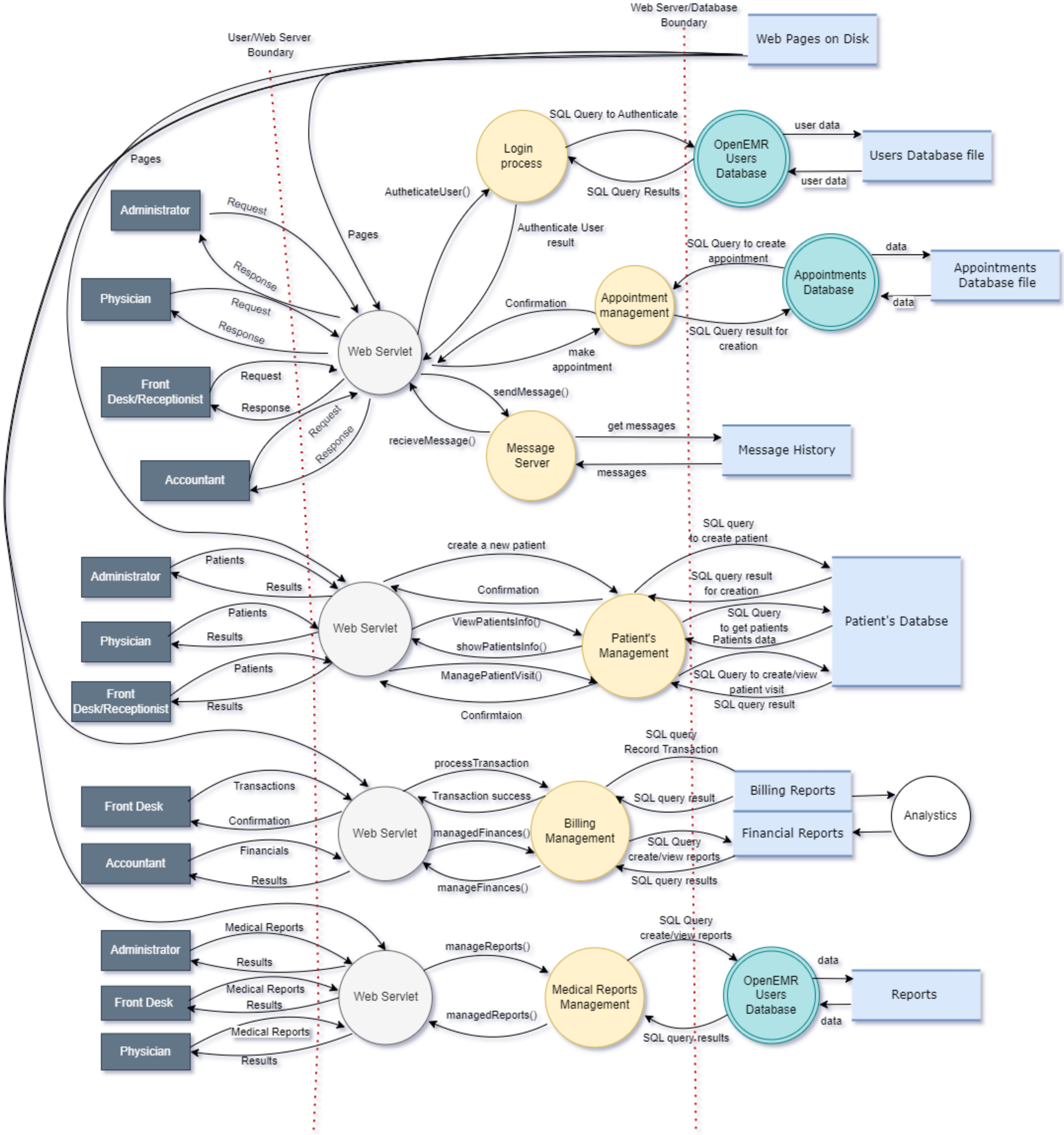
CSC 515
Software Security Course Project

Team:

Soha Bhatia(sbhatia6)
Akruti Sinha(asinha6)
Shivangi Chopra(schopra4)

Part 1:
Data Flow Diagram:



