen zum IDP beantwortet. Dabei konnten ein Befund und eine Verbesserung identifiziert werden (siehe B_01 und A_02).

Die Behebung der Anmerkung A_02 konnte am 20. September 2024 verifiziert werden.

5.2.1. Übersicht der Befunde

Tabelle 4: Übersicht der Befunde der Analyse

Nr.	Titel	Schweregrad	Seite
B_01	Protokollierung und Auswertung von Sicherheitsereignissen verbessern	Niedrig	15
A_01	„Token Audience“ implementieren (teilweise behoben)	Anmerkung	16
A_02	Account Management Console deaktivieren (behoben)	-	17

5.2.2. Beschreibung der Befunde

5.2.2.1. Befunde der Kategorie Kritisch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Schweregrad „kritisch“ identifiziert werden.

5.2.2.2. Befunde der Kategorie Hoch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Schweregrad „hoch“ identifiziert werden.

5.2.2.3. Befunde der Kategorie Mittel

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Schweregrad „mittel“ identifiziert werden.

5.2.2.4. Befunde der Kategorie Niedrig

Bei den Prüfungen konnte mit der angewandten Prüfmethodik im Testzeitraum eine Schwachstelle mit Schweregrad „Niedrig“ identifiziert werden.

B_01 Protokollierung und Auswertung von Sicherheitsereignissen verbessern

Beschreibung: Derzeit werden auftretende Ereignisse wie das gehäufte Vorkommen von HTTP-Fehlercodes vom Typ 400-500 nicht automatisiert ausgewertet Es wird lediglich ausgewertet, ob die Antwort des SAFE-Connectors, der die Signatur der Challenge verifiziert, korrekt war.

Auswirkung	Angriffe auf extern erreichbare Keycloak-Bestandteile auf Anwendungsebene werden zu spät erkannt.
Empfehlung	An den geeigneten Stellen (z. B. Loadbalancer oder Reverse-Proxys der Container) sollten Ereignisse definiert und diese automatisiert ausgewertet werden.
Referenzen	-
Schweregrad	Niedrig
Begründung	Die Umsetzung der Empfehlung würde eine Verbesserung des Sicherheitsniveaus in geringem Umfang bedeuten, sodass dies mit niedrigem Schweregrad bewertet wurde. Die Auswertung von Ereignissen ist ein zunehmend wichtiger Aspekt, insbesondere für erreichbare Schnittstellen. Es wird beispielhaft auf Anforderungen des IT-Grundschutz-Kompendiums verwiesen: DER.1.A6, DER.1.A9, DER.1.A11, DER.1.A15 sowie OPS.1.1.5.A9.
Behebungsstatus	Nicht verifiziert.

5.2.2.5. Anmerkungen

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum zwei Verbesserungen (Schwachstellen mit Schweregrad „Anmerkung“) identifiziert werden.

A_01 „Token Audience“ implementieren (teilweise behoben)

Beschreibung	In der Konfiguration der Keycloak Realm wird die Token Audience nicht gesetzt.
Auswirkung	Durch die fehlende Token Audience können vom IDP ausgestellte Access- oder Refresh-Tokens im Rahmen von Rechte-Delegierungen auch an potentiell nicht vertrauenswürdige Clients übergeben werden, um Zugriff auf Ressourcen zu erhalten. Diese könnten wiederum das Token selbst dafür missbrauchen, um unbefugt Zugriff auf Ressourcen zu erhalten.
Empfehlung	Es sollte überprüft werden, inwiefern ein Sicherheitsgewinn erreicht werden kann, indem die Token Audience implementiert wird. Tokens werden dabei neben dem Scope auch ein Audience-Parameter übergeben. Wird dieses Token dann von einem potentiell nicht vertrauenswürdigen Client zum Zugriff auf eine Ressource eines vertrauenswürdigen Clients verwendet und prüft dieser die Audience, wird Missbrauch eines Tokens vorgebeugt. Eine detaillierte Beschreibung kann der ersten Referenz entnommen werden.
Referenzen	https://www.keycloak.org/docs/latest/server_admin/#audience-support https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/BS_IAM_Dienst_Keycloak.html
Behebungsstatus	Verifiziert: Teilweise behoben. Aus dem Ticket-System wurde ersichtlich, dass in einer neuen, bisher nicht veröffentlichten Version die Token-Audience bereits implementiert wurde.

A_02 Account Management Console deaktivieren (behoben)

Beschreibung	Die Account- und Admin-Management-Konsolen von Keycloak werden nicht verwendet. Zum Zeitpunkt der Analyse war der Zugriff auf die Account Management Console von Keycloak in der Entwicklungsumgebung und in der Produktionsumgebung möglich.
Auswirkungen	Dies hat keine direkten Auswirkungen, da man sich laut Aussage des Ansprechpartners des Dienstleisters des Kunden nicht an den Konsolen anmelden konnte.
Empfehlung	Die Konsolen sollten durch die Konfigurationsanpassung bzw. die Istio-Reverse-Proxys deaktiviert bzw. der Zugriff darauf verhindert werden.
Referenzen	https://www.keycloak.org/server/reverseproxy#_exposed_path_recommendations
Behebungsstatus	Verifiziert: Behoben. Die Account-Management-Konsolen sind deaktiviert worden.

