Exercise walk-through

Application and Data Vulnerabilities and Attacks ▪ 5.1

eXercise

You must be able to

- identify an application attack from log evidence
- explain how unchecked user input enables injection attacks
- name **data validation 数据验证** as the core defense

Method — Reading the evidence

SQL injection shows OR 1=1 and – in a query. XSS shows a <script> tag. Directory traversal shows ../ in a URL. A buffer overflow shows an unusually long input string.

Method — The common cause

Every one of these attacks exploits unchecked user input. Data validation - checking input meets expected rules before processing - is the core defense.

Practice 2.1 ▪ 1 mark

A login field receives the input ' OR '1'='1. Name the attack.

Solution 2.1

Worked steps

SQL injection B1.

Practice 2.2 ▪ 2 marks

Explain how a **directory traversal** attack works.

Solution 2.2

Method: Reading the evidence

Worked steps

the attacker puts ../ sequences in a URL B1 to climb out of the intended folder and reach sensitive files B1.

Practice 2.3 ▪ 1 mark

A web application does not check what users type into its input fields.
(a) State the general name for the resulting class of attack.
(b) Name the defense that would prevent it.

Solution 2.3

Method: The common cause

Worked steps

(a) injection attacks B1. (b) data validation / input sanitization B1.

Exam-style 3.1 ▪ 1 mark

A URL request for ../../../etc/passwd is a

A SQL injection

B XSS attack

C directory traversal attack

D smurf attack

Solution 3.1

A SQL injection

B XSS attack

C directory traversal attack ✓

D smurf attack

Worked steps

C. ../ climbing folders is directory traversal.

Exam-style 3.2 ▪ 1 mark

Sending far more data than a memory buffer can hold is a

A buffer overflow

B cross-site scripting

C SQL injection

D directory traversal

Solution 3.2

A buffer overflow ✓

B cross-site scripting

C SQL injection

D directory traversal

Worked steps

A. overflowing a buffer into nearby memory is a buffer overflow.

Exam-style 3.3 ▪ 1 mark

A bank's log shows an input string containing ' OR '1'='1' – in its loan form.
(a) Name the attack.
(b) Explain what the attacker is trying to do.

Solution 3.3

Method: Reading the evidence

Worked steps

(a) SQL injection B1. (b) inject control characters into the database query B1 to make it return or change data it should not B1.