higher education & training

Department:
Higher Education and Training
REPUBLIC OF SOUTH AFRICA

NASIENRIGLYN

NASIONALE SERTIFIKAAT (BEROEPSGERIG)

MULTIMEDIADIENSTE
NKR VLAK 4

20 November 2024

Hierdie nasienriglyn bestaan uit 8 bladsye.

Kopiereg voorbehou

AFDELING A

VRAAG 1

1.1	1.1.1	Waar
	1.1.2	Waar
	1.1.3	Onwaar
	1.1.4	Waar
	1.1.5	Onwaar
	1.1.6	Waar
	1.1.7	Onwaar
	1.1.8	Waar
	1.1.9	Waar
	1.1.10	Onwaar
	1.1.11	Waar
	1.1.12	Onwaar
	1.1.13	Waar
	1.1.14	Waar
	1.1.15	Waar

(15 × 1) (15)

1.2	1.2.1	C
	1.2.2	B
	1.2.3	B
	1.2.4	B
	1.2.5	D
	1.2.6	C
	1.2.7	C
	1.2.8	B
	1.2.9	A
	1.2.10	D

(10 × 1) (10)
[25]

TOTAAL AFDELING A: 25

AFDELING B

VRAAG 2

2.1 2.1.1 FTP-bedieners is sagtewareoplossings wat gebruik word om lêers op die internet oor te plaas. FTP-bedieners het twee funksies, naamlik “gee” en “kry”. Dit stel die kliënt se toestel in staat om lêers na die bediener op te laai (put) en lêers van die bediener na die kliënt se toestel af te laai (get).

2.1.2 IP-adresse vir nuwe rekenaars of masjiene wat van een subnet na ’n volgende hervestig word, moet per hand sonder DHCP gestel word. IP-adresse vir rekenaars wat aan die netwerk onttrek word, moet per hand herwin word. Hierdie hele proses is geoutomatiseer en word sentraal deur gebruikmaking van DHCP bestuur.

2.1.3 Die doel van DNS is om ’n domeinnaam in die toepaslike IP-adres oor te sit. Dit vind plaas deur die DNS-rekords van die verlangde domein na te slaan. Daar is tipies agt stappe in hierdie DNS-naslaanproses wat die inligtingspad van die oorsprong-webblaaier na die DNS-bediener en weer terug volg.

2.1.4 E-posprotokolle, wat vir die bediener beduie hoe om inkomende versoeke te verwerk, waarheen om die boodskappe te roeteer en hoe om hulle na die aangewese poskliënt te stuur, word deur posbedieners gebruik om e-posboodskappe tussen poskliënte te vervoer. ’n E-posbediener, ook bekend as ’n posoordrag-agent, MTA, posvervoer-agent, posroeteerder of internetposbode (internet mailer), is ’n toepassing wat inkomende e-pos van plaaslike gebruikers en afstandsenders ontvang en uitgaande boodskappe vir aflewering aanstuur.

2.1.5 Webbedieners word oor die algemeen gebruik om HTTP/HTTPS-kliëntstelselversoeke en -response te hanteer en te administreer. ’n Webbediener stoor en beskerm ook webwerfdata. ’n Webbediener kan belangrike webwerfdata teen ongemagtigde gebruikers beveilig. Die primêre rol van ’n webbediener is om verlangde inligting of webblaaie te stoor, te verwerk en by eindgebruikers af te lewer. Alle webwerfdata word op ’n fisieke webbediener gestoor om die veiligheid daarvan te verseker.

(5 × 2) (10)

2.2 2.2.1

Toestel	Funksie	Voorbeeld
Herhaler	’n Herhaler regenereer en versterk seine om die afstand te verleng waaroor data kan beweeg sonder om te degradeer. Dit funksioneer op die fisieke vlak (Vlak 1) van die OIV-model.	’n Herhaler kan in ’n lang kabel tussen twee geboue gebruik word om die seinsterkte te versterk.
Roeteerder	’n Roeteerder lei/stuur datapakkies tussen verskillende netwerke en neem besluite op grond van IP-adresse. Dit funksioneer op die netwerkvlak (Vlak 3) van die OIV-model.	’n Tuisroeteerder verbind ’n plaaslike tuisnetwerk met die internet, ken plaaslike IP-adresse toe en bestuur verkeer.

