Erläuterung der CWSS-Bepunktung

1. Datenbank

Base Finding:

Technical Impact (TI): Critical (C)

Acquired Privilege (AP): Partially-Privileged User (P)

Acquired Privilege Layer (AL): System (S)

Internal Control Effectiveness (IC): Limited (L)

Finding Confidence (FC): Proven True (T)

Faktor	Wert	Begründung
TI	C	Der Angreifer erhält zwar keine vollkommene Kontrolle über die Software, jedoch kann er die Nutzung aufgrund des DROPTABLE-Angriffs vollständig verhindern.
AP	P	Die SQL-Injection ermöglicht dem Angreifer Handlungen, welche nicht auf dem Level des Root-Users sind, jedoch mehr Rechte als ein herkömmlicher User der Software. Die erlangten Rechte gleichen denen eines DB-Administrators am besten.
AL	S	Mittels SQL-Injection erhält der Angreifer Möglichkeiten zur Manipulation der Datenbankdatei des Systems.
IC	L	Nur die Validierung der Mailadresse fungiert als simple Methode der Inputvalidierung.
FC	T	Die verwundbare Stelle ist vom Angreifer erreichbar.

Attack Surface:

Required Priviledge (RP): None (N)

Required Priviledge Layer (RL): Network (N)

Access Vector (AV): Private Network (V)

Authentication Strength (AS): None (N)

Level of interaction (IN): Automated (A)

Deployment Scope (SC): All (A)

Faktor	Wert	Begründung
RP	N	Zur Ausführung der Injections sind keine besonderen Recht und kein Account nötig.
RL	N	Der Zugriff zum Netzwerk ist eine Voraussetzung für einen Angriff, da sich der Angreifer sonst nicht mit dem Server verbinden kann, wodurch er keine Eingaben tätigen kann.
AV	V	Der Angreifer benötigt Zugriff auf das (private) Netzwerk, in dem sich der Server befindet, da er sonst keine Verbindung herstellen kann.
AS	N	Da der Angriff vor beziehungsweise während der Authentifizierung stattfindet, muss sich der Angreifer in keiner Weise authentifizieren.
IN	A	Die Ausnutzung der Schwachstelle erfordert keine Informationen von anderen Usern und benötigt somit keine Interaktion mit anderen Menschen.
SC	A	SQL-Injections sind auf jedem OS mit jeder Architektur ausführbar.

Environmental:

Business Impact (BI): High (H)

Likelihood of Discovery (DI): High (H)

Likelihood of Exploit (EX): High (H)

External Control Effectiveness (EC): None (N)

Prevalence (P): Widespread (W)

Faktor	Wert	Begründung
BI	H	Durch die Manipulation und/oder Löschung aller Nutzerdaten würde, je nach Menge, eine signifikanter Schaden für das Unternehmen entstehen, jedoch nicht groß genug, um das Unternehmen komplett zu ruinieren.
DI	H	SQL-Injections sind sehr bekannt und es ist sehr wahrscheinlich, dass selbst weniger erfahrene Angreifer beim Login die Möglichkeit einer Injection überprüfen.
EX	H	Das Anhängen von „‘OR True;--“ ist eine sehr simple und bekannte SQL-Injection, weshalb eine Ausnutzung der Schwäche mit wenigen Versuchen sehr hoch ist.
EC	N	Es liegen keine externen Schutzmechanismen außerhalb der Software gegen diese Schwäche vor.
P	W	SQL-Injections sind bei Applikationen mit Datenbanken schon fast omnipräsent.

2. Passwörter und Aktivierunsgcode

Base Finding:

Technical Impact (TI): High (H)

Acquired Privilege (AP): Regular User (RU)

Acquired Privilege Layer (AL): Application (A)

Internal Control Effectiveness (IC): None (N)

Finding Confidence (FC): Proven True (T)

Faktor	Wert	Begründung
TI	H	Der Angreifer erhält keine Kontrolle über das System selbst, dafür aber sehr kritische Informationen (hier: Zugangsdaten) und somit Kontrolle über andere Accounts.
AP	RU	Durch das brute-forcen der Zugangsdaten erhält der Angreifer die Rechte des kompromittierten Accounts, welche immer den Rechten eines regulären Users entsprechen, da es keinen Account mit gehobenen Berechtigungen gibt.
AL	A	Durch den Angriff erhält der Ausführer Kontrolle über den angegriffenen Account, einen Bestandteil der Applikation
IC	N	Es wurden keine Schutzmechanismen wie Brute-Force-Protection oder Passwortrichtlinien implementiert
FC	T	Die verwundbare Stelle ist vom Angreifer erreichbar.

Attack Surface:

Required Priviledge (RP): None (N)

Required Priviledge Layer (RL): Network (N)

Access Vector (AV): Private Network (V)

Authentication Strength (AS): None (N)

Level of interaction (IN): Automated (A)

Deployment Scope (SC): All (A)

Faktor	Wert	Begründung
RP	N	Zur brute-forcen von Zugangsdaten sind keine besonderen Recht und kein Account nötig.
RL	N	Der Angreifer benötigt Berechtigungen auf Netzwerkebene, um eine Verbindung zum Server aufzubauen.
AV	V	Der Angreifer benötigt Zugriff auf das (private) Netzwerk, in dem sich der Server befindet, da er sonst keine Verbindung herstellen kann.
AS	N	Da sich der Angriff auf die Umgehung des Authentifizierungsverfahrens bezieht, muss sich der Angreifer in keiner Weise authentifizieren.
IN	A	Die Ausnutzung der Schwachstelle erfordert keine Informationen von anderen Usern und benötigt somit keine Interaktion mit anderen Menschen (Social Engineering würde den Prozess vereinfachen, jedoch wird dies hier aufgrund der mangelnden Stärke der Zugangsdaten nicht nötig).
SC	A	Das Anwenden von Brute-Force ist auf jedem OS mit jeder Architektur möglich.

