Hunting Tips

- jwt decoder
  - https://jwt.io/#debugger-io
- Some useful ways of breaking out of a string literal are:
  - '-alert(document.domain)-'
  - ';alert(document.domain)//
- A common behviour in cdn's is that injecting a host header belonging to the same account would serve that specific host, you can escalate request smuggling using that simple trick
- If we have site reandering your input as PDF and you can import it as PDF we can try SSRF with something like <iframe src="http://169.254.169.254/latest/meta-data">
- secert path in wp sites --> /wp-content/plugins/jsmol2wp/j2s/J/rendersurface/
- to find the clouding service you can search in youtubbe --> (siteName + cloud)
- Some AWS metadata pathes
  - http://169.254.169.254/latest/meta-data/local-hostname/
  - http://169.254.169.254/latest/meta-data/iam/security-credential
  - http://169.254.169.254/latest/dynamic/instance-identity/document
- If you wanna find some internal code of companies or some sample code or new features try:
  - repl.it intext:telekom.com
- If you got access denied message while using awscli try
  - aws s3 ls s3://[bucketname] --no-sign-request
- The HEAD method is the same as POST but without body maybe you need this trick !!
- If you found firebase API key in Android app use Pyrebase it's a simple python wrapper for the Firebase API to test Authentication,DB and storage permissions
- Always try to convert parameters to arrays you may get unexpected results maybe xss bypass
  - page?path=/abc
    - page?path[']=/abc
- To discover domains deployed on Github for subdomain takeover
  - intext:"There isn't a Github Pages site here"
  - Site not found . Github Pages
- payload to test XSS,SQLI and CSTI
  - '"<svg/onload=prompt(5);>{{7*7}}
- Extract Subdomains for ip range with nmap
  - nmap IP_range_sn | grep "domain" | awk'{print $5}'
- if you trying IDOR in APIs and got 401,403 you can try
  - {"id":1234}
    - {"id":[1234]}
  - {"id":1234}
    - {"id":{"id":1234}}
  - try HPP
    - url?id=real_id&id=victm
  - {"id":1234}
    - {"id":"*"}
- if we have domain like example.com try to make mail with max@example.com if there is no validation to the email maybe it's give you access or privileges
- if you test blacklist SSRF you can try to encode 1 or 2 or 3 octs of ip like 0251.254.169.254
- if you come across /api.json in AEM instance try cache poisoning (Host, X-Forwarded-Server,X-Forwarded-Host)
- trik to get uuid of any user try to register with the same username or email may be uuid will leak on the resbonse.
- https://dnsdumpster.com/ !!!
- https://www.ipvoid.com/udp-port-scan/ --> dns port scanner
- Maybe company uses deffrent domains or maybe there are applications on other domains so we can use "Copy Right Singture" on google (intext:"Facebook © 2019")
- if an app uses markdown (xss) : click here (javascript:alert(1))
- if you found "limit" parameter (/page?limit=10) you can try to change it to long value like (/page?limit=9999999999999) --> layer 7 dos atack
- when you test for SSRF try to change HTTP/1.1 to HTTP/0.9 and remove the host header (to bypass some fixes and validations)
- Run UDP scan if port 500 is open run (ike-probe) to see if it's vulnerable to Shared Secret Hash Leakage Weakness
- if you wanna bypass cloudflare protection and find the origin ip try
  - https://whoisrequest.com/history/
- you can enumerate directories in some buckets with Wfuzz
  - http(S)://<bucket-name-address-here>/FUZZ/
    - 200 status code without content
- For example to find any subdomain points to yahho on Censys
  - 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names:Yahoo.com
- Some Keywords to search for in JS files:
  - api
  - internal
  - url
  - var=
  - //
  - https://
  - CompanyName.com
  - Location.search
- CloudFlare
  - when you work with cloudflare firewall to bypass it try to send the request to the origin server (dig www.google.com)
  - try data:// in injections
- In url you can try those circumvents
  - https://expected-host@evil-host
  - https://evil-host#expected-host
  - https://expected-host.evil-host
  - You can URL-encode characters to confuse the URL-parsing code
- There are some endpoints shows json with the (content type: Text/html) CHANGE it to (Content Type : application/json) (the file contains spicial character)--> easy xss
- if the GET & POST methods are only allowed so we can use X-HTTP-Method-Override with PUT method leads to RCE.