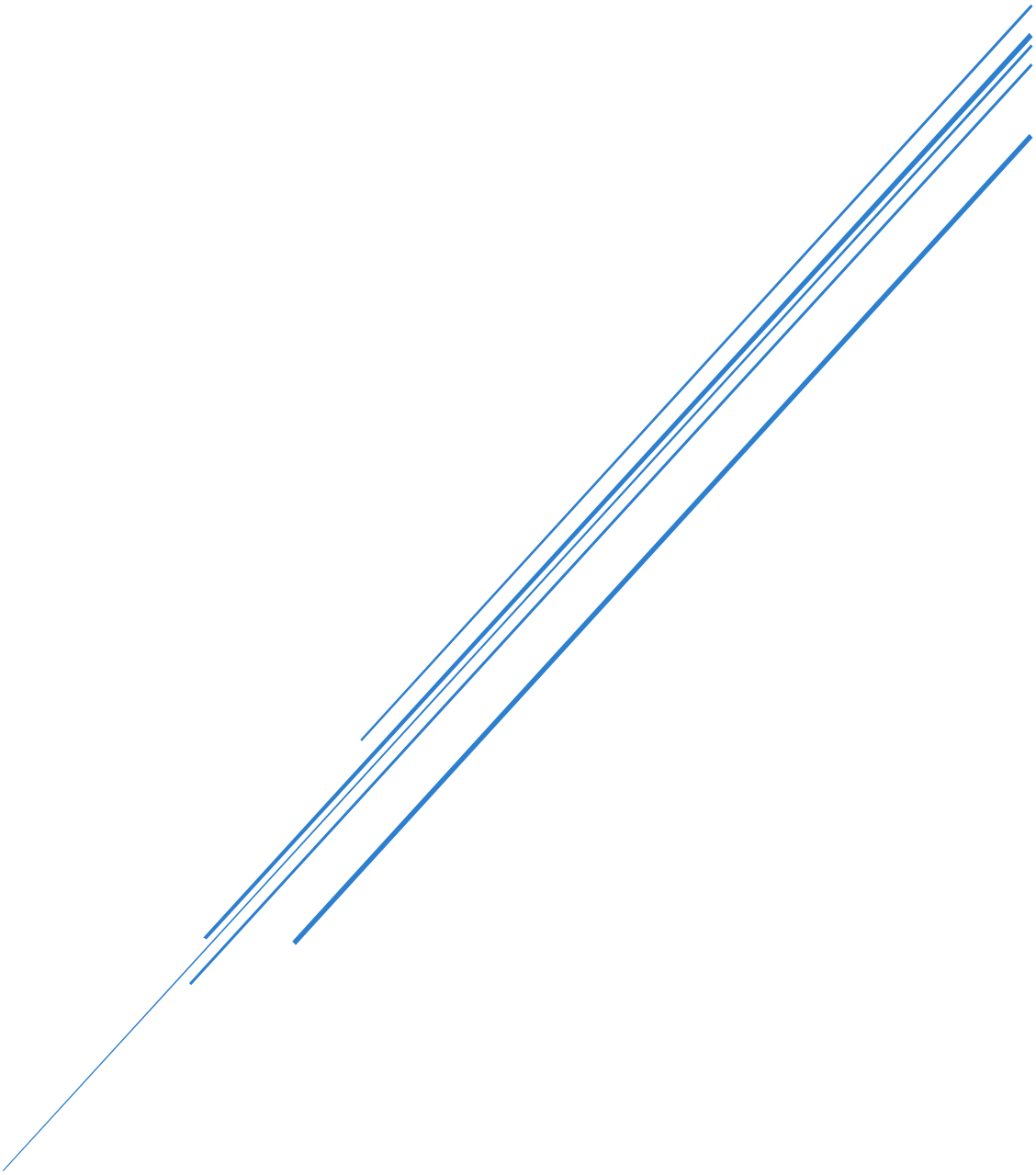
SICHERHEITSFEATURES DES BASEL COIN SYSTEMS



IBZ
Davud, Anthony, Sebastian & Nesim

Inhalt

1. Schutz gegen Injection

Der Basel Coin schützt sich gegen Injection-Angriffe durch die strikte Validierung aller Eingaben, die vom Benutzer kommen. Dies schließt sowohl SQL-Injection als auch Script-Injection ein. Eingaben werden gegen ein erlaubtes Muster geprüft, und nur alphanumerische Zeichen sind für Benutzernamen und Passwörter zulässig.

Code-Beispiel für die Validierung

```
if (/[^a-zA-Z0-9]/.test(username) || /[^a-zA-Z0-9]/.test(password)) {
    alert('Ungültige Eingabe.');
    return;
}
```

2. Session Management mit Idle/Absolut Timeout

Das System implementiert ein robustes Session-Management, das sowohl Idle-Timeouts als auch absolute Timeouts umfasst. Dies stellt sicher, dass Benutzersitzungen nach einer bestimmten Zeit der Inaktivität automatisch ablaufen und Benutzer nach einer maximalen Sitzungsdauer gezwungen sind, sich erneut anzumelden.

Code-Beispiel für Session-Management

```
const inactivityTimeout = 1 * 60 * 1000;
let inactivityTimer;

2 references
function startInactivityTimer() {
    inactivityTimer = setTimeout(() => {
        logEvent('INACTIVITY_TIMEOUT', currentUsername, 'Inaktivität - automatischer Logout');
        logout();
    }, inactivityTimeout);
}

2 references
function resetInactivityTimer() {
    clearTimeout(inactivityTimer);
    startInactivityTimer();
}

document.addEventListener('mousemove', () => resetInactivityTimer());
document.addEventListener('keypress', () => resetInactivityTimer());

1 reference
function logout() {
    logEvent('LOGOUT', currentUsername, 'Benutzer abgemeldet');
    clearTimeout(inactivityTimer);
    document.getElementById('loginContainer').style.display = 'block';
    document.getElementById('balanceContainer').style.display = 'none';
}

const authenticatedUsername = 'tatsächlicherBenutzername';
startSession(authenticatedUsername);
startInactivityTimer();
```

3. Applikationslog mit Datum/Uhrzeit, Eventtyp, Benutzer, Aktion

Jede Benutzeraktion innerhalb des Systems wird in einem Applikationslog festgehalten. Dieses Log enthält wichtige Informationen wie Datum und Uhrzeit des Ereignisses, den Typ des Events, den beteiligten Benutzer sowie die durchgeführte Aktion. Diese Logs spielen eine entscheidende Rolle bei der Überwachung und Analyse der Sicherheit des Systems.

Code-Beispiel für das Applikationslog

```
2 references
function logEvent(eventType, username, action) {
    const timestamp = new Date().toLocaleString();
    const logMessage = `${timestamp} - ${eventType} - Benutzer: ${username} - Aktion: ${action}`;
    logMessages.push(logMessage);
    console.log(logMessage);
}
```

4. Input Validierung aller Felder

Alle Eingabefelder im Basel Coin System, einschließlich Login und Passwort, unterliegen einer strengen Validierung. Dies verhindert die Eingabe schädlicher Daten, die das System kompromittieren könnten. Die Validierung umfasst die Überprüfung auf Länge, Format und Zeichensatz der Eingabe.

Code-Beispiel für die Input-Validierung

```
function validateInput(input) {
    const isAlphanumeric = /^[a-zA-Z0-9]+$/.test(input);
    const isValidLength = input.length >= 4 && input.length <= 20;
    return isAlphanumeric && isValidLength;
}
```