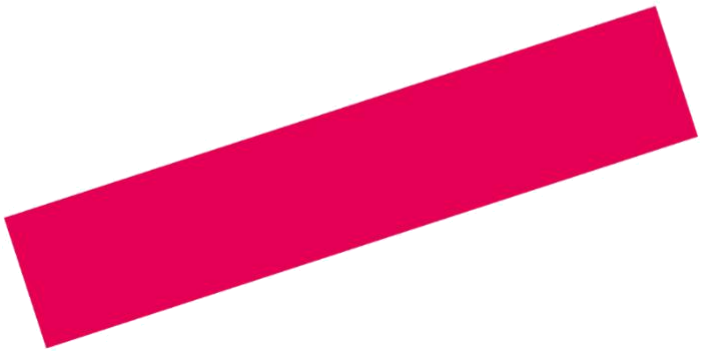
HAN_UNIVERSITY OF APPLIED SCIENCES

WTIS OWASP



Marijn Hazeveld
INT-CNP-A-S
WTIS
Fritz van Deventer
22-01-2025

OWASP 1

Risico	**BROKEN ACCESS CONTROL**
Aanvalstechniek	Omzeilen van rechten controles, Jezelf meet rechten geven
Kans	Hoog: staat op nummer 1 van de OWASP top 10 (OWASP Foundation, z.d.)
Gevolg	Ongeoorloofde toegang tot gegevens die niet bedoeld zijn voor de aanvaller

OWASP 1 is secure omdat ik rekening houd met rechten en niet iedereen overal access tot geef.
Hiernaast zijn de onderdelen die Alleen voor medewerkers zijn deny by default

```
<?php if (!empty($RESULT)) : ?>
    <?php foreach ($RESULT as $row) : ?>
        <tr>
            <td><?php echo $row['order_id']; ?></td>
            <td><?php echo $row['client_username']; ?></td>
            <td><?php echo $row['client_name']; ?></td>
            <td><?php echo $row['datetime']; ?></td>
            <td><?php echo $row['address']; ?></td>
            <td><span><?php echo $statusMapping[$row['status']]; ?></span></td>
            <td>
                <?php if(isMedewerker()){ ?>
                    <form method="post" action="Order.php">
                        <input type="hidden" name="order_id" value="<?php echo $row['order_id']; ?>">
                        <select name="status">
                            <option value="1" <?php if ($row['status'] == 1) echo 'selected'; ?>>Pending</option>
                            <option value="2" <?php if ($row['status'] == 2) echo 'selected'; ?>>Processing</option>
                            <option value="3" <?php if ($row['status'] == 3) echo 'selected'; ?>>Completed</option>
                            <option value="4" <?php if ($row['status'] == 4) echo 'selected'; ?>>Cancelled</option>
                        </select>
                        <button type="submit">Update</button>
                    </form>
                <?php } ?>
```

OWASP 2 CRYPTOGRAPHIC FAILURES

Risico	**CRYPTOGRAPHIC FAILURES**
Aanvalstechniek	Data aflezen omdat deze niet versleutelt zijn
Kans	Hoog: staat op nummer 2 van de OWASP top 10 (OWASP Foundation, z.d.)
Gevolg	Hacker kan data inzien die niemand zou mogen zien (bijvoorbeeld wachtworden)

Ik versleutel wachtwoorden wanneer er een nieuw account wordt gemaakt dus ik hoef mij geen zorgen te maken dat iemand deze kan in zien als er is ingebroken in het systeem

```php
$username = $_POST["username2"];
$password = password_hash($_POST["password2"], algo: PASSWORD_DEFAULT);
$voornaam = $_POST["voornaam"];
$achternaam = $_POST["achternaam"];
$adres = $_POST["adres"];


$sql = "SELECT * FROM [User] WHERE username = :username";
$stmt = $connect->prepare($sql);
$stmt->bindParam( param: ':username', &var: $username);
$stmt->execute();

if ($stmt->rowCount() > 0) {
    $melding = "Gebruikersnaam bestaat al.";
} else {
    $sql = "INSERT INTO [User] (username, password, first_name, last_name, address, role) VALUES (:username, :password, :voornaam, :achternaam, :address, 'Cli
    $stmt = $connect->prepare($sql);
    $stmt->bindParam( param: ':username', &var: $username);
    $stmt->bindParam( param: ':password', &var: $password);
    $stmt->bindParam( param: ':voornaam', &var: $voornaam);
    $stmt->bindParam( param: ':achternaam', &var: $achternaam);
    $stmt->bindParam( param: ':address', &var: $adres);

    if ($stmt->execute()) {
        $melding = "Registratie succesvol. U kunt nu inloggen.";
    } else {
        $melding = "Er is een fout opgetreden bij de registratie.";
    }
}
```

