MODULE G SECURITY · G6

SQL injection: mark scheme

20 marks · OCR J277 spec 1.4.1: the concept of SQL injection (how the attack is used, the purpose of the attack); 1.4.2: how to limit the threat (user access levels, penetration testing) and remove the vulnerability (input validation, also J277 2.3.1)

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. **...** at the start of a bullet means it builds on the bullet before. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1, 1.4.2	Enters SQL code into an input box: True Malware that copies itself: False Could change or delete records: True Encrypting browser–server data prevents it: False	**4**	1 mark per correct row. 2 ticks in a row = 0 for that row. Row 4: the code is typed into the site's own form, so it reaches the server whether or not the connection is encrypted.
2(a) J277 1.4.1	(Attacker) types / enters SQL code / commands into an input box / field / form (on a website) The code becomes part of the website's (SQL) query // the code is run / executed by the database To access / view / steal / change / delete data without permission // to bypass a login / authentication It takes advantage of input that is not validated / checked	**2**	1 mark per bullet, max 2. Do not accept "hacking a database" or "attacking a website" alone (NE). Do not accept answers that describe it as a virus / malware.
2(b) J277 1.4.1	The typed text is put directly into the query // the input is not validated / checked before it is used (1) ... so the database treats the typed code as part of the SQL command / runs it, instead of treating it as a plant name to search for (1) The code can change the condition / the WHERE part // can make the query return / affect other data (e.g. customer details) (1)	**2**	1 mark per bullet, max 2. Do not accept "the query will not work" or "it causes an error" alone. Answers do not need to quote any SQL.
2(c) J277 1.4.1	View / read / steal customers' names / addresses / order details Change / alter data, e.g. plant prices / orders / customer addresses Delete records / tables / data (e.g. the plant list or orders) Add (false) records, e.g. fake orders / accounts Get past a login / bypass authentication // gain access to an account (e.g. an administrator or customer account)	**2**	1 mark each, max 2. Mark the first two answers. Each must be a different action (view, change, delete, add, bypass login). Do not accept "hack the database", "get data" alone (NE), or "install a virus / malware".

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.1	The attacker types SQL code / commands (into the username or password box) instead of a normal username / password The input is not validated / checked / sanitised ... ... so the code becomes part of the login query / is joined into the query The code changes the query's condition so it is always true // so it no longer checks the password (correctly) The database finds / returns a matching record ... ... so the website logs the attacker in // authentication is bypassed	**3**	1 mark per bullet, max 3. Candidates do not need to give any actual SQL. Do not accept "guesses the password" or "tries every password" (that is a brute-force attack). Do not accept "hacks in" alone (NE).
3(b) J277 1.4.1, 2.3.1	The input is not validated / checked / sanitised (before it is used) // the typed values are put directly into the SQL query	**1**	Accept "it does not use parameterised queries / prepared statements". Do not accept "weak passwords", "no firewall" or "no encryption".
4(a) J277 1.4.2, 2.3.1	The program checks the input before it is used in the query / sent to the database (1) Input that contains SQL code / commands / unexpected characters (e.g. quote marks) // that is too long / not in the expected format is rejected / removed (1) ... so the attacker's code is never run by the database / never becomes part of the query (1)	**2**	1 mark per bullet, max 2. Accept "sanitisation" for validation. Do not accept "it checks the password is correct" (that is authentication, not validation). Do not accept "stops hackers" alone (NE).
4(b) J277 1.4.2	The account is given only the access it needs, e.g. read-only / only the tables needed for logging in (1) Injected code could then not change / delete data (1) Injected code could then not reach other tables, e.g. members' payment details (1)	**2**	1 mark per bullet, max 2. Do not accept "it stops SQL injection" (it limits the damage, not the attack). Do not accept "members get less access" (the question is about the program's account).
5(a) J277 1.4.2	Authorised testers / the security firm simulate / carry out an attack on the website (with permission) (1) e.g. they try entering SQL code into the login / input boxes (1) To find weaknesses / vulnerabilities (before a real attacker does) (1) ... so the weaknesses can be reported and fixed / the program can be changed before the form goes live (1)	**2**	1 mark per bullet, max 2. Do not accept "tests the website" or "tests the passwords" alone (NE). Do not accept answers that say penetration testing stops attacks by itself.

Total: 20 marks