secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

ABSCHLUSSBERICHT PENETRATIONSTEST

VERSION 0.92 | 06.10.2020

Abschlussbericht für Nova Building GmbH
In der Mordach 1a
64367 Mühltal

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden

Autor
Kai Dybionka

INHALTSVERZEICHNIS

1. ZUSAMMENFASSUNG

1.1. Prüfungen der Webanwendung im LAN

Im Zeitraum vom 05. Februar bis zum 08. Mai 2020 wurde die Webanwendung NOVA AVA zwei Sicherheitsüberprüfungen in Form von technischen Penetrationstests unterzogen. Das Ziel der Prüfungen war die Identifikation von technischen Schwachstellen auf Anwendungsebene.

Die Webanwendung wurde durch einen Download den Prüfern zur Verfügung gestellt, auf einem Server im lokalen Netzwerk der secuvera GmbH geladen und installiert. Der Penetrationstest wurde im Anschluss auf die Webanwendung auf diesem Server durchgeführt.

Geprüft wurde die Software NOVA AVA in der Version 3.0.

Es konnten während der Prüfungen der letzten Version der Webanwendung keine Schwachstellen festgestellt werden.

Tabelle 1: Statistik: Identifizierte Schwachstellen Webanwendung

Anzahl identifizierter Schwachstellen mit kritischem Risikograd	0
Anzahl identifizierter Schwachstellen mit hohem Risikograd	0
Anzahl identifizierter Schwachstellen mit mittlerem Risikograd	0
Anzahl identifizierter Schwachstellen mit geringem Risikograd	0
Anzahl identifizierter Schwachstellen ohne direkten Risikograd	0
Gesamtanzahl identifizierter Schwachstellen	0
Gesamtbewertung Sicherheitsniveau	Sehr hoch

Insgesamt lässt sich der Anwendung ein sehr hohes Sicherheitsniveau attestieren, da keine Schwachstellen identifiziert werden konnten.

1.2. Prüfung der API NOVA AVA im LAN und über das Internet

Im Zeitraum vom 06. bis zum 08. Mai 2020 wurde die API-Schnittstelle der Webanwendung NOVA AVA einer Sicherheitsüberprüfung in Form eines technischen Penetrationstests unterzogen. Das Ziel der Prüfungen war die Identifikation von technischen Schwachstellen auf Anwendungsebene.

Die Prüfungen der API erfolgten auf die im lokalen Netzwerk der secuvera GmbH installierten Webanwendung. Geprüft wurde die API-Schnittstelle in Version 1.2.1.

Am 09. Juni wurde eine Prüfung des Rate-Limiting über das Internet auf die in der Testumgebung unter https://labs.systender.net/nova/dev/public erreichbare API durchgeführt.

Es konnten während der Prüfungen keine Schwachstellen in der API oder beim Rate-Limiting festgestellt werden.

Tabelle 2: Statistik: Identifizierte Schwachstellen API

Anzahl identifizierter Schwachstellen mit kritischem Risikograd	0
Anzahl identifizierter Schwachstellen mit hohem Risikograd	0
Anzahl identifizierter Schwachstellen mit mittlerem Risikograd	0
Anzahl identifizierter Schwachstellen mit geringem Risikograd	0
Anzahl identifizierter Schwachstellen ohne direkten Risikograd	0
Gesamtanzahl identifizierter Schwachstellen	0
Gesamtbewertung Sicherheitsniveau	Sehr hoch

Insgesamt lässt sich der API ein sehr hohes Sicherheitsniveau attestieren, da keine Schwachstellen in der Gesamtumgebung ausgenutzt werden konnten.

2. 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.

2.1. Schwachstellenbewertung

Zur Ermittlung des Risikograds von Schwachstellen wird das Common Vulnerability Scoring System (CVSS) verwendet.[1] 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".

2.2. Darstellung

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

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

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

[1] 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:

- W_ Schwachstellen bei der Webanwendungsprüfung,
- A_ Schwachstellen bei der API-Prüfung.

