Sample Exam

Edition 201606

Content

Introduction

This is the sample exam EXIN Secure Programming Foundation (SPF.EN). The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

Good luck!

Sample Exam

1 / 40
Attackers and defenders are two players within the field of security.

Why is the attacker at an advantage?

A. An attacker only needs to find one flaw; defenders need to consider all possible flaws.
B. An attacker is more skilled and determined than a defender.
C. An attacker abuses new technologies that a defender has to install.
D. An attacker has more computing power that he can use for performing all kind of attacks.

2 / 40
Some well known security principles are used when designing secure systems. One of them is an application design that prevents single points of failure with security redundancies and layers of defense.

What principle is used to accomplish this design?

A. Defend in depth
B. Fail securely
C. Grant least privilege
D. Separate privileges

3 / 40
The following authorization header is sent by the browser to the server in response to a `"401 Authorization Required"` response:

```
Authorization: Basic bmFtZTpwYXNzd29yZA==
```

Is it safe to send this header using the HTTP protocol?

A. Yes, because the value is encrypted and cannot be reversed.
B. Yes, because the value is used only once and changes with every request. C.
No, because the value is encrypted using a weak algorithm.
D. No, because the value can be sniffed and reversed to valid credentials.

4 / 40
The term *SOP* most commonly refers to the mechanism that controls access for JavaScript and other scripting languages to the DOM properties and methods across domains.

Which conditions have to be satisfied to grand access between two interacting pages that do NOT use the document.domain property?

A. Protocol, IP number and - for browsers other than Microsoft Internet Explorer - port number.
B. Protocol, domain name and - for browsers other than Microsoft Internet Explorer - port number.
C. Protocol, PTR record and - for browsers other than Microsoft Internet Explorer - port number.
D. Protocol, FQDN and - for browsers other than Microsoft Internet Explorer - port number.

5 / 40
An application allows a user who is logged in to change his/her password. This function is only available for authenticated users and uses the HTTPS protocol to send the data.

What is considered BEST PRACTICE to perform the password change?

A. Ask the user for the login name, old password, new password and confirmation of this password.
B. Ask the user for the new password and confirmation of this password.
C. Ask the user for the old password, new password and confirmation of this password.
D. Use the session data to identify the user and ask for the new password and confirmation of this password.

6 / 40
When storing passwords in a file or a database, what is the BEST approach?

A. Store the hashed value of the password that the user has chosen including a random salt.
B. Store the hashed value of the password that the user has chosen including a fixed salt.
C. Store the plain text value of the password that the user has chosen.
D. Store the encrypted value of the password that the user has chosen including the initialization vector.

7 / 40
HTTP sessions are used to keep state between several requests and use a session ID for identification.

What is the MOST important practice in regard to the session ID?

A. The session ID should be kept secret at all times.
B. The session ID should change with every POST request.
C. The session ID should be at least ten characters long.
D. The session ID should be encrypted using a strong algorithm.

8 / 40
An application uses a single sign-on implementation that is specifically designed for web-based environments. The user logs in through the identity provider and uses two different applications that participate in the same single sign-on implementation. You are facing some challenges when implementing the logout feature.

What is the BEST way to solve implementing the logout feature for these two applications?

A. Implement a logout function that invalidates the session for the current application and not the single sign-on session.
B. Implement a logout function that invalidates the single sign-on session and depend on the session-timeout for participating applications.
C. Implement a logout function that invalidates the single sign-on session and the session for the current application.
D. Implement two logout functions: one for the current application and one that in addition invalidates the single sign-on session.

9 / 40
Your web application uses sessions to maintain state. A user logs in but does not allow cookies to be set. You have to implement an alternative solution for keeping track of the session ID. The session ID is a random 96 bits value and all communication is based on HTTPS.

Within this scenario, what is the BEST way to keep track of the session ID?

A. Use a URL parameter that contains the session ID.
B. Use a hidden parameter that contains the session ID.
C. Use a URL parameter that contains the encrypted session ID.
D. Use a combination of HTTP headers to generate the session ID.

10 / 40
What is the BEST solution to prevent CSRF attacks?

A. Use the Referrer-header to check the origin of the previous request.
B. Make requests unpredictable by adding a random value and check this value.
C. Use HTTPS to protect all communication between the client and the server.
D. Make sure that session fixation is not possible which also prevents CSRF attacks.

11 / 40
Vulnerabilities exist in different contexts. Two identifiable contexts are the server side and client side contexts. It is important to understand whether a vulnerability is focussed on the server portion of the application (server context) or the client running it (client context). SQL injection and XSS are two different types of vulnerabilities.

