



أونیورسیتی تکنیکال ملیسیا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER II
FINAL EXAMINATION SEMESTER II
SESI 2018/2019
SESSION 2018/2019

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS <i>COURSE CODE</i>	: BITS 3613 <i>BITS 3613</i>
KURSUS <i>COURSE</i>	: TEKNIK PENGGODAMAN DAN PENCEGAHAN <i>HACKING TECHNIQUES AND PREVENTION</i>
PENYELARAS <i>COORDINATOR</i>	: Dr. MOHD ZAKI MAS'UD
PROGRAM <i>PROGRAMME</i>	: 3 BITZ
MASA <i>TIME</i>	: 2.15 PTG <i>2.15 PM</i>
TEMPOH <i>DURATION</i>	: 2 JAM <i>2 HOURS</i>
TARIKH <i>DATE</i>	: 20 JUN 2019 (KHAMIS) <i>20 JUNE 2019 (THURSDAY)</i>
TEMPAT <i>VENUE</i>	: B. KULIAH FKM 3 & 4 K. TEKNOLOGI <i>BK FKM 3&4 TECHNOLOGY CAMPUS</i>

ARAHAN KEPADA CALON:
INSTRUCTION TO CANDIDATES:

1. Kertas soalan ini mengandungi DUA (2) Bahagian. Sila Jawab SEMUA Soalan di kedua-dua Bahagian
The exam paper consists of TWO (2) PARTS. Please ALL the questions in both part
2. Sila jawab di dalam buku jawapan yang disediakan.
Please answer in the answer booklet provided.
3. Kertas soalan ini mempunyai versi dwi-bahasa.
The exam paper consists of dual-language version.

**KERTAS SOALANINI TERDIRI DARIPADA LAPAN BELAS (18) MUKA SURAT
SAHAJA (TERMASUK MUKA SURAT HADAPAN)**
THIS QUESTION PAPER CONTAINS EIGHTEEN (18) PAGES INCLUSIVE OF FRONT PAGE

(BITS 3613)

PART A: STRUCTURED QUESTIONS (25 MARKS)

INSTRUCTION: Answer *ALL* questions.

(a) Define what is Ethical Hacking.

(2 marks)

(b) Hackers can be categorized as Black Hat, Gray Hat, Script kiddies and Cyber terrorist. Describe each of the hacker category.

(4 marks)

(c) Law is defined as a rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority which implies imposition by a sovereign authority and the obligation of obedience on the part of all subjects to that authority. List **FIVE (5)** of Malaysia's Cyberlaw acts.

(5 marks)

(d) Every Open Source Software are also under the copyright protection. State **FOUR (4)** rights an open source software possess.

(4 marks)

(e) There are four methods to break a cipher code. List and briefly describes the **TWO (2)** methods an attacker can use to break a cipher code.

(4 marks)

(f) Agent Jefri Zain successfully intercept a communication between the Japanese army in the World War II and believe they are using Caesar cipher to encrypt their message. As the cryptanalyst to Agent Jefri Zain you are assigned to decrypt and find the key for the ciphertext below.

KYVI VEUV QMFL JZJR KULI ZREK LEXX RC

(6 marks)

(BITS 3613)

PART B: STRUCTURED QUESTIONS (75 MARKS)

INSTRUCTION: *Answer ALL questions.*

QUESTION 1 (25 MARKS)

Case Study 1:

3ld14b10 is a black hat hacker that has successfully exploited and penetrated a server owned by Zainal Finance and Banking Bhd (ZFBB). As the Computer Security Senior Manager of ZFBB you are asked to do an investigation on this security breach, your first task is to explain to the top management of the general scenario of how a hacking is done.

Based on the scenario above, answer the following questions.

- (a) List all the phases involved in a hacking process?

(9 marks)

- (b) Social Engineering is one of the clever manipulation of the natural human tendency to trust and it is one of the approach to gather information from a target. Briefly describe the following social engineering methods and give an example of an act that can be done using each of the method.

- i. Phishing
- ii. Baiting
- iii. Pretexting

(6 marks)

- (c) During the incident, one of the network monitoring tool in ZFBB's network infrastructure was successfully captured a series of network traffic, suspected to be the communication between 3ld14b10's machine with one of ZFBB's server. The network traffic captured is shown in Figure 1.

(BITS 3613)

No.	Time	Source	Destination	Protoc	Lengt	Info
26	0.008287	192.168.1.150	192.168.1.100	TCP	60	41929 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	0.008301	192.168.1.100	192.168.1.150	TCP	54	110 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.008354	192.168.1.150	192.168.1.100	TCP	60	41929 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	0.008394	192.168.1.100	192.168.1.150	TCP	58	3306 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
30	0.008528	192.168.1.150	192.168.1.100	TCP	60	41929 → 3306 [RST] Seq=1 Win=0 Len=0
31	0.011085	192.168.1.150	192.168.1.100	TCP	60	41929 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.011102	192.168.1.100	192.168.1.150	TCP	54	256 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.011155	192.168.1.150	192.168.1.100	TCP	60	41929 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.011168	192.168.1.100	192.168.1.150	TCP	54	995 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	0.011260	192.168.1.150	192.168.1.100	TCP	60	41929 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	0.011275	192.168.1.100	192.168.1.150	TCP	54	1720 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	0.011338	192.168.1.150	192.168.1.100	TCP	60	41929 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	0.011351	192.168.1.100	192.168.1.150	TCP	54	199 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	0.011401	192.168.1.150	192.168.1.100	TCP	60	41929 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	0.011413	192.168.1.100	192.168.1.150	TCP	54	587 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	0.011489	192.168.1.150	192.168.1.100	TCP	60	41929 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	0.011503	192.168.1.100	192.168.1.150	TCP	54	1025 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	0.011557	192.168.1.150	192.168.1.100	TCP	60	41929 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	0.011633	192.168.1.100	192.168.1.150	TCP	58	21 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
45	0.011710	192.168.1.150	192.168.1.100	TCP	60	41929 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	0.011722	192.168.1.100	192.168.1.150	TCP	54	993 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	0.011803	192.168.1.150	192.168.1.100	TCP	60	41929 → 21 [RST] Seq=1 Win=0 Len=0
48	0.014084	192.168.1.150	192.168.1.100	TCP	60	41929 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	0.014156	192.168.1.100	192.168.1.150	TCP	58	80 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
50	0.014251	192.168.1.150	192.168.1.100	TCP	60	41929 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	0.014253	192.168.1.150	192.168.1.100	TCP	60	41929 → 8980 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	0.014255	192.168.1.150	192.168.1.100	TCP	60	41929 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	0.014294	192.168.1.100	192.168.1.150	TCP	54	5900 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 1: The network traffic captured during the hacking incidents in ZFBB

Based on the network traffic captured

- i. Suggest a tool that might be used by the hackers.
- ii. Identify the hacker's IP address
- iii. What type of scanning method the hackers use?
- iv. What are the **TWO (2)** services offered by ZFSB's server?

(5 marks)

- (d) In an attempt to cover the attack track, 3ld14b10 is believed to have used some types of covering track tools to delete several logs in the server. List **FIVE (5)** possible tools that 3ld14b10 might have used to cover his/her tracks.

(5 marks)

(BITS 3613)

QUESTION 2 (25 MARKS)**Case Study 2:**

RUNBYTES Sdn. Bhd. is a renounce software house company that is expert in developing web applications. Among the standard procedures this company practice is analysing each code developed by the programmer to make sure it is written securely. As a senior programmer you need to brief the junior programmer on the task and responsibilities to write a secure code for any web application project the company is developing.

Base on the scenario above, answer the following questions.

- (a) In a web application infrastructure several components exist and each of them serve a specific function. Each has its own vulnerabilities as well. Explain **FOUR (4)** components that can possibly expose a web application and web server to exploitation.

(8 marks)

- (b) There are several methods to attack a web application. Give any **FOUR (4)** of the attack methods.

(4 marks)

- (c) In order to show an example of a vulnerable coding in a web application, you have chosen a coding snippet as shown in Figure 2 to your junior programmer.

```
1. # Define POST variables
2. uname = request.POST('username')
3. passwd = request.POST('password')
4. sql = "SELECT id FROM users WHERE username=' + uname + '' AND password=' + passwd + ''"
5. # Execute the SQL statement
6. database.execute(sql)
```

Figure 2: example of web application source code with flaws

(BITS 3613)

- i. Based on the Figure 2, identify part of the code that can be exploited.
(1 mark)
- ii. Suggest the type of web application attack that can be used to attack this code.
(1 mark)
- iii. Suggest **TWO (2)** attack payloads that you can use as an input to the application?
(2 marks)
- iv. Describe the **TWO (2)** malicious impact from the attack in Q(iii) towards the application and the server holding the web application?
(2 marks)
- v. Suggest **ONE (1)** solution to improve this code.
(1 mark)

- (d) During the demonstration session on web application attack, you showed a sample of a web application that can be exploited through its GET request in the command URL as shown in Figure 3.

`http://Alhandrobizz.com/transfer.do?acct=Zain&amount=300000`

Figure 3.

- i. How does an attacker can exploit this flaw?
(1 mark)
- ii. Suggest one tool that you can use to exploit this flaws.
(1 mark)

CONFIDENTIAL

(BITS 3613)

- (e) A web application needs a web server platform to run and the security of the web server is equally important as developing a secure web application. Give any **FOUR (4)** methods that can be applied to the web servers in order to defend against Web Server Attacks.

(4 marks)

(BITS 3613)

QUESTION 3 (25 MARKS)**Case Study 3:**

K4L1 Sdn. Bhd. is hired by Johanis Tech and Resources Sdn. Bhd. (JTRSB) to perform a penetration testing to its ICT infrastructure and info structure. Among the scope that needs to be covered by the pen tester is social engineering, wireless and wired network infrastructure and the Web server and its application. As a senior Pen Tester in K4L1 you need to explain to the Chief Information Officer of JTRSB the issues and scope related to the penetration testing.

Based on the scenario above, answer the following questions.

(a) List and Explain **THREE (3)** categories of Security Assessment .

(6 marks)

(b) List **FOUR (4)** Penetration Testing scopes K4L1 can suggest to JTRSB.

(4 marks)

(c) To start the pentest on the wireless network infrastructure your team need to first identify all the open wireless access point in the campus. State **FOUR (4)** techniques to detect open wireless networks.

(4 marks)

(d) From the open wireless acces point survey done on (c), your team found two wireless acces points that have a vulnerability in the configuration setting. Suggest **FOUR (4)** countermeasure JTRSB can apply to the wireless network for preventing future attack.

(4 marks)

(BITS 3613)

- (e) List **THREE (3)** vulnerability scanner that K4L1 can use in the penetration testing on a web application server.

(3 marks)

- (f) Penetration Testing can be done either by external or internal approach. Describe each of the approach and list the advantage and disadvantage of each of the approach.

(4 marks)

-END OF QUESTIONS-

BAHAGIAN A: SOALAN BERSTRUKTUR (25 MARKAH)

ARAHAN: Sila jawab **SEMUA** soalan

- (a) Takrifkan *Ethical Hacking*?

(2 markah)

- (b) Penggodam boleh dikategorikan sebagai *Black Hat*, *Gray Hat*, *Script Kiddies* dan *Cyber Terrorist*. Terangkan setiap kategori penggodam tersebut.

(4 Markah)

- (c) Undang-undang ditakrifkan sebagai peraturan kepada kelakuan atau tindakan yang dilakukan oleh seorang individu, ia ditetapkan atau diiktiraf secara rasmi oleh pihak berkuasa yang mempunyai bidang kuasa terhadap mereka yang dikawalselia dibawah kuasa mereka. Senaraikan **LIMA (5)** akta undang-undang siber di Malaysia.

(5 markah)

- (d) Setiap perisian terbuka adalah dilindungi dibawah perundangan hak cipta. Nyatakan **EMPAT (4)** hak cipta yang melindungi perisian terbuka.

(4 markah)

- (e) Ada empat kaedah untuk memecah sesuatu kod sifer. Senarai dan terangkan secara ringkas **DUA (2)** kaedah yang boleh diambil oleh seorang penyerang untuk memecahkan kod sifer.

(4 markah)

- (f) Agen Jefri Zain telah berjaya memintas komunikasi antara tentera Jepun dalam perang dunia II dan beliau percaya, mereka ada menggunakan sifer *Caesar* untuk menyulitkan mesej mereka. Sebagai *cryptanalyst* kepada Agent Jefri Zain anda ditugaskan untuk mendekripsi dan mencari kunci untuk kod sifer di bawah.

KYVI VEUV QMFL JZJR KULI ZREK LEXX RC

(6 markah)
SULIT

BAHAGIAN B: SOALAN BERSTRUKTUR (75 MARKAH)

ARAHAN: Sila jawab **SEMUA** soalan

SOALAN 1 (25 MARKAH)

Kajian Kes 1:

3ld14bl0 adalah seorang penggodam *blackhat* yang telah berjaya mengeksplotasi dan menembusi komputer pelayan milik syarikat Kewangan dan Perbankan Zainal Bhd (ZFBB). Sebagai Pengurus Kanan Keselamatan Komputer ZFBB anda telah diminta untuk melakukan siasatan ke atas kejadian tersebut dan tugas pertama anda adalah untuk menjelaskan kepada pihak pengurusan tertinggi senario umum tentang bagaimana penggodaman itu berlaku.

Berdasarkan kajian kes di atas, jawab semua soalan berikut.

- (a) Senaraikan semua fasa godam yang telibat dalam kejadian penggodaman tersebut?

(9 markah)

- (b) Kejuruteraan Sosial adalah salah satu kaedah yang licik untuk memanipulasi kecenderungan semulajadi manusia untuk mempercayai seorang dan merupakan salah satu pendekatan untuk mengumpulkan maklumat dari sasaran. Terangkan secara ringkas kaedah kejuruteraan sosial berikut dan berikan contoh tindakan yang boleh dilakukan menggunakan setiap kaedah tersebut.

- i. *Phishing*
- ii. *Baiting*
- iii. *Pretexting*

(6 markah)

(BITS 3613)

- (c) Semasa kejadian, salah satu alat pemantauan rangkaian dalam infrastruktur rangkaian ZFBB berjaya menangkap satu siri trafik rangkaian yang disyaki menjadi komunikasi antara mesin 31d14b10 dengan salah satu pelayan ZFBB. Trafik rangkaian ditangkap ditunjukkan pada Rajah 1?

No.	Time	Source	Destination	Protoc	Lengt	Info
26	0.008287	192.168.1.150	192.168.1.100	TCP	60	41929 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	0.008301	192.168.1.100	192.168.1.150	TCP	54	110 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.008354	192.168.1.150	192.168.1.100	TCP	60	41929 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	0.008394	192.168.1.100	192.168.1.150	TCP	58	3306 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
30	0.008528	192.168.1.150	192.168.1.100	TCP	60	41929 → 3306 [RST] Seq=1 Win=0 Len=0
31	0.011085	192.168.1.150	192.168.1.100	TCP	60	41929 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.011102	192.168.1.100	192.168.1.150	TCP	54	256 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.011155	192.168.1.150	192.168.1.100	TCP	60	41929 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.011168	192.168.1.100	192.168.1.150	TCP	54	995 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	0.011260	192.168.1.150	192.168.1.100	TCP	60	41929 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	0.011275	192.168.1.100	192.168.1.150	TCP	54	1720 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	0.011338	192.168.1.150	192.168.1.100	TCP	60	41929 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	0.011351	192.168.1.100	192.168.1.150	TCP	54	199 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	0.011401	192.168.1.150	192.168.1.100	TCP	60	41929 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	0.011413	192.168.1.100	192.168.1.150	TCP	54	587 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	0.011489	192.168.1.150	192.168.1.100	TCP	60	41929 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	0.011503	192.168.1.100	192.168.1.150	TCP	54	1025 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	0.011557	192.168.1.150	192.168.1.100	TCP	60	41929 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	0.011633	192.168.1.100	192.168.1.150	TCP	58	21 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
45	0.011710	192.168.1.150	192.168.1.100	TCP	60	41929 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	0.011722	192.168.1.100	192.168.1.150	TCP	54	993 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	0.011803	192.168.1.150	192.168.1.100	TCP	60	41929 → 21 [RST] Seq=1 Win=0 Len=0
48	0.014084	192.168.1.150	192.168.1.100	TCP	60	41929 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	0.014156	192.168.1.100	192.168.1.150	TCP	58	80 → 41929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
50	0.014251	192.168.1.150	192.168.1.100	TCP	60	41929 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	0.014253	192.168.1.150	192.168.1.100	TCP	60	41929 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	0.014256	192.168.1.150	192.168.1.100	TCP	60	41929 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	0.014294	192.168.1.100	192.168.1.150	TCP	54	5900 → 41929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Rajah 1: Trafik rangkaian yang ditangkap semasa kejadian penggodaman di ZFBB

Berdasarkan trafik rangkaian di Rajah 1:

- Cadangkan perisian yang mungkin digunakan oleh penggodam.
- Kenal pasti alamat IP penggodam
- Apakah jenis kaedah pengimbasan yang digunakan penggodam?
- Apakah **DUA (2)** perkhidmatan yang ditawarkan oleh pelayan ZFSB??

(5 markah)

(BITS 3613)

- (d) Dalam usaha untuk menutupi jejak aktiviti penggodaman, 3ld14b10 dipercayai telah menggunakan beberapa jenis perisian yang boleh memadam beberapa log di dalam komputer pelayan tersebut. Senaraikan **LIMA (5)** perisian yang 3ld14b10 mungkin gunakan untuk menutupi kesan-kesan penggodaman tersebut.

(5 markah)

SOALAN 2 (25 MARKAH)**Kajian Kes 2:**

RUNBYTES Sdn. Bhd. ialah sebuah syarikat perisian yang terkenal dan berkepakaran dalam membangunkan aplikasi web. Antara tatacara standard syarikat ini adalah menganalisis setiap kod yang dibangunkan oleh pengaturcara untuk memastikan ia ditulis dengan selamat. Sebagai pengaturcara kanan anda telah ditugaskan untuk memberi taklimat kepada pengaturcara junior mengenai tugas dan tanggungjawab untuk menulis kod selamat untuk mana-mana projek aplikasi web yang sedang dibangunkan.

Berdasarkan Kajian Kes di atas, jawab soalan-soalan berikut.

- (a) Beberapa komponen penting wujud dalam infrastruktur aplikasi web, setiap komponen mempunyai fungsi yang tertentu. Setiap komponen juga mempunyai beberapa kelemahan, Jelaskan **EMPAT (4)** komponen yang boleh mendedahkan aplikasi web dan pelayan web kepada eksplotasi.

(8 markah)

- (b) Terdapat beberapa kaedah untuk menyerang aplikasi web. Berikan mana-mana **EMPAT (4)** kaedah serangan.

(4 markah)

- (c) Untuk menunjukkan contoh kelemahan dalam pengekodan aplikasi web, anda menunjukkan keratan aturcara seperti di Rajah 2 kepada pengaturcara junior anda.

```
1. # Define POST variables  
2. uname = request.POST('username')  
3. passwd = request.POST('password')  
4. sql = "SELECT id FROM users WHERE username=''" + uname + "' AND password=''" + passwd + "'"  
5. # Execute the SQL statement  
6. database.execute(sql)
```

Rajah 2: contoh kod aplikasi web yang lemah.

