1)

In developing incident response strategies, it's important to first understand how security incidents, vulnerabilities and threats relate. A *vulnerability* is a weakness in the IT or business environment. A *threat* is an entity -- whether a malicious hacker or a company insider -- that aims to exploit a vulnerability in an attack. To qualify as an *incident*, an attack must succeed in accessing enterprise resources or otherwise putting them at risk. Finally, a *data breach* is an incident in which attackers successfully compromise sensitive information, such as personally identifiable information or intellectual property.

When it comes to cybersecurity, an ounce of prevention is worth a pound of cure. Experts say organizations should fix known vulnerabilities and proactively develop response strategies for dealing with common security incidents. These include the following:

- Unauthorized attempts to access systems or data.
- Privilege escalation attacks.
- Insider threats.
- Phishing attacks.
- Malware attacks.
- Denial-of-service (DoS) attacks.
- Man-in-the-middle attacks.
- Password attacks.
- Web application attacks.
- Advanced persistent threats.

Since all security events are not equally serious, and because enterprises simply do not have the resources to aggressively address each and every one, incident response requires prioritization. Weigh an incident's urgency and importance to determine if it warrants a full-fledged response. For example, an active ransomware attack is both urgent -- i.e., time-sensitive -- and important -- i.e., it can put critical IT assets and business continuity at risk. Such an attack logically warrants a major, expedited response.

incident response plan:

An incident response plan is an organization's go-to documentation that details the following:

- **What.** Which threats, exploits and situations qualify as actionable security incidents, and what to do when they occur.
- **Who.** In the event of a security incident, who is responsible for which tasks and how others can contact them.
- **When.** Under what circumstances team members should perform certain tasks.
- **How.** Specifically, how team members should complete those tasks.

An incident response plan acts as a detailed, authoritative map that guides responders from initial detection, assessment and triage of an incident to its containment and resolution.

To create an incident response plan:

1. **Establish a policy.** An incident remediation and response policy should be an evergreen document describing general, high-level incident-handling priorities. A good policy empowers incident responders and guides them to make sound decisions when the proverbial excrement hits the fan.
2. **Build an incident response team.** An incident response plan is only as strong as the people involved. Establish who will handle which tasks, and ensure everyone has adequate training to fulfill their roles and responsibilities.
3. **Create playbooks.** Playbooks are the lifeblood of incident response. While an incident response policy offers a high-level view, playbooks get into the weeds, outlining standardized, step-by-step actions responders should take in specific scenarios. Playbook benefits include greater consistency, efficiency and effectiveness -- in both incident response and incident responder training.

   Learn how to create playbooks.
4. **Create a communication plan.** An incident response plan can't succeed without a solid communication plan among diverse stakeholders. These could include the incident response, executive, communications, legal and HR teams, as well as customers, third-party partners, law enforcement and the general public.

In general, an incident response plan should include the following components:

- A plan overview.
- A list of roles and responsibilities.

- A list of incidents requiring action.
- The current state of network infrastructure and security controls.
- Detection, investigation and containment procedures.
- Eradication procedures.
- Recovery procedures.
- The breach notification process.
- A list of post-incident follow-up tasks.
- A contact list.
- Incident response plan testing.
- Ongoing revisions.

Incident response frameworks: Phases of incident response

Rather than trying to recreate the wheel, an organization looking to build an incident response plan can refer to established incident response frameworks for high-level guidance and direction.

Well-known frameworks from NIST, ISO and SANS Institute all differ slightly in their approaches, yet they each describe similar phases of incident response:

1. **Preparation/planning.** Build an incident response team and create policies, processes and playbooks; deploy tools and services to support incident response.
2. **Detection/identification.** Use IT monitoring to detect, evaluate, validate and triage security incidents.
3. **Containment.** Take steps to stop an incident from worsening and regain control of IT resources.
4. **Eradication.** Eliminate threat activity, including malware and malicious user accounts; identify any vulnerabilities the attackers exploited.
5. **Recovery.** Restore normal operations and mitigate relevant vulnerabilities.
6. **Lessons learned.** Review the incident to establish what happened, when it happened and how it happened. Flag security controls, policies and procedures that functioned suboptimally and identify ways to improve them. Update the incident response plan accordingly.

