

Kurs: CY-B-3 Sichere Programmierung

Dozent: Michael Heigl

**Absichern eines terminalbasierten Online-Schachservers (Chess Online)**

Autoren:

Sandro Schamberger (22102471) [33%]

Florian Hagengruber (22101608) [33%]

Christian Joiko (22111097) [33%]

**Inhaltsverzeichnis**

**1. Einleitung**

Die Digitalisierung betrifft momentan fast jeden Bereich unseres Lebens. Sei es nun am Arbeitsplatz, im Auto oder im eigenen zuhause, die Digitalisierung ist mittlerweile omnipräsent. Doch so viele Vorteile der digitale Wandel auch bringt, so wird sie jedoch stets von einem schwerwiegenden Problem begleitet, dass leider noch nicht dieselbe Aufmerksamkeit wie die Digitalisierung erhält wie die Digitalisierung selbst. Bei dieser bösartigen Nebenwirkung handelt es sich um die Cyber Sicherheit oder besser gesagt der Mangel davon. Mit jeder digitalen Neuerung und jedem neuen Gerät bilden wir eine weitere Angriffsfläche, auf der wir von Cyberkriminellen attackiert werden können, weshalb diese Dienste bestmöglich geschützt werden müssen. Viele denken hierbei wahrscheinlich an kritische Infrastruktur wie Krankenhäuser oder Stromversorgung, wobei jedoch alle Aspekte hinreichend abgesichert werden müssen, auch wenn sie noch so unscheinbar sind.

Ein Beispiel hierfür kommt aus dem Bereich der Freizeitgestaltung, die Videospielindustrie. Doch warum ist Informationssicherheit hier so wichtig? Dank der Digitalisierung ist diese Freizeitaktivität mittlerweile weit verbreitet, sodass im Jahr 2021 bereits jeder Zweite in Deutschland ab 16. Jahren gelegentlich Videospiele spielt [1]. Allein 2021 wurden 6,17 Milliarden Euro für Videospielsoftware ausgegeben [2]. Somit entsteht ein sehr großes Risiko für Firmen, da Vorfälle in der IT-Sicherheit einen großen Reputationsschaden mit sich führen können, wodurch der Anteil der Firma an dieser Geldsumme drastisch sinken kann. Doch nicht nur die Anbieter und Produzenten selbst sind von Cyberangriffen betroffen, sondern auch die Konsumenten, welche ihre persönlichen Daten, ihre Zahlungsinformationen und ihr investiertes Vermögen in die Hände der Firmen geben. Werden Nutzerdaten nicht ausreichend geschützt, so könnten diese gestohlen werden und zu Schäden beim Nutzer führen.

Wie dringlich ein solcher Schutz gegen Hackangriffe wirklich ist, wurde den Unternehmen und Nutzern immer wieder aufs Neue verdeutlicht: 2011 gab es einen Angriff auf das Unternehmen Sony [3]. Durch das Eindringen einer unbefugten Person wurde das PlayStation-Network für 23 Tage abgeschaltet [4]. Da PSN-Spieler sich somit nicht mehr mit dem Netzwerk verbinden konnten, verzeichnete das Unternehmen einen Schaden von 171 Millionen US-Dollar [5]. Jedoch nahm nicht nur das Unternehmen Sony Schaden an dem Angriff, auch persönliche Daten der damals 77 Millionen Nutzer, darunter Namen, Anschrift, Geburtsdatum sowie Passwörter und Kreditkarteninformationen wurden entwendet [3].

Doch wie schwer ist es eigentlich, ein Videospiel mit all seinen verknüpften Diensten und Nutzerdaten gegen Cyberkriminelle und Hacker zu schützen? Um diese Frage zu beantworten, wird in diesem Projekt ein Server, mit dem Nutzer gegeneinander Schach spielen können, genauer unter die Lupe genommen. Dabei werden zuerst mögliche Schwachstellen analysiert und aufgrund ihres Gefahrenpotentials für Nutzer und Firma bewertet. Anschließend werden die erkannten Schwachstellen repariert, um eine möglichst sichere Version zu erstellen. Durch den Vergleich der beiden Versionen und die Aufzählung der möglichen Angriffsvektoren wird versucht, diese Frage zu beantworten.

