Exam Report: 12.3.9 Practice Questions

Date: 5/11/2020 1:47:24 pm
Time Spent: 1:47

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 13%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

In 2011, Sony was targeted by an SQL injection attack that compromised over a million emails, usernames, and passwords. Which of the following could have prevented the attack?

- Blocking, or at least monitoring, activity on ports 161 and 162.
- Careful configuration and penetration testing on the front end.
- Using VPN technology to protect client data when connecting from a remote system.
- ~~Scanning the operating system and application coding regularly for bugs and errors.~~

Explanation

SQL attacks such as with Sony, United States Department of Energy, and MySQL could have been prevented with careful configuration and penetration testing on the front end.

One of the steps for preventing privilege escalation is to scan the operating system and application coding regularly for bugs and errors.

To defend against WPA/WPA2 cracking is to use VPN technology to protect client data when connecting from a remote system.

How can we prevent SNMP exploitation? The easiest way is to block, or at least monitor, activity on ports

161, 162, and any other port you've configured for SNMP traffic.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_FACTS_01_EH1]

Question 2: Incorrect

SQL injections are a result of which of the following flaws?

- The file system
- The web server
- ~~The database~~
- Web applications

Explanation

A SQL injection is an attack that attacks a web application by manipulating SQL statements entered into a web page.

It's important to note that SQL injections are a result of flaws in web applications, not in the database,

file system, or web server. These attacks target non-validated input vulnerabilities and use them to send SQL commands to the database through the web application. This is done by injecting a code into an existing line of code before sending it onto the database for execution. Assuming the injection is successful, the malicious code could be run on the backend database and would return the requested information.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_FACTS_02_EH1]

Question 3: Incorrect

Which of the following functions does a single quote (') perform in an SQL injection?

- Indicates that the comment has ended and data is being entered.
- Indicates that everything after the single quote is a comment.
- Indicates that data has ended and a command is beginning.
- ~~Indicates that code is ending and a comment is being entered.~~

Explanation

A single quote (') indicates that data has ended and a command is beginning.

The double dashes (--) indicate that code is ending and a comment is being entered. Comments are code that a program does not execute and are usually used for explanations or reminders for the coder. Applications know to ignore the comments.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_FACTS_03_EH1]

Question 4: Incorrect

A hacker has used an SQL injection to deface a web page by inserting malicious content and altering the contents of the database. Which of the following did the hacker accomplish?

- ~~Bypass authentication~~
- Compromise data availability
- Compromise data integrity
- Information disclosure

Explanation

To compromise data integrity, an SQL injection is used to deface a web page by inserting malicious content or altering the contents of the database.

To compromise data availability, an attacker uses an SQL injection to remove information from a database, delete logs, or alter information that has been stored in a database.

With information disclosure, an SQL injection is used to access sensitive information from a database.

To bypass authentication, an attacker uses an SQL injection to log into an application with administrative-level privileges without the required username and password.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_FACTS_04_EH1]

Question 5: Correct

There are several types of signature evasion techniques. Which of the following best describes the obfuscated codes technique?

- Uses the CHAR function to represent a character.
- Code can be used to represent an SQL query.
- Inserts in-line comments between SQL keywords.
- Is an SQL statement that is hard to read and understand.

Explanation

Obfuscated code is an SQL statement that is hard to read and understand.

The char encoding technique uses the CHAR function to represent a character.

With the in-line command technique, comments are inserted between SQL keywords. As a result, the strings are obscured.

With the Hex coding technique, hexadecimal code can be used to represent an SQL query.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_TYPES_EVASION_01_EH1]

Question 6: Incorrect

The SQL injection methodology has four parts. Which of the following parts is similar to playing the game 20 questions?

- ~~Test for SQL injection vulnerabilities~~
- Launch a SQL attack
- Information gathering
- Advanced SQL injection

Explanation

In part three, launch a SQL attack, there are two main categories for SQL injection: in-band and blind. Blind SQL, also known as inferential SQL injection, is time-consuming because instead of receiving data, you're receiving true or false results. If you've ever played 20 questions, you know that it can be difficult to investigate using yes or no questions, but not impossible.

In part one, information gathering, you'll poke around to see what information you can find in the process.

In part two, testing for SQL injection vulnerabilities, function testing is performed, which requires little knowledge of the inner design of the code or logic.

In part four, advanced SQL injection, the database, table, and column enumeration can assist in identifying user level privilege and database structure.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_TYPES_METHOD_01_EH1]

Question 7: Incorrect

Which of the following best describes the SQL Power Injector tool?

- A tool used to find SQL injections on a web page.
- A tool used for heavy queries to complete time-based blind SQL injection attacks.
- ~~An injection tool that be can used for retrieving user and password hashes, fingerprinting, accessing a file system, and executing commands.~~
- An injection framework that can exploit SQL injection vulnerabilities on most databases.

Explanation

SQL Power Injector is used to find SQL injections on a web page.

BSQLHacker is an injection framework that can exploit SQL injection vulnerabilities on most databases.

Havij is an SQL injection tool that an attacker can use for retrieving user and password hashes, fingerprinting, accessing a file system, and executing commands.

An attacker can use the Marathon Tool to use heavy queries to complete time-based blind SQL injection attacks.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECTIONS_TYPES_TOOLS_01_EH1]

Question 8: Incorrect

As a penetration tester, you have found there is no data validation being completed at the server, which could leave the web applications vulnerable to SQL injection attacks. Which of the following could you use to help defend against this vulnerability?

- ~~Always use default error messaging.~~
- Use a higher privileged account for database connectivity.
- Be sure that the database server account is being run with maximum rights.
- Decline any entry that includes binary input, comment characters, or escape sequences.

Explanation

The most important SQL injection countermeasure is to ensure validation at the server. Limit the size and data type of any input data. Accept only the expected values, and test the content of all string variables. Decline any entry that includes binary input, comment characters, or escape sequences. Enforce type and length checks so that input is viewed as a value and not as a potentially executable code. Ideally, you want to implement various layers of data validation, filtering, and sanitizing. You want to be sure that questionable or unvalidated data does not make it to your web application.

Since a database server is able to run OS commands, you'll want to be sure that the database server account is being run with minimal rights. Also, you'll want to disable powerful commands that would provide an attacker with too much access to the network. Next, instead of using a privileged account to connect to the database, you'll want to use a lower privileged account for database connectivity. You'll also want to monitor all database traffic with your intrusion detection system. Because error messages can be used to gather information, you'll want to turn off default error messaging. You could choose to disable error messaging completely, or, if you would prefer to have an error message in place, use a custom error message so you are able to control the information that is shared in the message.

References

TestOut Ethical Hacker Pro - 12.3 SQL Injections
[e_sql_injections_eh1.exam.xml Q_SQL_INJECT_COUNTER_FACTS_01_EH1]