6. TECHNISCHE PRÜFUNG

6.1. Methodik und Vorgehensweise

Vor der Prüfungsdurchführung wurden die Vorgehensweise sowie die Prüfungsgegenstände im Rahmen einer Auftaktbesprechung behandelt.

Im Zeitraum vom 22. bis einschließlich 28. August 2024 wurden die extern erreichbaren Anteile des Identitätsanbieters (Identity Provider, IDP) mithilfe von insgesamt zwei beA-Anwendungsbestandteilen einer Sicherheitsüberprüfung in der Form eines technischen Penetrationstests unterzogen. Das Ziel der Prüfungen war die Identifikation von Schwachstellen auf Anwendungsebene in den Komponenten des IDP.

Es wurden IDP-Funktionen der Anwendungsbestandteile überprüft, die aus den im Folgenden definierten Rollen heraus aufrufbar sind:

- Benutzer mit Login-Berechtigung beA und
- Anonym.

Die Anteile „Login in BRAK-beA-Webanwendung“ und „Login über KSW-Schnittstelle“ wurden in der Partnertest-Umgebung betrachtet. Die Webanwendungen wurden zunächst ohne gültige Benutzerdaten, d. h. aus der Sicht eines anonymen Angreifers, überprüft. Durch den Kunden wurden zudem drei X.509-Zertifikate zur Authentifizierung gegenüber dem IDP übermittelt: zwei für das beA-Login und eines für die KSW-Schnittstelle.

Die Anwendungen wurden zunächst mittels automatisierter Scanwerkzeuge abgetastet. Verwendet wurden hierfür das Werkzeug „Burp Suite Pro“[7]. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. Falsch-Positiv-Meldungen (False Positives) möglichst ausschließen zu können. Die Tests wurden durch manuelle Methoden ergänzt, um prinzipbedingte Schwächen des toolgestützten Tests auszugleichen.

Bei Webservice-Schnittstellen, die eine Webservice-Definition nach der Web Service Description Language (WSDL) anboten, wurde diese mit der Burp-Suite-Pro-Erweiterung „WSDLer“[8] eingelesen, um Webservice-Aufrufe zu erstellen und diese mit dem Scanner der Burp Suite zu scannen.

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.

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

[8] https://github.com/portswigger/wsdler

Informationsbasis

Die Tests wurden als White-Box-Tests durchgeführt, das heißt, dass die Tester zusätzlich zu Adresse und Anmeldedaten der Webanwendungen noch folgende, weitere Informationen zum technischen Aufbau und der Implementierung erhalten haben:

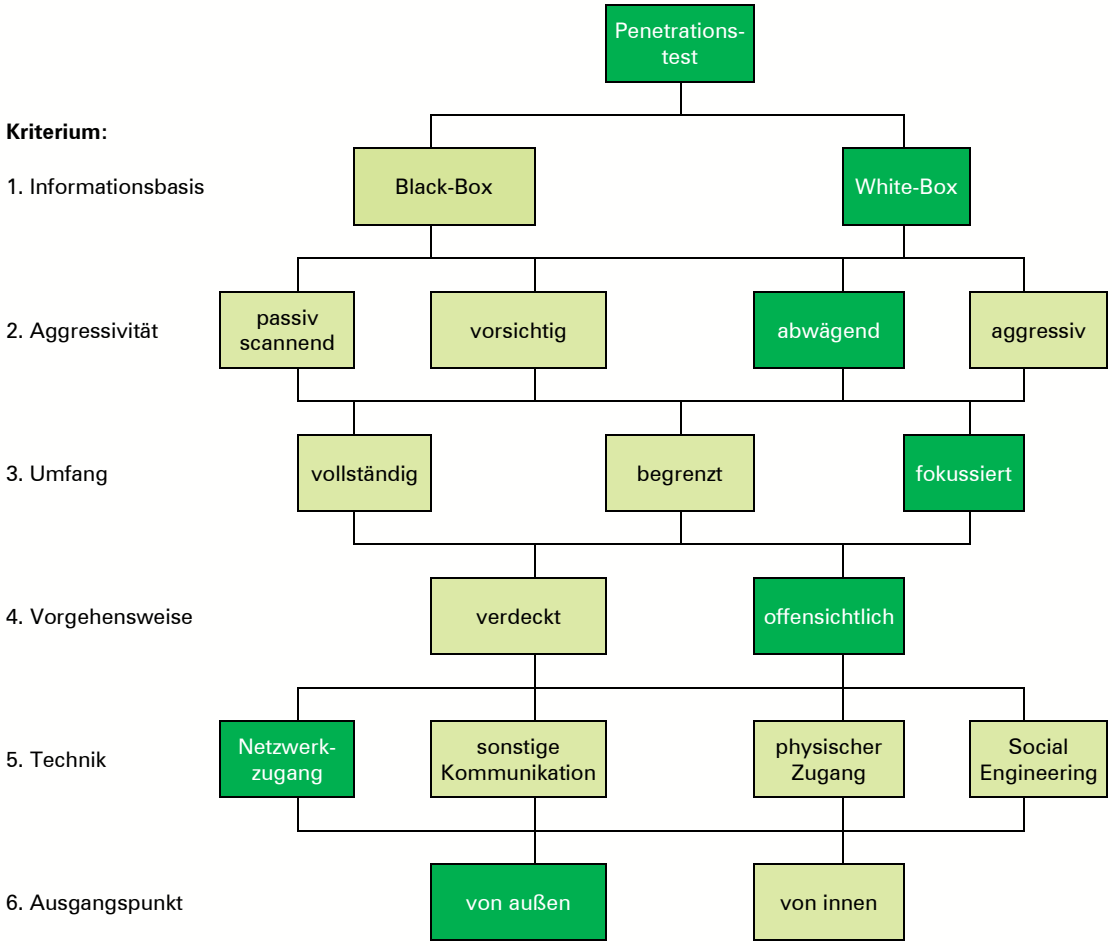
- Zugriff auf das beA-Wiki[9] mit technischen Details zur Implementierung.