**2. Funktionsweise der schwachen Version**

**2.1 Login und Menü**

Bevor ein Benutzer per „Chess Online“ Schach spielen kann, muss er mit dem Server eine Verbindung aufbauen. Dafür wird das Protokoll „Telnet“ verwendet, womit sich ein Client unter Eingabe der IP-Adresse des Servers und der Portnummer 8080 verbinden kann. Nachdem die Verbindung erfolgreich hergestellt wurde, wird dem Benutzer das Menü angezeigt, wo er aufgefordert wird, sich anzumelden oder sich zu registrieren, falls er noch keinen Account besitzt (siehe Abb. 1).



Abbildung : Benutzer wird im Menü zum Login / zur Registrierung aufgefordert

Für den Fall, dass der Benutzer noch kein Konto besitzt, kann er den Menüpunkt „Registration“ auswählen, um sich eines anzulegen. Für die Registrierung wird zuerst eine gültige Mailadresse eines Studenten oder Mitarbeiters der Technischen Hochschule Deggendorf benötigt. Die eingegebene E-Mail wird zur Kontrolle auf ihren Aufbau hin überprüft, ob sie eine Mailadresse der THD sein kann (siehe Abb. 2). Ist dies der Fall, so wird der Benutzer nach einem Passwort gefragt. Schlussendlich wird dem Nutzer dann mitgeteilt, dass ihm per E-Mail ein Aktivierungscode, bestehend aus vier Ziffern, gesendet wurde (siehe Abb. 3). Die Mailadresse, das Passwort und der Aktivierungscode werden außerdem zusammen mit einem automatisch generierten Nutzernamen in der Tabelle „Spieler“ der Datenbank abgespeichert (siehe Abb. 4).



Abbildung : Registrierung des Accounts und Abweisung einer invaliden Mailadresse

**

Abbildung : Empfang des Aktivierungscodes

**

Abbildung : Design der Datenbank

Sollte der Nutzer bereits ein Konto besitzen, so kann er den Menüpunkt „Login“ benutzen, um sich anzumelden. Dafür wird seine Mailadresse und sein Passwort benötigt. Ist dies seine erste Anmeldung, so wird er zudem noch nach seinem Aktivierungscode gefragt (siehe Abb. 5). Wurde dieser richtig eingegeben, so ist der Benutzer eingeloggt und kann nun die Funktionen des Servers benutzen. Zu diesen zählen das Abrufen der Statistik eines anderen Spielers mittels einer Datenbankabfrage mit dem Befehl **--stats**, dem Ausloggen durch den Menüpunkt „Logout“**,** das Laden oder Starten eines Spiels gegen eine KI, dem Beitreten eines Online-Matches und dem Verlassen der Applikation. Im Zuge dieser Arbeit wird hauptsächlich der Vorgang eines Online-Matches betrachtet, da dieser Aspekt die meisten Risiken birgt.



Abbildung : Anmeldung des Nutzers mit Abfrage des Aktivierungscodes

**2.2 Während eines Online-Matches**

Entschließt sich ein eingeloggter Nutzer, dass er online eine Partie gegen einen anderen Spieler austragen möchte, so betritt er durch Eingabe des dazugehörigen Menüzeichens eine Wartschlange. Betritt ein weiterer Spieler die Warteschlange, so werden die Daten der beiden Kontrahenten in einem Array gespeichert und ein Spiel wird gestartet. Nun können die Nutzer abwechselnd durch die Eingabe einer Zeichenkette, bestehend aus dem Anfangsfeld und dem Zielfeld, ihre Figuren bewegen (e.g. „G1E1“). Neben diesen Aktionen können die Spieler Befehle wie **--stats**, **--surrender** und **--remis** verwenden.

