MODULE G SECURITY · G6

SQL injection

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.1, 1.4.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **20 marks**.

1

Total: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement about SQL injection is true or false. **[4]**

Statement	True	False
The attacker enters SQL code into an input box, such as a search box or a login form		
SQL injection is a type of malware that copies itself from one computer to another		
A successful SQL injection attack could let the attacker change or delete records in a database		
Encrypting the data sent between the browser and the web server prevents SQL injection		

2

Total: 6 marks

A mail-order plant nursery has a website with a search box. When a visitor types the name of a plant and clicks Search, the website's program puts the typed text straight into this SQL query and sends it to the nursery's database:

```
SELECT PlantName, Price FROM Plants WHERE PlantName = '[text typed in the search box]'
```

The same database also stores customers' names, addresses and order details.

(a) Describe what is meant by **SQL injection**. **[2]**

(b) Explain why typing SQL code into the search box could change what this query does. **[2]**

(c) Give **two** things an attacker could try to do to the nursery's database using SQL injection. **[2]**

1

2

3

Total: 4 marks

A community energy cooperative has a members' website. Members log in by typing a username and a password. The website's program builds an SQL query from the two values typed in. If the database finds a matching record, the member is logged in.

(a) Explain how SQL injection could let an attacker log in to the website without knowing a member's password. **[3]**

(b) State the weakness in the website's program that makes SQL injection possible. **[1]**

4 **Total: 4 marks**

The energy cooperative from Question 3 wants to protect its members' website against SQL injection.

(a) Explain how **input validation** could help to prevent an SQL injection attack on the login form. **[2]**

(b) The website's program connects to the database using an account that can read, change and delete the data in every table, including members' payment details.
Explain how restricting the **access level** of this account would limit the damage an SQL injection attack could cause. **[2]**

5 **Total: 2 marks**

Before the new login form goes live, the cooperative pays a security firm to carry out penetration testing on the website.

(a) Describe how **penetration testing** could help the cooperative protect its website from SQL injection. **[2]**

Total for this worksheet: 20 marks