Environmental:

Business Impact (BI):	Medium (M)
Likelihood of Discovery (DI):	High (H)
Likelihood of Exploit (EX):	High (H)
External Control Effectiveness (EC):	Limited (L)
Prevalence (P):	Widespread (W)

Faktor	Wert	Begründung
BI	M	Die Erstellung mehrerer invalider Accounts und der Kompromittierung anderer Account ist, je nach Ausmaß, ein ernstzunehmender Schaden, sollte die Existenz des Unternehmens jedoch in keiner Weise gefährden.
DI	H	Das Entdecken der Schwachstelle ist spätestens beim Betrachten des Aktivierungscode sicher. Zudem sind schwache Passwörter leider weit verbreitet, weshalb ein Angreifer ohne Betrachten der Software diese Schwäche testen wird.
EX	H	Die Wahrscheinlichkeit, dass jemand versucht Zugangsdaten zu brute-forcen ist aufgrund der Einfachheit sehr groß.
EC	L	Durch das Auftreten des RecursionError liegt eine unbeabsichtigte, aber sehr simple Komplikation beim Angriff vor.
P	W	Das Anwenden von Brute-Force ist wahrscheinlich das bekannteste und trivialste Verfahren zum Brechen der Authentifizierung.

3. Verbindung

Base Finding:

Technical Impact (TI): High (H)

Acquired Privilege (AP): Regular User (RU)

Acquired Privilege Layer (AL): Application (A)

Internal Control Effectiveness (IC): None (N)

Finding Confidence (FC): Proven True (T)

Faktor	Wert	Begründung
TI	H	Der Angreifer erhält keine Kontrolle über den Server selbst, erlangt aber durch Abfangen der unverschlüsselten Daten Zugriff auf Zugangsdaten der Nutzer.
AP	RU	Ähnlich wie beim Brute-Force erlangt der Angreifer durch das Wissen über die Zugangsdaten die Rechte des dazugehörigen Accounts, wobei alle Accounts nur normale Nutzerrechte besitzen.
AL	A	Durch den Angriff erhält der Ausführer Kontrolle über den angegriffenen Account, einen Bestandteil der Applikation.
IC	N	Es ist kein Mechanismus zum Schutz der Daten implementiert, weder Verschlüsselung, Integritätskontrolle noch Authentifizierung.
FC	T	Durch die Benutzung von Programmen wie Wireshark ist die Schwäche erreichbar und das Fehlen der Verschlüsselung verifizierbar.

Attack Surface:

Required Priviledge (RP): None (N)

Required Priviledge Layer (RL): Network (N)

Access Vector (AV): Private Network (V)

Authentication Strength (AS): None (N)

Level of interaction (IN): Typical / Limited (T)

Deployment Scope (SC): All (A)

Faktor	Wert	Begründung
RP	N	Der Angreifer agiert bei diesem Angriff nicht mit der Software selbst und benötigt deswegen auch keine Rechte.
RL	N	Um versendete Daten anderer User abfangen zu können benötigt ein Angreifer Zugang zum Netzwerk des Servers.
AV	V	Das Abfangen der Daten geschieht im (privaten) Netzwerk des Servers.
AS	N	Zum Abfangen von Daten muss der Angreifer nicht mit der Software arbeiten und sich somit nicht authentifizieren.
IN	T	Zum Erfolg des Angriffs ist grundsätzlich keine Interaktion mit anderen Menschen nötig, jedoch muss der Angreifer auf die Anmeldung oder Registrierung eines anderen Users warten. Bringt er durch Social Engineering das Opfer dazu, dies zu tun, so kann der Täter die Zeit überspringen.
SC	A	Daten können, unabhängig vom benutzten Betriebssystem oder dessen Architektur, abgefangen werden

Environmental:

Business Impact (BI):	Medium (M)
Likelihood of Discovery (DI):	High (H)
Likelihood of Exploit (EX):	High (H)
External Control Effectiveness (EC):	None (N)
Prevalence (P):	Widespread (W)

Faktor	Wert	Begründung
BI	M	Ähnlich wie bei den Passwörtern ist dieser Faktor abhängig von Ausmaß des Angriffs. Auch wenn der verursachte Schaden groß wäre, so sollte das Unternehmen in keine Existenznot geraten.
DI	H	Das Auffinden der Schwäche ist sehr simpel, da ein kurzer Blick auf das Datenpaket in Wireshark genügt, um diesen Fehler zu erkennen.
EX	H	Die Wahrscheinlichkeit, dass ein Angreifer auf diese Schwäche überprüft, wird als hoch eingeschätzt und da das Auffinden der Schwachstelle schon zum erfolgreichen Ausnutzen genügt ist die Erfolgschance demensprechend ebenfalls sehr hoch.
EC	N	Außerhalb der Software gibt es keine Schutzmechanismen, welche die Sicherheit der Übertragung von Daten erhöhen würden.
P	W	Dieser Fehler ist in unserer Software omnipräsent und tritt auch in anderen Softwareprojekten auf, sofern die Daten nicht stark genug abgesichert wurden.