Securitate Software

Home / My courses / SS / Lab12 / TEST 4 2022-2023

Quiz navigation

RD

Ruben Duliba

1 2 3 4 5 6
7 8 9 10

Show one page at a time

Finish review

Started on	Thursday, 12 January 2023, 11:10 AM
State	Finished
Completed on	Thursday, 12 January 2023, 11:26 AM
Time taken	16 mins 42 secs
Grade	**9.00** out of 10.00 (**90**%)

Question **1**
Complete
Mark 1.00 out of 1.00
Flag question

How can an application protect against brute force login attempts? /

Cum poate o aplicație să fie protejată împotriva încercărilor de login de tip brute force?

Select one:

○ Validate user input against SQL injection. / Să se valideze datele de intrare de la user impotriva SQL injection.

○ Validate user input against XSS attacks. / Să se valideze datele de intrare de la user impotriva atacurilor XSS.

● Limit the number of unsuccessful successive attempts / Să se limiteze numărul de încercări succesive nereușite.

○ Implement session time-out. / Să se implementeze session time-out.

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

Which of the following is NOT a part of a URL?

Select one:

○ GET data

○ Protocol

○ Server name or IP

● Cookie

Question **3**
Complete
Mark 0.00 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:

● No, because XSS attacks have nothing to do with the session

○ 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

○ Yes, because a stolen cookie will contain an invalid session ID after the session expires

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

What couldn't a XSS attack lead to?

Select one:

● Changing the layout of the page

○ Credentials theft

○ Cookie stealing

○ IFRAME injection

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

Where can a web application specify the session ID?

Unde poate specifica o aplicație web ID-ul sesiunii?

Select one:

○ A hidden POST field (in a FORM) . / Un câmp ascuns de tip POST (într-un FORM).

○ A cookie field. / Intr-un câmp de tip cookie.

○ A GET parameter. / Într-un parametru de tip GET.

● All are correct. / Toate răspunsurile sunt corecte.

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

Which of the following is considered to be the best practice to prevent CSRF attacks?

Care dintre următoarele este considerată cea mai bună practică pentru a preveni atacurile CSRF?

Select one:

○ Verifying the Referer field in the HTTP request and reject the requests that come from sources different from the application itself. / Verificarea câmpului Referer în solicitarea HTTP și respingerea solicitărilor care provin din surse diferite de aplicația în sine.

● Insert a secret token in each request, and reject the requests which don't contain the token. / Introducerea unui token secret in fiecare request și rrejectarea cererilor care nu conțin acel token.

○ Only accept POST requests, as they cannot be subject of CSRF attacks. / Acceptarea doar a cererilor de tip POST, deoarece nu pot face obiectul atacurilor CSRF.

atacurilor CSRF?

○ Implement session time-out, so that the user can't resume the session after a given period of inactivity. / Implementați un timp-out de sesiune, astfel încât utilizatorul să nu poată relua sesiunea după o anumită perioadă de inactivitate.

Question **7**
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:

○ Displaying as less error information as possible when errors occur. / Afișarea cât mai puțin detaliată a informațiilor despre erori când acestea au loc.

○ Encrypting sensitive data in the database. / Criptarea datelor sensibile în baza de date.

○ Running the database server daemon as a limited user. / Rularea serverului de baze de date sub un user cu privilegii limitate.

● Have the database server located on another machine. / Localizarea serverului de baze de date pe o altă mașină.

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

Which of the following operations could NOT be performed using SQL injection?

Care din următoarele operații nu pot fi realizate folosind SQL injection?

Select one:

○ Dump any information from the database. Dumparea oricăror informații din baza de date.

○ Authentication with any valid username. / Autentificarea cu orice nume de utilizator valid.

● Perform a MITM attack on a second machine from the network./ Efectuarea unui atac MITM pe o a doua mașina din rețea.

○ Find all column names from a specific table. / Găsirea tuturor numelor de coloane dintr-un anumit tabel.

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

Which of the following practices can mitigate an SQL injection attack? (reduce the effects, or limit the potential of the attack)

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

Select one:

○ Running the database server daemon as a privileged user. / Rularea serverului de baze de date sub un user cu privilegii sporite.

● Running the database server daemon as a limited user. / Rularea serverului de baze de date sub un user cu privilegii limitate.

○ Displaying detailed error information when errors occur. / Afișarea detaliată a informațiilor despre erori când acestea au loc.

○ Using HTTPS instead of HTTP./ Folosirea protocolului HTTPS in loc de HTTP.

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

Select TRUE:

Select one:

● True

○ False

Finish review

◄ Lab11 - Exerctii 2

Jump to...

Colocviu 2021-2022 ►

You are logged in as Ruben Duliba (Log out)
SS
Data retention summary