(6)

2.2.2

Toestel	Funksie	Voorbeeld
Skakelaar	'n Skakelaar verbind meerdere toestelle binne 'n lokalearea-netwerk (LAN) en gebruik MAC-adresse om data na die korrekte bestemming te stuur. Dit funksioneer op die dataskakelvlak (Vlak 2) van die OIV-model.	'n Ethernet-skakelaar in 'n kantoornetwerk verbind rekenaars, drukkers en bedieners, en stel hulle in staat om doeltreffend te kommunikeer.
Brug	'n Brug verbind en filter verkeer tussen twee of meer netwerksegmente, verminder botsings en bestuur verkeer meer doeltreffend. Dit funksioneer op die dataskakelvlak (Vlak 2) van die OIV-model.	'n Brug kan 'n bedrade netwerk met 'n draadlose netwerk verbind, en die netwerk uitbrei sonder om botsings tussen die twee segmente toe te laat.

(6)

✓✓ vir 'n funksie van elke toestel
✓ vir 'n voorbeeld van elke toestel (3 x 4)

2.3 'n Draadlose LAN (WLAN) is 'n rekenaarnetwerk wat draadlose kommunikasie gebruik om twee of meer toestelle te verbind om 'n lokalearea-netwerk binne 'n bepaalde streek te vorm, byvoorbeeld 'n huis, skool, rekenaarlaboratorium, kampus of sakegebou. (3)

[25]

VRAAG 3

3.1 3.1.1

```
SELECT✓ empName,✓ birthDate,✓ Salary✓
FROM employee✓
```

(5)

3.1.2

```
SELECT *✓
FROM employee✓
ORDER BY✓ empNo ASC✓
```

(4)

3.1.3

```
SELECT  empName ✓
FROM Employee✓
WHERE Salary✓ > R5 000✓
```

(4)

3.1.4

```
INSERT INTO employee✓ (empNo,✓ empName,✓ birthDate,✓ Salary✓)
VALUES✓ (800331,✓ Tshego,✓ 23/09/1995,✓ R3 600✓)
```

(10)

3.2 Normalisering is die proses waarvolgens data in 'n databasis gerangskik word, wat insluit om tabelle te skep en skakels tussen daardie tabelle te bou op grond van reëls wat daarop gerig is om die data te beveilig terwyl dit ook die databasis meer buigsaam maak deur oortolligheid en inkonsekwente afhanklikheid te verwyder. (2)

[25]

VRAAG 4

4.1 4.1.1 Dit is ’n voorbeeld van ’n swak ontwerpte webblad. (2)

4.1.2
- Die webwerf het ’n deurmekaar uitleg met geen fokuspunt wat die gebruiker se oog vang nie. Die uitleg is te besig, wat dit verwarrend maak.
- Die versteekte navigasiespyskaart maak dit moeilik en vertraag die gebruiker as dit oopgemaak moet word om toegang tot opsies te kry.
- Die gebrek aan kleurkontras maak die webtuiste vervelig. Dit is nie kreatief nie en die gebruiker sal vinnig belangstelling verloor.
- Nie-responsiewe ontwerp is ’n nadeel as die webtuiste op verskillende toestelle met verskillende skermgroottes besigtig word, aangesien dit nie by die skermgrootte aanpas nie.
- Inkonsekwente lettertipes en swak ontwerp, omdat dit verwarrend vir die gebruiker is wanneer daar geen konsekwente struktuur op die bladsy is nie.
- As daar ’n gebrek aan gebruikersentrisiteit op ’n webblad is, is die webblad nie gebruikersvriendelik nie en sal gebruikers dit moeilik vind om te gebruik en te navigeer.
- Besoekers kom na jou webwerf om iets te koop, oor jou produk uit te vind, op ’n nuusbrief in te teken of om ’n pos aansoek te doen. Swak webwerfontwerp is waarskynlik te blameer as hulle sukkel om enige van hierdie take te verrig.
- Webwerwe met swak bruikbaarheid kan groot frustrasie veroorsaak en selfs beteken dat jou besoekers vinnig vertrek. (Enige 5 × 2) (10)

4.1.3 Sommige kleiner toestelle kan dikwels nie raampies hanteer nie omdat die skerm nie groot genoeg is om verdeel te word nie. Soms vertoon die bladsy anders op verskillende rekenaars gevolg van skermresolusie wat verskil. Die webblaaier se *Back*-knoppie werk dalk nie soos die gebruiker hoop dit sal nie. Daar is steeds enkele webblaaiers wat nie raamtegnologie ondersteun nie. (3)