Eine Runde kann aus verschiedenen Gründen enden. Die verschiedenen Möglichkeiten hierfür sind das manuelle Beenden mittels den oben genannten Befehlen **--surrender** und **--remis** (nur wenn sich beide Spieler für ein Remis einigen), das Besiegen des gegnerischen Königs oder das Verlassen der Runde beziehungsweise das Abbrechen der Verbindung. Letzteres führt hierbei zu einer automatischen Niederlage für den Spieler, welcher die Runde verlassen hat.

Am Ende der Runde wird das Ergebnis außerdem in der Datenbank vermerkt. Dazu zählt das Vermerken des Endergebnisses in der Tabelle „Spiele“, sowie das Abändern der Statistiken der Spieler. Dabei wird den beiden Spielern je nach Situation der Wert des Attributs „siege“, „niederlagen“ oder „remis“ um eins erhöht und die ELO-Bewertung wird für beide Spieler neu kalkuliert (siehe Abb. 6) [6].

**

Abbildung : Berechnung der ELO-Änderung

**3. Analyse der Schwachstellen**

Im folgenden Kapitel wird der Code der schwachen Version analysiert und die Funktionen des Programms werden auf mögliche Angriffsmöglichkeiten und Schwächen untersucht. Die Schwächen werden dafür in Gruppen zu ihrer jeweiligen Programmfunktion eingeteilt. Dabei werden, nach einer kurzen Einführung zur Schwachstelle, zuerst die betroffenen Codestellen genannt und der Grund für die Schwachstelle aufgezeigt. Danach wird ein möglicher Angriff mit seinen möglichen Konsequenzen zur Veranschaulichung des Problems vorgestellt. Zuletzt wird die jeweilige Klassifizierung der CVE / CWE? (Dann eher Schwächen schreiben) und eine Bepunktung des Schweregrads angegeben. Die Punkteverteilung beinhaltet die allgemeine Punktzahl nach dem CVSS und eine eigene, ans Programm angepasste, Berechnung des Schweregrads. Zur Berechnung der Punktzahl wird der „Axelsec-Rechner“ verwendet.

**3.1 Datenbank**

Da „Chess Online“ zur Verwaltung der Nutzerdaten, der Spielehistorie und der Speicherstände eine Datenbank verwendet, sollte jedem Programmierer sofort die Gefahr einer SQL-Injection in den Sinn kommen. Die SQL-Injection ist nicht ohne Grund sowohl im Jahr 2020 als auch im Jahr 2022 auf Platz 3 der „CWE Top 25 Most Dangerous Software Weaknesses“ [7]. Die Möglichkeit einer SQL-Injection kann somit katastrophale Folgen haben, wie nachfolgend aufgezeigt wird.

Bei unserem Projekt werden die meisten Datenbankbefehle unabhängig von Eingaben des Nutzers ausgeführt. Jedoch werden für manche Abfragen Nutzereingaben zwingend benötigt, genauer gesagt bei den Datenbankabfragen, welche während der Anmeldung und der Registrierung benötigt werden. Die Ursache für die SQL-Injection ist eine Kombination aus dem Verwenden von schwachen Softwarekonstruktionen, obwohl sicherere vorhanden wären und dem Fehlen der Input Validation. Ersteres bezieht sich hierbei auf die Verwendung der Funktion **executescript()** und dem **%s-Platzhalter**. Des Weiteren wird die Datenbank unverschlüsselt und ohne Schutzvorrichtungen am Server abgelegt, was ebenfalls zu Problemen führen kann, wenn ein Angreifer Zugriff auf den Server erlangt.

