15 Secure development practices (4 points)

You are put in charge of improving the software security of a new tech company. Briefly explain some of the practices you would want to recommend using (at least 4).

Skriv ditt svar her

Format

Words: 0

Maks poeng: 4

16 Symmetric algorithm (1 point)

What is a symmetric algorithm and how can it be used in software to ensure secure data transmission?

Velg ett alternativ:

- A symmetric algorithm is a type of routing algorithm that is used to direct network traffic between different nodes. In software, symmetric algorithms can be used to optimize network routing and ensure that data is transmitted along the most efficient path. This can help to improve network performance and reduce latency.
- A symmetric algorithm is a type of encryption algorithm that uses the same key for both encryption and decryption. In software, symmetric algorithms can be used to encrypt data before it is transmitted over a network, and then decrypt it on the receiving end usir ✔ ıe same key. This ensures that the data is secure and cannot be intercepted or read by unauthorized parties.
- A symmetric algorithm is a type of compression algorithm that is used to reduce the size of data before it is transmitted over a network. In software, symmetric algorithms can be used to compress large files or data sets, making them easier and faster to transmit over a network. This can help to improve network performance and reduce bandwidth usage.

Maks poeng: 1

17 Encrypting messages (1 point)

In an asymmetric key system, each user has a pair of keys: a private key and a public key. To send an encrypted message to someone, what must you encrypt the message with?
Velg ett alternativ:

- Your private key
- Your public key
- The recipient's public key ✔
- The recipient's private key

Maks poeng: 1

18 CVE and CVSS (1 point)

Which of following most accurately describe the purposes of CVE and CVSS?
Velg ett alternativ:

- CVSS provides a score that indicates the severity of a vulnerability. CVE integrates all the security tools available in an organization and automates incident responses.
- CVSS is a "low and slow" style of attack executed to infiltrate a network and remain inside undetected. CVE is a list of publicly known vulnerabilities containing ID numbers, descriptions, and references.
- CVSS provides a list of top vulnerabilities. CVE is a list of scores for vulnerabilities in a system.
- CVSS provides a score that indicates the severity of a vulnerability. CVE is a list of publicly known vulnerabilities containing ID numbers, descriptions, and references. ✔

Maks poeng: 1

19 Security requirements (1 point)

What is a good security requirement?
Velg ett alternativ:

- Defining the choice of protection mechanism
- Stating what should be achieved, not how ✔
- A zero-knowledge proof
- A functional requirement
- Stating what should not happen to the system

Maks poeng: 1

20 CIA (1 point)

Which of the following describes the CIA triad when applied to software security?
Velg ett alternativ:

- Confidentiality deals with countermeasures to prevent denial of service to authorized users, integrity prevents unauthorized modification, and availability prevents unauthorized access.
- Confidentiality prevents unauthorized modification, integrity prevents unauthorized access, and availability deals with countermeasures to prevent denial of service to authorized users.
- Confidentiality prevents unauthorized access, integrity prevents unauthorized modification, and availability deals with countermeasures to prevent unauthorized access.
- Confidentiality prevents unauthorized access, integrity prevents unauthorized modification, and availability deals with countermeasures to prevent denial of service to authoriz ✔ users.

Maks poeng: 1

21 Mitigating Risks (1 Point)

In a scenario where a cyber attack has already compromised a company's database, which of the following countermeasures would provide the least effective return of investment (ROI) in terms of mitigating the damage caused by the breach?

Velg ett alternativ:

- Conducting regular vulnerability assessments and penetration testing
- Deploying endpoint protection solutions and intrusion detection systems
- Investing in incident response and digital forensics capabilities
- Pursuing legal action against the attackers. ✔
- Implementing network segmentation and access controls

Maks poeng: 1

22 Session hijacking (1 point)

A web developer is looking to mitigate the risk of session hijacking attacks on their website. Which of the following options would be effective in preventing session hijacking?
Velg ett alternativ:

- Ensuring that only AES is used to encrypt TLS traffic
- Setting the "HttpOnly" and "secure" flags on session cookies ✔
- Signing the website certificate with a quantum-safe signature algorithm
- Deploying the website on a blockchain
- Enforcing a password policy of minimum 16 characters

Maks poeng: 1

23 Buffer overflow protection (1 point)

What are some recommended ways of defending against buffer overflow attaks?