4.2.1 Die DOCTYPE-verklaring dui vir die webblaaier aan in watter HTML-weergawe die bladsy geskryf is. Dit verseker dat verskillende webblaaiers die webblad op dieselfde manier parseer. (2)

4.2.2 Hierdie reël inisieer ’n porboks (prompt box) wat die gebruiker in staat stel om ’n naam in te tik. (2)

4.2.3 Reël 13 word slegs uitgevoer as die gebruiker nie ’n naam in die porboks intik nie. (3)

4.2.4 Reël 20 skep ’n knoppie waarop die gebruiker sal klik. Hierdie knoppie sal die funksie askUserName inisieer, wat ’n porboks sal vertoon om die gebruiker te versoek om ’n naam in te tik. (3)

[25]

VRAAG 5

5.1
```
<!DOCTYPE html>✓
<html>
<body>✓

<h1>The Happy Birthday Song</h1>✓

<p>Click on the play button to Play Happy Birthday Song</p>✓

<audio controls>✓
  <source src✓ ="birthday.mp3"✓ type="audio/mpeg✓">

</audio>✓
</body>
</html>✓
```
(10)

5.2
```
<!DOCTYPE html>
<html>
<body>

<h1>Enter Your email and Password to Proceed</h1>✓

<form>✓
 <label for="email">Email:</label>✓
 <input type="email"✓ id="email"✓ name="email✓"><br><br>
 <label for="pwd"✓>Password: ✓</label>
 <input type="password"✓ id="pwd"✓ name="pwd" minlength="8"✓><br><br>
 <input type="submit">✓✓
</form>
</body>
</html>
```
(12)

5.3 5.3.1 Die <footer> -merker in HTML word gebruik om ’n voetteks (footer) van HTML-dokumente te definieer. Hierdie gedeelte bevat die voetteks-inligting (outeurinligting, kopiereginligting, draers, ens). Die voetteksmerker (footer tag) word in die lyfmerker (body tag) gebruik.

5.3.2 Die <nav> -merker word gebruik om die navigasiegedeelte in HTML-dokumente te verklaar. Webwerwe het tipies dele wat aan navigasieskakels toegewys word, wat gebruikers in staat stel om die werf te navigeer. Hierdie skakels kan in ’n nav-merker geplaas word.

5.3.3 Die <time> merker word gebruik om die mens-leesbare datum/tyd te vertoon. Dit kan ook gebruik word om datums en tye in ’n masjienleesbare vorm te enkodeer.

(3 × 1) (3)

[25]

VRAAG 6

6.1 ’n Brandmuur is ’n netwerksekuriteitstoestel wat inkomende en uitgaande netwerkverkeer monitor en filter op grond van ’n organisasie se voorheen gevestigde sekuriteitsbeleide. Op sy basiesste is ’n brandmuur die versperring tussen ’n private interne netwerk en die openbare internet. (3)

6.2 6.2.1 Pakketfiltrering kan op laag 3 of laag 4 plaasvind. Een van die groot voordele van pakketfiltrering-brandmure is hul doeltreffendheid. Pakketfiltrering beheer toegang tot ’n netwerk deur die inkomende en/of uitgaande pakkette te ontleed en hulle op grond van gegewe kriteria aan te stuur of te verwerp. Nog ’n voordeel is deursigtigheid. Terwyl gebruikers bewus is van brandmure wanneer hulle ’n pakket verwerp, werk pakketfilters tipies vinnig en onopvallend, sonder om met gebruikerfunksionaliteit in te meng.

6.2.2 In ’n veilige web- of toepassing-infrastruktuur word proksiebrandmure dikwels as die eerste verdedigingslinie gebruik. Hulle beveilig die netwerk teen eksterne bedreigings, terwyl hulle ook verseker dat interne webdienste en -toepassings veilig gebruik kan word en sonder om werkverrigting te beïnvloed. ’n Proksiebediener is ’n toestel of roeteerder wat as ’n aansluitpunt tussen gebruikers en die Internet gebruik word. Gevolglik help dit om kuberindringers te verhoed om ’n private netwerk te infiltreer. Dit is ’n bediener wat as ’n ‘tussenganger’ dien tussen eindgebruikers en die webblaaie waarop hulle soektogte uitvoer en waar aanlyn bedreigings skuil. Dit verseker ook dat interne webdienste en toepassings veilig gebruik kan word en sonder om werkverrigting te raak.