Sollte ein Angreifer die Datenbank per SQL-Injection angreifen wollen, so muss er lediglich die richtige Anzahl der Parameter für das SQL-Statement herausfinden, sodass dieses ausgeführt wird und nicht vor der Ausführung abbricht. Da dafür jedoch ein wenig Trial-and-Error genügt, kann der Angreifer schnell, einfach und, im Falle der Registrierung, ohne Account und funktionierende Mailadresse per SQL-Injection die Datenbank in vollem Umfang nach seinen Wünschen manipulieren oder sich bei anderen Accounts ohne Passwort anmelden. Einzig die Validierung der Mailadresse erschwert dem Angreifer das Herausfinden einer korrekten Eingabe, da seine Injection die Überprüfung des Domänenteils überstehen muss und dann bereits beim Überprüfen, ob diese Mailadresse bereits registriert ist, ausgeführt werden muss. Jedoch ist dies nicht allzu schwer und kann durch Umsteigen auf die anderen drei Eingabefelder sogar vollständig umgangen werden. Nachfolgend wird eine mögliche Eingabe für beide Vorgänge mit ihren Folgen für die Anwendung aufgezeigt, wobei ein Stern (\*) für eine beliebige Texteingabe steht:

|  |  |  |
| --- | --- | --- |
| **Registrierung** | | |
| Feld | Eingabe | Konsequenzen |
| E-Mail | \*@th-deg.de | Löscht die Tabelle Spieler mit allen Accountdaten |
| Passwort | \*‘, ‘\*‘, ‘\*‘); DROP TABLE Spieler;-- |
| E-Mail | \*' OR 1 = 1; UPDATE Spieler SET siege = 1000 WHERE nutzername = 'c.joiko';--@th-deg.de | Setzt die Anzahl der Siege des Spielers mit dem Nutzernamen „c.joiko“ auf 1000 |
| Passwort | *Eingabe egal* |
|  | | |
| **Anmeldung** | | |
| Feld | Eingabe | Konsequenzen |
| E-Mail | *Eingabe egal* | Einloggen mit ersten registrierten Account |
| Passwort | \* ‘ OR True;-- |

[Punkte!!! CVSS oder CWSS???]

**3.2 Passwort und Aktivierungscode**

Das Passwort ist wahrscheinlich eines der ältesten und am weitest verbreiteten Authentifizierungsverfahren. Sie sind einfach als Schutz zu implementieren und können trotz ihrer Simplizität dennoch großen Schutz bitten, vorausgesetzt sie werden auch richtig verwendet. Noch immer verwenden fast 50% der Deutschen meistens Passwörter mit einer Länge von maximal 10 Zeichen [8]. In Kombination mit zu einfach gewählten Passwörtern wie „hallo123“ oder dem Notieren an unsicheren Orten verlieren sie relativ schnell jegliche Bedeutung beim Schutz der eigenen Daten, was nachfolgend auch bei „Chess Online“ aufgezeigt wird.

Das erste Problem entsteht bereits bei der Erstellung des Passwortes bei der Registrierung eines neuen Accounts. Das Passwort wird bei der Eingabe am Terminal angezeigt und kann somit bereits durch einen Blick auf den Bildschirm erlangt werden. Zudem wird der Nutzer nicht um eine Bestätigung des Passwortes gebeten, was in Kombination mit der fehlenden Möglichkeit zum Ändern des Passwortes bei einem Tippfehler schnell zu einem Problem führt. Doch die eingeschränkte Effektivität der Passwörter ist nicht nur Schuld des Benutzers, sondern auch des Entwicklers. Die Passwörter werden kein einziges Mal verschlüsselt und liegen permanent als Plaintext vor. Zudem wurde von Programmierern ein Passwort für einen Account im Quelltext der Datei mail.py vergessen (siehe Abb. 7).

**

Abbildung : Hard-coded Credentials in mail.py

Neben den Passwörtern weisen auch die Aktivierungscodes zum Freischalten eines neuen Accounts einen verheerenden Mangel auf. Die 4-stelligen Codes sind sehr einfach per Brute-Force-Attacke zu knacken, was aufgrund der fehlenden Limitierung der Eingabeversuche zu einem kompletten Verlust der Authentifizierungsfunktion des Aktivierungscodes führt.