Velg ett alternativ:

- Use parameterized queries, limit access to memory, escape special characters, sanitize all input and ouput.
- Use non-standard C functions to manipulate strings, such as strcpy and strcat. These will not lead to buffer overflow vulnerabilities found in standard C functions, such as strncpy and strncat.
- Close all unused ports in the firewall, reduce the number of buffers, fine programmers making coding mistakes.
- Use safe functions, leverage defences in compilers, use static analysis tools, rewrite in a type-safe language. ✔

Maks poeng: 1

24 Symmetric encryption (1point)

Which of the following is a disadvantage of the symmetric encryption compared to asymmetric encryption?

Velg ett alternativ:

- Key size
- Key strength
- Speed
- Key management ✔

Maks poeng: 1

25 Vulnerabilities (1 point)

Consider the following code snippet:

```
#include <stdio.h>
#include <string.h>
int main() {
  char data[5];
  strcpy(data, "Hello World");
  printf("%s\n", data);
  return 0;
}
```

What is the security vulnerability in this code and how can it be prevented?

Velg ett alternativ:

- The security vulnerability in this code is Cross-Site Scripting (XSS), which allows an attacker to inject malicious scripts into a web page viewed by other users. To prevent this vulnerability, the code should sanitize user input and encode any output to prevent the execution of malicious scripts.
- The security vulnerability in this code is buffer overflow, which allows an attacker to overwrite memory beyond the bounds of the buffer and potentially execute arbitrary code or cause a denial of service. To prevent this vulnerability, the code should use safe ✔ functions, such as strncpy() and strlcpy(), to copy strings and ensure that the buffer is not overflowed.
- The security vulnerability in this code is SQL injection, which allows an attacker to manipulate the database by sending malicious SQL queries. To prevent this vulnerability, the code should use parameterized queries and input validation to ensure that user input is safe to use in database operations.

Maks poeng: 1

26 Captcha (1 point)

Consider a web application that allows users to create accounts, login, and access sensitive data. Which of the following statements is true about the use of captchas and other security measures in secure coding practices?

Velg ett alternativ:

- Captchas can be effective in preventing automated attacks, but should not be relied upon as the sole means of protecting user data. Additional security measures, such as input validation, parameterized queries, and user authentication and authorization, should also ✔ be used.
- Captchas are effective in preventing automated attacks, but can also be bypassed by sophisticated attackers using machine learning or other advanced techniques. Therefore, they should not be used in secure coding practices.
- Captchas are unnecessary and can actually decrease the security of a website by creating a false sense of security, and should not be used in secure coding practices.
- Captchas are an effective security measure that can prevent automated attacks and protect user data, and should be used as the primary means of preventing such attacks.

Maks poeng: 1

27 Injection attack (1 point)

A web application allows users to search for files on the server by entering a file name into a search form. The application takes the user's input and runs it as a command on the server using the function system(). Which of the following inputs would be an example of a successful command injection attack?

Velg ett alternativ:

- "file.txt"
- "file.txt && echo 'hello'"
- "file.txt | grep 'secret'"
- "file.txt; rm -rf /" ✔

Maks poeng: 1

28 Crypto concepts (1 point)

Which statement regarding cryptography concepts is FALSE?

Velg ett alternativ:

- Symmetric key algorithms use the same private key for encryption and decryption.
- Symmetric key algorithms are typically faster than asymmetric systems.
- ECC is an example of an asymmetric public key cryptosystem.
- Symmetric key algorithms are often referred to as public key algorithms. ✔

Maks poeng: 1

29 Vulnerabilities (1 point)

Consider the following code snippet:

```
from django.shortcuts import render
from django.http import HttpResponseRedirect
from django.urls import reverse
from .forms import ContactForm
def contact(request):
    if request.method == 'POST':
        form = ContactForm(request.POST)
        if form.is_valid():
            # Do something with the form data, like saving it to a database
            name = request.POST.get('name')
            email = request.POST.get('email')
            message = request.POST.get('message')
            return HttpResponseRedirect(reverse('contact_thanks'))
    else:
        form = ContactForm()
    return render(request, 'contact.html', {'form': form})
def contact_thanks(request):
    return render(request, 'contact_thanks.html')
```

What is the security vulnerability in this code and how can it be prevented?

