Jimmy is a security consultant that has been hired by an organization to conduct software testing of their new web application. As part of the test for this application, Jimmy is provided with an authenticated user account complete with the username and password, but he has not been given access to the web application’s source code. Which type of testing method is the organization expecting Jimmy to use?

White box

Blue box

Gray box

Black box

Answer: C

Explanation: Since he has been given some information about the web application, including user credentials, this would be classified as a gray box test of the software. If Jimmy was given the complete details of the web application, including the source code, then he would be conducting a white box test. If he were given no information about the web application, then it would be a black box test.

Your organization is concerned that they might become the victim of a SQL injection attack. What is the best way to prevent a SQL injection from occurring?

Force all web pages to transmit information over HTTPS

Install the latest security patches to the database server

Install a host-based firewall on the database server

Conduct input validation

Answer: d

Explanation: The best method of preventing any kind of code injection is to utilize input validation on any data received from a user. Additionally, all web applications should be programmed to use the lowest level of privilege when communicating to backend databases to minimize the threat if a code injection is successful.

Allison is concerned that she might fall victim to a malware attack. To prevent this, she has purchased the latest anti-malware solution from a well-known software company. After installing the software, she ensures the software is set to update its signature every evening and scan her computer for threats. Everything has been fine for several months, but today, her computer begins to run very slowly and Allison noticed that her processor and network utilization continue to rise even when she isn’t performing processor-intensive functions. What kind of threat might Allison has become a victim of?

XSS

Zero-day

SQL injection

XSRF

Answer: B

Explanation: A zero-day is a type of malware or attack that exploits a previously unknown vulnerability. Since Allison is relying on a signature-based anti-malware solution, a zero-day could have exploited her machine before the anti-malware software company has created a signature to detect it.

Tina is conducting a penetration test of a web application. During the testing, she attempts to login to the website using admin as the username and enters her password as ` OR 3=3; in an attempt to conduct an attack. What type of attack did Tina attempt?

Buffer overflow

Code injection

SQL injection

Rootkit

Answer: C

Explanation: During an SQL injection, an attacker attempts to submit an always true condition as part of the SQL query statement being forwarded to the database. In this case, Tina assumed that there is a user account named admin in the database and she entered the condition of 3=3, which will always return a value of TRUE to the web application.