Wie bereits erwähnt kann der Aktivierungscode in der schwachen Version mit geringem Ressourcen- und Zeitaufwand durch Brute-Forcing herausgefunden werden. Dies ermöglicht einem Angreifer eine beliebige Anzahl an Accounts anzulegen, da die Prüfung der Echtheit einer E-Mail durch den Aktivierungscode verifiziert wird.

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungUm eine solche Brute-Force-Attacke durchzuführen, muss der Angreifer eine Anwendung schreiben, die eine automatische TCP-Verbindung zum Server aufbaut, sich anschließend versucht anzumelden und die Zahlen 1000 bis 9999 für den Aktivierungscode einsetzt. Hierbei ist zu beachten, dass bei einem fehlerhaften Aktivierungscode das Menü in der Funktion **get\_menu\_choice(…)** durch **self.get\_menu\_choice(self.view.get\_menu\_choice())** rekursiv aufgerufen wird (siehe Abb. 8).

Abbildung : Rekursiver Aufruf in controller.py

Wenn mehr als 490 Rekursionen, in unserem Fall Aktivierungscode, durchgeführt werden stoppt der Server die Verbindung mit dem Client durch einen **RecursionError**. Dies muss der Angreifer abfangen und eine erneute Verbindung aufbauen, was Performanceeinbrüche nach sich zieht (siehe Anhang).

Durch das unkontrollierte Erstellen von Accounts kann z. B. versucht werden, die Performance der Datenbank und dadurch das Schutzziel Verfügbarkeit durch ständige Registrierungen zu beinträchtigen. Auch erhöht sich die Gefahr einer DOS bzw. einer DDOS-Attacke, da der Angreifer z. B. mit einer großen Anzahl an Accounts gegen die KI spielen könnte. Hierbei ist der Rechenaufwand zu betrachten, der durch das Spielen mit der KI benötigt wird, da durch genügend Spieler der Server ausgelastet werden könnte und somit das Schutzziel Verfügbarkeit bedroht wird. Ein solcher Denial-of-Service-Angriff ist ähnlich wie die Brute-Force-Attacke aufgebaut: der Angreifer muss automatisiert so viele TCP-Verbindungen wie möglich zum Server aufbauen und diesen somit überlasten, was im nachfolgenden Angriff mittels Threads realisiert worden ist. Um die Effektivität des Angriffes zu steigern, spielt jeder Thread gegen die KI in einer Endlosschleife, was die Rechenlast des Servers zusätzlich steigern soll (siehe Abb. 9). Die Effizienz des Angriffes ist anhand der Zeit in Sekunden gemessen, die ein Spieler benötigt, um sich am Server anzumelden und die KI den ersten Zug macht, welche nachfolgend als Zug-dauer bezeichnet wird. Anhand Abbildung 10 kann man erkennen, dass schon 49 erzeugte Spieler die Zug-dauer von ca. 5 Sekunden auf 120 Sekunden bringen und die CPU dauerhaft auslasten. Da im Laufe des Spieles die Anwendung immer mehr Züge zu berechnen hat, steigt die Antwortzeit der KI in der Mitte des Spieles bei nur einem Nutzer schon auf ca. 5 Minuten. Bei 49 aktiven Spielern ist daher eine Antwortzeit von mehreren duzenden Minuten bis zu Stunden nicht auszuschließen.

Auch ist eine Statistik von 100 Spielern erhoben worden (siehe Abb. 11). Hierbei ist zu beachten, dass die Zug-dauer bei fast 600 Sekunden liegt, was das Spielen gegen die KI enorm beeinträchtigt.