Weitere Randbedingungen

Die Anwendung wird üblicherweise von einer Webanwendungsfirewall (WAF) geschützt. Diese wurde zunächst für die Prüfungen deaktiviert, um direkt die Sicherheit der Komponenten ohne Einflussnahme durch vorgelagerte Sicherheitsmechanismen prüfen zu können. Dies wurde durch eine Ausnahme der festen IP-Adressen in der WAF-Konfiguration erreicht. Im Prüfungsverlauf wurde dann die Konfiguration wieder deaktiviert und etwaig gefundene Schwächen selektiv einer Nachprüfung unterzogen. Dies ermöglicht zum einen eine effiziente Identifikation von Schwachstellen, zum anderen eine Aussage über risikomindernde Fähigkeiten der vorgelagerten Sicherheitsmechanismen in Bezug auf die identifizierten Schwachstellen zu treffen.

Für den Penetrationstest wurde für die Prüfungen auf Anwendungsebene die folgende Vorgehensweise (siehe markierte Felder) nach der BSI-Studie „Durchführungskonzept für Penetrationstests“[10] zugrunde gelegt:

Abbildung 1: Vorgehensweise nach BSI-Studie Prüfungen



[9] https://wiki.westernacher.com/

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

Sofern in einzelnen Punkten von dieser Vorgehensweise abgewichen wurde, wird dies entsprechend in der Beschreibung der Vorgehensweise erwähnt.

6.2. Ergebnisdarstellung und Projektverlauf

Die Prüfungen konnten wie vorab geplant durchgeführt werden.

Im Prüfungsverlauf wurden alle Befunde auch im Issue-Tracking des Dienstleisters in Form von Tickets aufgenommen, nachdem diese in diesem Dokument aufgenommen waren.

Bei den Prüfungen merkten die Werkzeuge an, dass durch den Identitätsanbieter der *Auth-Code-Flow* ohne *Proof for Key Exchange* verwendet wird. Dies wurde im Rahmen der Sicherheitsanalyse bereits mit verantwortlichem Personal besprochen. Es konnte jedoch kein gängiger Angriffsvektor damit in Verbindung gebracht werden, da innerhalb der Authentisierung zusätzliche Schritte unternommen werden, um die Sitzung zweifelsfrei zu authentifizieren (CRAM mit Signatur der Response). Daher wird dies nicht mehr im Rahmen des technischen Tests aufgeführt.

Am 27. August wurde durch den Prüfer per E-Mail angefordert, dass die Ausnahmen in den der Anwendung vorgelagerten Sicherheitsmechanismen am 28. August wieder entfernt werden sollen. Dies wurde am 28. August per E-Mail vom Dienstleister bestätigt.

Am 28. August wurde auch der Behebungsstatus der Befunde aus der Sicherheitsanalyse des Prüfers (siehe oben) sowie der internen Sicherheitsanalyse des Kunden untersucht, sofern diese im Status „offen“ und im Rahmen eines technischen Penetrationstests mit der gewählten Vorgehensweise prüfbar waren (siehe Bezug zu „SCHW-xx“ in der folgenden Aufstellung).

Am 20. September 2024 fand eine Verifizierung der Behebung identifizierter Schwachstellen des Penetrationstests statt. Das Ergebnis wurde um die neuen Erkenntnisse entsprechend aktualisiert.