1. **Threat Category**: Spoofing
   Threat Description: An attacker could spoof their identity (as admin) to gain unauthorized access to patient records.
   Mitigation Description: Implement multi-factor authentication to prevent unauthorized access and ensure all user accounts have strong passwords.
   DREAD Score: 6/10
   Damage potential: 6 -The potential harm that may be caused by an attacker getting unauthorized access to medical information is quite severe, hence we gave the damage factor of 6 a rating. Instead of changing the records, this would include disclosing private data to unauthorized persons. Sensitive information, including personal and medical data, is contained in patient records and may be utilized for identity theft or other bad intentions. Moreover, the healthcare practitioner can face legal and financial repercussions as a result of a patient record data breach. They could be subject to legal action, penalties, and reputational harm.
   Reproducibility: 4 - The ease with which this attack can be reproduced is relatively low, as it requires the attacker to successfully spoof their identity as an admin.
   Exploitability: 5 We gave the exploitability factor of 5 because it could take some amount of technical know-how or competence on the side of the attacker to leverage this vulnerability to obtain unauthorized access to patient information. Moreover, since the healthcare provider has put in place appropriate security measures such access restrictions and user authentication procedures, it could be harder for the attacker to successfully exploit this vulnerability.
   Affected users: 9 - The number of users who could be affected by this attack is high, as it could potentially compromise the privacy and security of many patients. I will rate this factor as 9.
   Discoverability: 3 - Due to the possibility that an attacker's identity spoofing may not be immediately obvious, this vulnerability can be found with relatively little difficulty.

2. **Threat Category**: Tampering
   Threat Description: An attacker could change medical histories or medications in patient records.
   Mitigation Description: To avoid unwanted changes, use data encryption and access controls.
   DREAD Score: 8/10 (Damage potential: 8, Reproducibility: 6, Exploitability: 6, Affected users: 6, Discoverability: 9)
   Damage potential: 8/10 - Tampering with patient records might have serious ramifications for both patients and healthcare providers. If an attacker is able to change a patient's medical history or prescriptions, they may receive erroneous treatments or medications, potentially resulting in catastrophic health implications or even death.
   Reproducibility: 6/10 - While tampering with patient records is a major hazard, the risk of it occurring is smaller than that of other forms of assaults, such as phishing or ransomware. This is due to the fact that tampering with patient records may necessitate a greater level of system access and may be more difficult to perform without discovery.
   Exploitability: 6/10 - While tampering with patient information may be more difficult than other types of assaults, there are still potential channels for exploitation, such as exploiting flaws in access controls or encryption used to secure patient records. The difficulty of exploiting this vulnerability, on the other hand, may prevent some attackers.
   Affected users: 6/10 - This hazard only affects the patients whose records have been tampered with, as well as the healthcare practitioners that rely on correct patient records. While the impact on individual

patients may be severe, the total number of affected users may be restricted in comparison to other forms of attacks that disrupt entire systems or networks.
Discoverability: 9/10 - Any tampering with patient records is likely to be caught quickly, especially if suitable access limits and monitoring mechanisms are in place. This may shorten the amount of time an attacker has to exploit the vulnerability and hence reduce the total impact of the assault.

3. **Threat Category**: Repudiation
   Threat Description: An attacker could deny their involvement in modifying or accessing patient records.
   Mitigation Description: Implement audit trails to track user activity and prevent unauthorized access.
   DREAD Score: 5/10
   Damage potential: 3- The damage potential is medium because, while patient data can be altered or deleted, the impact may be less severe than in other types of attacks. They can result in the modification or deletion of sensitive patient information, which can have legal or financial ramifications for the healthcare provider or the patient. Furthermore, if the healthcare provider is unable to provide accurate and reliable patient information, the integrity and trustworthiness of the entire healthcare system may be jeopardized.
   Reproducibility: 5- This is because an attacker may require a specific skill set or knowledge to carry out the attack successfully.
   Exploitability: 5- Repudiation has a low to medium exploitability since an attacker may need access to the system or data in question to deny their involvement.
   Affected users: 5 -Repudiation may have an effect on a particular group of users who are involved in security incidents within the OpenEMR system, therefore the number of impacted individuals is moderate.
   Discoverability: 7 Because audit trails and other security measures may be used to detect any illegal access to or alteration of data and because forensic analysis may be used to disprove an attacker's denial of involvement, repudiation is highly discoverable.