Ein geplanter Absturz des Servers ist dennoch nicht erzielt worden, jedoch stört die DOS-Attacke den Spielfluss außerordentlich und somit wird die Verfügbarkeit ebenso beeinträchtigt.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Codeabschnitt eines Threads, der gegen die KI spielet

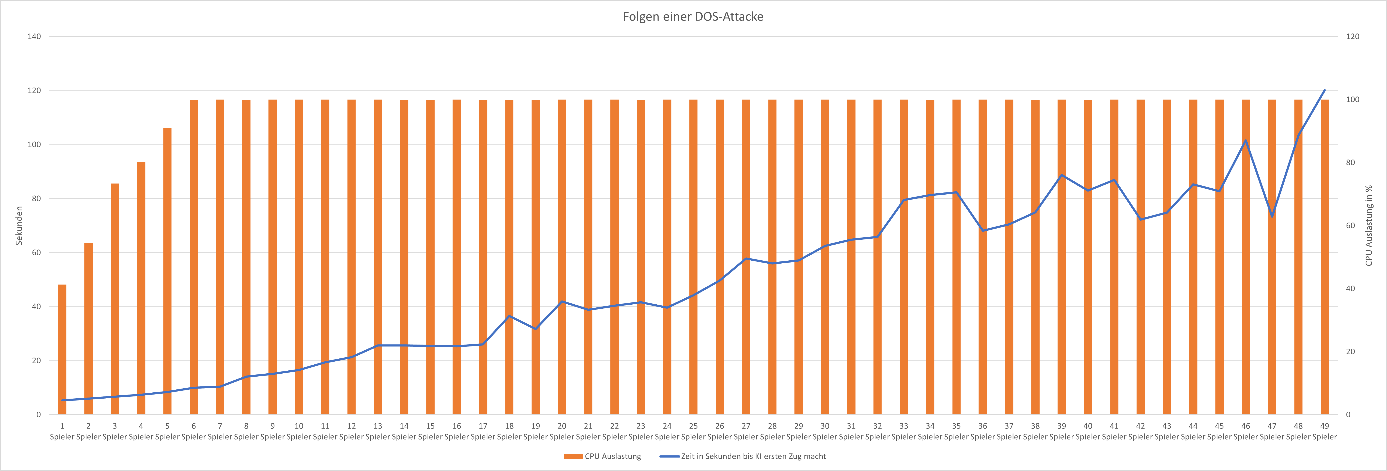


Abbildung : Statistik über die Folgen der DOS-Attacke

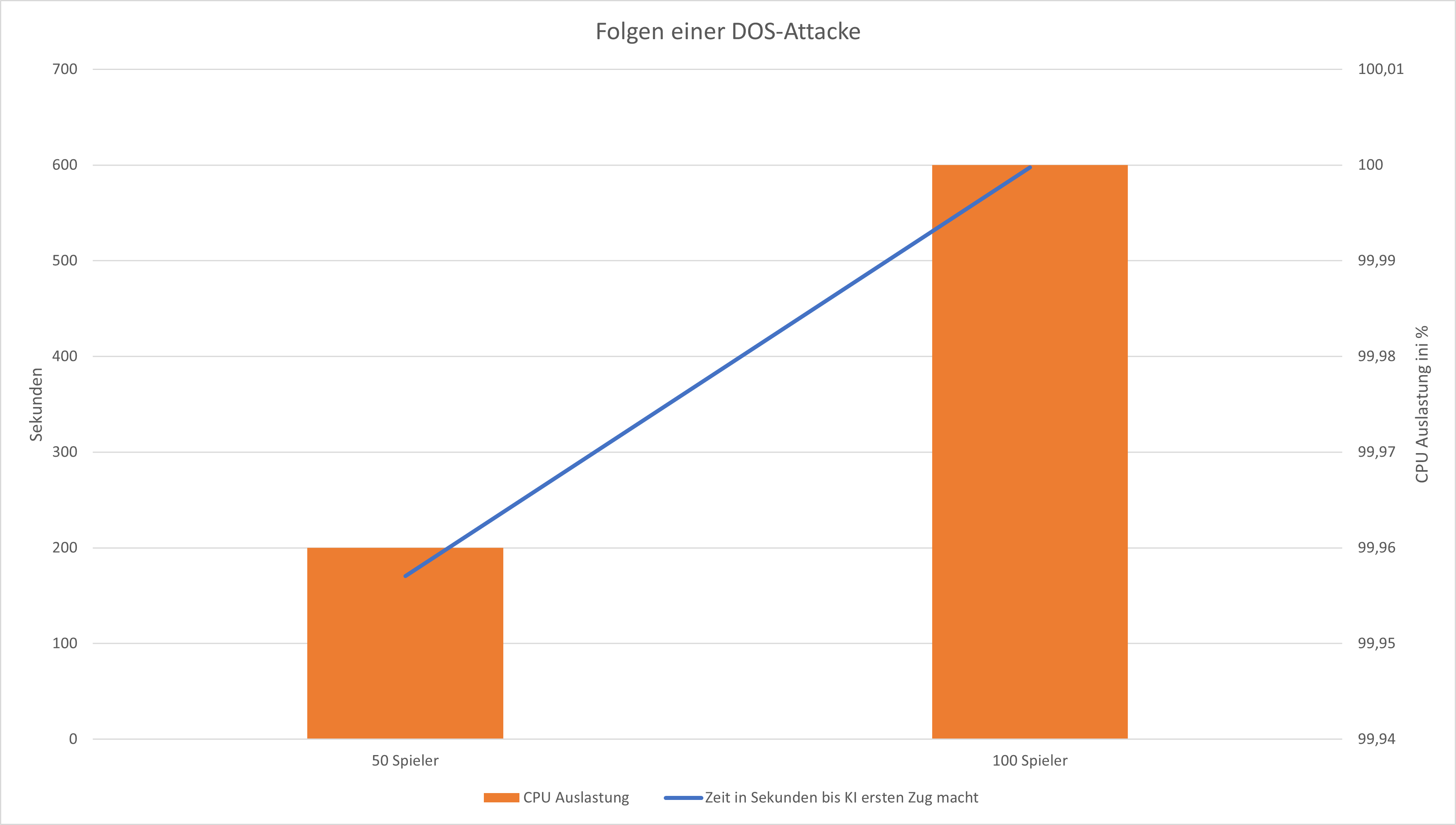


Abbildung : Statistik über die Folgen der DOS-Attacke in 50er Schritten

[CWSS Score Sonntag]

**4. Beheben der Schwächen**

**4.1 Datenbank**

Um die in 3.1 angesprochene SQL-Injection zu beheben, sollten zuerst die verwendeten unsicheren Softwarekonstruktionen durch sichere Alternativen ersetzt werden. Die erste Änderung ist das Ersetzen der Funktion **executescript ()** durch **execute()**. Der Unterschied zwischen diesen beiden Funktionen ist, dass **execute()** nur einen SQL-Befehl ausführen kann, während **executescript()** mehrere Statements verarbeitet [9]. Da unsere Funktionen zur Manipulation der Datenbank sowieso immer nur ein Statement ausführen müssen, ist dies ein sehr einfacher Schutz vor angehängten, unerwünschten SQL-Statements des Angreifers. Nach Anwendung des Fixes sind die beiden Injections, welche zuvor während der Registrierung möglich waren, nicht mehr möglich (siehe Abb. 7).