Dabei wurden folgende Aspekte betrachtet:

Tabelle 5: Nachgeprüfte Befunde/Schwächen aus Sicherheitsanalysen des Prüfers und des Kunden

Index	**Titel/Beschreibung**	**Behebungs-status**	**Bemerkung**
A_01	„Token Audience“ implementieren (teilweise behoben)	Verifiziert: Teilweise behoben	Die Token Audience wurde implementiert, jedoch ist diese zum Zeitpunkt der Prüfung noch nicht abgeschlossen.
A_02	Account Management Console deaktivieren (behoben)	Verifiziert behoben	Die Anmerkung wurde behoben.
SCHW-02	Session-Übernahme	Nicht Prüfbar	Nicht prüfbar bzw. invalide. Für den Prüfer gab es keinerlei Anhaltspunkte einer realen Sitzungsübernahme nach derzeitigem Stand der Technik

Index	Titel/Beschreibung	Behebungs-status	Bemerkung
			ohne Aushebeln eines oder mehrerer etablierter Sicherheitsmechanismen.
SCHW-03	Ein Angreifer übernimmt Cookies	Nicht verifiziert	Siehe Anmerkungen A_04 und A_05.
SCHW-04	Ein Angreifer übernimmt den Auth Code „Durch einen OpenRedirect-Angriff kann ein Angreifer den *Auth-Code* abgreifen. Dieser ist Base64-codiert und enthält bspw. die SafeID. Dafür muss die Redirect-URI im ersten Request Richtung IDP in der Art modifiziert werden, dass sie auf eine Ressource zeigt, auf die der Angreifer Zugriff hat.“	Verifiziert behoben.	Ist aus Sicht des Prüfers behoben, es scheint eine Allow-List für die Weiterleitung innerhalb Keycloaks eingerichtet zu sein, sodass eine Weiterleitung zu fremden Zielen im Testzeitraum nicht möglich war.
SCHW-05	Ein Angreifer überfordert die Ressourcen des IDP (DDos)	Nicht prüfbar	Aufgrund der gewählten Vorgehensweise können keine DoS-Prüfungen durchgeführt werden.
SCHW-06	Ein Angreifer greift das Zertifikat und die PIN ab	Nicht prüfbar	Nicht im Rahmen des Pentests prüfbar mangels weiterer Beschreibung. Dass ein Zertifikat und PIN abhandenkommen, ist aus Prüfersicht immer möglich und lässt sich technisch nur bedingt verhindern. Es erscheint unwahrscheinlich, dass das Zertifikat inkl. privatem Schlüssel für den Angreifer über eine Webseite ausgelesen werden kann.

6.2.1. Übersicht der Schwachstellen

Tabelle 6: Übersicht der Schwachstellen aus der technischen Prüfung

Nr.	Titel	Schweregrad	Seite
W_01	Account-Management-Konsole noch aktiv (A_02, behoben)	-	22
W_02	Keycloak-Metriken öffentlich einsehbar (behoben)	-	25
A_03	Typangabe und Versionsnummer in HTTP-Kopfzeilen enthalten	Anmerkung	28
A_04	*Secure*-Merkmal im Cookie fehlt	Anmerkung	28
A_05	*HttpOnly*-Merkmal im Cookie fehlt	Anmerkung	29
A_06	Unsichere Content-Security-Policy im Einsatz	Anmerkung	30

6.2.2. Beschreibung der Schwachstellen

6.2.2.1. Schwachstellen der Kategorie Kritisch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „kritisch“ identifiziert werden.

6.2.2.2. Schwachstellen der Kategorie Hoch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „hoch“ identifiziert werden.

6.2.2.3. Schwachstellen der Kategorie Mittel

W_01 Account-Management-Konsole noch aktiv (A_02, behoben)

Beschreibung: Die in A_02 bereits beschriebene Account-Management-Konsole ist noch aktiv und über das Internet erreichbar.

Auswirkung: Ein angemeldeter Benutzer ist in der Lage, die Konsole aufzurufen und darin seinen Benutzernamen (SAFE-ID) zu editieren. Ferner können interne Informationen, wie z. B. interne IP-Adressen eingesehen werden.

Beispiel: Im Test konnte die Account-Management-Konsole über die URL https://schulung.bea-brak.de/auth/realms/brak/account/ als angemeldeter Benutzer aufgerufen werden.

