Kennis Check Blok 8

Cyber Security

Hoofdstuk 1: Wat is Cyber Security?

1. Wat is de primaire focus van Cyber Security?

- a) Het beschermen van websites tegen computer-bugs
- b) Het beschermen van computersystemen tegen aanvallen en misbruik.
- c) Het ontwikkelen van nieuwe softwareprogramma's.
- d) Het beheren van netwerkinfrastructuur.

Antwoord

b) Het beschermen van computersystemen tegen aanvallen en misbruik.

2. Welke van de volgende cyberaanvallen omvat het misleiden van iemand om wachtwoorden af te geven, vaak via nep-e-mails?

- a) Malware
- b) DDoS-aanval
- c) Phishing
- d) SQL-injection

Antwoord

c) Phishing

Welke term wordt gebruikt voor software die ontworpen is om ongevraagd advertenties te tonen en je naar bepaalde webwinkels stuurt?

- a) Adware
- b) Spam
- c) Malware
- d) Commerceware

Antwoord

c) Adware

Welke vorm van malware kan zichzelf verspreiden naar andere bestanden of programma's zodra het op een computer is geïnstalleerd?

- a) Worm
- b) Spyware
- c) Virus
- d) Adware

Antwoord

c) Virus

Hoofdstuk 2: HTTPS en netwerkveiligheid

3. Wat is het belangrijkste verschil tussen HTTP en HTTPS?

- a) HTTPS is alleen voor professionele websites, HTTP voor persoonlijke.
- b) HTTPS staat voor HyperText Transfer Protocol Secure en versleutelt de communicatie tussen browser en server.
- c) HTTP is sneller dan HTTPS.
- d) HTTP gebruikt een SSL-certificaat, HTTPS niet.

Antwoord

b) HTTPS staat voor HyperText Transfer Protocol Secure en versleutelt de communicatie tussen browser en server.

4. Waarvoor biedt HTTPS geen bescherming?

- a) Het onderscheppen van ingevulde wachtwoorden door derden.
- b) Het veranderen van informatie terwijl deze onderweg is.
- c) Het downloaden van virussen of malware.
- d) Verbinding maken met de echte website in plaats van een nepserver.

Antwoord

c) Het downloaden van virussen of malware.

Hoofdstuk 3: Encryptie

5. Wat is de definitie van encryptie?

- a) Het proces van het verbergen van bestanden op een computer.
- b) Het omzetten van gegevens zodat ze onleesbaar zijn voor onbevoegden, tenzij men de juiste ‘sleutel’ heeft.
- c) Het back-uppen van gegevens naar een externe schijf.
- d) Het controleren van de integriteit van gegevens.

Antwoord

b) Het omzetten van gegevens zodat ze onleesbaar zijn voor onbevoegden, tenzij men de juiste ‘sleutel’ heeft.

6. Welk type encryptie gebruikt dezelfde sleutel voor zowel versleuteling als ontsleuteling?

- a) Asymmetrische encryptie
- b) Hash-encryptie
- c) Symmetrische encryptie
- d) Kwantumencryptie

Antwoord

c) Symmetrische encryptie

Hoofdstuk 4: Hashing

7. Waarom wordt hashing vaak gebruikt voor het opslaan van wachtwoorden?

- a) Omdat de wachtwoorden dan eenvoudig terug te rekenen zijn voor de gebruiker.
- b) Omdat het een eenrichtingsversleuteling is die niet terug te rekenen is naar het origineel.
- c) Omdat het wachtwoorden comprimeert om opslagruimte te besparen.
- d) Omdat het helpt bij het snel ophalen van verloren wachtwoorden.

Antwoord

b) Omdat het een eenrichtingsversleuteling is die niet terug te rekenen is naar het origineel.

8. Hoe controleert een systeem een ingevoerd wachtwoord als het opgeslagen wachtwoord gehasht is?

- a) Het systeem probeert de opgeslagen hash terug te rekenen naar het originele wachtwoord.
- b) Het systeem stuurt een resetlink naar het e-mailadres van de gebruiker.
- c) Het systeem zet het ingevoerde wachtwoord om met de hash-functie en vergelijkt het resultaat met de opgeslagen hash.
- d) Het systeem vraagt de gebruiker om een tweede authenticatiefactor.

Antwoord

c) Het systeem zet het ingevoerde wachtwoord om met de hash-functie en vergelijkt het resultaat met de opgeslagen hash.

Hoofdstuk 5: Brute Force-aanvallen en Loginbeveiliging

9. Wat is een brute force-aanval?

- a) Een aanval waarbij een server wordt overspoeld met aanvragen.
- b) Een aanval waarbij kwaadaardige software op een systeem wordt geïnstalleerd.
- c) Een aanval waarbij systematisch heel veel verschillende wachtwoorden worden geprobeerd om toegang te krijgen.
- d) Een aanval waarbij via een formulier een database wordt gehackt.