In which context do these two vulnerabilities exist?

A. SQL injection vulnerabilities exist on the client side and XSS vulnerabilities exist on the server side.
B. SQL injection vulnerabilities exist on the server side and XSS vulnerabilities exist on the client side.
C. Both SQL injection and XSS vulnerabilities exist on the client side. D.
Both SQL injection and XSS vulnerabilities exist on the server side.

12 / 40
Direct and parameterized queries are two techniques to execute queries that are partly based on user input.

Which of the following statements in regard to direct and parameterized queries when used properly is correct?

A. A direct query filters meta-characters more efficiently than parameterized queries.
B. A direct query filters meta-characters less efficiently than parameterized queries.
C. A direct query uses placeholders to process input and a parameterized query uses the supplied parameters.
D. A direct query uses the supplied parameters for input and a parameterized query processes input through placeholders.

13 / 40
You are assigned the honorable task to prevent SQL injection in a small web application. You have listed all lines of code where user input ends up in a SQL query. You also want to make sure that future involvements do not introduce new SQL injection vulnerabilities.

What is the BEST solution to accomplish this task?

A. Write and use your own routines that escape all input for all database products and rewrite the necessary lines of code.
B. Use a transparent layer provided through standard libraries that escapes all input and rewrite the necessary lines of code.
C. Prevent the leakage of information about the database product that is used to make SQL injection impossible.
D. Prevent the application from showing detailed error messages since these are needed to exploit a SQL vulnerability.

14 / 40
Testing input against a list of known negative inputs which is implemented when you compile a listing of all the negative or bad conditions and then verify if the received input is not included in the list is a technique for filtering input.

What is the name of this filtering technique?

A. Implementing the Graylist method for input validation.
B. Implementing the Blacklist method for input validation.
C. Implementing the Whitelist method for input validation.
D. Implementing Regular Expressions for input validation.

15 / 40
Validation of user input is possible at the client (browser) and at the server portion of the application.

What is the BEST solution to perform validation of user input?

A. Perform validation of user input at the client (browser).
B. Perform validation of user input at the server portion of the application.
C. Perform validation of user input both at the client (browser) and the server portion of the application.
D. Perform validation of user input either at the client (browser) or the server portion of the application.

16 / 40
Your web server is set to use UTF-8 encoding for input and output. Some of your validation routines are based on legacy libraries that only accept ISO/IEC 8859 character sets. You have written conversion routines to be used for handling input and output to the validation routine.

A user is allowed to enter his/her name in a web form. The input is validated by the validation routines and reflected to the user in the HTML body.

What needs to be done with the input to display the output properly and safely?

A. The input needs to be normalized, converted and HTML encoded.
B. The input needs to be normalized, stripped and HTML encoded.
C. The input needs to be converted, stripped and HTML encoded.
D. The input needs to be normalized, stripped and converted.

17 / 40
An attacker has found two input fields that result in a buffer overflow condition. This condition happens within a function that converts all upper case input into lower case and is then used to execute a search.

Where does the buffer overflow reside and what does it allow for?

A. This buffer overflow resides on the heap and allows for code execution.
B. This buffer overflow resides on the heap and allows for data manipulation.
C. This buffer overflow resides on the stack and allows for data manipulation.
D. This buffer overflow resides on the stack and allows for code execution.

18 / 40
An attacker found a vulnerability within a web application. He discovered that one of the parameters in the URL can be used to add JavaScript code which is executed within the browser when he sends the request to the website.

Which of the following statements BEST describes this vulnerability?

A. This is a stored XSS vulnerability. The attacker needs to entice the victim to visit the URL.
B. This is a stored XSS vulnerability. Exploitation occurs when someone uses the web application.
C. This is a reflected XSS vulnerability. The attacker needs to entice the victim to visit the URL.
D. This is a reflected XSS vulnerability. Exploitation occurs when someone uses the web application.

19 / 40
As the developer of a web application, you are assigned the task to implement a strong defense against server XSS.

What is the easiest and strongest defense against Server XSS?

A. Stripping all JavaScript from user input.
B. Context-sensitive server side output encoding.
C. Using safe JavaScript APIs.
D. Using safe third-party JavaScript code.

20 / 40
Members of the HR department within your company are responsible for maintaining your personal information that resides in the HR application. Information in regard to your working performance is also stored through the HR application but read/write access to this information is limited to the manager of your department. One of the HR members is allowed to read the working performance for monitoring purposes.

Authorization for the HR application is implemented according to the desired access model.