OWASP 3 INJECTION

Risico	**CRYPTOGRAPHIC FAILURES**
Aanvalstechniek	Sql statements meegeven in post om data in te zien die niet voor de gebruiker bedoeld was of om data ongeautoriseerd aan te passen
Kans	Hoog: staat op nummer 3 van de OWASP top 10 (OWASP Foundation, z.d.)
Gevolg	Hacker kan data inzien en aanpassen. Dit is een databreuk en het maakt de database onbetrouwbaar

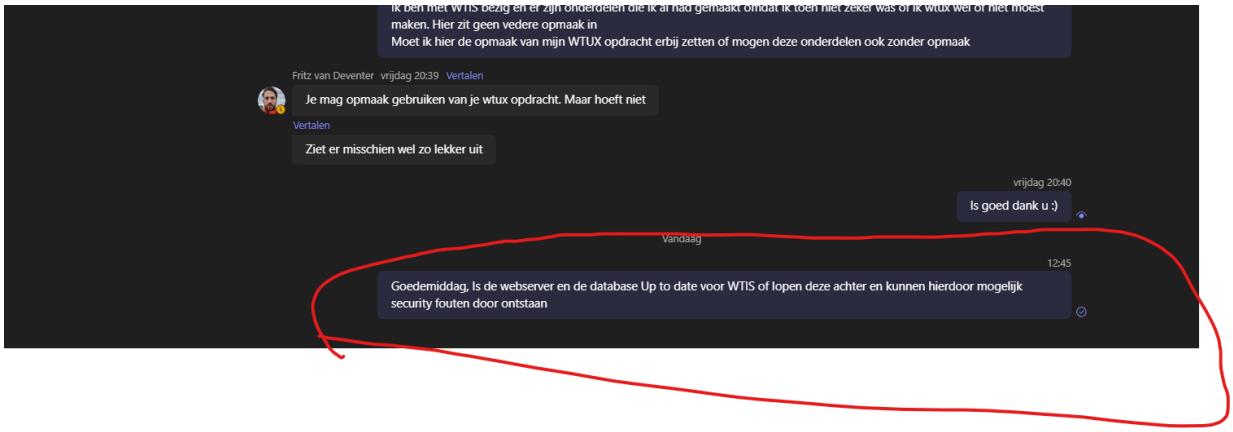
Ik heb mijzelf hiertegen beveiligt door prepared statements te maken voordat ik een query naar de database stuurde

```
$sql = "SELECT * FROM Pizza_Order WHERE client_username = :username";
$data = $db->prepare($sql);
$data->execute(array(':username' => $_SESSION["username"]));
$RESULT = $data->fetchAll();
```

OWASP 6 ULNERABLE AND OUTDATED COMPONENTS

Risico	ULNERABLE AND OUTDATED COMPONENTS
Aanvalstechniek	Aanvaller maakt gebruik van een oude fout in het systeem die in een nieuwere versie eruit gehaald os
Kans	Gemiddeld: staat op nummer 6 van de OWASP top 10 (OWASP Foundation, z.d.)
Gevolg	Dit kan extreem verschillend zijn maar in het ergste geval kan de aanvaller overal bij en alles overnemen

Dit heb ik gecheckt door bij beheerder van de database en webserver (de docent) te vragen of de omgeving nog up to date is



OWASP 10 SERVER-SIDE REQUEST FORGERY

Risico	**Server-Side Request Forgery**
Aanvalstechniek	De aanvaller doet alsof hij de server is en stuurt requests naar de aplicatie om data op te halen
Kans	Laag: staat op nummer 7 van de OWASP top 10 (OWASP Foundation, z.d.)
Gevolg	Hacker kan bij data waar hij/zij niet bij zou mogen komen

Dit is geen probleem want de applicatie maakt geen gebruik van requests die buiten de applicatie worden gebruikt en deze kunnen dus ook niet nagedaan worden


OPEN UP
NEW
HAN_UNIVERSITY
OF APPLIED SCIENCES
HORIZONS.