Abbildung : Fehlermeldung nach Ausführung der ersten SQL-Injection

Leider schützt diese Verbesserung noch nicht vor dem Login ohne Passwort, weshalb eine weitere Verbesserung vorgenommen werden muss. Diese Verbesserung betrifft die Platzhalter in den SQL-Statements, welche später durch die Eingaben des Nutzers ersetzt werden. Die schwache Version verwendet momentan **%s-Platzhalter**, welche laut der Dokumentation des sqlite3-Moduls in Python unsicher und anfällig für SQL-Injections sind. Als Verbesserung wird hierfür die Verwendung der moduleigenen **?-Platzhalter** vorgeschlagen, welche nach Einbindung die dritte SQL-Injection verhindern sollten [9]. Da dies jedoch nicht der Fall ist, wird zusätzlich der Input des Users auf maliziöse Absichten überprüft, bevor er verarbeitet wird. Um dies zu erreichen, wird einfach ein Array mit verbotenen Zeichen eingefügt und über dieses iteriert, ob in der eingegebenen Mailadresse oder dem Passwort ein verbotenes Zeichen vorhanden ist. Um die SQL-Injection zu verhindern, ohne den zulässigen Zeichensatz für Passwörter unnötig einzuschränken wird sich im Projekt auf vier Sonderzeichen beschränkt (siehe Abb. 8).