Abbildung 2: Keycloak-Account-Management-Konsole

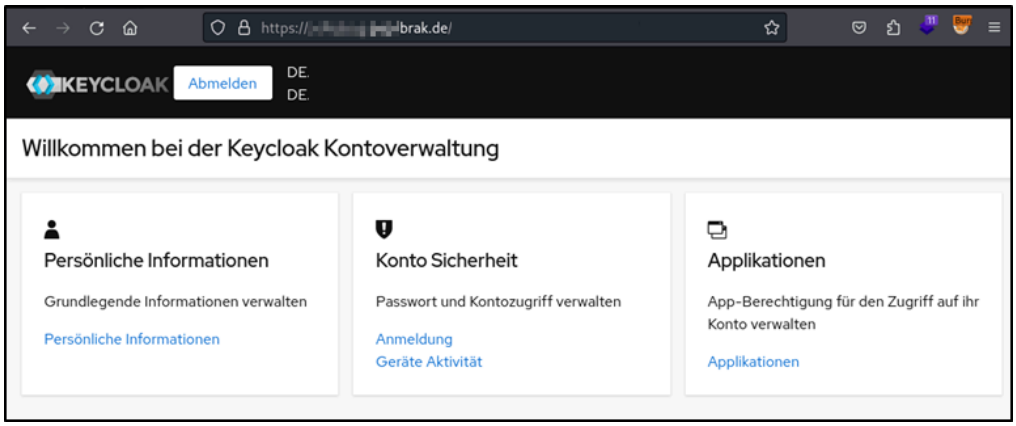
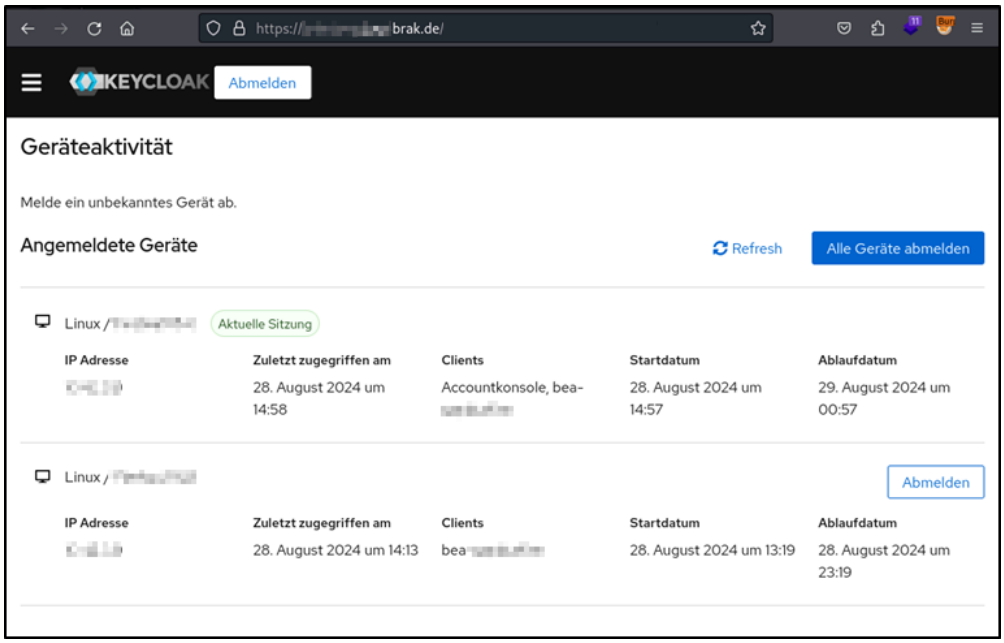


Abbildung 3: Keycloak-Account-Management-Konsole mit internen IP-Adressen



Hinweis	Mit aktivierter WAF war dasselbe Ergebnis erreicht worden, sodass diese bei der Bewertung des Schweregrads keinen Einfluss nimmt.
OWASP Top 10	2021 A05 – Security Misconfiguration
Empfehlung	Siehe Empfehlungen zu A_02.
Referenzen	-
Schweregrad	War: Medium

Tabelle 7: 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.

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Attack Complexity (AC)	Low	Es müssen keine Gegenmaßnahmen umgangen werden, die zu einer hohen Komplexität des Exploits führen.
Attack Requirements (AT)	None	Zum Ausnutzen der Schwachstelle sind keine besonderen Rahmenbedingungen erforderlich, und ein Angriff ist daher beliebig wiederholbar.
Privileges Required (PR)	Low	Ein erfolgreiches Aufrufen der Account Management Console setzt einen Zugang zum beA voraus.
User Interaction (UI)	None	Es ist keine Interaktion mit einem Opfer notwendig, um die Schwäche ausnutzen zu können.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	None	Die Schwachstelle hat keine Auswirkung auf die Vertraulichkeit von Daten der verwundbaren Anwendung.
Integrity Impact (VI)	Low	Die Schwachstelle hat geringe Auswirkung auf die verwundbare Anwendung, dies beschränkt sich jedoch auf den eigenen Benutzer.
Availability Impact (VA)	None	Die Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der verwundbaren Anwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Die Schwachstelle hat keinerlei Auswirkungen auf nachgelagerte Systeme.
Integrity Impact (SI)	None	
Availability Impact (SA)	None	

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
CVSS-B	5,3 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	

Behebungsstatus Verifiziert: Schwachstelle behoben.

Die Schwachstelle wurde behoben. Beim Nachtest konnte die Account Management Konsole nicht mehr aufgerufen werden.

