INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

Examinations Control Office

Examination	B TECH VI SEMESTER END EXAMINATIONS REGULAR JUNE 2025 REG UG20		
Month & Year	1-Jun	**Date**	25/06/2025
Course Name	NETWORK AND WEB SECURITY		
Course Code	ACIC03	**E-Code**	5843

Instructions to Evaluators

- Evaluators should spend at least 3-5 minutes on one answer booklet during the evaluation.
- Evaluators should cross check that marks are allotted for all the attempted questions.
- The marks should be assigned fairly according to the mark distribution specified in the scheme of evaluation.
- For questions that were attempted incorrectly, evaluators are required to award zero marks.
- The evaluator must give a proper justification in case of any mistakes identified in the marks provided.

START WRITING FROM HERE

Q.No.

8a) Ans

Browser fingerprinting:

Browser fingerprinting is a technique used by the attacker where attacker can steal your data without using traditional cookies.
Here in this technique after connecting to the client by phishing, the attacker steals your id (IP address).

After securing your ip address the attaker finds your system id address.

He then clones your system and pretends to be you.

In this way the attacker can steal your data by pretending to be you. The attacker used his VPN to mask his/her real id address.

To prevent this from happening one must follow:

Q.No.

1) Not click on molish/fishy adds.

2) Not to open random links.

3) Use TOR, Brave.

4) Only click on google verified websites.

Device finger printings:

Device finger printing is another technique used by attackers.
In this technique the attacker clones the device of client and accesses all the data.

Here basically the attacker clones the clinets/users device. By cloning the device now the attacker can monitor your every move. He can see you, your texts, messages, files, etc.

Q.No.

This technique is ~~a~~ often implemented by attacker when a user ~~tryin~~ tries to download a file from a sketchy website.

We can see this technique implemented not only by attackers but also by some major companies. They implement it to enhance the users experience.

To prevent this technique from happening:

1) Do not try to downloda software from an unsafe website.

2) Don't download and open any random pdf files.

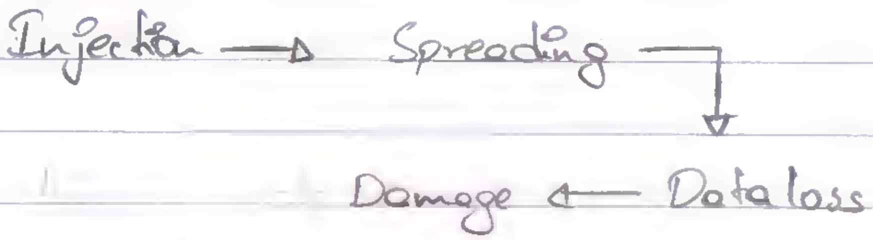
Q.No.

3a) Ans:

Viruses:

In computer science viruses refer to a kind of ~~k~~ code which either damage, steal or corrupt data from users system.

Viruses ~~xx~~ is a malware. Malware mea malicious software. Viruses is a malware which damages ~~and the~~ the computer and causes harm to the software /hardware



A ~~vo~~ virus has several stages before the damage caused by it.

1) Injection:

A small code which contains malware is injected into the system. The code is infected through either

Q.No.

http or DNS.
As these are mostly used methods.

2) Spreadings:

After code injection the code spreads accross the users system. It contiminates the system code. The code is ~~corrou~~ corrupted.

~~8) Code Data is stolen:~~

3) Data loss:

After the spreading the data of the user is either lost or stolean bye the attacker.

4) Repeation:

This process is repeated until all the data in the system is either lost or stolean.

5) Damage:

Huge damage is caused by the attacker to the user as the system is corrupted or lost or stolen. There is no gurantee that the virus

Q.No.

is eleminted. Even if small part of it survives the virus takes over the system again.

Q.No.

2a) Ans:

There are many challenges faced by the developer to detect and protect the data from falling into wrong hands.

The developer uses ~~the~~ various detection and protection system to safe guard the data.

1) DOS:

DOS which is also known as Denial of service attack used by attacks. ~~to protect~~

In this attack the attacker spams the requests to the server by which server over loads and crashes.

Clients/ users use firewalls to prevent this from happening.

We face many challenges in detecting intrusions in the network.

1) Hackers/attacker and clients are tough to identify.

Q.No.

2) Repeatedly sconning the server would slow down the server and decrease the client experience.

3) Server connot distinguish between the cliant and the attacker.

We can implement some of the methods to avoid this.

1) Port scanning

This is one of the most reliable technique as it scans the port using different methods like Nmap for virtual machine testing. By which it gives a detailed scan report and we can identify potential security risks through this technique.

2) HTTPS:

This is one of the protocol. It ~~save~~ saves the data and converts it into cypher text. By this even if the data is seen by other person they would not understand the meaning of it.

Q.No.

Key components of a real-time intrusion detection are:

1) Correctness

The system should be able to identify the attacker before the attack.

2) Effectiveness:

The system should be more effective in ~~detectil.~~ detecting the attackers.

We can implement methods likes:

1) DNS SEC : This is also known as Domain name system security network. This directly solves all the problems we face in real time error detection. It protects DNS server from getting these type of attacks.

2) NES 3 : This ~~a~~ is also known as Net 3
This is an extention for DNS SEC. It acts as an outer layer to protect and prevent any intrusions from ever happening.

Q.No.	

