RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R01	DDoS-Angriff	[Hoch]	Hoch	[Hoch]	[Transferieren]
Beschreibung					
Der Angreifer schickt sehr viele Anfragen an den Server, um dessen Verfügbarkeit einzuschränken.					
Anforderungen					
Der Server darf bei vielen Anfragen keine Performance verlieren oder andersweitig eingeschränkt sein.					
Maßnahmen				Überprüfung	TestID
Der Server darf nur eine begrenzte Anzahl an Anfragen akzeptieren und bearbeiten. Verwendung einer WAF oder eines Load Balancers mithilfe von CloudFlare.				Last Test Design Review	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R02	SQL-Injection	[Sehr hoch]	[Sehr hoch]	[Sehr hoch]	[Reduzieren]
Beschreibung					
In Eingabefelder werden SQL-Statements geschrieben, welche unerlaubte Anfragen an die Datenbank schickt, mit dem Ziel, Informationen aus der DB zu erhalten oder deren intigrität zu kompromittieren					
Anforderungen					
Durch Eingabefelder darf keiner ausführbarer SQL-Code in die DB gelangen.					
Maßnahmen				Überprüfung	TestID
Alle Eingaben werden geprüft und bereinigt, dass sie nur als Text gesehen werde und niemals dazu in der Lage sind SQL-Code ausgeführt zu werden Benutzung eines ORM-Frameworks (Django).				[Automatisierter Test] [Pentest]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R03	Cross-Site-Scripting-Angriff (XSS)	[Hoch]	[Hoch]	[Hoch]	[Reduzieren]
Beschreibung					
Cross-Site-Scripting-Angriffe zielen darauf ab, dass in Eingabefeldern oder Kommentarfeldern schädlicher Java-Script-Code geschrieben werden kann. Bei anderen Usern wird dieser Code dann ausgeführt, sollten sie auf die Seite gehen, auf welchem sich der Code befindet (z.B. Kommentare lesen).					
Anforderungen					
In Eingabefeldern darf kein Code geschrieben werden oder stehen.					
Maßnahmen				Überprüfung	TestID
				[Manueller Test]	

Alle Eingaben müssen geprüft und bereinigt werden, dass sie nur als Text gesehen werde und niemals dazu in der Lage sind Code auszuführen.	[Pentest]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R04	Man-in-the-Middle-Angriff (MitM)	[Hoch]	[Hoch]	[Hoch]	[Reduzieren]
Beschreibung					
Beim MitM-Angriff fängt der Angreifer User-Anfragen ab und kann dessen Daten bzw. Inhalte einsehen und verändern. Diese kann er wiederum zurück an die eigentliche Seite schicken, um es so aussehen zu lassen, als wäre nichts passiert. Außerdem sind die Daten extrem kompomitiert, sollten sie in unverschlüsselter Form vorliegen.					
Anforderungen					
Alle Anfragen müssen grundsätzlich über verschlüsselte Kanäle laufen. Alle Anfragen müssen authentifiziert sein, um zu überprüfen, dass es sich um den richtigen User handelt.					
Maßnahmen				Überprüfung	TestID
Keine Anfragen dürfen unverschlüsselt sein. Hierzu wird HTTPS genutzt und HTTP Anfragen werden abgelehnt. Überprüfung, dass es sich um den richtigen User handelt.				[Automatisierter Test]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R05	Automatisierte Angriffe	[Hoch]	[Mittel]	[Mittel]	[Reduzieren]
Beschreibung					
Automatisierte Angriffe könnte beinhalten, dass Bots Registrierungs oder Anmelde-Formulare ausfüllen und damit das System zumüllen. Da eine Registrierung mit einem initialen Mitarbeiter verbunden ist, können hier erhöhte Kosten anfallen.					
Anforderungen					
Formulare dürfen nicht von Bots ausgefüllt bzw. abgeschickt werden.					
Maßnahmen				Überprüfung	TestID
CAPTCHA-Überprüfung notwendig zum abschicken des Formulares				[Manueller Test]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R06	Cross-Site-Referenz-Forgery	[Hoch]	[Hoch]	[Hoch]	[Reduzieren]