On what type of authorization is access to data within the HR application based?

A. on horizontal authorization
B. on vertical authorization
C. on object and attribute authorization
D. on horizontal and vertical authorization

21 / 40
An authenticated user is authorized to edit, view and delete records that describe all individual parts that belong explicitly to a product that is manufactured by the department he is working for. The company manufactures other products, but the user is not authorized to access parts that belong to these other products.

The authenticated user discovers that he is able to get access to unauthorized parts by simply changing a form value that represents the part-number.

What is the most likely reason for this authorization failure?

A. The authorization is based on insecure direct object references. B.
The authorization is based on insecure indirect object references.
C. The authorization is based on incomplete indirect object references.
D. The authorization is based on incomplete direct object references.

22 / 40
Suppose that two separate actions operate on the same resource and that checks are used to validate if the process is allowed to use the resource.

What is the attack called that abuses the time window between the check (TOC) and use (TOU) of the resource?

A. A session poisoning attack.
B. A race condition attack.
C. An atomic operation attack.
D. An application flow attack.

23 / 40
Why is hardening of systems a very important security control?

A. Third party software is not always written with security in mind.
B. Third party Firewalls do not protect the exposed services properly.
C. Third party services are always on and insecure by default and need protection.
D. Third party software is not both functional and secure out-of-the-box.

24 / 40
Hardening of a system consists of various adjustments.

Which of the following is NOT considered hardening of a system?

A. Applying the latest security patches.
B. Disabling or removing debug features.
C. Compiling code with ASLR and DEP protection.
D. Changing default passwords.

25 / 40
A web application detects an error when handling a request. Instead of displaying full information about the error, a general page including a reference about the error is returned. All information about the error is logged locally, including the reference.

What is most likely the primary reason for this solution?

A. This prevents unnecessary leakage of internal information.
B. This is more user friendly than displaying the full error message.
C. This prevents unnecessary usage of bandwidth.
D. This is the preferred way for developers to solve and administer errors.

26 / 40
A web application is designed with logging various types of information in mind.

Which type of information is MOST important for logging information with regard to security?

A. Version information of the modules that are started.
B. Stack traces that are generated during an error.
C. The entrance, duration and exit timestamps of procedure calls.
D. Increase and decrease of privilege levels for logged-in users

27 / 40
As a developer you have coded to catch every potential error and you have provided a solution that ensures that the code will not be left in an insecure state.

What application security principle is described above?

A. complete mediation
B. fail securely
C. detect intrusion
D. fail-safe defaults

28 / 40
As a developer you are concerned about performance and availability of your application. Instead of depending solely on the implementation of a large and extensible server farm, you also implement a solution that limits the amount of resources that can be allocated to a single user.

Which purpose BEST describes the reason behind this solution?

A. to speed up processing
B. to prevent unexpected behavior
C. to mitigate a DoS attack
D. to reduce the server farm

29 / 40
When developing an application that uses cryptography, what is the BEST strategy to choose a cryptographic library?

A. Develop it yourself: open source libraries can't be trusted. Proof is Heartbleed.
B. Use an open source library and audit it yourself.
C. Use a commercial library like RSA's Bsafe; they have been audited by professionals.
D. Use either an open source or a commercial library and write a security assumption that they are out of scope for your security requirement.

30 / 40
What is the difference between symmetric cryptography and asymmetric cryptography?

A. Symmetric cryptography is based on symmetric passwords. Asymmetric cryptography allows all passwords.
B. Symmetric cryptography needs the same operating system for user and browser. Asymmetric cryptography does not.
C. Symmetric cryptography is based on both user and software using the same key. Asymmetric cryptography uses a public key.
D. Symmetric cryptography checks a password against a stored password. Asymmetric cryptography uses a randomly added string.

31 / 40
Why is a website, of which the certificate is revoked, a risk?

A. Because a website with a revoked certificate may not be the website you intended to visit.
B. Because the certificate authority that gives out the certificate has been proven to be bad.
C. Because the browser is not working correctly, you are shown this error. You need to update.
D. It is not a risk, because the original certificate was given out by a trusted certificate authority.

32 / 40
You are assigned to set up a website that uses HTTPS. For this purpose you have requested and installed a certificate that is signed by a well-known CA (Certification Authority).

What is NOT something that you have to do in order to implement the HTTPS server securely?

A. Disable all protocols that are not supported by the server's OS. B. Configure the server to allow only strong protocols and ciphers. C. Implement HSTS to allow for browser based mitigation.
D. Configure the server or application to add the 'secure' flag on session cookies.

