Securitate Software

Quiz navigation

RD

Ruben Duliba

1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17 18
19

Show one page at a time

Finish review

Started on	Thursday, 19 January 2023, 8:10 AM
State	Finished
Completed on	Thursday, 19 January 2023, 8:24 AM
Time taken	14 mins 14 secs
Grade	**16.00** out of 20.00 (**80**%)

Question **1**
Complete
Mark 2.00 out of 2.00
Flag question

Select TRUE if you believe programmers should be more concerned with delivering non-vulnerable code:

Select one:
- True
- False

Question **2**
Complete
Mark 0.00 out of 1.00
Flag question

Which of the following can NOT be overwritten by a buffer overflow on a buffer allocated on the stack?
Care din urmatoarele nu poate fi suprascris de un buffer overflow pe un buffer alocat pe stiva?

Select one:
- a. Function parameters. / Parametrii de functii.
- b. Return address. / Adresa de revenire.
- c. Heap variables. / Variabile pe heap.
- d. Other local variables. / Alte variabile locale.

Question **3**
Complete
Mark 1.00 out of 1.00
Flag question

Which of the following memory zones can be affected by buffer overflows? /
Care din urmatoarele zone de memorie pot fi afectate de buffer overflow?

```
Heap
Stack / Stiva
```

Select one:
- a. Both
- b. Heap
- c. None
- d. Stack

Question **4**
Complete
Mark 1.00 out of 1.00
Flag question

When performing arithmetic operations on pointer types the following is not allowed: /
Atunci când se efectuează operații aritmetice pe tipuri de pointeri, nu sunt permise următoarele:

Select one:
- Compare two pointers. /
  Compararea a doi pointeri.
- Add integer to a pointer. /
  Adunarea unui intreg la un pointer.
- Add a pointer to a pointer. /
  Adunarea unui pointer la un pointer.
- Substract two pointers. /
  Scaderea a doi pointeri.

Question **5**
Complete
Mark 1.00 out of 1.00
Flag question

When auditing code that contains unbounded string functions the programmer: /
Când codul de audit care conține funcții de stringuri unbounded, programatorul:

Select one:
- a. these functions are safe to use, the programmer doesn't need to take action. /
  aceste funcții sunt în siguranță, programatorul nu trebuie să ia măsuri.
- b. must find out whether those functions can be reached when the size of the destination buffer can't contain the source content. /
  trebuie să afle dacă aceste funcții pot fi folosite atunci când dimensiunea buffer destinație nu poate conține conținutul sursei.
- c. must wait for an error triggered by an end user to find the bug in the code. /
  trebuie să aștepte o eroare declanșată de un utilizator final pentru a găsi eroarea în cod.
- d. must find out whether those functions can be reached when the size of the destination buffer can contain the source content. /
  trebuie să afle dacă aceste funcții pot fi folosite atunci când mărimea tamponului destinație poate conține conținutul sursei.

Question **6**
Complete
Mark 1.00 out of 1.00
Flag question

Common issues when working with C strings are: /
Cele mai comune probleme in lucrul cu stringurile in C sunt:

Select one:
- a. All of them. /
  Toate acestea.
- b. Caracter expansion. /
  Expansiunea caracterului.
- c. Unbounded copies.
- d. Incorrect pointer increment. /
  Incrementarea incorecta a pointerului.

Question **7**
Complete
Mark 1.00 out of 1.00
Flag question

On Windows platform, which of the following locations are searched when looking for DLL files loaded by applications?

Select one:
- The directory the applications is loaded from
- System32 directory
- All answers are correct
- Directories specified in PATH environment variable

Question **8**
Complete
Mark 1.00 out of 1.00
Flag question

Which of the following is the recommended form to call CreateProcess for the given example, from a security perspective? Assume that "..." contains the rest of the arguments, correcly specified.

```
A: CreateProcess(NULL, "\"C:\\Program Files\\My Applications\\my app.exe\"", ...);
B: CreateProcess(NULL, "C:\\Program Files\\My Applications\\my app.exe", ...);
```

Select one:
- neither A nor B is correct
- both are equally correct
- B
- A

Question **9**
Complete
Mark 0.00 out of 1.00
Flag question

What happens in the following example if the function check_user() returns false? Assume it runs on Linux with root privileges, and the function check_user() checks if username is present in /etc/shadow.

```
close(2);
fd = open("/etc/shadow", O_RDWR);
if (!check_user(fd, username))
        perror("Invalid user: %s\n", username);
```

Select one:
- The process can't open /etc/shadow
- The process has no unwanted behavior
- The message printed with perror is written to /etc/passwd
- The process crashes when calling close(2);

Question **10**
Complete
Mark 1.00 out of 1.00
Flag question

Time-Of-Check-To-Time-Of-Use (TOCTOU) is a vulerability caused by:

Select one:
- Using design patterns in application development
- Synchronization issues
- Complex programming logic
- Developing in a high level programming language

Question **11**
Complete
Mark 1.00 out of 1.00
Flag question

Which of the following is true about race conditions?

```
A: Race conditions could be inherent to the application logic
B: Race conditions could be triggered by (unexpected) external events
```

Select one:
- Both
- None
- B
- A

Question **12**
Complete
Mark 1.00 out of

What is two-factor authentication?
Ce înseamna doi factori de autentificare?