Incident response team members

The size of an incident response team and the members included will vary based on the individual organization's needs. Some members could even fill multiple roles and responsibilities.

In general, an incident response team consists of the following members:

- **Technical team.** This is the core incident response team of IT and security members who have technical expertise across company systems. It often includes an incident response manager, incident response coordinator, team lead, security analysts, incident responders, threat researchers and forensic analysts.
- **Executive sponsor.** This is an executive or board member, often the CSO or CISO.
- **Communications team.** This includes PR representatives and others who manage internal and external communications.
- **External stakeholders.** Members include other employees or departments within the organization, such as IT, legal or general counsel, HR, PR, business continuity and disaster recovery, physical security and facilities teams.
- **Third parties.** These external members might include security or incident response consultants, external legal representation, MSPs, managed security service providers, cloud service providers (CSPs), vendors and partners.

2)

Cyberattackers 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 cyberattackers 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.

According to MITRE ATT&CK, cyberattackers often exploit public-facing applications to gain the initial foothold within an organization's network. These applications are generally websites but can also include databases like SQL.

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.

According to MITRE ATT&CK, cross-site scripting is an example of a drive-by compromise technique used by adversaries to gain initial access within the network. The technique aims to exploit website vulnerabilities through malicious client side scripts or code. This provides them with access to systems on the internal network and also allows them to use compromised websites to direct the victims to malicious applications meant to steal and acquire Application Access Tokens (used to make authorized and legitimate API requests on behalf of users/services to access resources in cloud or SaaS applications).

XSS attack work:

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.

The attacker injects the malicious script in the DOM through a URL for instance, and when the user performs any action on that page or visits the page through that URL, the application updates the DOM to execute the malicious script.

Differences between SQL injection and XSS attack

Even though both SQL injection and XSS attack are common web hacking techniques, there are a few key differences between the two.

	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.

Although SQL injection and cross-site scripting attack continue to be popular among attackers, continuous monitoring, testing, and deploying the best preventive measures will help organizations keep their websites from becoming prey to such attacks and neutralize any threats preemptively.

3)

Privilege Escalation Attack:

Privilege escalation is a common method attackers use to gain unauthorized access to systems and networks within a security perimeter. It's an attack vector faced by many organizations due to a loss of focus on permissions. As a result, existing security controls within organizations are often insufficient to prevent attacks. Attackers initiate privilege escalation attacks by detecting the weak points in an organization's IT infrastructure.

Privilege escalation attacks take place when a malicious actor gains access to a user account, bypasses the authorization channel, and successfully accesses sensitive data. The attacker can use obtained privileges to execute administrative commands, steal confidential data, and cause serious damage to server applications, operation systems, and the company's reputation. While deploying these attacks, attackers are generally attempting to disrupt business functions by exfiltrating data and creating backdoors.

Privilege Escalation Attacks Work:

Privilege escalation attacks represent the layer of a cyberattack chain where criminals take advantage of a vulnerable system to access data from an unauthorized source. However, there are various vulnerable points within a system, but some common entry points include Application Programming Interfaces and Web Application Servers. Attackers authenticate themselves to the system by obtaining credentials or **bypassing** user accounts to initiate the attack. Apart from it, attackers find different loopholes in account authorization access to sensitive data.

Regarding how a privilege escalation attack works, attackers usually use one of these five methods, including **credential exploitation**, system vulnerabilities, and exploits, **social engineering**, malware, or system misconfigurations. By implementing one of these techniques, malicious actors can gain an entry point into a system. Depending on their goals, they can continue to uplift their privileges for taking control of a root or administrative account.

Common Privilege Escalation Attacks Examples

Here are some common examples of real-world privilege escalation attacks.

- **Windows Sticky Keys:** It's one of the most common examples of privilege escalation attacks for Windows operating systems. This attack requires physical access to the targeted system and the ability to boot from a repair disk.

- **Windows system internals:** commands provide a source of privilege escalation attacks in Windows. This method assumes that the attacker has a backdoor from a previous attack, such as Windows sticky keys method. The attacker must have access to local administrative rights and then logs into backdoor accounts to escalate permissions to the system level.

