Investigate the key steps in managing security incidents and how to apply them.

**Incident Response Plan – Just Pick**

**Incident categories:** OAuth2 exploitation, Data exposure, API abuse, LLM model misuse

**Session hijacking - Incident Response Steps**

1. Preparation – SESSION\_COOKIE\_HTTPONLY = True prevent from accessing session cookies if an XSS attack occurs, cookies are only transmitted over HTTPS (Kloda, 2025)
2. Identification – monitor suspicious session tokens and XSS payloads
3. Containment – restrict login until the cause is patched
4. Eradication – identify and patch XSS vulnerabilities
5. Recovery – require affected user to reauthenticate
6. Lessons learned – investigate cause of the session hijacking, improve protection, re-evaluate session timeout

**Data breach - Incident Response Steps**

1. Preparation – use strong hashing algorithm, use unique salts (Kloda, 2025)
2. Identification – detection unauthorized access, data leakage
3. Containment – restrict access to account, implement firewall rules to block harmful traffic
4. Eradication – identify and patch vulnerabilities
5. Recovery – restore data from backups
6. Lessons learned – investigate cause of the breach and improve data protection

**Example of Incident response team**

Member 1 - Coordinates the incident response effort, identifies attack

Member 2 – manages database recovery and handles firewall changes

# References

Kloda (2025). [online] github. Available at: https://github.com/Jkloda/movie\_recommendation\_system/blob/main/server/app.py [Accessed 22 Apr. 2025].

Kloda (2025). [online] github. Available at: https://github.com/Jkloda/LOJuliaKloda/blob/main/Assets/DB\_hashing.png [Accessed 2 May 2025].