Antwoord

c) Een aanval waarbij systematisch heel veel verschillende wachtwoorden worden geprobeerd om toegang te krijgen.

10. Welke van de volgende is ***geen*** methode om brute force-aanvallen te voorkomen?

- a) Een limiet stellen op het aantal pogingen.
- b) Tijdelijk een gebruiker of IP-adres blokkeren.
- c) Twee-factor authenticatie toepassen.
- d) Het gebruik van $_GET voor het versturen van inloggegevens.

Antwoord

d) Het gebruik van $_GET voor het versturen van inloggegevens.

Hoofdstuk 6: Rainbow tables

11. Wat is een rainbow table?

- a) Een lijst van alle mogelijke wachtwoorden.
- b) Een database van gehackte IP-adressen.
- c) Een lijst van veelgebruikte wachtwoorden met hun bijbehorende hashes.
- d) Een hulpmiddel om SSL-certificaten te genereren.

Antwoord

c) Een lijst van veelgebruikte wachtwoorden met hun bijbehorende hashes.

12. Waarom zijn rainbow tables gevaarlijk voor wachtwoordbeveiliging?

- a) Ze zorgen ervoor dat servers overbelast raken.
- b) Ze maken het mogelijk om gehashte wachtwoorden snel terug te vertalen naar het origineel als het wachtwoord in de tabel staat.
- c) Ze installeren malware op het systeem van de gebruiker.
- d) Ze versleutelen de communicatie tussen de gebruiker en de website.

Antwoord

b) Ze maken het mogelijk om gehashte wachtwoorden snel terug te vertalen naar het origineel als het wachtwoord in de tabel staat.

Hoofdstuk 7: Salting en encryptie

13. Wat is het hoofddoel van 'salting' bij het hashen van wachtwoorden?

- a) Om het hash-algoritme complexer te maken.
- b) Om ervoor te zorgen dat hetzelfde wachtwoord elke keer een unieke hash krijgt, wat rainbow tables minder effectief maakt.
- c) Om de snelheid van het hashen te verhogen.
- d) Om te controleren of een wachtwoord sterk genoeg is.

Antwoord

b) Om ervoor te zorgen dat hetzelfde wachtwoord elke keer een unieke hash krijgt, wat rainbow tables minder effectief maakt.

14. Hoe wordt een gehasht wachtwoord met een 'salt' gecontroleerd bij het inloggen?

- a) Het systeem probeert de opgeslagen hash te ontsleutelen met de salt.
- b) Het ingevoerde wachtwoord wordt gehasht zonder de salt en vergeleken met de opgeslagen hash.
- c) Het ingevoerde wachtwoord wordt opnieuw gehasht samen met dezelfde opgeslagen salt, en het resultaat wordt vergeleken met de opgeslagen hash.
- d) De gebruiker wordt gevraagd om de salt handmatig in te voeren.

OOP

Wat betekent OOP en hoe verschilt het van procedureel programmeren?

OOP staat voor *Objectgeoriënteerd programmeren*. In plaats van functies en variabelen apart te gebruiken, bundel je bij OOP data en gedrag in objecten. Zo kun je code beter organiseren, hergebruiken en opsplitsen in logische blokken .

Wat is een klasse in OOP?

Een klasse is een blauwdruk of sjabloon waarin je beschrijft welke gegevens (*properties*) en functies (*methods*) een object moet hebben .

Wat is een object?

Een object is een concreet exemplaar van een klasse, gemaakt met new. Je kunt meerdere objecten maken van dezelfde klasse, elk met eigen waarden .

Hoe noem je in OOP een variabele en een functie binnen een klasse?

In OOP noem je variabelen **properties**, en functies **methods**

Wat is encapsulation?

Encapsulation betekent dat je de data (properties) van een object beschermt. Je maakt gegevens vaak private en gebruikt methods om ze gecontroleerd te lezen of aanpassen .

Wat is het verschil tussen public en private properties/methods?

- **public**: toegankelijk en aanpasbaar van buiten de class.
- **private**: alleen toegankelijk binnen de class zelf. Dit beschermt de interne gegevens.

Waarom is OOP handig bij grote projecten?

Omdat je code makkelijker kunt organiseren in logische blokken (objecten), hergebruiken, uitbreiden en onderhouden. Daardoor is je programma stabieler en schaalbaarder .

Waarvoor genbruik je '$this' -> in PHP?

`$this->` verwijst naar een property of een object uit **dit** object. Met dit object wordt bedoeld het object waar `$this->` in staat.

Opdracht

Maak de kennis-check.

Inleveren

Aan het einde van de kennis-check ontvang je een certificaat. Maak een schermafdruk en lever deze in.

Revision #4
Created 1 July 2025 03:37:27 by Max
Updated 4 July 2025 06:00:49 by Max