3. PRÜFUNGEN DER WEBANWENDUNG NOVA AVA

3.1. Beschreibung der Vorgehensweise und des Ziels

Im Zeitraum vom 05. Februar bis zum 08. Mai 2020 wurde die Webanwendung NOVA AVA zwei Sicherheitsüberprüfung in Form von technischen Penetrationstests unterzogen. Das Ziel der Prüfungen war die Identifikation von technischen Schwachstellen auf Anwendungsebene.

Hierfür wurde die Anwendung in der Version 3.0 auf einem System der Prüfer installiert.

Die Prüfungen der Anwendung erfolgten sowohl als anonymer Benutzer als auch als Benutzer mit internen und externen Berechtigungsstufen. Dabei konnten die internen Benutzer Projekte anlegen und bearbeiten, die externen Nutzer konnten auf eine Einladung hin ein Angebot für ein bestimmtes Leistungsverzeichnis erstellen. Die API-Schnittstelle wurde während der Prüfungen nicht betrachtet.

Die Anwendung wurde zunächst mittels automatisierter Scanwerkzeuge abgetastet. Verwendet wurden hierfür die Werkzeuge „Acunetix Web Vulnerability Scanner“[2] und „Burp Suite Pro“[3]. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. False Positives möglichst ausschließen zu können und durch die Funktionsweise der automatischen Werkzeuge bedingte Schwächen auszugleichen. Zur Überprüfung von SQL-Schwachstellen wurde das Open-Source-Tool „sqlmap“[4] genutzt.

Im Rahmen der Penetrationstests der Webanwendung wurden alle technisch prüfbaren Inhalte der OWASP Top 10 (konsolidiert aus den Versionen 2004, 2007, 2010, 2013 und 2017) sowie weitere Schwachstellen geprüft.

Tabelle 3: Konsolidierte Liste der Risiken aus der OWASP Top 10

Risiko
2017 A1 - Injection
2017 A2 - Broken Authentication
2017 A3 - Sensitive Data Exposure
2017 A4 - XML External Entities (XXE)
2017 A5 – Broken Access Control
2017 A6 - Security Misconfiguration
2017 A7 - Cross Site Scripting (XSS)
2017 A8 – Insecure Deserialization
2017 A9 - Using Components with Known Vulnerabilities
2017 A10 – Insufficient Logging & Monitoring
2013 A8 - Cross Site Request Forgery (CSRF)
2004 A5 - Buffer Overflow
2004 A9 - Application Denial of Service
2007 A3 - Malicious File Execution