(BITS 3613)

- i. Berdasarkan Rajah 2, kenalpasti bahagian kod yang boleh dieksplotasi.
(1 markah)
- ii. Cadangkan jenis serangan aplikasi web yang boleh digunakan untuk menyerang kod ini.
(1 markah)
- iii. Cadangkan **DUA (2)** muatan serangan yang anda boleh masukkan ke dalam aplikasi ini?
(2 markah)
- iv. Apakah **DUA (2)** kesan buruk yang boleh berlaku kepada aplikasi web dan pelayan web akibat daripada serangan dalam soalan (iii)?
(2 markah)
- v. Cadangkan **SATU (1)** penyelesaian untuk meningkatkan keselamatan kod ini.
(1 markah)
- (d) Semasa sesi demonstrasi serangan aplikasi web, anda telah menunjukkan contoh aplikasi web yang boleh dieksplotasi melalui permintaan *GET* dalam URL arahan, seperti ditunjukkan dalam Rajah 3.

http://Alhandrobizz.com/transfer.do?acct=Zain&amount=300000

Rajah 3.

- i. Nyatakan **SATU (1)** Jenis serangan yang boleh mengeksplotasi kelemahan ini ?
(1 markah)

(BITS 3613)

- ii. Cadangkan satu perisian yang boleh digunakan untuk mengeksplotasi kelemahan ini?

(1 markah)

- (e) Aplikasi web memerlukan platform pelayan web untuk menjalankan perkhidmatannya, platform pelayan web juga memerlukan tahap keselamatan yang sama seperti pembangunan aplikasi web. Berikan **EMPAT (4)** kaedah yang boleh diaplikasikan kepada platform pelayan web bagi mempertahankan aplikasi web dari serangan.

(4 markah)

SOALAN 3 (25 MARKAH)**Kajian Kes 3:**

K4L1 Secure Sdn. Bhd. telah diberikan tanggungjawab oleh Johannis Tech and Resources Sdn. Bhd. (JTRSB) untuk melaksanakan ujian penerobosan terhadap infrastruktur dan info struktur ICT. Antara skop yang perlu diuji adalah kejuruteraan sosial, infrastruktur rangkaian tanpa wayar dan berwayar serta keselamatan pelayan Web dan aplikasi web. Sebagai penguji penerobosan kanan dalam K4L1, anda perlu menjelaskan kepada Ketua Pegawai Maklumat JTRSB menegenai isu dan skop yang berkaitan dengan ujian tersebut.

Berdasarkan Kajian Kes di atas, jawab soalan-soalan berikut.

- (a) Jelaskan **TIGA (3)** kategori penilaian keselamatan.

(6 markah)

- (b) Senaraikan **EMPAT (4)** Skop Pengujian Penembusan yang K4L1 boleh cadangkan kepada JTRSB.

(4 markah)

- (c) Untuk memulakan pengujian penerobosan pada infrastruktur rangkaian tanpa wayar, pasukan anda perlu mengenal pasti terlebih dahulu semua pusat akses tanpa wayar di dalam kampus. Nyatakan **EMPAT (4)** teknik untuk mengesan rangkaian tanpa wayar yang terbuka.

(4 markah)

- (d) Dari pemerhatian yang dijalankan di (c), pasukan anda mendapati dua pusat akses tanpa wayar masih mempunyai konfigurasi keselamatan yang lemah . Cadangkan **EMPAT (4)** langkah untuk keselamatan yang JTRSB boleh laksanakan terhadap rangkaian tanpa wayar untuk mengelakkan dari serangan pada masa akan datang.

(6 markah)

(BITS 3613)

- (e) Senaraikan **TIGA (3)** perisian pengimbasan kelemahan yang K4L1 boleh gunakan dalam ujian penembusan pada pelayan aplikasi web.

(3 markah)

- (f) Ujian Penerobosan boleh dilakukan seacara dari luar dan juga dari dalam. Bincangkan kedua-dua pendekatan tersebut serta nyatakan kelebihan dan kekurangan setiap pendekatan.

(4 markah)

-SOALAN TAMAT-