1.00

Flag question

Select one:

- An authentication method which replaces the password with a code sent by SMS. / O metodă de autentificare ce inlocuieşte parola cu un cod trimis prin SMS.
- An authentication method which requires the user to remember two different passwords. / O metodă de autenficiare ce necesită ca utilizatorul să țină minte două parole diferite.
- An authentication method which always requires passwords from two different users. O metodă de autentificare ce necesită întotdeauna parole de la doi utilizatori diferiți.
- An authentication method which requires an information from a different source, along with the password. / O metoda de autentificare ce necesită o informație dintr-o sursă diferită, împreună cu parola.

Question **13**

Complete

Mark 1.00 out of 1.00

Flag question

Which of the following is a part of a URL?

Select one:

- User-agent
- POST data
- Referrer
- Port

Question **14**

Complete

Mark 0.00 out of 1.00

Flag question

Considering the following SQL statement (the "id" field is provided by user)."

Se consideră următoarea instrucțiune SQL (câmpul "id" este furnizat de utilizator):

```
$sql = "SELECT * FROM users WHERE id=" . $_GET['id'];
```

Which one of following techniques may be used to find the number of columns from the table by providing a proper input the 'id' field?

Care din următoarele tehnici pot fi folosite pentru a afla numărul de coloane din tabelă furnizând input pentru câmpul 'id'?

Select one:

- 0 ORDER BY 5
- 0 UNION ALL SELECT table_name FROM information_schema.tables
- 0 OR 1=1
- 0 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL

Question **15**

Complete

Mark 1.00 out of 1.00

Flag question

Which of the following practices can NOT mitigate an SQL injection attack? (reduce the effects, or limit the potential of the attack)

Care din următoarele practici NU pot mitiga un atac de tip SQL injection? (reduce efectele sau limiteaza potentialul atacului)

Select one:

- Have the database server located on another machine. / Localizarea serverului de baze de date pe o altă mașină.
- Displaying as less error information as possible when errors occur. / Afișarea cât mai puțin detaliată a informațiilor despre erori când acestea au loc.
- Running the database server daemon as a limited user. / Rularea serverului de baze de date sub un user cu privilegii limitate.
- Encrypting sensitive data in the database. / Criptarea datelor sensibile în baza de date.

Question **16**

Complete

Mark 1.00 out of 1.00

Flag question

Is there any way session time-out could mitigate XSS attacks? (reduce the effects or potential of the attack)

Select one:

- Yes, because the injected code will expire once the session expires
- No, because after a cookie has been stolen, an attacker can perform session hijack at any time
- No, because XSS attacks have nothing to do with the session
- Yes, because a stolen cookie will contain an invalid session ID after the session expires

Question **17**

Complete

Mark 0.00 out of 1.00

Flag question

What is the difference between stored XSS and DOM-based XSS?

Select one:

- The stored XSS involves the code to be stored on the client
- DOM-based XSS is a full client-based attack
- DOM-based XSS is an attack which targets a specific web domain
- There is no significant difference between them

Question **18**

Complete

Mark 1.00 out of 1.00

Flag question

What does 'session hijacking' mean?

Ce înseamna 'session hijacking' ?

Select one:

- An attacker uses the brute force technique to log in to a web application with a specific user. / Un atactor folosește technica brute force să se logheze intr-o aplicație web cu un anumit user.
- Force a user to logout of an application he is logged in to. / Forțarea unui utilizator să se delogheze de la o aplicație la care acesta este logat.

- An attacker reuses a valid session to gain access to an application, with session information stolen from the victim. / Un atacator refolosește o sesiunea validă ca să obțină acces la aplicație, folosindu-se de informații despre sesiune furate de la victimă.
- An attacker convinces a user who's logged in to an application to perform a specific action (by sending the victim a specific URL). / Un atacator convine un utilizator logat la o aplicație sa efectueze o acțiune specifică (trimisă victimei specificând o adresă URL).

Question **19**

Complete

Mark 1.00 out of 1.00

Flag question

Which of the following should never be exposed to users, as it is considered information leakage?

Care dintre următoarele ar trebui să nu fie niciodată expuse utilizatorilor, deoarece se consideră scurgeri de informații?

Select one:

- Detailed SQL error information / Informații detaliate despre erorile SQL.
- None of those should be exposed to users / Niciuna dintre acestea nu ar trebui să fie expuse utilizatorilor.
- Comments left in code. / Comentariile rămase în cod.
- Detailed PHP error information. / Informații detaliate despre erorile PHP.

Finish review