- **Android and Metasploit:** **Metasploit** is a well-known tool, including a library of known exploits. This library contains the privilege escalation attack against rooted Android devices. It creates an executable file, known as superuser binary, which allows attackers to run commands with administrative or root access.

Privilege Escalation Attack Techniques

The goal of the privilege escalation attack is to get high-level privileges and find entry points to critical systems. There are various techniques attackers use for privilege escalation. Here are three of the most common ones.

- **Bypass user account control:** The user account control serves as a bridge between users and administrators. It restricts application software to standard permissions until an admin authorizes privilege increase.

- **Manipulating access tokens:** In this case, the attacker's main task is to trap the system into believing that the running processes belong to another user other than the authorized user that started the process.

- **Using valid accounts:** Criminals can leverage credential access techniques to get credentials of certain user accounts or steal them using **social engineering**. Once attackers access the organization's network, they can use these credentials to bypass access control on IT systems and various resources.

The Types Of Privilege Escalation Attacks:

There are two types of privilege escalation attacks. These include.

1. Horizontal Privilege Escalation

It's a type of attack in which attackers expand their privileges by taking control of another account and misusing the authorized privileges granted to the legitimate user. Phishing campaigns are used to gain access to user accounts. For elevating the permissions, attackers either exploit vulnerabilities in the OS to gain root-level access or leverage hacking tools, such as Metasploit.

2. Vertical Privilege Escalation

This type of attack occurs when a criminal gains direct access to an account with the intent to perform similar actions as the legit user. Vertical privilege attack is easier to perform as there is no desire to elevate permissions. In this scenario, the attack focuses on account identification with necessary privileges and gaining access to that account.

Impact Of Privilege Escalation Attack

Privilege escalation attacks can impact in the following ways.

- It can enter the organization's IT infrastructure

- Modify permissions to steal sensitive information

- Add, delete, or modify users

- Create a backdoor for future attacks

- Gain access to systems and files and disrupt the operations
- Crash the website

To Prevent Privilege Escalation Attacks:

Here are some best practices to prevent privilege escalation attacks.

1. Protect and scan your systems, network, and application. You can use effective vulnerability **scanning tools** to detect insecure and unpatched operating systems, applications, weak passwords, misconfigurations, and other vulnerabilities.
2. It's essential to manage privileged accounts and ensure their security. The **security team** needs an inventory of all accounts where they exist and their purpose.
3. Establish and enforce robust policies to ensure that users and strong and unique passwords. Use **multi-factor authentication** to add an extra security layer while overcoming vulnerabilities arising due to weak passwords.
4. Users are the weakest link in the security chain, putting the entire organization at risk. Businesses should implement robust security awareness programs with effective training.
5. Secure databases and sanitize user inputs. Databases are attractive targets of criminals as web applications store all their data in databases, such as login credentials, configuration settings, and user data. With one successful attack, such as SQL injection, criminals can access all sensitive information and leverage it for further attacks.

4)

Password Cracking:

Password cracking is the process of identifying an unknown password to a computer or network resource using a program code. It can also assist a threat actor in gaining illegal access to resources. Malicious actors can engage in various criminal activities with the information obtained through password cracking. Among these include the theft of banking credentials and the use of the information for fraud and identity theft. Passwords are recovered by a password cracker employing a variety of approaches. The procedure might entail comparing a set of words to guess credentials or using an algorithm to guess the password repeatedly.

Techniques of Password Cracking

Passwords are usually kept in a hashed format, be it on website databases or operating system caches. Storing passwords in plaintext is too big a risk from a development perspective since a single lapse in security can release countless gigabytes of confidential user data. In this process, the passwords are converted into chunks of unreadable data, which can only be used for cross-verification when a user tries to log in. Despite hashing, hackers manage to capture fresh passwords, depending on how complex the initial password was. Some of the most widely used techniques are -

Phishing

Asking the customer for their password is a simple approach to hack. A phishing email directs the unwary reader to a counterfeit log-in page linked with whatever service the hacker wants to access, generally by demanding the user fix some critical security flaw or aid in a database reset. That page then captures their password, which the hacker can subsequently exploit for their own purposes.