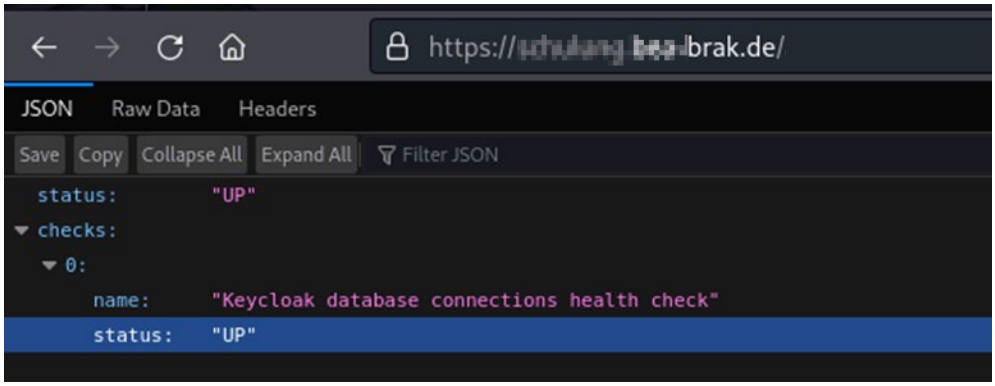
W_02 Keycloak-Metriken öffentlich einsehbar (behoben)

Beschreibung Die Keycloak-Metriken (Gesundheitszustand) sind öffentlich erreich- bzw. einsehbar.

Auswirkung Ein unauthentisierter Benutzer ist durch das Ausnutzen der Schwachstelle in der Lage, den Systemzustand auszulesen und dadurch ggf. Rückschlüsse auf den Systemzustand zu ziehen oder weitere Angriffe zu präzisieren.

Beispiel Im Test konnte der Zustand der Datenbankverbindung und die Zustandsmetriken eingesehen werden (siehe Abbildung 4).

Abbildung 4: Keycloak Health Checks



Hinweise Mit aktivierter WAF war dasselbe Ergebnis erreicht worden, sodass diese bei der Bewertung des Schweregrads keinen Einfluss nimmt.

OWASP Top 10 2021 A05 – Security Misconfiguration

Empfehlung Die Empfehlungen des Herstellers zu den exponierten Endpunkten sollten beachtet und die nicht empfohlenen Endpunkte in der Konfiguration von Keycloak (Configuration as Code) oder des Reverse-Proxys deaktiviert werden.

Referenzen https://www.keycloak.org/server/reverseproxy#_exposed_path_recommendations

Schweregrad War: Medium

Tabelle 8: Bewertung des Schweregrades Schwachstelle W_02

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	Es müssen keine Gegenmaßnahmen umgangen werden, die zu einer hohen Komplexität des Exploits führen.
Attack Requirements (AT)	None	Zum Ausnutzen der Schwachstelle sind keine besonderen Rahmenbedingungen erforderlich, und ein Angriff ist daher beliebig wiederholbar.
Privileges Required (PR)	None	Vor dem Ausnutzen der Schwachstelle benötigt ein Angreifer keine Authentifizierung an der Anwendung.
User Interaction (UI)	None	Es ist keine Interaktion mit einem Opfer notwendig, um die Schwäche ausnutzen zu können.
Auswirkungen auf das verwundbare System		
Confidentiality Impact (VC)	Low	Die Schwachstelle hat geringe Auswirkung auf die Vertraulichkeit von Daten, ein Angreifer hat jedoch keinerlei Kontrolle über Art und Umfang der Daten.
Integrity Impact (VI)	None	Die Schwachstelle hat keine Auswirkung auf die Integrität von Daten der verwundbaren Anwendung.
Availability Impact (VA)	None	Die Schwachstelle hat keine Auswirkung auf die Verfügbarkeit der verwundbaren Anwendung.
Auswirkungen auf nachgelagerte Systeme		
Confidentiality Impact (SC)	None	Die Schwachstelle hat keinerlei Auswirkungen auf nachgelagerte Systeme.
Integrity Impact (SI)	None	

Schwachstellenbewertung entlang CVSS v4.0 (Base Score, CVSS-B)		
Metrik	**Bewertung**	**Begründung der Wertewahl**
Availability Impact (SA)	None	
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	

Behebungsstatus Verifiziert: Schwachstelle behoben.

6.2.2.4. Schwachstellen der Kategorie Niedrig

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „niedrig“ identifiziert werden.

6.2.2.5. Schwachstellen der Kategorie Anmerkungen

A_03 Typangabe und Versionsnummer in HTTP-Kopfzeilen enthalten

Beschreibung	Der Webserver/Reverse-Proxy gibt Informationen über die im Einsatz befindlichen Technologien preis. Folgende Informationen konnten im Testverlauf aus den Antwortkopfzeilen identifiziert werden: • `Server` • `X-Powered-By`
Auswirkung	Ein Angreifer kann diese Informationen verwenden, um Wissen über den Untersuchungsgegenstand aufzubauen, und damit ggf. weitere Angriffe präzisieren.
OWASP Top 10	2021 A05 – Security Misconfiguration
Empfehlung	Die Konfiguration des Webservers/Reverse-Proxys sollte angepasst werden, sodass eingesetzter Server/Technologien sowie Versionsangaben nicht preisgegeben werden. Um nachhaltig für eine Verbesserung zu sorgen, sollten die zur Härtung der Konfiguration notwendigen Schritte in verbindlich umzusetzende Vorgaben zur Härtung dokumentiert werden.
Referenzen	-
Schweregrad	Anmerkung
Behebungsstatus	Nicht verifiziert.

