TASK 3 (29-08-23)

Overview of the Assignment:

Explain about any 10 web server attacks.

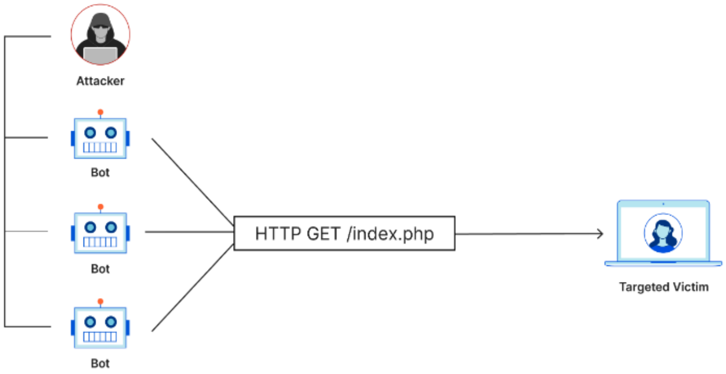
What is a WEB SERVER ?

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users.

WEB SERVER ATTACKS

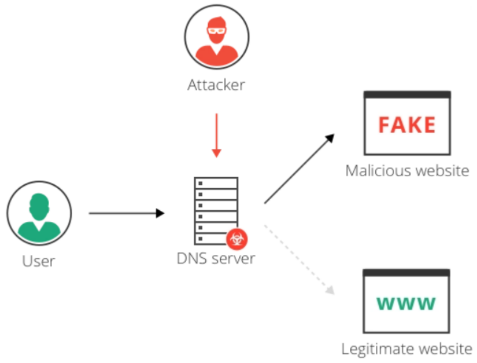
1. DoS/DDoS attack :

DoS and DDoS attacks are used to flood a web server with too much traffic that the server can't sustain. It then goes down and stops working for the intended users. An internet server Dos/DDoS attack often targets high-profile web servers like banks, credit card payment gateways, and even root name servers.



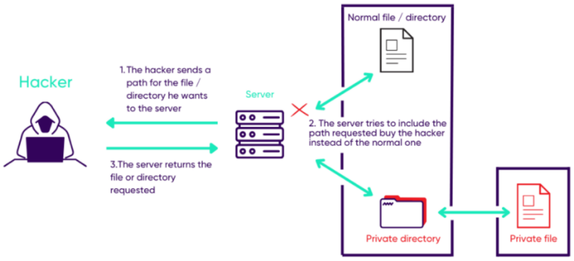
2. DNS Server Hijacking :

When the hackers exploit a DNS server and modify the mapping settings to redirect it to a rogue DNS server, it is called DNS server hijacking. Once hijacked, all the requests by the users will be sent to the rogue server and the users will be redirected to the website desired by the attackers.



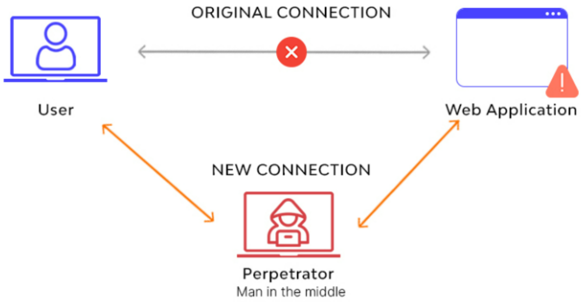
3. Directory traversal attack :

To run a web server securely, it is important to control the access to web content properly. If not controlled, the attackers can access the restricted directories by launching a directory traversal attack. It is an HTTP attack that also allows them to write and run commands outside the root directory of the server.

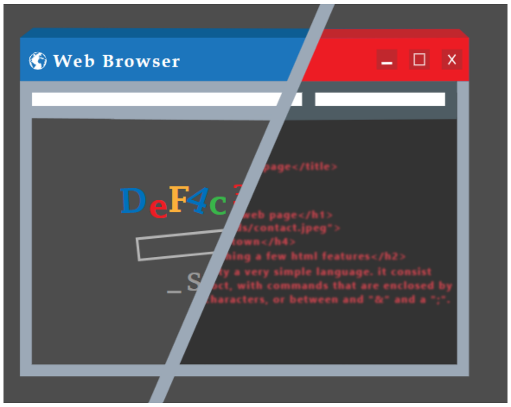

Hacker
1. The hacker sends a path for the file / directory he wants to the server
Server
3.The server returns the file or directory requested
Normal file / directory
2. The server tries to include the path requested buy the hacker instead of the normal one
Private directory
Private file

4. Man-in-the-Middle/Sniffing Attack :

Sniffing and man-in-the-middle attacks can be used to monitor and compromise the communication between the end-user and web server. Attackers can also modify the information and steal sensitive data, like banking details, contact information, credentials, etc.