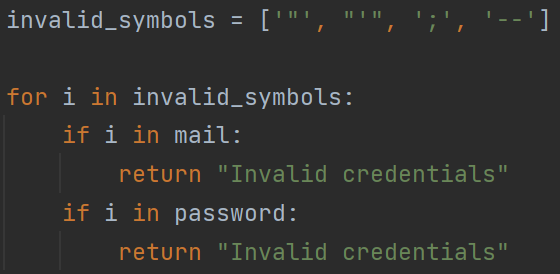


Abbildung : Einbindung der Überprüfung auf invalide Zeichen

Gegen die ungesicherte und unverschlüsselte Ablage der Datenbank sollte ebenfalls vorgegangen werden. Dazu könnte beispielsweise **SQLCipher** verwendet werden [10]. Zur weiteren Absicherung der Datenbank sollte ein regelmäßiges Backup der Datenbank gemacht werden, damit im Falle der ersten beiden SQL-Injections der Schaden zumindest wieder behebbar wäre und die Integrität nicht vollständig verloren geht. Diese beiden Fixes wurden jedoch aus Zeitgründen und der höheren Relevanz und Gefährlichkeit der SQL-Injection nicht ins Programm eingebaut.

**Literaturverzeichnis**

[1] Bitkom (2022): „Anteil der Computer- und Videospieler in Deutschland in den Jahren 2013 bis 2022“ auf Statista;

Zugriff: 13. Dezember 2022; https://de.statista.com/statistik/daten/studie/315860/umfrage/anteil-der-computerspieler-in-deutschland/

[2] game.de (2022): „Umsatz im Markt für Computer- und Videospiele (ohne Hardware) in Deutschland von 2009 bis 2021 (in Millionen Euro)“ auf Statista; Zugriff: 13. Dezember 2022; https://de.statista.com/statistik/daten/studie/317808/umfrage/umsatz-im-markt-fuer-computer-und-videospiele-in-deutschland/

[3] heise.de (2011): „Welcome Back PSN: The Winners“; Zugriff: 14. Dezember 2022; https://kotaku.com/welcome-back-psn-the-winners-5804318

[4] kotaku.com (2011): „Angriff auf Playstation Network: Persönliche Daten von Millionen Kunden gestohlen“; Zugriff: 14. Dezember 2022; https://www.heise.de/newsticker/meldung/Angriff-auf-Playstation-Network-Persoenliche-Daten-von-Millionen-Kunden-gestohlen-1233136.html

[5] pcmag.com (2011): „PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher“; Zugriff: 14. Dezember 2022; https://www.pcmag.com/archive/playstation-hack-to-cost-sony-171m-quake-costs-far-higher-264796

[6] Wikipedia: “ELO-Zahl: Anpassung nach einer Partie“; Zugriff: 13. Dezember 2022; https://de.wikipedia.org/wiki/Elo-Zahl#Anpassung\_nach\_einer\_Partie

[7] The MITRE Corporation (2022): „2022 CWE Top 25 Most Dangerous Software Weaknesses”; Zugriff: 13. Dezember 2022; https://cwe.mitre.org/top25/archive/2022/2022\_cwe\_top25.html

[8] Web.de (2022): „Wie lang sind Ihre am häufigsten verwendeten Passwörter?“ auf Statista; Zugriff: 13. Dezember 2022; https://de.statista.com/statistik/daten/studie/988439/umfrage/laenge-von-passwoertern-in-deutschland/

[9] “sqlite3”-Dokumentation (Python Software Foundation): https://docs.python.org/3/library/sqlite3.html

[10] About SQLCipher (Zetetic): https://www.zetetic.net/sqlcipher/about/