[2] http://www.acunetix.com/

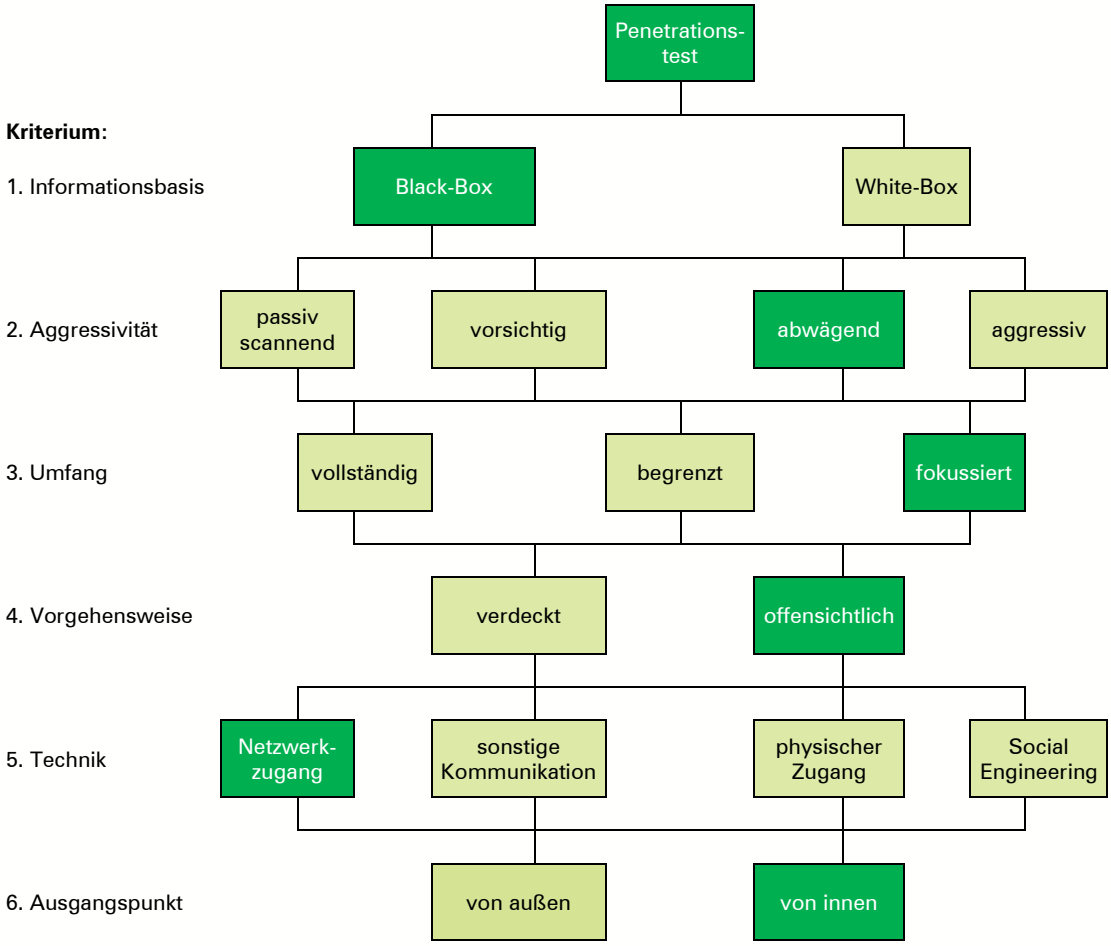
[3] https://www.portswigger.net

[4] http://www.sqlmap.org

Die Webanwendung wurde abschließend in der Version 3 Build 200505 geprüft.

Für den Penetrationstest wurde die folgende Vorgehensweise nach der BSI-Studie „Durchführungskonzept für Penetrationstests“[5] zugrunde gelegt:

Abbildung 1: Vorgehensweise nach BSI-Studie



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

3.2. Projektverlauf und Ergebnisdarstellung

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

3.2.1. Übersicht der Schwachstellen

In der Version 3 Build 200505 konnten keine Schwachstellen identifiziert werden.

3.2.2. 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 4: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-Top-10-Risiken

Risiko	**Fail/Pass**
2017 A1 - Injection	Pass
2017 A2 - Broken Authentication	Pass
2017 A3 - Sensitive Data Exposure	Pass
2017 A4 - XML External Entities (XXE)	Pass
2017 A5 – Broken Access Control	Pass
2017 A6 - Security Misconfiguration	Pass
2017 A7 - Cross Site Scripting (XSS)	Pass
2017 A8 – Insecure Deserialization	Pass
2017 A9 - Using Components with Known Vulnerabilities	Pass
2017 A10 – Insufficient Logging & Monitoring	Pass
2013 A8 - Cross Site Request Forgery (CSRF)	Pass
2004 A5 - Buffer Overflow	Pass
2004 A9 - Application Denial of Service	Pass
2007 A3 - Malicious File Execution	Pass

4. PRÜFUNG DER API NOVA AVA

4.1. Beschreibung der Vorgehensweise und des Ziels

Die API-Schnittstelle wurde sowohl automatisiert als auch manuell geprüft. Verwendet wurde hierfür zunächst das Werkzeug „Burp Suite Pro“[6]. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. False Positives auszuschließen. Zur Überprüfung von SQL-Schwachstellen wurde das Open-Source-Tool „sqlmap“[7] genutzt.

Die Anwendung wurde in der Version 3.0 für die Prüfungen auf einem System der Prüfstelle installiert. Geprüft wurde die API-Schnittstelle in Version 1.2.1.

