A1 - Injection

SQL-injectie vormt een groot risico voor de beveiliging van je database. Het ontstaat vaak door het onveilig combineren van strings in SQL-query's, waardoor aanvallers eigen code kunnen invoeren. Dit kan leiden tot datalekken, ongeautoriseerde toegang of gegevensverlies.

Oplossing:

Gebruik Prepared Statements om invoer veilig te verwerken en SQL-injecties te voorkomen.

Voorbeeld van veilige query:

$stmt = $sql->prepare("SELECT \* FROM users WHERE username = ?");

$stmt->bind\_param("s", $username);

$stmt->execute();

$res = $stmt->get\_result();

-

A2 - Broken Authentication

Onveilige authenticatie maakt accounts kwetsbaar voor aanvallen zoals session hijacking. Dit gebeurt wanneer beschermende maatregelen zoals sessiebeveiliging ontbreken.

Oplossingen:

1. Cryptografische session tokens: voor tijdelijke sessies.

2. IP-filtering: beperkt sessies tot het inlog-IP.

3. Tweefactorauthenticatie: vereist extra verificatie bij inloggen.

-

A3 - Sensitive Data Exposure & A7 - Cross-Site Scripting (XSS)

XSS-aanvallen ontstaan wanneer gebruikersinput niet goed gesanitized wordt, waardoor aanvallers eigen HTML of JavaScript kunnen toevoegen. Dit gebeurt vaak bij platforms met gebruikersgegenereerde content. Gebruik frameworks die invoer automatisch ontsmetten.

Veilig gebruik van invoer:

$sanitized = htmlspecialchars($content);

echo "<div class='user-comment'>$sanitized</div>";

-

A5 + A6- Broken Access Control - Security Misconfiguration

Goede configuratie van je server voorkomt ongeautoriseerde toegang. Zorg voor veilige instellingen, zoals het uitschakelen van directory listing en foutmeldingen in productie. Beveilig gevoelige bestanden met toegangsrechten.

9 - Veilig werken met externe libraries

Houd libraries up-to-date en verwijder niet-gebruikte libraries om risico's te beperken. Kies actief onderhouden libraries van betrouwbare bronnen om kwetsbaarheden te voorkomen.

10 - Audit Loggen

Log verdachte activiteiten zoals mislukte inlogpogingen en systeemfouten om snel te reageren op aanvallen. Sla logs veilig op in een logbestand of logdatabase, en pas SQL-injectie- en XSS-maatregelen toe om logging zelf veilig te houden.