33 / 40
A Swiss bank needs a non-repudiation requirement for the following functional requirement:

"As an account holder, I can transfer money from one account to another."

You are asked to help them. What is an appropriate non-repudiation requirement?

A. All login attempts should be logged.
B. Transfers can only be done from one of the account holder's accounts.
C. Every transfer must be logged.
D. Negative amounts are not allowed.

34 / 40
Given this requirement:

"When a user has forgotten his/her password, the user must be able to change it."

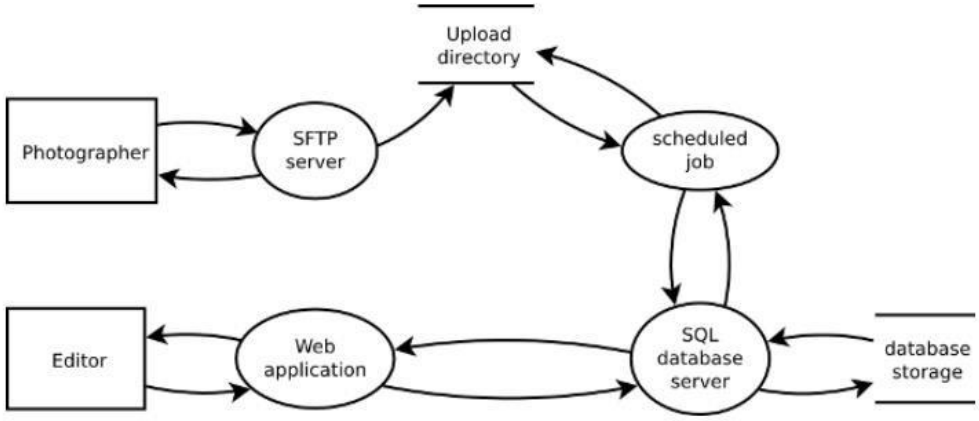
What is the hidden assumption here?

A. It is assumed that users should only be able to change their own password.
B. It is assumed that passwords should have a minimum length.
C. It is assumed that users do not write down their passwords.
D. It is assumed that a user's identity can be established before changing the password.

35 / 40
What security principle states that access is denied and the security scheme identifies when access is permitted?

A. Default deny
B. Defense in depth
C. Least privilege
D. Input validation

36 / 40
A newspaper has deployed an editing platform. Its architecture is described below and illustrated with a Data Flow Diagram (DFD).



1. Photographers all over the globe can log in and upload photos using SFTP (Secure FTP).
2. The photos are placed in an upload-directory.
3. The system runs a regularly scheduled process to move the photos from the upload-directory into a SQL database.
4. Editors at the office use the web application to browse the photos and add some photos to articles for publication. (There is no photo-editing feature, photos are published as-is).

A threat analysis identified this risk: Photographers can create malformed filenames that trigger a shell injection attack. If an attacker uploads a file that contains shell commands, the code that should copy the file will execute those shell commands.

The architects replace the SFTP file-upload and the scheduled job with a web interface that inserts the photos directly into the database, hoping to get a more secure system.

Choose the BEST answer. Will the system be more secure?

A. Yes, this solves the problem completely.
B. Yes, but only if the web interface is free of security problems.
C. No, this fix does not deal with identity spoofing attacks.
D. No, this does not fix the problem at all.

37 / 40
Which of the following is NOT a principle of secure design?

A. Allow for future security enhancements.
B. Design security through secrecy.
C. Implement least privilege.
D. Isolate security controls.

38 / 40
Which definition BEST describes a vulnerability scan?

A. A series of automated tests for known problems.
B. A test performed by security experts.
C. A stress test to make the application crash.
D. A review of vulnerabilities in the design.

39 / 40
Which of the following things should effective security testing involve?

A. Testing of people
B. Testing of process
C. Testing of technology
D. All of the above

40 / 40
What is a significant disadvantage of MANUALLY inspecting code?

A. The review is performed too quickly to be thorough, when done manually.
B. Manual inspection cannot be applied to many situations.
C. Manual inspection requires significant human thought and skill to be effective.
D. The manual review requires the assistance of complex technologies.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	A	21	A
2	A	22	B
3	D	23	D
4	D	24	C
5	C	25	A
6	A	26	D
7	A	27	B
8	D	28	C
9	B	29	B
10	B	30	C
11	B	31	A
12	D	32	A
13	B	33	C
14	B	34	D
15	C	35	A
16	A	36	B
17	D	37	B
18	C	38	A
19	B	39	D
20	D	40	C

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER