ASSIGNMENT- 7

1. ***Case Study:*** *XYZ Corporation, a leading financial institution, recently experienced a security breach where sensitive customer data was compromised. As part of the incident response team (IRT), outline the steps you would take to address this incident effectively. Consider incident categorization, detection, communication plan, documentation, and legal/regulatory considerations in your response. Evaluate the importance of incident response planning in mitigating such incidents and maintaining trust with stakeholders.*

1. Preparation :

Preparation is the key to effective incident response. Even the best incident response team cannot effectively address an incident without predetermined guidelines. A strong plan must be in place to support your team. In order to successfully address security events, these features should be included in an incident response plan:

- Develop and Document IR Policies: Establish policies, procedures, and agreements for incident response management.
- Define Communication Guidelines: Create communication standards and guidelines to enable seamless communication during and after an incident.
- Incorporate Threat Intelligence Feeds: Perform ongoing collection, analysis, and synchronization of your threat intelligence feeds.
- Conduct Cyber Hunting Exercises: Conduct operational threat hunting exercises to find incidents occurring within your environment. This allows for more proactive incident response.

2. **Detection and Reporting**

The focus of this phase is to monitor security events in order to detect, alert, and report on potential security incidents.

- Monitor: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- Detect: Detect potential security incidents by correlating alerts within a SIEM solution.
- Alert: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- Report: Your reporting process should include accommodation for regulatory reporting escalations.

3. **Triage and Analysis**

The bulk of the effort in properly scoping and understanding the security incident takes place during this step. Resources should be utilized to collect data from tools and systems for further analysis and to identify indicators of compromise. Individuals should have in-depth skills and a detailed understanding of live system responses, digital forensics, memory analysis, and malware analysis.

As evidence is collected, analysts should focus on three primary areas:

- Endpoint Analysis
    - Determine what tracks may have been left behind by the threat actor.
    - Gather the artifacts needed to build a timeline of activities.
    - Analyze a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device.

- Binary Analysis
    - Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways.
        1. Behavioral Analysis: Execute the malicious program in a VM to monitor its behavior
        2. Static Analysis: Reverse engineer the malicious program to scope out the entire functionality.
- Enterprise Hunting
    - Analyze existing systems and event log technologies to determine the scope of compromise.
    - Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed.

4. **Containment and Neutralization**

This is one of the most critical stages of incident response. The strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume.

- Coordinated Shutdown: Once you have identified all systems within the environment that have been compromised by a threat actor, perform a coordinated shutdown of these devices. A notification must be sent to all IR team members to ensure proper timing.
- Wipe and Rebuild: Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.

- Threat Mitigation Requests: If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication from all egress channels connected to these domains.

5. **Post-Incident Activity**

There is more work to be done after the incident is resolved. Be sure to properly document any information that can be used to prevent similar occurrences from happening again in the future.

- Complete an Incident Report: Documenting the incident will help to improve the incident response plan and augment additional security measures to avoid such security incidents in the future.
- Monitor Post-Incident: Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any signs of indicators tripping that may have been associated with the prior incident.
- Update Threat Intelligence: Update the organization's threat intelligence feeds.
- Identify preventative measures: Create new security initiatives to prevent future incidents.
- Gain Cross-Functional Buy-In: Coordinating across the organization is critical to the proper implementation of new security initiatives.

2. Investigate the exploitation of vulnerabilities such as SQL injection and cross-site scripting (XSS) in ethical hacking scenarios.

ANS:

Cyber attackers are always on the lookout for any potential vulnerability that can be exploited by multiple tactics and techniques like phishing, brute force attack, malware injection, social engineering, web hacking and more to fulfill their malicious intentions and bring organizations and businesses to a standstill.

In this blog we will shed light on two of the most common yet popular web hacking techniques among hackers: SQL injection attack and cross-site scripting (XSS).

SQL injection attack

SQL injection is a common and prevalent method of attack that targets victims' databases through web applications. It enables cyber attackers to access, modify, or delete data, and thus manipulate the organization's databases. For any organization, data is one of the most critical and valuable assets, and an attack on its database can wreak havoc on the entire business.

Data can include customer records, privileged or personal information, business-critical data, confidential data, or financial records of an organization.

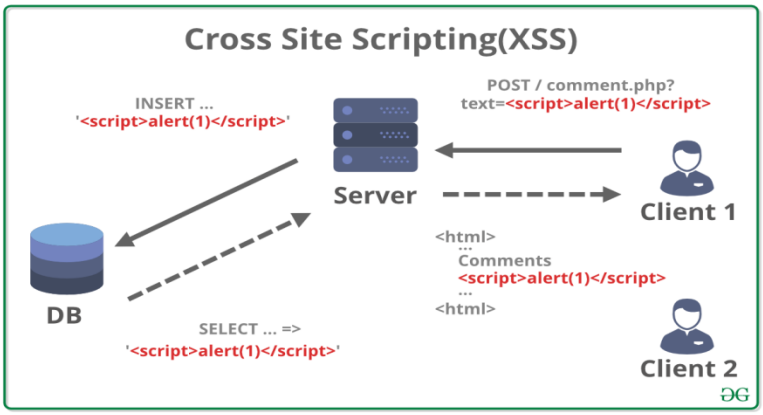
An SQL injection attack is carried out through the following steps:

1. An attacker researches the targeted database.
2. The attacker identifies vulnerabilities in the webpage or application to exploit. One example of an SQL vulnerability is insufficient user input validation. The attacker can create and submit their own input content by exploiting this vulnerability.

3. They further create malicious SQL inputs and inject them into the standard SQL queries.
4. This enables the attacker to carry out nefarious and malicious actions on the web application and exploit the database. They then can extract confidential information, bypass security controls, modify records, or delete the entire database.

Cross-site scripting

Cross-site scripting (XSS) attack is a popular attack technique used by hackers to target web applications. Here, the attackers inject malicious client-side scripts into a user's browsers or web pages, allowing them to download malware into the target user's system, impersonate the target, and carry out data exfiltration, session hijacking, changes in user settings, and more.



An XSS attack is carried out through the following steps:

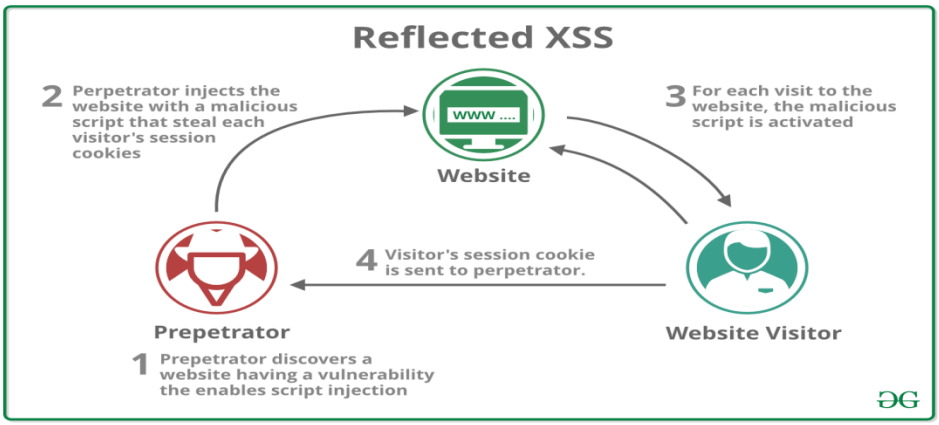
1. The attacker exploits the vulnerabilities of a website, such as using its form to inject a malicious script into the website's database.
2. The malicious script gets saved in the database of the vulnerable website.
3. The victim user requests a webpage from the website.
4. The website database includes the malicious script in response to the requested webpage and sends it to the victim user.
5. The malicious script gets activated every time the victim user performs any action on the webpage or visits the compromised website.

6. The malicious script sends the victim's private data (such as session cookies) to the attacker's server.

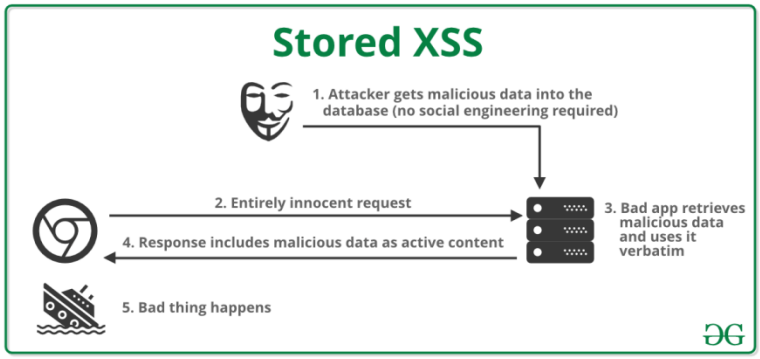
Types of XSS attack

XSS is broadly categorized into three types, which are:

1. **Reflected XSS:** The victim user (client) unknowingly sends a malicious script (payload) as part of the regular request to the vulnerable web application or website (server). As a response, the application will return the malicious script to the victim user, which upon loading, will execute the malicious script. Since the malicious script gets reflected back from the server to the client, it is called a reflected XSS.



2. **Stored XSS:** The attacker stores payload into the compromised servers, which gets delivered as and when the user visits the website. Since the malicious script is stored in the web application, it is called a stored XSS.



3. **DOM-based XSS:** The attacker exploits the vulnerability of those applications using a Document Object Model (DOM)—a programming web interface for web pages.

Differences between SQL injection and XSS attack

	SQL injection attack	**Cross-site scripting attack**
Attack definition	An attack technique where attackers target data-driven applications and compromise user/organization databases by performing certain actions.	An attack technique where attackers execute malicious code in the victim users browsers which they can control.
Entry point	The initial access in SQL attack is achieved through drive-by compromise technique.	The initial access in XSS attack is achieved through exploiting public-facing application technique.
Attack technique	The attacker injects malicious SQL queries into web form input field.	The attacker injects malicious client-side scripts into webpages/websites.
Impact	Upon successful execution, the attacker can add, delete, or modify the existing database and bypass the security controls.	Upon successful execution, the attacker can perform session hijacking, credential theft, data exfiltration, impersonate victim user, account hijacking, etc.
Attack language	The most common language used in the attack is SQL.	The most common language used in the attack is JavaScript.

3. *Discuss privilege escalation as a hacking technique, its implications, and preventive measures.*

ANS:

A Privilege Escalation Attack

Privilege escalation is an attack vector that many businesses face due to loss of focus on permission levels. As a result, security controls are not sufficient to prevent a privilege escalation.

Privilege escalation attacks occur when a threat actor gains access to an employee's account, bypasses the proper authorization channel, and successfully grants themselves access to data they are not supposed to have. When deploying these attacks threat actors are typically attempting to exfiltrate data, disrupt business functions, or create backdoors.

The Types Of Privilege Escalation Attacks

Not every attack will provide threat actors with full access to the targeted system. In these cases, a privilege escalation is required to achieve the desired outcome. There are two types of privilege escalation attacks including vertical and horizontal.

Vertical Privilege Escalation

Vertical privilege escalation occurs when an attacker gains access directly to an account with the intent to perform actions as that person. This type of attack is easier to pull off since there is no desire to elevate permissions. The goal here is to access an account to further spread an attack or access data the user has permissions to.

Day in and day out I analyze numerous phishing emails that attempt to perform this attack. Whether it's a "bank", "Amazon", or any other countless number of ecommerce sites, the attack is the same. "*Your account will be deactivated due to inactivity. Please click this link and login to keep your account active."* This is, however, one example of many cookie-cutter phishing templates seen in "the wild".

Horizontal Privilege Escalation

Horizontal privilege escalation is a bit tricky to pull off as it requires the attacker to gain access to the account credentials as well as elevating the permissions. This type of attack tends to require a deep understanding of the vulnerabilities that affect certain operating systems or the use of hacking tools.
Phishing campaigns have been used to perform the first part of the attack to gain access to the account. When it comes to elevating permissions, the attacker has a few options to choose from. One option is to exploit vulnerabilities in the operating system to gain system or root-level access. The next option would be to use hacking tools, like Metasploit, to make the job a bit easier.

Examples Of Privilege Escalation Attacks

5 real-world examples including:

1. Windows Sticky Keys
2. Windows Sysinternals
3. Process Injection
4. Linux Passwd User Enumeration
5. Android Metasploit

1. **Windows Sticky keys**– The ‘sticky key’ attack is the most common and fairly easy way of performing a privilege escalation attack. It does not require high technical skill sets. Attackers must have physical access to the system and should be able to boot it from a repair disk. By pressing the Shift key five times, an attacker can gain access to the Command Prompt with administrator privileges, allowing them to execute malicious code.
2. **Windows Sysinternals**– The Windows Sysinternals tool suite is another common method to conduct a privilege escalation attack. In this case, an attacker first performs a ‘sticky key’ attack to gain a backdoor into the system and then executes “psexec.exe -s cmd” to gain administrator privileges.
3. **Process Injection**– This privilege escalation attack targets weak processes. This process involves injecting malicious codes into running processes to elevate the privileges of that process.
4. **Linux Password User Enumeration**– This is another prevalent privilege escalation method where the attacker can use tools to enumerate valid usernames on a target system. Attackers first identify target accounts on a Linux system to carry out this attack by gaining access to the system’s shell. This is mostly performed by exploiting misconfigured FTP servers.
5. **Android Metasploit**– Android Metasploit refers to using the Metasploit framework to exploit vulnerabilities in Android devices. The Metasploit framework is a popular hacking tool used by attackers that contains a library of known exploits. Attackers can leverage these exploits to perform privilege escalation attacks against rooted android devices.

How To Prevent A Privilege Escalation Attack

Unfortunately, users are the weakest link in the security chain. With just a single click, they could compromise a system or network. To mitigate this risk, businesses implement security awareness programs along with a methodology for validating the effectiveness of the training. In most cases, phishing simulation software, like KnowBe4, GoPhish, or Phishme can adequately train users to identify phishing email attempts.

Privilege escalation, like other cyber attacks, takes advantage of system and process vulnerabilities. In order to prevent these attacks, consider implementing proper processes for patch management, new software development/implementation, and user account modification requests as well as an automated tool to monitor for such changes.

Implementing these process will give you the proper safeguards in place to prevent or deter and attacker from attempting privilege escalation. Finally, an intrusion detection system (IDS) and/or intrusion prevention system (IPS) provides an additional layer of security to derail attempts at escalating privileges.

New exploits are being created daily and it is our responsibility to ensure we protect ourselves from the attack. A proper patch management process will help ensure all systems and applications are current with the latest patches.

During the quest for new and improved software, we must not forget to include security in the process. Oftentimes, security is set aside to meet the business or client needs. Software code reviews or vendor management processes will help keep security in the loop and strengthen your development practices.

During the attack, the attacker may try to elevate their permissions with a phone call or service ticket request to the helpdesk. Without a proper process in place to validate the user's request, this may go unnoticed until an access level review is conducted.

4. *Explain the process of password cracking and discuss its ethical implications.*

ANS:

What is password cracking?

Password cracking, also known as password hacking, is any type of cyber attack that involves intercepting or otherwise compromising user passwords. The ultimate goal is to "crack" (or successfully guess) the passwords that are used to protect sensitive accounts.

Hackers can then use stolen credentials to breach or take over a user's account and gain access to sensitive data, confidential business records, and other valuable online assets.

How a password hack works

Password cracking can be divided into two categories: online and offline attacks.

In an online password attack, a hacker attempts to enter the correct password on an app's login page, directly on the server. Online password attacks can be challenging to carry out, as they're limited by the speed of the network. They're

also relatively easy to detect, due to the web noise generated by constant login requests.

On the other hand, offline password attacks provide hackers with more time and flexibility. In an offline password attack, a hacker intercepts one or more password hashes — algorithms used to encrypt passwords, converting plaintext passwords into unintelligible strings of letters, numbers, and symbols, so they're harder to read and recognize when stored in a database. The hacker can then take these password hashes offline and unencrypt them using a password cracking tool.

Common password cracking techniques

There are many types of online and offline strategies cybercriminals use to crack user passwords. Ten of the most common include:

1. BRUTE FORCE ATTACK

In a brute-force password attack, a hacker tries to access a secure user account through trial and error. This typically involves systematically entering every possible combination of letters, numbers, and symbols into a password field until one works.

Today, almost all brute force attacks are carried out by bots, or automated software that can be programmed to carry out repetitive, predetermined tasks. Among other actions, bots can randomly generate passwords and quickly enter them into an app or website. This eliminates a lot of the time and hassle required to mount a brute force attack, making it a much more efficient and attractive method for hackers.

Simple cyber security measures — like account lockout systems, which block entry to certain IP addresses after a certain number of incorrect login attempts —

can thwart a basic brute force attack. That's why, in recent years, hackers have developed the more sophisticated brute force methods outlined below.

2. PASSWORD SPRAYING

A password spray attack is a type of brute force attack in which, rather than trying many random passwords against a single account, a hacker tries the same password against many user accounts at once. This allows them to get around rudimentary security measures like account lockouts.

To maximize the impact of password spraying, hackers often employ weak or commonly used passwords (such as "password" or "123456") in their attacks, which they can source from public reports like NordPass's annual list of the 200 most common passwords.

3. CREDENTIAL STUFFING

Credential stuffing is another brute-force technique. In a credential stuffing attack, hackers use compromised credentials (which they've purchased from the dark web or obtained from a data breach) to log in to other, unrelated user accounts.

Unlike a traditional brute force attack, credential stuffing attacks aren't entirely random, as they rely on known username and password pairs. Since users tend to recycle the same credentials across multiple accounts, it's likely that one breached password will appear again on one of the other apps or websites that they use.

4. DICTIONARY ATTACK

In a dictionary attack, a hacker systematically enters common words and word variations from a specific, preselected list — kind of like a hacker "dictionary."

A dictionary attack can be tailored to a specific group or region that a hacker is targeting. For example, a hacker might use terms and phrases related to local businesses, landmarks, and sports teams when mounting a dictionary attack against a particular company or city.

While custom dictionary attacks can be dangerously effective, they tend to only work when users employ ordinary, everyday terms as passwords. That means enforcing strict password rules — like requiring users to create strong passwords with unique, randomized strings of characters — can be enough to prevent a dictionary attack.

5. MASK ATTACK

A mask attack is similar to a dictionary attack, but it's a far more targeted brute-force technique.

In a mask attack, a hacker analyzes recognizable password creation patterns and/or password hashes they've picked from known data breaches and uses them to apply a filter (or "mask") to their dictionary list of possible passwords. This dramatically reduces the total number of password guesses they must make for a given account, resulting in a much more efficient attack.

6. SPIDERING

Spidering is also intended to support a dictionary attack and similarly requires some dedicated effort on the part of the hacker.

In a spidering attack, a hacker gets to know their intended victim — generally, a larger, more established company — by studying their internal and external

communications. This can include social media posts, web content, employee handbooks, product manuals, and even marketing style guides.

From there, the hacker can compile a list of identifying information and common keywords and business/product terms that are unique to the company. They can use these terms to generate a shortlist of possible credentials, which makes guessing passwords on key corporate accounts that much easier.

7. MAN-IN-THE-MIDDLE (MitM) ATTACK

Man-in-the-middle (MitM) attacks involve eavesdropping on or otherwise intercepting sensitive communications between the app or website a user is connected to and another, separate platform.

MitM attacks can take active or passive form. Active MitM attacks often manifest as session hijacking, where a hacker spies on web traffic over a given network, identifies active session IDs, and then uses the attached session tokens to breach a user's account.

In a passive MitM attack, a hacker might create a free, public wifi hotspot, like the kind offered at airports, cafes, and public parks. They then get a full view of all of the online activities and data exchanges carried out by unsuspecting users who join their fraudulent network.

8. RAINBOW TABLES

Rainbow tables are comprehensive directories that use a password hash algorithm to list out every possible plaintext version of an encrypted password. Think of it like a hacker "cheat sheet" that allows cybercriminals to skip the work of actually having to hack passwords or a password hash themselves.

In a rainbow table attack, a hacker consults this directory and matches the list of solved password hashes to encrypted passwords they find in a breached database, allowing them to successfully sign in to a user's account.

9. PHISHING

A phishing attack is less about cracking passwords and more about getting users to share them voluntarily, albeit through deceitful means.

Essentially, phishing is a form of social engineering. In a typical phishing attack, a hacker sends their intended victim a persuasive message via email or text, hoping to trick them into sharing their credentials or other sensitive information.

This can happen by way of a fraudulent link that, when clicked, downloads malicious software on a user's device, or via a spoofed website that gets the user to type their credentials into a fake login screen.

Phishing attacks can be random, or they can target specific individuals or organizations.

A common example of a random phishing attack involves an email scam, in which the author pretends to be the executor of a will, which they claim comes from a recipient's (fictional) long-lost relative. This fake executor promises to transfer a large sum of inheritance money to the recipient, but claims they need the recipient's bank account credentials in order to wire the funds. Of course, if the recipient provides these credentials, the hacker behind the scheme will simply breach their account and quickly drain their balance.

A more targeted phishing attack, on the other hand, might mimic the messages a certain company sends to help users reset passwords. By clicking an embedded

reset-password link and/or entering their credentials, a user is actually giving a hacker access to their account or allowing them to install dangerous programs on their device.

10. MALWARE

Malware, short for "malicious software," refers to programs that are designed specifically for stealing passwords and other private information from a device where they have been (often unknowingly) installed.

Malware can piggyback on a link embedded within a phishing text or email, or it can hide within attachments, files, or websites that a user is tricked into opening or downloading.

Malware can take many different forms and work in a number of ways. Two categories of malware that can be used to crack passwords are:

- **Spyware:** Spyware hides on a user's system and secretly gathers information about their internet activity and behaviors, including any passwords, pins, and payment information they enter on an app or website.
- **Keyloggers:** Keyloggers are a specific type of spyware that monitors and records a user's keystrokes, or everything a user types into their device. That makes it easy for hackers to track and recognize common typing patterns, like a user's password for a given app or website.

Password cracking tools

Password cracking tools help hackers, well, crack passwords. They're especially useful in offline password attacks, where there might be thousands or even millions of possible plaintext combinations for each of the password hashes

uncovered in a database breach. In this case, the right cracking tool can do all the computational work, applying strategic algorithms and machine learning to unencrypt each hash.

Some of the most popular password cracking tools include:

JOHN THE RIPPER

John the Ripper (JTR) is one of the oldest and most well-known password crackers on the market. It's a command-based app that works in Linux and Mac OS environments, and it can automatically detect and support a wide range of hash types and ciphers.

While John the Ripper's basic platform comes as free, open-source software, there is also a "pro" version of the app that includes a more extensive wordlist, as well as support for specific operating systems.

CAIN AND ABEL

Another leading password cracker is Cain and Abel (frequently shortened to just Cain). It's available for Windows only, and it uses a graphical user interface (GUI) format, which makes it particularly attractive to amateur or beginner hackers.

Much like John the Ripper, Cain and Abel can recover passwords using a variety of password cracking and decrypting methods, including through brute-force and dictionary attacks.