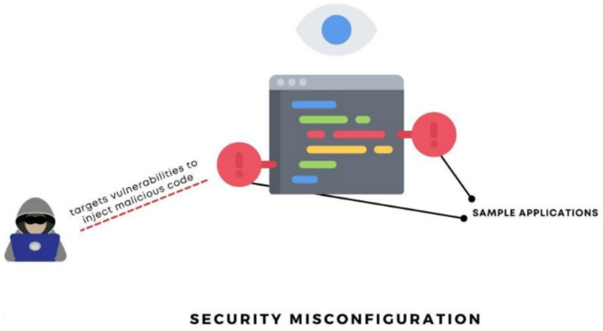


5. **Website defacement :** Website defacement is the method of modifying the website content or the entire website in an unauthorized way. The hackers can change the written content or add visual elements like pop-ups and featured images, etc. In some instances, they completely replace the website with a new one.

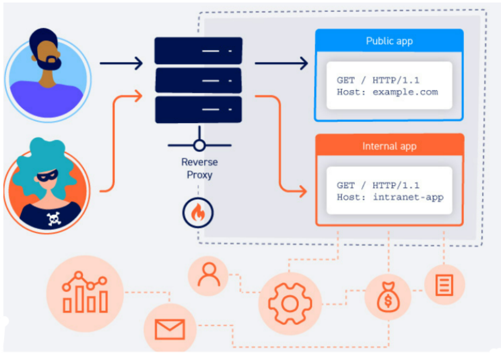


```
page</title>
web page</h1>
s/contact.jpeg">
own</h4>
ing a few html features</h2>
y a very simple language. it consist
ct, with commands that are enclosed by
haracters, or between and "&" and a ";".
```

6. **Web Server Misconfiguration :** Web server misconfiguration refers to the configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers like directory traversal, server intrusion, and data theft.


targets vulnerabilities to inject malicious code
SAMPLE APPLICATIONS
SECURITY MISCONFIGURATION

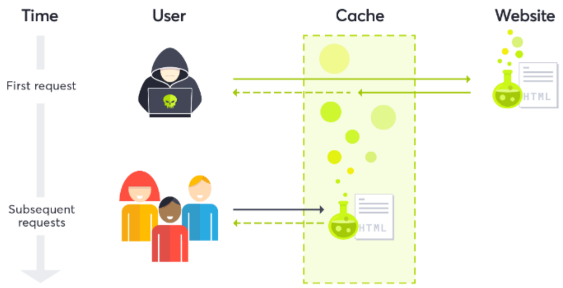
7. **HTTP Response-Splitting Attack :**An HTTP response-splitting attack may be a web-based attack during which the attacker tricks the server by injecting new lines into response headers, alongside arbitrary code. It involves adding header response data into the input field in order that the server splits the response into two responses. this sort of attack exploits vulnerabilities in input validation.



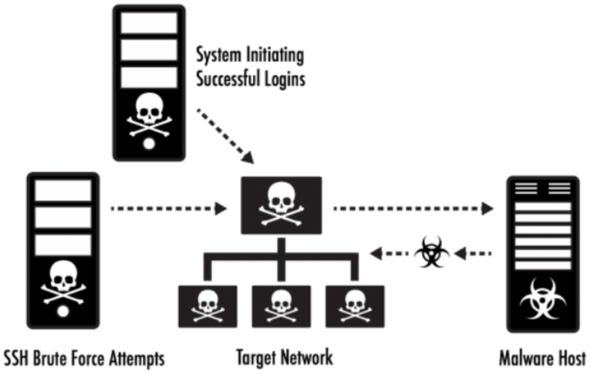
```
GET / HTTP/1.1
Host: example.com
```

```
GET / HTTP/1.1
Host: intranet-app
```

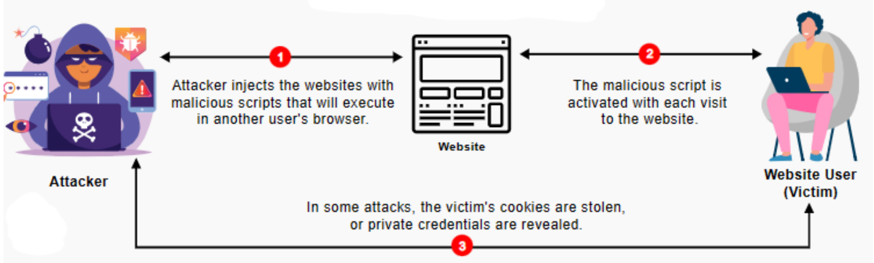
8. Web cache poisoning attack : It is the attack where the hackers replace the cached content for a web page with malicious content. This way, the end-users will see the poisoned content instead of the original content.During this case, all the users of that web server cache will get malicious content until the servers flush the online cache. Web cache poisoning attacks are possible if the online server and application has HTTP Response-Splitting flaws.



9. SSH Bruteforce attack : An SSH brute force attack is a hacking technique that involves repeatedly trying different username and password combinations until the attacker gains access to the remote server. The attacker uses automated tools that can try thousands of username and password combinations in a matter of seconds, making it a fast and effective way to compromise a server.



10.Cross Site Scripting (XSS) : This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.


1
Attacker injects the websites with malicious scripts that will execute in another user's browser.
Website
2
The malicious script is activated with each visit to the website.
Attacker
Website User (Victim)
In some attacks, the victim's cookies are stolen, or private credentials are revealed.
3