A_04 *Secure*-Merkmal im Cookie fehlt

Beschreibung	Durch die Anwendung werden Cookies ohne das *Secure*-Merkmal ausgeliefert.
Auswirkung	Ist das *Secure*-Merkmal nicht gesetzt, so kann das Cookie potentiell auch über einen unverschlüsselten Kanal versendet werden. Dies würde einem Angreifer, der Daten passiv mitlesen kann, erlauben, das übertragene Cookie mitzulesen und so unberechtigten Zugang zur Session eines Benutzers zu erlangen. Die Anwendung setzt den HSTS-Header. Daher werden alle Daten generell verschlüsselt vom Browser gesendet. Das *Secure*-Flag zu setzen, folgt jedoch dem Defense-in-Depth-Gedanken und bleibt empfehlenswert.
Beispiel	Die Cookies `AUTH_SESSION_ID_LEGACY`, `KEYCLOAK_SESSION_LEGACY`, `KC_RESTART`, `KEYCLOAK_IDENTITY_LEGACY` werden ohne das *Secure*-Merkmal gesetzt.

Abbildung 5: KEYCLOAK_IDENTITY_LEGACY Cookie ohne das *Secure*-Merkmal

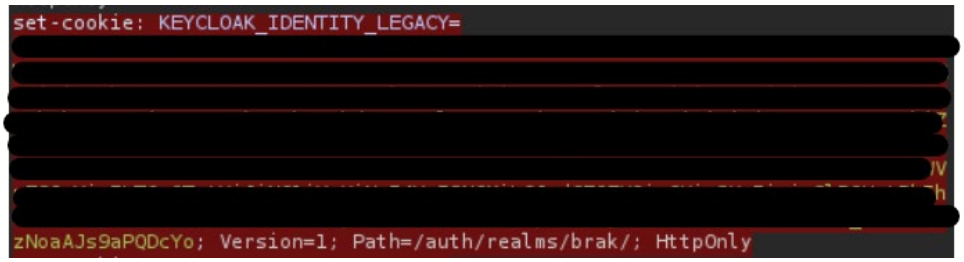


Abbildung 6: KEYCLOAK_SESSION_LEGACY Cookie ohne das *Secure*-Merkmal

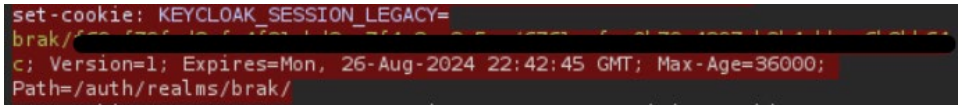


Abbildung 7: AUTH_SESSION_ID_LEGACY Cookie ohne das *Secure*-Merkmal

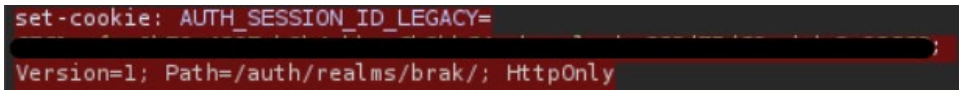
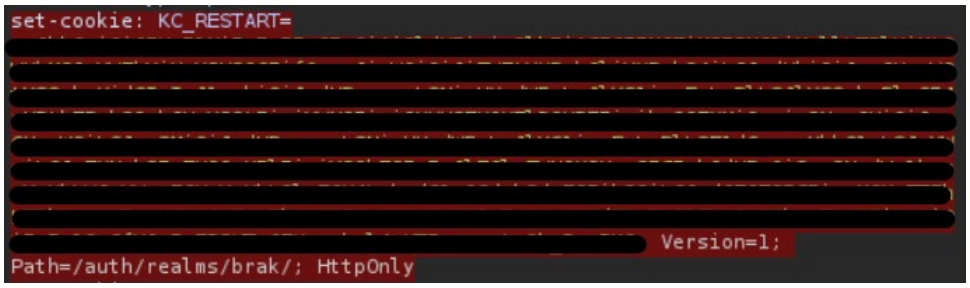


Abbildung 8: KC_RESTART Cookie ohne das *Secure*-Merkmal



Hinweis	Dies wird lediglich als Anmerkung bewertet, da vom Ziel HTTP-Strict-Transport-Security (HSTS) umgesetzt wird. Um den Defence-in-Depth-Ansatz zu verfolgen, sollten dennoch alle möglichen Sicherheitsmerkmale verwendet werden.
OWASP Top 10	2021 A05 – Security Misconfiguration
Empfehlung	Setzen des *Secure*-Merkmals, sofern möglich.
Referenzen	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html https://www.keycloak.org/docs/latest/server_admin/#_ssl_modes
Schweregrad	Anmerkung
Behebungsstatus	Nicht verifiziert.

