

**Den här koden innehåller minst fem sårbarheter ifrån olika kategorier i OWASP Top 10 2021-listan.**

**Vilka kan du identifiera?**

* A1: Broken Access Control
* A2: Cryptographic Failure
* A3: Injection
* A4: Insecure Design
* A5: Security Misconfiguration
* A6: Vulnerable and Outdated components
* A7: Identification and Authentication Failures
* A8 Software and Data Integrity Failures
* A9 Security Logging and Monitoring Failures
* A10 Server-Side Request Forgery

**Facit**

A1: Broken Access Control  
Funktionen **view\_admin\_data** saknar någon form av av autentisering vilket möjliggör att vem som helst kommer åt admin data.

A3: Injection

Sökningen i **ldap\_authenticate** använder osanitiserad indata, vilket gör det möjligt för en angripare att manipulera sökningen.

A5: Security Misconfiguration / A7: Identification and Authentication Failures

JWT-token i **generate\_token** använder en hårdkodad hemlighet (ABCDEF) direkt i källkoden, vilket innebär att en som får tillgång till koden kan skapa egna giltiga tokens. JWT token saknar även en giltighetstid

A10: Server-Side Request Forgery

**fetch\_data()** tillåter användaren att ange en valfri URL utan begränsningar, vilket gör det möjligt för en angripare att skicka förfrågningar till interna system och nätverk som normalt inte är åtkomliga.