# 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** | 6021 |

### 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.

1(a) SMTP or Simple Mail Transfer Protocol is the protocol that is used in transferring the mail across different devices in a network. SMTP is used to send and receive the mail, i.e it lays the groundwork and sets the rules on how the mail is transmitted and how the exchange of informations happens. SMTP protocol has different agents that are working together and it helps the withstand of the protocol. There are three main agents in SMTP, mail users agent, mail transfer agent and mail delivery agents in SMTP. Mail User Agent (MUA) are the agents that are responsible for providing the users with the interface. The users agents are responsible for the mail. GMail, Outlook etc are known as the users agents. These users agents provide the users with the access to the SMTP protocol. The users agents form a key role in the protocol where the users can draft an email and then the users agent is responsible to show the mail to the users since it is the only users that interacts with the users. Therefore, mail users agent

Q.No.

(MUA) like GMail, Outlook etc are used by the users to interact with SMTP protocol. Mail Delivery Agent (MDA) in Simple Mail transfer protocol is the agent that overlooks the delivery and transit of the mail in SMTP. It ensures that the mail is successfully delivered to the end user from the sender and that it isn't lost. MDA also is responsible for maintaining the integrity of the SMTP protocol since its responsible to maintain the delivery pipeline of the protocol. It is responsible for delivery of packages. Mail Transfer Agent (MTA) is an agent in SMTP protocol that is responsible for relaying and then sending the mail to the user across the protocol. The MTAgent will gather the message and all of its contents along with information like its source and the destination, which will then be relayed for the delivery. Then at the destination, it will take the message and pass it to the user agent. Therefore, this is only possible because of the interaction between all this agents

Q.No.

essentially, mail users agent will relay the information and the contents to the transfer agent, it will properly identify the destination and dispatch it, transferring to the delivery agent, who is responsible for delivering the mail between users and then the transfer agent will collect and manage and send to user agent, which allows the user to view the mail. This is the interaction between mail transfer agent (MTA), mail user agent (MUA) and mail delivery agent (MDA).

1(b) DNS or Domain Name server is the distributed database that contains the IP addresses of websites corresponding with their domain names. DNS is also referred to as the phone book of the internet before it contains all the IP addresses of different websites in its database so users can access them by simply typing the domain name in the address bars. It helps the users from remembering the complex IP addresses. DNS works by, when the user enters a domain name in the browser, then the DNS

Q.No.

servers will search for its IP address in the DNS cache to check and it's not present it moves on to OS resolvers to find the respective IP address and if it is not found there either, it will redirect to the DNS resolver. Therefore, DNS plays a important in the web and is an essential aspect. Thus, DNS is prone to many attacks alone due to its importance so we have to ensure that such attacks doesn't happen and we need to mitigate the errors. DNS is prone to many attacks online like DNS spoofing, DNS cache poisoning, DNS ID hacking etc. All these attacks are performed with the malicious intent. DNS cache poisoning is the attack in which the attackers will inject the DNS servers with fake addresses and thus it poisons the DNS servers. It attack works by when a users enters a legitimate website due to the DNS cache poisoning, the IP addresses of the website and its domain names are poisoned in the DNS servers and thus,

| Q.No. | |
|---|---|
| | the users will be redirected to the attackers website. This is cache poisoning attacks. To mitigate such attacks, we need to enhance the security to DNS. We need to use good security practises (implement) and ensure that the user input is validated and sanitised before entering into the system which can attack. We also need to be vary of SQL injection and ensure that we safe our database and prevent unauthorised queries. We also need to implement DNSSEC so that it provides infrastructure for digital signature and we verify the request is legitimate. It also strengthens the resolution process because we can keep a log of the attacks and therefore we can learn and manage from the attacks will help in faster resolution in the future. It helps prevents the large-scale attack so we can mitigate the attacks and strengthen the resolution process. |
| 2(a) | Network intrusions are the phenomenon where they will be unwanted attacks or access to the network without any |

Q.No.