A_05 *HttpOnly*-Merkmal im Cookie fehlt

Beschreibung	Durch die Anwendung werden Cookies (`KEYCLOAK_SESSION`, `KEYCLOAK_SESSION_LEGACY`) ohne das *HttpOnly*-Merkmal ausgeliefert.

Auswirkung	Ist das *HttpOnly*-Merkmal nicht gesetzt, so kann das betroffene Cookie auch durch JavaScript ausgelesen werden. Angreifer könnten hierüber potentiell das Cookie auslesen, was weitere Angriffe vereinfachen kann. Hierzu müsste aber in der Anwendung eine Schwachstelle vorliegen, über die Angreifer eigenen JavaScript-Schadcode ausführen können („Cross Site Scripting“). Eine solche Schwachstelle konnte aber nicht im Rahmen der Prüfung festgestellt werden, weshalb dieser Umstand nur als Hinweis dokumentiert wurde. Die Verwendung des *HttpOnly*-Merkmals bleibt aus Sicht des „Defense-in-Depth“-Gedankens dennoch empfehlenswert.
OWASP Top 10	2021 A05 – Security Misconfiguration
Empfehlung	Setzen des *HttpOnly*-Merkmals, sofern möglich.
Referenzen	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
Schweregrad	Anmerkung
Behebungsstatus	Nicht verifiziert.

A_06 Unsichere Content-Security-Policy im Einsatz

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

Abbildung 9: Eingesetzte Content-Security-Policy

```
content-security-policy: default-src 'self'; img-src 'self' data:;
connect-src 'self' wss://127.0.0.1:* ws://127.0.0.1:*; script-src 'self'
'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-src
'self' https://easy-feedback.de;
```

	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, • `unsafe-eval`: ermöglicht die Ausführung von Code, der in DOM-API-Funktionen wie `eval()` 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 nicht verhindert.
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 `<script>`-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
Schweregrad	Anmerkung
Behebungsstatus	Nicht verifiziert.

6.2.3. 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 9: Ergebnisreferenzierung Penetrationstest zu OWASP-Top-10-Risiken

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

7. ANHANG A: VERSIONEN UND VERZEICHNISSE

7.1. Versionshistorie

Tabelle 10: Versionshistorie

Version	Datum	Änderungen
1.4	31.10.2024	Redaktionelle Änderungen abgenommen
1.3	02.10.2024	Interne Rückmeldung zu Darstellung und Redaktion eingearbeitet
1.2	20.09.2024	Einpflegen der Änderungen nach Verifikation von Schwachstellen
1.1	11.09.2024	Einarbeitung der Änderungen aus dem Lektorat
1.0	10.09.2024	Lektorat des Ergebnisberichts
0.9	05.09.2024	Zusammenfassung des Dokuments ergänzt
0.8	29.08.2024	Abnahme der Änderungen aus der fachlichen Qualitätssicherung
0.7	29.08.2024	Einarbeitung der Änderungen aus der fachlichen Qualitätssicherung
0.6	29.08.2024	Fachliche Qualitätssicherung
0.5	22.08.2024	Dokumentation technischer Prüfungen ergänzt
0.4	22.05.2024	Zwischenversion für den Kunden erstellt
0.3	07.05.2024	Ergebnisse der Workshops und abgeleitete Empfehlungen dokumentiert
0.2	30.04.2024	Fortschreibung des Dokuments
0.1	10.04.2024	Fortschreibung des Dokuments
0.0	22.03.2024	Initialisierung des Dokuments

7.2. Abbildungsverzeichnis

7.3. Tabellenverzeichnis

8. ANHANG B: GLOSSAR

In diesem Abschnitt werden verwendete Begriffe oder Abkürzungen erläutert.

Tabelle 11: Glossar

Begriff	Bedeutung
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISMS	Informationssicherheits-Managementsystem
IAM	Identitäts- und Zugriffsverwaltung (Identity and Access Management)
IDP	Identitätsanbieter (Identity Provider). Im beA-Kontext wird hierfür auch der Begriff „BRAK-IdP“ bzw. „IdP“ verwendet.
Autent	Auch: Governikus Autent – Softwarelösung des Herstellers Governikus für IAM
Autent-DB	Datenbank, die die Identitätsinformationen bereithält
SAFE-BRAK	Früherer Name für Autent. Wird sukzessive durch BRAK-IAM, bestehend aus IdP und IdM zusammen mit der Autent-Datenbank, abgebildet.

9. ANHANG C: ERMITTLUNG DES SICHERHEITSNIVEAUS

9.1. Ermittlung Sicherheitsniveau Webanwendungspenetrationstest

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

Tabelle 12: 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.