Verslag OWASP 10 Risicoanalyse

Eli van Holland (2109770)
Docent/Coördinator: Fritz van Deventer
WEBTEI03 TOETS-02
Versie 3.0

Risico 1

Risico	SQL-injectie vanuit views met logincomponent.
Aanvalstechniek	Broncodeinjectie: SQL.
Kans	Hoog: staat op nummer één van de OWASP Top 10 en op nummer drie van 2021 (A1:2017-Injection, z.d.). (*A03 Injection - OWASP Top 10:2021*, n.d.)
Gevolg	Hoog: PHP-broncode die het SQL statement uitvoert heeft minstens de rechten om de hele gebruikerstabel uit te lezen.

Gevolg

Bij een succesvolle SQL-Injection kan het leiden tot het verlenen van toegang tot de database. Dit kan zeer ernstige gevolgen hebben met als een van de ergste gevolgen een datalek van gevoelige informatie.

Maatregelen

In dit stuk code zijn er de volgende maatregelen toegepast:

- Htmlspecialchars
    - Dit zodat er geen speciale karakters direct in de query kunnen worden gezet.
- Prepared statements
    - Zodat veilig de query wordt uitgevoerd.

“Login-logic.php line 8-25”

```
if (isset($_POST['Login'])) {
    $username = htmlspecialchars($_POST['username']);
    $password = htmlspecialchars($_POST['password']);
    $query = 'SELECT * FROM "User" WHERE username = :username';
    $stmt = $db->prepare($query);
    $data_array = [
        'username' => $username
    ];
    $stmt->execute($data_array);
    $user = $stmt->fetch();
    if (password_verify($password, $user['password'])) {
        $_SESSION['username'] = $username;
        $_SESSION['role'] = $user['role'];
```

```
        header('Location: index.php');
    } else {
        header('Location: login.php?error=4001');
    }
}
```

Risico 2

Risico	A01:2021 - Broken Access Control
Aanvalstechniek	Omzeilen van autorisatiechecks.
Kans	Hoog: Staat op nummer één van de OWASP Top 10 2021. (*A01 Broken Access Control - OWASP Top 10:2021*, n.d.)
Gevolg	Hoog: Kan leiden tot gegevensdiefstal, wijziging of vernietiging van gegevens.

Gevolg

Als er niet gecheckt wordt op autorisatie. Bijvoorbeeld of een personeelslid wel ingelogd is. Dan zou een hacker op delen van de website kunnen komen die gevoelige gegevens bevat.

Maatregelen

Zoals te zien in dit stuk code worden er verschillende technieken gebruikt om er voor te zorgen dat de persoon die op de pagina komt er wel mag zijn.

- ID checking.
    - Kijken of de ID die in post wordt meegegeven wel valide is.
- Role checking.
    - Kijken of de role van het de persoon in de session wel een personeelslid is.
- Referal checking
    - Kijken of de vorige pagina wel een pagina is die mag

“Detail-personnel.php Line 14-26”

```
$_POST['orderid'] = htmlspecialchars($_POST['orderid']);
$orderValid = false;
foreach ($orders as $order) {
    if ($order['order_id'] == $_POST['orderid']) {
        $orderValid = true;
    }
}

if(!isset($_POST['orderid']) || $_SESSION['role'] != 'Personnel'||
!$orderValid || !($_SERVER['HTTP_REFERER'] ==
'http://localhost:8080/Personnel.php' || $_SERVER['HTTP_REFERER'] ==
'http://localhost:8080/detail-personnel.php')){
```

```
{
    header('Location: index.php?error=403');
}
```

Risico 3

Risico	A07:2021 - Identification and Authentication
Aanvalstechniek	onveilige opslag van inloggegevens.
Kans	Hoog: Veelvoorkomend probleem. (*A07 Identification and Authentication Failures - OWASP Top 10:2021*, n.d.)
Gevolg	Hoog: Kan leiden tot accountovername en/of ongeautoriseerde toegang.

Gevolg

Het onveilig opslaan van wachtwoorden kan ertoe leiden dat hackers kunnen inloggen op accounts met privileges. Dit is natuurlijk niet de bedoeling en zou tot veel problemen kunnen leiden.

Maatregelen

Zoals te zien in dit stuk code worden er verschillende technieken gebruikt om er voor te zorgen dat er veilig met wachtwoorden om worden gegaan

- Hashing
    - Het gebruiken van password_hash voor het hashen van het wachtwoord wanneer het in de database komt,
    - Password_verify om te checken of het wachtwoord overeen komt.

“Register-logic.php line 20”

```
$password = password_hash($_POST['password'], PASSWORD_DEFAULT);
```

“Login-logic.php line 18”

```
    if (password_verify($password, $user['password'])) {
```

Risico 4

Risico	A02:2021 - Cryptographic Failures

Aanvalstechniek	Gebruik van gebroken technieken. Of ontbreken van.
Kans	Hoog: Veelvoorkomend probleem staat op nummer 2. (*A02 Cryptographic Failures - OWASP Top 10:2021*, n.d.)
Gevolg	Hoog: Gevoelige gegevens kunnen worden onderschept of gestolen.

Gevolg

Het onveilig opslaan van wachtwoorden, zoals zonder hashing of met verouderde algoritmen, kan leiden tot datalekken. Hackers kunnen zo eenvoudig accounts overnemen en gevoelige gegevens stelen.

Maatregelen

Voor het hashen van wachtwoorden wordt er password_hash() gebruikt.

- password_hash()
    - Het gebruik van PASSWORD_DEFAULT zorgt ervoor dat de standaard voor php password hashing gebruikt wordt.

“Register-logic.php line 20”

```
$password = password_hash($_POST['password'], PASSWORD_DEFAULT);
```

Risico 5

Risico	A06:2021 - Vulnerable and Outdated Components
Aanvalstechniek	Het gebruiken van vulnerabilities die gevonden zijn in oude bibliotheken
Kans	Hoog: door afhankelijkheden van derden. Staat op nummer 6 (*A06 Vulnerable and Outdated Components - OWASP Top 10:2021*, n.d.)
Gevolg	Hoog: Gevoelige gegevens kunnen worden onderschept of gestolen.

Gevolg

Het gebruiken van verouderde bibliotheken kunnen hackers de mogelijkheid geven tot het gebruiken van vulnerabilities die gevonden zijn.

Maatregelen

Altijd de laatste versies van libraries gebruiken zorgt ervoor dat de kans op vulnerabilities via derde klein zijn. Zoals het downloaden van de laatste versie van pdo_sqlsrv (David-Engel, 2024)

Bronnen

OWASP Top Ten 2017 | A1:2017-Injection | OWASP Foundation. (n.d.). https://owasp.org/www-project-top-ten/2017/A1_2017-Injection

A01 Broken Access Control - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/A01_2021-Broken_Access_Control/

A07 Identification and Authentication Failures - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

A02 Cryptographic Failures - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

A06 Vulnerable and Outdated Components - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

David-Engel. (2024, June 25). *Download the Microsoft Drivers for PHP for SQL Server - PHP drivers for SQL Server*. Microsoft Learn. https://learn.microsoft.com/en-us/sql/connect/php/download-drivers-php-sql-server?view=sql-server-ver16

A03 Injection - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/A03_2021-Injection/