6.2.3 ’n Volgendegeslag-brandmuur, of NGFW, is ’n netwerksekuriteitstelsel wat ongewenste verkeer uitfiltreer, terwyl dit ook ekstra kubersekuriteit-eienskappe voorsien. NGFW gaan verder as tipiese brandmure deur dieppakketfiltrering, geïntegreerde indringing-opsporing, toepassingsbeheer en verhoogde netwerksigbaarheid te voorsien. ’n NGFW is ’n brandmuur wat ontwerp is om beskerming te bied teen die moderne kuberbedreigings waarmee maatskappye te make het.

(3 × 3) (9)

6.3 6.3.1 Uitvissing (phishing) is die tegniek waarvolgens onwaar kommunikasies afgelewer word wat op die oog af lyk asof dit van ’n geldige en betroubare bron afkomstig is, tipies deur middel van e-pos- en teksboodskappe. Die aanvaller se doel is om geld te steel, sensitiewe data te bekom of indringerware op die slagoffer se toestel in te plant.

6.3.2 Losprysware (ransomware) is ’n tipe indringerware wat daarop gerig is om ’n gebruiker of organisasie te verhoed om toegang tot lêers op hul rekenaar te kry. Kuberaanvallers plaas organisasies in ’n posisie waar betaling van die losprys die maklikste en goedkoopste opsie is om toegang tot hul lêers te kry deur hierdie lêers te enkripteer/enkodeer en ’n losprys vir die dekripsie-/dekoderingsleutel te eis.

6.3.3 GNT-inspuiting (SQLi) is ’n tipe kuberaanval waartydens kwaadwillige GNT-kode in ’n toepassing ingespuit word, wat die aanvaller in staat stel om data in ’n databasis te sien of te redigeer. Volgens die Oop Webtoepassing-sekuriteitsprojek (Open Web Application Security Project) was inspuitingaanvalle, wat GNT-inspuitings insluit, in 2021 die derde ernstigste webtoepassing-veiligheidsrisiko.

6.3.4 Kruiswerfskrip (XSS) is ’n tipe aanval waartydens ’n kwaadwillige uitvoerbare skrip in die kode van ’n vertroude program of webwerf ingespuit word. ’n XSS-aanval word dikwels geïnisieer deur ’n kwaadwillige skakel aan ’n gebruiker te stuur en hulle uit te lok om daarop te klik. XSS-aanvalle vind plaas wanneer data ’n HTTP-toepassing vanaf ’n onbekende bron binnekom, gewoonlik ’n HTTP-versoek. Die data word in dinamiese inhoud ingesluit wat aan ’n webgebruiker gestuur word sonder om te kontroleer of dit gevaarhoudende materiaal bevat.

6.3.5 Verspreide diensweiering- (DDoS)-aanval is ’n kwaadwillige poging om gereelde verkeer na ’n spesifieke bediener, diens of netwerk te ontwrig deur die teiken of sy omringende infrastruktuur met internetverkeer te oorstroom. DdoS-aanvalle is effektief omdat dit talle gekompromitteerde rekenaarstelsels as aanvalverkeersbronne gebruik. Rekenaars en ander netwerkgekoppelde hulpbronne, soos IoT-toestelle, kan uitgebuit word. ’n DdoS-aanval kan vergelyk word met ’n onvoorsiene verkeersopeenhoping wat die hoofweg belemmer, en gewone verkeer verhoed om hul bestemming te bereik.

(5 × 2) (10)

6.4 ’n Indringing-opsporingstelsel (IDS) is ’n stelsel wat netwerkverkeer ontleed om verdagte aktiwiteit op te spoor, en genereer kennisgewings wanneer dit opgespoor word. Terwyl die belangrikste pligte van IDS die opsporing en aanmelding van teenstrydighede is, kan sekere indringing-opsporingstelsels ook optree wanneer kwaadwillige gedrag of abnormale verkeer ontdek word, soos om verkeer te beperk wat van twyfelagtige Internetprotokol- (IP) adresse afkomstig is. (3)

[25]

TOTAAL AFDELING B: 125
GROOTTOTAAL: 150

Copyright reserved