authorisations. Network intrusions occur when there is unauthorised request from an unknown users to access the network. These network intrusions are used by the attackers to gain access to the network to perform illeligimate actions and these attackers are often reffered to as intruders. Network intrusions are one of the most common methods to attack a website. There are several methods, therefore to detect the network intrusions in real-time. The first method, is to monitor our network and scan for any requests that are coming from any unknown or illeligimate sources. If such requests occur, they it may be a possible network intrusion. The request will aim to gain access to the website or our network and thus attack is performed on our network. Then, after scanning for any ill requests, we can check if there is any flood of messages to the servers which means the attackers are trying to overwhelm our network from requests and therefore

Q.No.

try to gain illegal access to our network. We can also try to maintain a log book of the activity and have a theoritical idea of the activity and then check if it aligns with it any check for any suspicious activity. Networks intrusion can be detected but it has its challanges, like intrusions can come in any form, so it may act legitimate and cause intrusion. If is also difficult to keep track of all the network in real time. These are the challenges of detecting intrusions. Intrusion Detection System (IDS) is the system that is responsible to identify and detect for any possible intrusions in the network. The key components are — we first scan the network and we keep file of the known intruders and check for them. If found, we detect the intrusion and notify. After scanning, we keep logs of the activity and if any suspicious activity is found, we raise the flag. Then we detect the intrusion after identifying it and we diagnose it. These are the components of real-time intrusion detection system.

Q.No.

2(b) Port scanning refers to the technique where we scan the ports of the network and deem if they're available or not for a connection. We perform port scan to analyse the network and if we establish a connection with it or not. The Nmap is also a technique used for port scanning and to determine if the ports are open or full. If the given ports are full then we can't establish a connection and we can only connect when the port is open. Here, we perform a detailed port scan using Nmap on a virtual test machine. Nmap is a port scan technique where we scan all the available ports in the network and then map the ports. These ports are mapped based on if they're open or close. After mapping the n-number of ports, then we determine if a connection can be established successfully or not. The Nmap is a great technique for a port scan because it gives us a detailed port scan report and when compared to other

Q.No.

techniques, it is faster because it is more organised. In Nmap, we scan the ports. These ports are scanned by using the SYN signals. First, SYN signals are sent to the ports and it will wait for acknowledgement. Instead of performing the entire operation, it will waits where after sending the signal, if the RST message is sent back, then it signals that the port is closed and that we cannot establish any connection. So, if any signal is not relayed then the port is open to establish the connection. So, instead of full acknowledgement, we perform partially and thus it is faster and lightweight. It also gives detailed insights. The scan report analysis shows that the ports are open to establish a connections, we can identify the potential risks before the port is not encrypted where attackers can steal our data, the ports are also visible to the attackers so he can perform DOS attack and overwhelm the ports with requests thus denying access to the legitimate requests. These are the analysis of the report.

Q.No.

3(a) Computer viruses are the type of malware where they are a piece of code that replicate rapidly once they enter or system. Computer viruses are used by attackers to gain access to the system, have unauthorised actions and perform actions with a malicious intent. Computer Virus are a self-replicating software that rapidly make copies of each other once it enters the host ecosystem. The viruses will spread to all parts of the system and try to gain access to the system. Computer Viruses can be occurred in many different ways. Viruses can be entered into a user's system when they download from malicious websites or by clicking unknown links or links from phising mails. Therefore, once the virus has entered into the system, it infects the all parts of the system by replicating rapidly and affecting the entire system. These viruses can spread from one computer to another rapidly and if one computer in a

Q.No.

network is affected, all others are prone to virus attacks. Viruses are used to control the user's system and gain unauthorised access to the user's data and the control of the system. The viruses will take control and perform actions without the user's knowledge. The Virus will replicate in the background without the user noticing. It can stay under the radar for a long time undetected, until it performs any illegal activity. Therefore, it is hard to detect and then diagnose a virus. The Lifecycle of a virus is simple. It enters the host system when they enter a malicious website and after inside the host, it begins to repeat uncontrollably and replicate until it is in every part of the system. The virus will stay dormant until the command is given by the attackers which they will perform unauthorised action and gain illegal access to the system. The virus will stay in the host system until it is removed by an antivirus software and it will perform illegitimate actions until then

| Q.No. | |
|---|---|
| | or stay dormant before moving onto another system through self-replicating and this is the lifecycle of a Computer virus and it continues. |
| 3(b) | If there are any known exploits, we have to protect the program and secure it using defensive techniques before any bad actors can identify or exploit them. Exploits are the vulnerabilities or any flaws in the program that can lead to attackers exploiting it to gain unauthorised access, bypass security regulations/measures etc. Therefore, we need to have defensive techniques to secure a sample program against known exploits. First, we need to implement good security measures, it means that we have to follow the standard set of rules and protocols to ensure that our code is free from exploits. It is part of the proactive approach to web security where instead of reacting to errors and then fixing them, we can more proactively |

