|  |  |  |
| --- | --- | --- |
| **Funktion** | **OWASP** | **CWE** |
| def view\_admin\_data(): | A01: Broken Access Control | 200, 285 |

Svar: Funktionen saknar någon form av autentisering

|  |  |  |
| --- | --- | --- |
| **Funktion** | **OWASP** | **CWE** |
| def ldap\_authentication(): | A03: Injection | 20, 90 |

Svar: Funktionen är sårbar för kodinjektion eftersom inmatade data körs direkt utan validering eller filtrering.

|  |  |  |
| --- | --- | --- |
| **Funktion** | **OWASP** | **CWE** |
| def generate\_token(): | A02: Cryptographic failure | 312, 613, 798 |

Svar: Koden innehåller en hemlig nyckel i klartext för att generera JSON web token som dessutom saknar en giltighetstid.  
  
HMAC-SHA256 (HS256) är i viss kontext en sårbarhet då en och samma nyckel används för kryptering och dekryptering men ger en bättre prestanda.

|  |  |  |
| --- | --- | --- |
| **Funktion** | **OWASP** | **CWE** |
| def fetch\_data(): | A10: Server-Side Request Forgery | 610, 918 |

Svar: Funktionen är sårbar eftersom en angripare kan ange valfri adress utan validering eller begränsningar. En HTTP GET förfrågan kommer skickas från server till den angivna adressen, vilket möjliggör att angriparen kan komma åt resurser som annars inte skulle vara tillgängligt.

A05: Security Misconfiguration & A04: Insecure Design  
Båda är övergripande sårbarhetskategorier