Velg ett alternativ:

- The security vulnerability in this code is Cross-Site Request Forgery (CSRF), which allows an attacker to trick a user into performing unintended actions on a website. To prevent this vulnerability, the code should use CSRF tokens to ensure that form submissions are coming from legitimate sources. ✔
- The security vulnerability in this code is Cross-Site Scripting (XSS), which allows an attacker to inject malicious scripts into a web page viewed by other users. To prevent this vulnerability, the code should sanitize user input and encode any output to prevent the execution of malicious scripts.
- The security vulnerability in this code is SQL injection, which allows an attacker to manipulate the database by sending malicious SQL queries. To prevent this vulnerability, the code should use parameterized queries and input validation to ensure that user input is safe to use in database operations.

Maks poeng: 1

30 Cryptography (1 point)

Which of the following methods is NOT a recommended approach for generating cryptographic keys?

Velg ett alternativ:

- Deriving keys from a passphrase using a key derivation function
- Collecting entropy from user-generated input, such as mouse movements or keyboard strokes.
- Employing a software-based secure pseudo-random number generator with unique seeds
- Using a hardware random number generator
- Reusing a previously generated key for a new encryption task ✔

Maks poeng: 1

31 Threat agents (1 point)

Which of the following statements best describe the characteristics of different threat agents?

Velg ett alternativ:

- Geeks are driven by curiosity, have technical skills and unlimited resources. Cyber warriors are malicious individuals or groups who seek to exploit vulnerabilities in systems for personal gain or to cause harm. Insiders may be motivated by financial gain, revenge, or ideology and can be particularly difficult to detect and prevent.
- Terrorists have limited skills, but can be highly motivated and have enough resources to finance others to perform cyber attacks. Geeks are individuals who perform hacking activities legally and with the intention of improving security. Hackers-for-hire are individuals or groups who offer their services to conduct cyber attacks on behalf of others. ✔
- Insiders know the systems well and have access, and therefore do not many resources to perform attacks against their own organisation. Terrorists use methods such as penetration testing, social engineering, and vulnerability scanning. Spooks are hired by organizations to identify and exploit vulnerabilities in their systems in order to improve security.
- CEO criminals are highly skilled and motivated to spy on their own employees. Geeks are individuals who perform hacking activities for personal gain or to cause harm. Script Kiddies are typically young or inexperienced individuals who use pre-packaged tools or scripts to launch simple attacks on websites or online services.
- Swamps are associated with online harassment and bullying. Often very skilled and with many resources. Crooks are motivated by financial gain and may target individuals or organizations to steal sensitive data or extort money. Cyber warriors are independent hackers that attack other systems mainly based on their cultural beliefs.

Maks poeng: 1

32 Vulnerabilities (1 point)

Consider the following code snippet:

```
name = fetchNamefromDatabase()
print('Hello, ' + name + '!')
```

What is the security vulnerability in this code and how can it be prevented?

Velg ett alternativ:

- The security vulnerability in this code is Cross-Site Scripting (XSS), which allows an attacker to inject malicious scripts into a web page viewed by other users. To prevent this vulnerability, the code should sanitize user input and encode any output to prevent the execution of malicious scripts. ✔
- The security vulnerability in this code is Cross-Site Request Forgery (CSRF), which allows an attacker to trick a user into performing unintended actions on a website. To prevent this vulnerability, the code should use CSRF tokens to ensure that form submissions are coming from legitimate sources.
- The security vulnerability in this code is SQL injection, which allows an attacker to manipulate the database by sending malicious SQL queries. To prevent this vulnerability, the code should use parameterized queries and input validation to ensure that user input is safe to use in database operations.

Maks poeng: 1

33 Vulnerabilities (1 point)

Consider the following code snippet:

```
import xml.etree.ElementTree as ET
xml_string = input("Enter some XML: ")
root = ET.fromstring(xml_string)
```

What is the security vulnerability in this code and how can it be prevented?

Velg ett alternativ:

- The security vulnerability in this code is SQL injection, which allows an attacker to manipulate the database by sending malicious SQL queries. To prevent this vulnerability, the code should use parameterized queries and input validation to ensure that user input is safe to use in database operations.
- The security vulnerability in this code is Cross-Site Scripting (XSS), which allows an attacker to inject malicious scripts into a web page viewed by other users. To prevent this vulnerability, the code should sanitize user input and encode any output to prevent the execution of malicious scripts.
- The security vulnerability in this code is XML injection. An attacker could send a malicious XML payload that includes an external entity reference, allowing the attacker to read arbitrary files on the server. To prevent this type of attack, we can disable external entities in the XML parser ✔

Maks poeng: 1