Q.No.

and implement defensive programming techniques to secure our sample code against known vuns. We have to use input validation and sanitization so that we can validate the input before entering and sanitize it of any special characters that may cause any errors. We have periodically check our code and update it accordingly so that the practises don't become outdated. We also need to ensure that the packages are up-to-date and there are no redundancies that any attackers can exploit. This contributes to security by enhancing the structure of the code and that the current measures are fault-tolerant and we can effectively enhance security by following the latest standard protocols. We also need to implement the testing at the early stage because it helps the developers to identify any errors or exploits because if we use the different test cases like boundary value test cases, we can observe any misbehaviours or if it leads to any exploits the attackers can use - thereby we can ensure that our

| Q.No. | |
|---|---|
| | programming is robust and secure a sample program against known exploits. |
| 5(a) | HTTP header is the component in the HTTP protocol where it contains all the necessary information about the HTTP request and it helps in the routing of the information from the users to the servers. HTTP headers contains information like the source and its destinations, the contents of the request etc. HTTP is the protocol that is used to send information across the internet through different computers in the network. It is the pipeline for data to transfer as it provides the transmitting of the data over the internet. It contains the critical information about the route of the data. Therefore, we need to protect it from attacks from the malicious people. But HTTP headers has its own vulnerabilities which can be exploited like HTTP headers injections. HTTP headers injection is the attack where the attackers will inject the malicious code into the HTTP headers with a malicious intent. |

| Q.No. | |
|---|---|
| | The HTTP header is injected with malicious code and the code will alter the data that is present in the headers. The code will wipeout the important information and rewrite the information. With the help of HTTP header injection, the attacker will reroute the users from accessing the website to the attacker's website so that they can gain unauthorised access and perform illegal actions using the user's credentials by stealing the users data in the header. We can avoid such vulnerabilities by input validation and sanitisation where before the input is entered, we perform and validate the input to ensure that is free from any malicious code and we sanitise the input to prevent it from performing any unwarranted or unwanted actions. We need to enhance the security of the HTTP protocol so that only authorised users can access the elements. |
| 5(b) | DOM or Document Object Model is the model that is used in modern web applications |

Q.No.

to the websites that contain all the information of the website. DOM is essential in maintaining the integrity of the website and therefore it plays a key role in modern web application. DOM is used to display the contents on a website and it helps in designing the attributes of a website. It defines the attributes and the behaviour of the website. It is a client-side model that works and interacts with the servers to provide the necessary actions of a website. DOM also plays a critical role in maintaing the integrity and the security of website because it employs security measures so that the attackers can't alter DOM and attack the website. This is about the role of Document Object Model (DOM) in modern web applications.

```
!DOCTYPE
<html>
<head>
    <title> Demo Page </title>
    <style>
        header{
```

