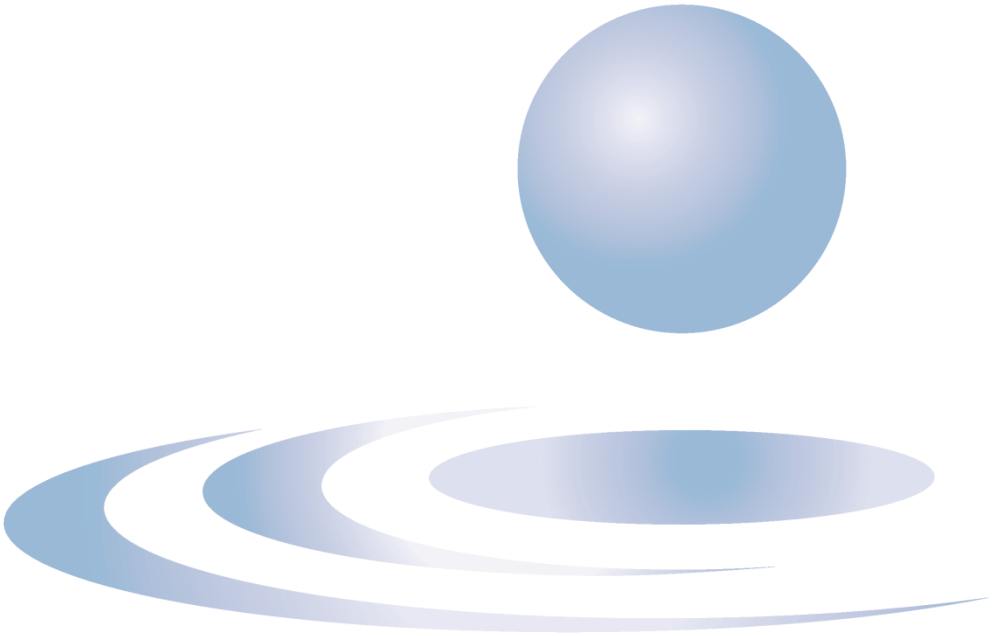
Zusammenfassung der Ergebnisse des Penetrationstests

SeaTable GmbH



Herausgeber:	SRC Security Research & Consulting GmbH Emil-Nolde-Straße 7 D-53113 Bonn
Dokumentenreferenz:	Seatable-2401_Management_Summary_v1.2.docx
Datum:	14.10.2024
Autor:	Hirschberg, Tim, SRC Security Research & Consulting GmbH
Qualitätssicherung:	Celik, Devrim, SRC Security Research & Consulting GmbH

Inhaltsverzeichnis

Änderungshistorie

Version	Datum	Art	Author
0.1	07.10.2024	Initialer Entwurf	Tim Hirschberg
0.3	08.10.2024	Risikobewertung	Tim Hirschberg
0.4	11.10.2024	Qualitätssicherung	Devrim Celik
0.5	11.10.2024	Einpflegen Änderungen der QS	Tim Hirschberg
1.0	11.10.2024	Finalisierung	Tim Hirschberg
1.1	14.10.2024	Konkretisierung des Setup	Tim Hirschberg
1.2	14.10.2024	Einarbeitung vom Feedback des Kunden	Tim Hirschberg

1. Management Summary

Für den Kunden SeaTable GmbH (Seatable) wurde im Zeitraum 09.09.2024 bis 23.09.2024 ein Penetrationstest mit Grey-Box-Ansatz durchgeführt. Der Grey-Box-Ansatz spiegelt die Sichtweise eines Angreifers mit Insiderwissen wider. So wie dem Insider, liegen auch dem Penetrationstester gewisse Informationen über die Kundensysteme vor, die für Angriffe genutzt werden können.

Gegenstand des Penetrationstests ist die SeaTable-Software, explizit in der selbstgehosteten Variante in Version 5.1.4, die so auch in der Cloudumgebung der SeaTable GmbH im Einsatz ist, mit Hauptaugenmerk auf die API und die Webanwendung. Social-Engineering-Angriffe waren nicht Bestandteil des Penetrationstests.

Die Software wurde nach offizieller Anleitung des Kunden vom Penetrationstester installiert und mit Standardparametern konfiguriert. Es wurde keine speziell gehärtete Version verwendet.

Das Ergebnis dieses Penetrationstests ist in der folgenden Grafik zusammenfassend aufgeführt:

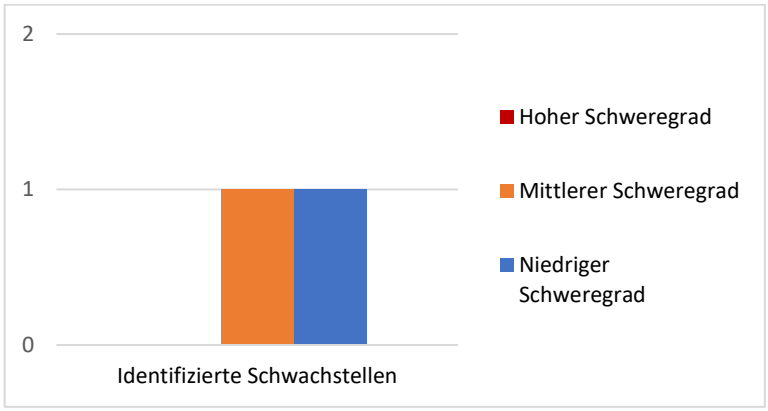


Abbildung 1: Anzahl der identifizierten Schwachstellen

Während des Penetrationstests wurde 1 Schwachstelle mit Schweregrad „mittel“ und 1 Schwachstelle mit Schweregrad „niedrig“ identifiziert.

Zusammenfassend kann das Sicherheitsniveau der Seatable-Software als gut eingestuft werden.

SRC empfiehlt die folgenden Maßnahmen um das Sicherheitsniveau weiter zu verbessern:

- Sicherstellen, dass es keine sensitiven Daten in zugänglichem Code der Anwendung gibt oder den Zugriff auf diesen ganz zu unterbinden.

2. Einleitung

Die SeaTable GmbH ist verantwortlich für den Vertrieb und Support von SeaTable sowie den Betrieb der SeaTable Cloud. Gegründet wurde die SeaTable GmbH im Juli 2020.

Die Seafile Ltd. ist ein Software-Unternehmen aus Peking, China. Seit 2019 entwickelt die Seafile Ltd. die Low-Code-Anwendung SeaTable. Gegründet wurde die Seafile Ltd im Jahr 2012, um die selbstentwickelte Software Seafile Server zu vermarkten. Seafile Server ist eine Enterprise File-Sync-and-Share-Lösung, die sich insbesondere im europäischen Hochschul- und Forschungsbereich großer Beliebtheit erfreut. Seafile Server gibt es in zwei Editionen. Die Seafile Server Community Edition ist quelloffen; die Seafile Server Professional Edition wird unter einer proprietären Lizenz vertrieben.

Die Seafile Ltd. hält einen 50-prozentigen Anteil an der SeaTable GmbH. An der Geschäftsführung ist sie weder direkt noch indirekt beteiligt.

Gegenstand des Penetrationstests ist die SeaTable-Software, explizit in der selbstgehosteten Variante in der Version 5.1.4, die so auch in der Cloudumgebung der SeaTable GmbH im Einsatz ist, mit Hauptaugenmerk auf die API und die Webanwendung. Das im Geltungsbereich liegenden System wurde auf Netzwerk- und Anwendungsebene, hinsichtlich der Integrität, Vertraulichkeit und Verfügbarkeit, untersucht.

Die Zielsetzung der Penetrationstests wurde gemeinsam mit den zuständigen Mitarbeitern Seatables abgestimmt. Der Penetrationstest wurde in den Räumlichkeiten der SRC durchgeführt.

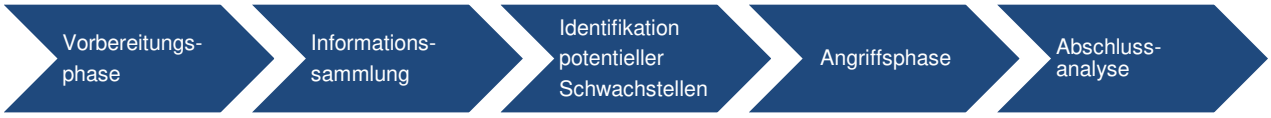
Es wurde vereinbart, einen Grey-Box-basierten Ansatz für den Penetrationstest zu wählen. Der Grey-Box Ansatz spiegelt die Sichtweise eines Angreifers mit teilweisem Insiderwissen wieder. Dem Tester stehen somit begrenzte Informationen über die Testsysteme zur Verfügung, er hat jedoch keine Informationen über die interne Funktionsweise der Systeme, was den Grey-Box-basierten Ansatz vom White-Box-basierten Ansatz unterscheidet.

3. Methodik

SRC orientiert sich bei der Durchführung von Penetrationstests am „Durchführungskonzept für Penetrationstests“ vom *Bundesamt für Sicherheit in der Informationstechnik* (BSI) und an:

- OWASP Testing Guide (v.4.2)
- *Web Application Security Consortium* (WASC)
- weiteren anerkannten Best Practices und Industrie-Standards

Auf Basis dieser Modelle hat SRC nachfolgendes Vorgehensmodell zur Durchführung von Penetrationstests entwickelt:



In der **Vorbereitungsphase** vereinbart SRC mit dem Kunden die Rahmenbedingungen des Penetrationstests, dazu gehören u.a. die Benennung der Verantwortlichkeiten und Ansprechpartner bei beiden Parteien. Anschließend wird die genaue Vorgehensweise während des Penetrationstests abgestimmt. Es wird abgestimmt, bzgl. welcher Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit) der Systeme untersucht werden sollen.

Während der **Informationssammlung** sammelt SRC Informationen über die Zielsysteme im Geltungsbereich, die für spätere Angriffe genutzt werden können. Zudem werden die vom Kunden bereits gestellten Informationen geprüft und validiert.

In dem Schritt **Identifikation potentieller Schwachstellen** (*vulnerabilities*) stellt SRC eine Menge von potentiellen Schwachstellen in den Zielsystemen zusammen. Potentielle Schwachstellen können aus den eingesetzten Technologien (z.B. Applikationsserver, Betriebssysteme, eingesetzte Programmiersprachen) bzw. derer Kombinationen auf den Systemen im Geltungsbereich abgeleitet werden. Dafür greift der Penetrationstester auf Werkzeuge und seinen Erfahrungsschatz zurück. Die zusammengestellten Schwachstellen werden an dieser Stelle noch als *potentiell* bezeichnet, weil zu diesem Zeitpunkt lediglich die Indikation für das Vorhandensein vorliegt, aber noch belastbarer Nachweis.

Die **Angriffsphase** dient der Verifikation von potentiellen Schwachstellen (siehe Abbildung 2). Zu diesem Zweck definiert SRC für jede Schwachstelle einen Angriffsvektor. Ein Angriffsvektor ist eine Beschreibung für einen Angriff, der es einem Angreifer erlaubt, eine oder mehrere Schwachstellen auszunutzen, um Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit) zu verletzen. An dieser Stelle kann der Penetrationstester entscheiden, gewisse Angriffsvektoren nicht zu untersuchen (d.h. nicht anzugreifen). Gründe für diese Entscheidung können z.B. sehr hoher Aufwand oder mögliche unerwünschte Auswirkung auf die Zielsysteme sein. Diese Schwachstellen werden im weiteren Verlauf als „nicht-verifiziert“ bezeichnet. Die Angriffsvektoren der „nicht-verifizierten“ Schwachstellen stellen eine Dokumentation der möglichen aber nicht weiter untersuchten Gefährdungen dar. „Nicht-verifizierte“ Schwachstellen werden weiterhin in der nächsten Phase einer Risikobewertung unterzogen.

Mittels der Durchführung von Angriffen gemäß den definierten Angriffsvektoren kann der Penetrationstester für die übrigen potentiellen Schwachstellen feststellen, ob es sich um verifizierte Schwachstellen oder um Falsch-Positive handelt. Verifizierte Schwachstellen sind durch einen erfolgreichen Angriff auf die betreffende Schwachstelle tatsächlich nachgewiesen worden.

Potentielle Schwachstellen, bei denen der Penetrationstester aufgrund von vorliegenden Informationen ermittelt hat, dass diese nicht vorhanden sind, werden als Falsch-Positive bezeichnet. Sie werden in den nachfolgenden Phasen nicht weiter betrachtet und damit keiner Risikobewertung unterzogen.

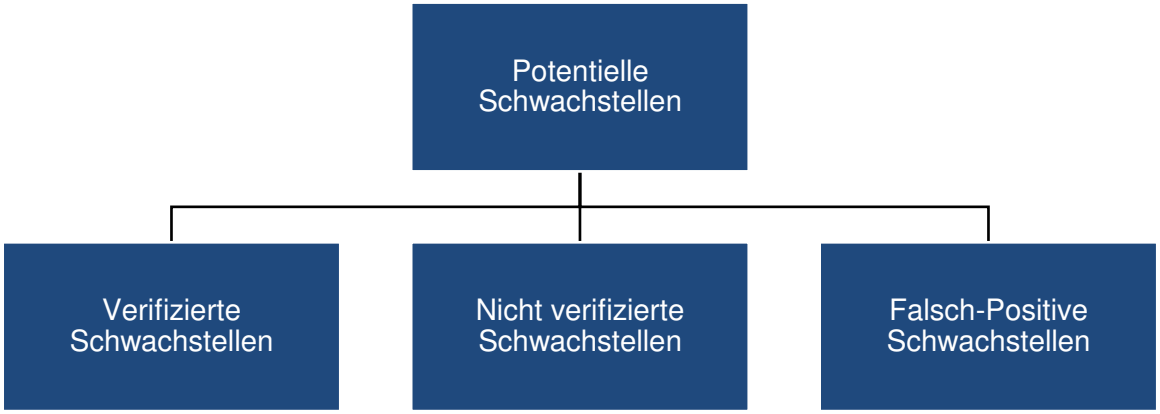


Abbildung 2 Schwachstellen im Laufe des Penetrationstests

In der **Abschlussanalyse/Dokumentation** führt SRC eine Risikoabschätzung der verifizierten und potentiellen Schwachstellen durch. Diese Risikoabschätzung dient unter anderem als Orientierungshilfe für die Priorisierung der Umsetzung der von SRC empfohlenen Maßnahmen zu deren Beseitigung. Die verifizierten und potentiellen Schwachstellen, ihr Sicherheitsrisiko und die Empfehlungen zur Beseitigung/Risikominimierung werden in der Dokumentation festgehalten.

4. Vorbereitungsphase

Zu Beginn des Penetrationstests wurde ein Kickoff-Meeting durchgeführt. Während des Kickoff-Meetings wurden die Rahmenbedingungen wie Verantwortlichkeiten und Ansprechpartner auf Kundenseite sowie Durchführende und Ansprechpartner seitens der SRC abgestimmt.

Ansprechpartner	Firma	Aufgabe
Dyllick-Brenzinger, Ralf	SeaTable GmbH	Co-Geschäftsführer
Hirschberg, Tim	SRC	Penetrationstester

Zudem wurde die Vorgehensweise während des Penetrationstests abgestimmt. Es wurde vereinbart, welche Systeme getestet und in welcher Reihenfolge diese getestet werden sollen.

4.1 Setup

Bei dem Setup handelt es sich um eine Basisinstallation nach der Anleitung von SeaTable. Diese wurde zuletzt am 9.9.2024 unter https://admin.seatable.io/installation/basic-setup/ abgerufen. Das System, welches von SeaTable zur Installation zur Verfügung gestellt wurde, ist ein den Anforderungen entsprechende Standartinstallation von Debian 12 mit aktiviertem SSH Zugang. Auf dieses System konnte der Penetrationstester sich per SSH verbinden und die Installation der SeaTable Software nach der oben genannten Anleitung durchführen. Einzig die Zeile welches Docker-Image für den SeaTable-Server gezogen werden sollte wurde durch den Penetrationstester, nach Anleitung des Kunden, angepasst. Dies war nötig um die aktuellste Version der Software installieren zu können und die Version 5.1.4 zu bekommen.

In der Datei “/opt/seatable-compose/seatable-server.yml” wurde die Zeile

```
image: ${SEATABLE_IMAGE:-seatable/seatable-enterprise:5.0.8}
```

zur folgenden Zeile angepasst:

```
image: ${SEATABLE_IMAGE:-seatable/seatable-enterprise-testing:5.1.4}
```

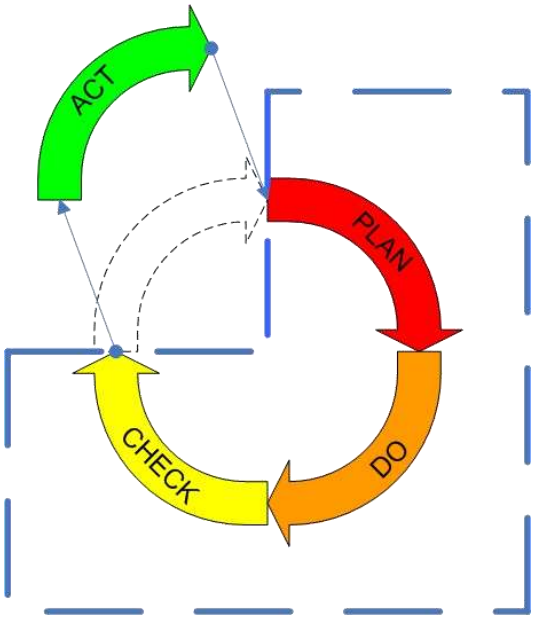
Alle weiteren Installationsschritte wurden nach der Anleitung durchgeführt.

5. Grenzen der durchgeführten Tests

Im Rahmen der Sicherheitsanalyse werden Schwächen im Zielsystem aufgedeckt, welche die Grundlage für zu definierende Abhilfemaßnahmen bilden. Die Erhaltung von Sicherheit ist ein dynamischer Prozess, da jeden Tag neue Schwächen in Sicherheitssystemen aufgedeckt werden. Auch Sicherheitsanalysen, die im Ergebnis ohne Befund ausfallen, dürfen nicht als Garantie verstanden werden, dass das Zielsystem dauerhaft gegen jegliche Art von Angriffen immun ist.

Sicherheitsanalysen sind nur als eine Momentaufnahme der Systemsicherheit aufzufassen. Werden nach der Durchführung der Sicherheitsanalysen Änderungen an den Systemen vorgenommen, kann dies sowohl zu einer positiven als auch zu einer negativen Veränderung der Systemsicherheit führen. SRC empfiehlt daher die Durchführung von Sicherheitsanalysen in regelmäßigen Abständen, insbesondere jedoch nach jeder größeren Konfigurationsänderung.

Hinsichtlich des IT-Sicherheitsmanagements verdeutlicht der PDCA-Zyklus (**P**lan-**D**o-**C**heck-**A**ct) diesen iterativen Prozess. Aufgrund der Gegebenheiten des Penetrationstests und der Abgrenzung der Verantwortlichkeiten stellt sich jedoch ein leicht abweichendes Bild dar. Die Planungs-, Durchführungs- bzw. Vorbereitungs- und Überprüfungsphase sollten als ein durchgehender Prozess innerhalb des Penetrationstests betrachtet werden. Nach Abschluss dieser Prozesse obliegt es dem Auftraggeber, die notwendigen Maßnahmen durchzuführen („Act“). Aus diesem Grunde soll der PDCA die Verantwortlichkeiten dieses iterativen und interaktiven Prozesses verdeutlichen.



iPDCA
interactive PLAN-DO-CHECK-ACT

Dauerhafte Sicherheit kann nur durch die ständige Überprüfung der Wirksamkeit der etablierten Prozesse, Maßnahmen und Systeme im Sinne eines Regelkreises gewährleistet werden. Nur ein kontinuierlicher Sicherheitsprozess, welcher mit einer Ist-Analyse startet, darauf aufbauende Schutzmaßnahmen konzipiert und deren Wirksamkeit in einem Kontrollschritt überprüft, ist ein Garant für dauerhaft ausreichenden Schutz gegen aktuelle Sicherheitslücken. Insbesondere die Wartung der kritischen Systeme fällt hierbei unter den Kontrollaspekt und ist ein wichtiger Punkt in der Systemsicherheit. Nur ein System, welches regelmäßig aktualisiert und überprüft wird, kann auch dauerhaft als ausreichend resistent gegen Angriffe angesehen werden. Die Beobachtung von Sicherheitsmeldungen ist hierfür eine wesentliche Grundlage des Kontrollschritts.