Die Prüfungen der API erfolgten sowohl als anonymer Benutzer als auch mit Benutzerberechtigungen. Hierfür wurde zum einen mit Benutzerberechtigung und zum anderen mit Administrationsberechtigung geprüft.

In einer Prüfung am 09. Juni wurde des Rate-Limiting über das Internet auf die in der Testumgebung unter https://labs.systender.net/nova/dev/public erreichbare API durchgeführt.

Im Rahmen der Penetrationstests der Webanwendung wurden alle technisch prüfbaren Inhalte der OWASP-API-Top-10 2019 sowie weitere Schwachstellen geprüft.

Tabelle 5: Liste der Risiken aus der OWASP-API-Top-10 2019

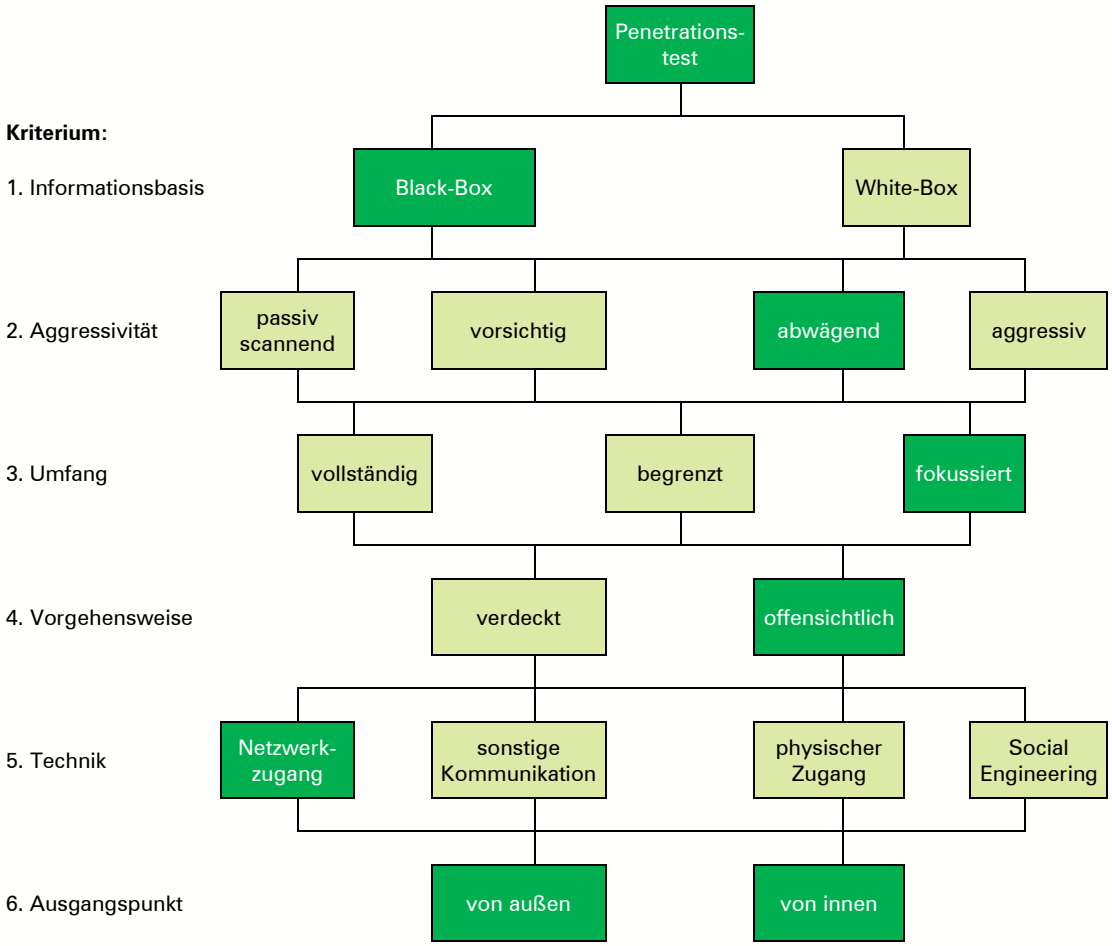
Risiko
2019 A1 – Broken Object Level Authorization
2019 A2 – Broken User Authentication
2019 A3 – Excessive Data Exposure
2019 A4 – Lack of Resources & Rate Limiting
2019 A5 – Broken Function Level Authorization
2019 A6 – Mass Assignment
2019 A7 – Security Misconfiguration
2019 A8 – Injection
2019 A9 – Improper Assets Management
2019 A10 – Insufficient Logging & Monitoring

