VIDEO Intypedia007en

LESSON 7: WEB APPLICATION SECURITY - INTRODUCTION TO SQL INJECTION TECHNIQUES

EXERCISES

AUTHOR: Chema Alonso

Security Consultant at Informatica 64. Microsoft MVP Enterprise Security

EXERCISE 1

SQL Injection vulnerabilities are caused by:

a) Bugs in the firewall settings

b) Bugs in the application that creates the queries

c) Bugs in the database settings

d) Bugs in the parameter filtering of the browser

EXERCISE 2

What happens in an inbound SQL injection attack?

a) The SQL injection occurs within a query

b) The query results are obtained from the returned HTML page

c) The SQL injection is performed from the outside towards the inside

d) The firewall allows you to include the results in the SQL query

EXERCISE 3

What is a blind attack?

a) An injection in which the attacker doesn't see the SQL query that is being made
b) An attack in which the response time should be measured
c) An attack in which you infer the results because you can't see them
d) An injection in which the parameters are blind

EXERCISE 4

How can you recognize a True result in a blind attack?

a) There will be a True when you remove the ID from the database on screen
b) By the identifier of the process that generates the query
c) By a keyword in the search results page
d) By the response time

EXERCISE 5

Which of the following is an effective way to avoid SQL injection vulnerability?

a) Filtering quotes in all the queries
b) Filtering quotes and blank spaces
c) Avoiding the concatenation of strings of commands and parameters
d) Using a firewall to publish web applications

ANSWERS

1. b
2. b
3. c
4. c and d
5. c

Madrid, Spain. May 2011

http://www.intypedia.com

http://twitter.com/intypedia