R06	(CSRF)				
Beschreibung					
Beim CSRF-Angriff will der Angreifer den User dazu zu verleiten Aktionen auszuführen, die der User eigentlich gar nicht ausführen möchte.					
Anforderungen					
Es dürfen keine CSRF-Angriffe möglich sein bzw. dürfen sie nur geringe Auswirkungen auf das laufende System haben. Es muss sichergestellt werden, dass Anfragen tatsächlich vom User stammen.					
Maßnahmen				Überprüfung	TestID
Implementierung eines Anti-CSRF-Token: Hierbei handelt es sich um ein eideutiger Token, der in jedes Formular eingebettet wird. Beim Absenden oder Anfragen wird dieses verglichen, dass es gültig ist und mit der korrekten Sitzung verknüpft ist. Nutzung Same-Site-Cookie-Attribut: Attribut, dass für Cookies gesetzte wird (Strict/Lax). Cookie wird eingeschränkt und kann von Angreifern nicht mehr genutzt werden.				[Manueller Test] [Pentest]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R07	Unsicherheit Inlinescripten	[Hoch]	[Hoch]	[Hoch]	[Vermeiden]
Beschreibung					
Inlinescripte sind anfällig für XSS-Angriffe. Sie stellen eine unsicher Codepraktik dar, die zu bösartiger Ausführung von JavaScript führen kann.					
Anforderungen					
Keine Sicherheitsrisiken durch Inlinescripte.					
Maßnahmen				Überprüfung	TestID
Keine Nutzung von Inlinescripten bzw. nur sehr geringe Nutzung.				[Design Review] [Code Review]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R08	Brute-Force-Angriffe	[Sehr hoch]	[Sehr hoch]	[Sehr hoch]	[Reduzieren]
Beschreibung					
Brute-Force-Angriffe beschreiben das wiederholte Ausprobieren von Benutzernamen und/oder Passwörtern, bis die richtige Kombination gefunden wurde, um Zugriff auf das Konto zu erhalten. Dies gilt für User-Kontos.					
Anforderungen					
Brute-Force-Angriffe sollen verhindert oder verringert bzw. erschwert werden.					
Maßnahmen				Überprüfung	TestID
Maximale Anzahl an Login Versuchen auf 5 Versuche. Nach Aufbrauchen dieser wird die Login-Funktion für eine Minute nicht mehr möglich sein.				[Manueller Test] [Automatisierter Test]	[TId]

Alle Auffälligkeiten werden geloggt.		

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R09	URL Traversal	[Hoch]	[Hoch]	[Hoch]	[Vermeiden]
Beschreibung					
Bei einem URL-Traversal-Angriff,versucht ein Angreifer, auf Dateien oder Seiten zuzugreifen, für die er keine Berechtigung hat, indem er die Seitenstruktur einer Website ausnutzt. Dazu gehört auch, dass manipulieren von Parametern.					
Anforderungen					
Es muss sichergestellt werden, dass keine Seiten welche nur mittels Login erreichbar sind und kundenbezogene Daten aufweisen für Angreifer einsehbar sind.					
Maßnahmen				Überprüfung	TestID
Verwendung eines individuellen Authentication-Tokens je User/Usersession.				[Manueller Test] [Automatisierter Test]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R10	Session Hijecking	[Mittel]	[Mittel]	[Mittel]	[Reduzieren]
Beschreibung					
Bei einem Session-Hijacking Angriff übernimmt der Angreifer die Session eines Users. Dies kann durch die Session-ID erfolgen, welche z.B. In Cookies enthalten ist. Mit dieser kann der Angreifer die Konttrolle übernehmen ohne Benutzername oder Passwort zu kennen.					
Anforderungen					
# Die Generieung der Session ID darf nicht deterministisch sein. # Session IDs dürfen nicht unbegrenzt gültig sein, sollte es doch dazu kommen, dass ein Angreifer diese erlangt.					
Maßnahmen				Überprüfung	TestID
# Zur Generieung der Session ID nutzen wir die von Django mitgelieferten Funktionen. # Session ID innerhalb des Cookies sind nur für eine begrenzte Zeit gültig. Nach Ablauf der Gültigkeit wird der Token vom System nicht mehr akzeptiert, somit können keine Aktionen durchgeführt werden.				[Pentest]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R11	Ungewollte Änderungen		[Hoch]		[Reduzieren]

RT1	Ungewollte Änderungen	[Mittel]		[Mittel]	
Beschreibung					
Ein Angreifer erhält Zugriffe/Kontrolle auf ein User-Konto und führt Änderungen an diesem durch.					
Anforderungen					
Ein User muss für bestimmte Handlungen im System gesondert autorisiert werden, um ungewollte Änderungen zu vermeiden.					
Maßnahmen				Überprüfung	TestID
# Erneutes Abfragen des User-Passwortes ist notwendig für Änderungen an z.B. User-Daten, Bankdaten oder Vertragsdaten. # CAPTCHA-Abfrage für Änderungen im Zusammenhang mit dem Abfragen des erneuten Passwortes. # Multi-Faktor-Authentifizierung.				[Manueller Test] [Code Review]	