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

[7] http://www.sqlmap.org

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

Abbildung 2: 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.

Im Verlauf der Prüfungen konnten zwei undokumentierte Pfade der API identifiziert werden. Dies stellt keine Schwachstelle dar und wird an dieser Stelle lediglich als Hinweis aufgenommen. Die undokumentierten Pfade betreffen:

- GET /checkstatus,
- GET /boqtypes.

4.2.1. Übersicht der Schwachstellen

In der Version 1.2.1 konnten keine Schwachstellen identifiziert werden.

4.2.2. 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 6: Ergebnisreferenzierung Penetrationstest Webanwendung zu OWASP-API-Top-10-Risiken

Risiko	**Fail/Pass**
2019 A1 – Broken Object Level Authorization	Pass
2019 A2 – Broken User Authentication	Pass
2019 A3 – Excessive Data Exposure	Pass
2019 A4 – Lack of Resources & Rate Limiting	Pass
2019 A5 – Broken Function Level Authorization	Pass
2019 A6 – Mass Assignment	Pass
2019 A7 – Security Misconfiguration	Pass
2019 A8 – Injection	Pass
2019 A9 – Improper Assets Management	Pass
2019 A10 – Insufficient Logging & Monitoring	Pass

5. ANHANG A: VERSIONEN UND VERZEICHNISSE

5.1. Versionshistorie

Tabelle 7: Versionshistorie

Version	Datum	Bearbeiter	Änderungen
0.92	10.06.2020	Dybionka, secuvera	Dokumentation der Prüfung des Rate-Limiting
0.91	29.05.2020	Dybionka, secuvera	Einarbeitung der Rückmeldung des Kunden
0.9	27.05.2020	Dybionka, secuvera	Einpflegen der Änderungen aus der Qualitätssicherung, Version zur Abstimmung mit dem Kunden
0.8	27.05.2020	Glemser, secuvera	Qualitätssicherung
0.7	26.05.2020	Dybionka, secuvera	Initiale Dokumentenerstellung, Version für die Qualitätssicherung

5.2. Abbildungsverzeichnis

5.3. Tabellenverzeichnis

6. ANHANG B: ERMITTLUNG DES SICHERHEITSNIVEAUS

6.1. Ermittlung Sicherheitsniveau systembasierter Penetrationstest

Das Sicherheitsniveau pro System wird aus dem Risikograd 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 8: 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 Risikograd 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 Risikograd gering und mittel identifiziert wurden.	Wird gewählt, sofern auf höchstens 20% der Prüfziele ein niedriges Sicherheitsniveau, und auf keinem erreichbaren Prüfziele ein kritisches Sicherheitsniveau identifiziert wurde.
Niedrig	Wird gewählt, sofern mindestens eine Schwachstelle mit Risikograd 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 Risikograd kritisch identifiziert wurde.	Wird gewählt, sofern auf mehr als 20% der erreichbaren Prüfziele ein kritisches Sicherheitsniveau identifiziert wurde.

6.2. Ermittlung Sicherheitsniveau Webanwendungspenetrationstest

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

Tabelle 9: 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 Risikograd gering identifiziert wurden.
Mittel	Wird gewählt, sofern nur Schwachstellen mit Risikograd gering und mittel identifiziert wurden.
Niedrig	Wird gewählt, sofern mindestens eine Schwachstelle mit Risikograd hoch identifiziert wurde.
Kritisch	Wird gewählt, sofern mindestens eine Schwachstelle mit Risikograd kritisch identifiziert wurde.