5a) Ans

HTTP header injection means injecting a malware into the header / web page. The header injection is usually done by injecting malware into either html header injection, sql injection, java script injection or XSS.

Html header injections: In this method the attacker attacks and injects the malware into the html code. Html is the back-bone of the web page. So by this method the attacker gets the access of the entire structure of webpage. The attacker can modify the page as they desire.

SQL injections: Here the attacker injects a malware in to the data base of the web page. Most web pages use sql or sql related database to develop the web page. Through this method the attacker gains access to the data collected by the web page. The data can now be used by the attacker as he intendeds to use it.

Q.No.

By using sql injection all the data would be in control of the attacker.

JS injections: In java script injection the attacker injects malware into js of the web page. Java script acts as the back end for the webpage. All the process in the backend is controled by java script. If the attacker attacks this part of the page the brain of the page / functionality of the / web page would be gone.

XSS: Cross ~~Syte~~ Site Scripting (XSS) is a type of Scripting used by attacker. In this attack the attacker clones the web page perfectly / almost identical to the original webpage where the client gets confused and clicks on wrong website as he enter his username and password the control of the accout goes to the attacker.

Q.No.

CSRF: It is another type of attack where the attacker tries to take over the control of the web page.

We can easily avoid all such vulerabilities if we shift towards HTTPS structure.
As HTTPS (Hypertext Transfer Protocol Secured) is an advance version of HTTP.
It resolves all the short comings of HTTP.
It gives the user more privacy and more data security.

Q.No.

10Mrks

SMTP:

It is also known as Simple Mail Transfer Protocol. Through this protocol we can share data with each other. The data share by smtp is more ~~&~~ secured.

There is a step by step process in data transfer.

1) Mail user agents:

This is a software that helps in collection of data from user. This agent collects the data from user and turns that data into cypher text. After converting the text into unreadable form this data now is transfered to next agent to continue the delivery of the data.

2) Mail transfer agents:

This is a software that helps in collection of data from one agent to other agent. This agent decides a quick and short path between user & and reciver. The agent than travels this path after reciving data from previous agent to deliver this data to another agent.

Q.No.

The agent make sures that the data is transfered successfully. This agent even protects data from malware.

Mail delivery agents:

Mail delivery agent is the one responsible for delivering the mail to the reciver. After reciving the data from the transfer agent the delivery agent unpacks the data and delivers the data [illegible] to the reciver.

Q.No.

8(b) Ans:-

If we inspect a website using browser dev tools we can find any abnormalities present in website. Like:

1) We can detect third-party tracking scripts

2) We can detecte tracking pixels.

3) We can check the security of the website.

We can do all of this by ~~p~~ performing some tests.
Tests like GUI testing is a type of testing that helps in finding any errors in the UI (User Interface) of the website.

We can also do parameter testing and test if multiple parameters of ~~same~~ same name are there/given and check the result of it then.

Q.No.

5b) Ans:

DOM in modern web applications help us in many many ways. It helps in standardize the website. It gives the standard size of containers in the web site. It tells how the web site should be by which the ~~cos~~ customer is spend more time and loving to spend that time.

HTML Script.

```
<html>
  <head>
     < title = " test.html>
     < link type = "style sheet" src = "style.css" >
  </head>
  <body>
     <h1> Welcome to our web page </h1>
     <nav>
        <td> Home </td>.
        <td> About </td>
        <td> Contact </td>
     </nav>
    <script>
    nav = iframe 1 {
```

Q.No.

```
    console.log. display(Home)
    console.log display(About)
    }
     nove= frame2 {
      console.log display (Contact)
     }.
</Script>
</body>
</html>

 CSS:

  body {
   bg colour: blue;
   font size : 24 px;
  }
   h1 {
     font weight: bold;
     font color : Red;
   }
  td {
   colour : Green;
   }
```

Q.No.	
1b) Ans	DNS ~~ch~~ cache poisoning is a type of attack performed by attacker on a dns sever.

In this attack the data from the web server is stolean.

The attacker first injects a ~~p~~ poision or a malware into the computer/server.

This poision is the malware that helps the attacker to steal the from the web page.

~~ch~~ Cache is the data that is a small amount of data that is stored by the web page to make the ~~a~~ login in future easy for client /user.

Stealing this ~~ch~~ cache means that get all the user name and passwords which are saved in the system cache by the user in there system.

We can implement DNSSEC which is the secured version of dns which is developed after dns. This over comes most of the vulnerabilities that are there in dns. This over comes and strengthens

Q.No.

the resolution of the process. Another idea is we can add an extention to enhance the security of dns which is more viable option This process does not have to to be more lengthy. This saves a lot of time. It takes less time to implement this technique.

Q.No.

2b Ans

We can scan port on a virtual machine using Nmap. We perform this scanning operation to analyze the risks and also detect potential security risks.

A virtual machine is a software where each task is performed and results are given virtually. We use virtual machines in various fields. Like we use virtual machine ~~to~~ in sports (F1 racing) we can test the performance by it. We can also save up alot of money using these virtual machines.

A test virtual machine means a virtual machine which is developed only to test and improve software.

If we scan a test virtual machine this machine would be/show somany security risks.

As we only use that machine ~~only~~ only to test but not to deploy the program

Q.No.	

Q.No.

Q.No.

Q.No.

Q.No.

Q.No.	

Q.No.	

Q.No.

Q.No.

Q.No.

Q.No.

Q.No.

Q.No.

ROUGH WORK

Content written here will not be considered for valuation