Social Engineering

Social engineering influences the victim to get personal information such as bank account numbers or passwords. This strategy is popular among hackers because they realize that humans are the gateway to vital credentials and information. And, through social engineering, they employ tried-and-true tactics to exploit and influence age-old human tendencies rather than devising novel means to breach secure and advanced technologies. It has been demonstrated that many firms either lack adequate security or are overly friendly and trustworthy when they should not be, such as granting someone access to critical facilities based on a uniform or a sob story.

Dictionary Attack

A hacker searches a password dictionary for the correct password in this case. Password dictionaries cover many themes and mixtures of topics, such as politics, movies, and music groups. Users' failure to create a strong password is why this approach efficiently cracks passwords. Simply said, this assault employs the same terms that many individuals use as passwords. A hacker can compare the password hash obtained to hashes of the password dictionaries to find the correct plaintext password.

Rainbow Table

Now that the passwords have been hashed, the hackers attempt to achieve authentication by breaking the password hash. They accomplish this by employing a Rainbow table, which is a set of pre-computed hashes of probable password combinations. Hackers can use the rainbow table to crack the hash, resulting in guessing your password. As a result, it retrieves the password hash from the system and eliminates any need to break it. Furthermore, it does not necessitate the discovery of the password itself. The breach is accomplished if the hash matches.

Brute Force

In a brute-force assault, the attacker attempts multiple password combinations until the correct one is identified. The attacker uses software to automate this process and run exhaustive password combinations in a substantially shorter length of time. With the growth of hardware and technology in recent years, such programs have been invigorated. It won't be quick if your password is more than a few characters lengthy, but it will eventually reveal your password. Brute force assaults can be sped up by throwing more processing resources at them.

But when learning how to crack passwords, consumers must be aware of the tools being used by hackers to attain the same. Now, you will go through some of these tools being circulated on the internet.

Some Password-Cracking Tools:

1. Cain and Abel - This password recovery program can recover credentials for Microsoft Windows user accounts and Microsoft Access passwords. Cain and Abel employ a graphical user interface, making it easier to use than equivalent applications. The program employs dictionary lists and brute-force attack techniques.
2. John the Ripper - John the Ripper (JtR) is a password cracking application first released in 1996 for UNIX-based computers. It was created to evaluate password strength, brute-force encrypted (hashed) passwords, and break passwords using dictionary attacks. It can use dictionary attacks, rainbow tables, and brute force attacks depending on the target type.
3. Rainbow Crack - It belongs to the hash cracker tool category, which uses a large-scale time-memory trade-off technique to break passwords quicker than standard brute force tools. Time and memory trade-off is a computing process in which all plain text and hash pairs are generated using a certain hash algorithm. The outcomes are then saved in the rainbow table. This procedure might take a long time. However, once the table is ready, it can break passwords far quicker than brute force methods.

Now that you understand how to crack passwords using hash tables and ready-made tools, it’s time to look at ways to protect your credentials from falling prey to such techniques.

Some of the methods to prevent passwords from being cracked are-

1. Longer Passwords: Longer passwords are required, making the brute force mechanism tougher to implement. Longer passwords and passphrases have been demonstrated to boost security significantly. However, it is still critical to avoid lengthier passwords that have previously been hacked or that feature often in cracking dictionaries.
2. No Personal Details: This password policy encourages users to establish passwords that do not contain personal information. As previously said, most users create passwords utilizing personal information such as hobbies, nicknames, pet or family member names, etc. If a hacker has access to personal information about a specific user (for example, via social media), they will test password combinations based on this knowledge.
3. Different Passwords for Different Accounts: Password regulations should compel users to distinguish between security and convenience. Users should be prohibited from using the same passwords for all services. Password sharing between users – including those who work in the same department or use the same equipment – should be avoided. A single breached password doesn't affect your other accounts with this policy.
4. Use Passphrases: Some password regulations necessitate the creation of a passphrase rather than a password. While passes serve the same objective, their length makes them more difficult to break. In addition to letters, a good pass should include numbers and symbols. Passwords may be easier for users to remember than passphrases. However, the latter is much more breach-resistant.
5. Two-Factor Authentication: Two-factor authentication(2FA) can help secure an online account or even a smartphone. 2FA does this by asking the user to provide two forms of information—a password or personal identification number (PIN), a code texted to the user's smartphone, or a fingerprint—before accessing whatever is secured. This helps discourage unauthorized entries to an account without the original user's permission.