Julie Kraanen

OITSDO2A

1. Meerdere lagen beveiliging
2. XSS is als iemand als een user slechte code stuurt naar de server, je can htmlspecialcharts en ENT\_QUOTES gebruiken
3. CSRF zorgt ervoor dat een ingelogde gebruiker kwaadaardige verzoeken indient door op bijvoorbeeld links te drukken zonder dat de gebruiker dat realiseerd, Je voorkomt het door token based authenticatie te gebruiken zoals dit:

if (empty($\_SESSION['token'])) {

    $\_SESSION['token'] = bin2hex(random\_bytes(32));

}

$token = $\_SESSION['token'];

1. Iemand die een website aanvalt door kwaadaardige SQL query’s in te vullen via input velden en daardoor de database te veranderen of informatie te stelen. Je kan het voorkomen door het voor te berijden. Zoals dit:

$stmt = $pdo->prepare("SELECT \* FROM gebruikers WHERE username = :username");

    $stmt->bindParam(":username", $username);

    $stmt->execute();

1. Broken access control is als een gebruiker bijvoorbeeld admin toegang heeft maar dat niet de bedoeling is.
2. Authenticatie is kijken of de identiteit van de gebruiker klopt, Autorisatie is aangeven hoeveel rechten een geauthenticeerde gebruiker heeft en kan doen.
3. Broken Access Control, Cryptographic Failures, Injection
4. De code is niet beschermd teken SQL Injection omdat de input gegevens nergens wordt voorbereid, en de code is niet beschermd tegen XSS omdat nergens in de code htmlspecialcharts word gebruikt om te zorgen dat er geen kwaadaardige code wordt gestuurd. En het is moelijk te zien of de token overeenkomt met de gebruiker die iets uitvoert.
5. D
6. A
7. D
8. C