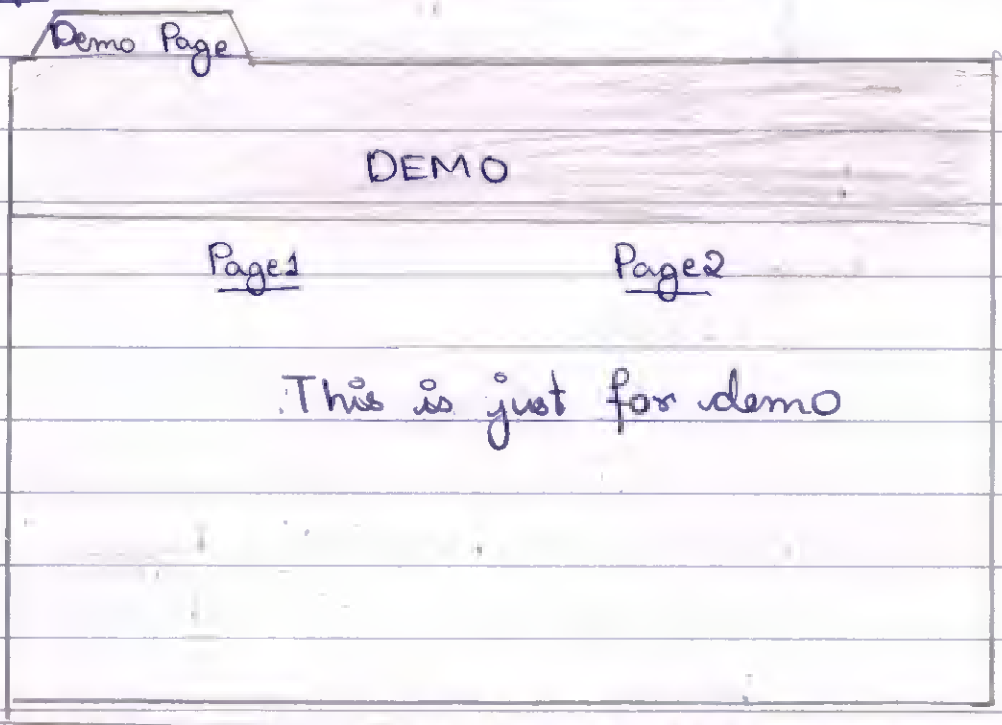
Q.No.

```
        font-color : black ;
        background: white ;
        font-family: Sans Serif ;
    }
    Body {
            font-color: blue;
            font-family: Arial;
        }
    </style>
</head>
<body>
        <header>
            <h1> DEMO </h1>
            <hr>
    <nav>  <a href="#"> Page 1 </a></nav>
    <nav>  <a href="#"> Page 2 </a> </nav>
        </header>
    <script>
            class frame {
                public static main {
                void Page 1 = echo("Moving
                                to page 1");
                void Page2 = echo("Moving
                                to Pag 2");
```

Q.No.

```
        }
    }
</script>
    <h2> This is just for demo </h2>
</body>
</html>
```

output:




7(a) HTTP parameters pollutions (HPP) is the type of attack where the HTTP server is overwhelmed with the different and large numbers of parameters so that the server gets overloaded and leads to denial of service. HTTP parameters are the parameters that contains the

Q.No.

information about the HTTP protocol that can be used to handle the information sent across the internet.

8(a) Browser fingerprinting is the technique that is used to identify and track the user across different website, even without traditional cookies. It is because the traditional cookies, that collect and store the information about the user and their behaviour across the different websites but the cookies can be deleted with relative ease so that the user identity can stay anonymous. But Browser fingerprinting is the technique that employs the browser to track the user activity. The browser is responsible to identify the user and not the individual websites or the cookies. The browser will identify the user and it will track the user's activity across the entire web browser so that it can collect the same information without using traditional cookies. The browser also has more access to our data and therefore can be used to

| Q.No. | |
|---|---|
| | identify and track users at a greater scale. Similarly, device fingerprinting is the technique, where our device is responsible to handle all our usage and it tracks the users and monitors the user continuously. Device fingerprinting will leave behind the traces of the user activity so that the user can easily be tracked across the entire device and across the different websites. Since, they have greater control over the user's activity and their requests, they essentially have the same if not more information about the users than traditional Cookies, so browsers and device fingerprinting techniques are used to identify and track users across different websites. |
| 8 (b) | A website can be inspected using the browsers dev tools that are available in the browsers. These dev tools are used to inspect and analyse the appearance / working of our websites. It is a safe to inspect our website because the dev tools prevent |

Q.No.

the user from accessing the server-side application of the server and can only interact with the client-side application where only their website is affected, leaving the other users from any adverse affects. The website provides the information about it the content of the website is structured and also helps with the styling of the website and how it appears to the users. We can inspect and modify these elements and therefore, we can play around and learn about how a website has been designed. The website also follows a componental approach, where it is divided into components and therefore each individual component of the has been independently working. It also has <script> tag which is the logic of the website which can be inspected and therefore any flaws can be found. It also has DOM (Document Object model) where 3rd party scripts or pixels are found like logics from different algorithms or photos or videos that are embedded in the website.

| 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