4. **Threat Category**: Information Disclosure
   Threat Description: By taking advantage of a vulnerability, an attacker could gain unauthorised access to sensitive patient data such as a patient's name, address, medical history, diagnoses, and treatment plans. This can also happen when a user unintentionally leaves their computer unlocked and unattended while logged into OpenEMR, giving someone else access to patient records. This may occur, for instance, if a person leaves their workstation without locking the screen of their computer, allowing a passerby to view the private data that is displayed.
   Mitigation Description: Implement data encryption, access controls, and regular security updates to prevent unauthorized access, requiring users to lock their computer screens when they leave their desks.
   DREAD Score: 7/10
   Damage potential: 10: There is a substantial risk that unauthorized access to sensitive patient information may cause harm, including the loss of patient confidence, legal and financial repercussions, and reputational harm to the healthcare provider.
   Reproducibility: 4: Because this vulnerability relies on human mistake (forgetting to lock the computer screen), which can happen often in a busy healthcare setting, it is simple to replicate.
   Exploitability: 7 - Easy to exploit
   Affected users: 8 - Many Users can be affected although not all users.

Discoverability: 5 - Although vulnerabilities may be found by attackers using automated techniques or by scanning the system for flaws, they are nevertheless typically thought to be more difficult to find than other sorts of vulnerabilities like open ports or unpatched software.

5. **Threat Category**: Denial of Service
   Threat Description: An attacker might flood the system with requests, causing it to crash or go down.
   Mitigation Description:To prevent overload, incorporate rate restriction and request throttling, as well as backup and disaster recovery procedures.
   DREAD Score: 8/10 (Damage potential: 8, Reproducibility: 8, Exploitability: 7, Affected users: 7, Discoverability: 9)
   Damage potential: 8/10 - A denial of service attack has the potential to cause severe harm, both in terms of user service disruption and system damage. For example, if the system under attack is vital to healthcare operations, a denial of service assault could prohibit healthcare providers from accessing patient data or scheduling appointments, potentially resulting in treatment delays or other undesirable repercussions.
   Reproducibility: 8/10 - Denial of service attacks can be relatively simple to carry out, especially if the attacker has access to botnets or other automated tools that can overwhelm the system with requests. Furthermore, these attacks can be difficult to identify and avoid, making them a chronic threat.
   Exploitability: 7/10 - While denial of service assaults can be very simple to carry out, the success of the attack may be dependent on the system's countermeasures. A well-protected system, for example, with rate limitation and request throttling, may be more difficult to bring down with a denial of service attack.
   Affected users: 7/10 - A denial of service assault can have a major impact, especially if the system under attack is crucial to healthcare operations. Patients may be unable to access their medical records or make appointments, and healthcare practitioners may be unable to administer required treatments or services. The attack's impact, however, may be limited to a small set of users rather than the entire system or network.
   Discoverability: 9/10 - Denial of service attacks are reasonably straightforward to detect since they often entail a flood of requests that security software can identify and stop. However, the success of the assault may be determined by the speed with which it is identified and mitigated, which may be difficult if the attack is carried out by a skilled and persistent attacker.

6. **Threat Category**: Elevation of Privilege
   Threat Description: An attacker could gain elevated permissions within the system, allowing them to access or modify data they shouldn't have access to.
   Mitigation Description: Implement access controls and permission levels to prevent unauthorized access and modifications, and regularly review user access privileges to ensure they are appropriate.
   DREAD Score: 7/10 (Damage potential: 6, Reproducibility: 8, Exploitability: 6, Affected users: 7, Discoverability: 8)
   Damage potential: 6/10 Elevation of Privilege has a high damage potential because an attacker who is successful in doing so can access confidential data and take actions that they are not otherwise authorized to. This can entail changing user passwords, removing or altering patient data, or even seizing control of the entire system.
   Reproducibility: 8/10 Because the vulnerability that allows an attacker to elevate their power level is frequently duplicated and exploited by other attackers, the reproducibility of Elevation of Privilege is high.

Exploitability: 6/10 Elevation of Privilege has a medium to high risk of being exploited, depending on the system in question and the security precautions in place. To take advantage of the vulnerability, an attacker may need to have some level of access to the system, but this access may not be difficult for them to obtain through social engineering or other techniques.
Affected users: 7/10 The number of affected users is enormous because an attacker who raises their degree of privilege could potentially harm every user of the system by accessing or changing information they shouldn't have access to.
Discoverability: 8/10 Elevation of Privilege is somewhat too highly discoverable. Security measures may find it challenging to catch the initial exploitation of the vulnerability that permits privilege elevation, but monitoring and auditing may make it easier to catch unusual behavior by an attacker with elevated privileges.

7. **Threat Category**: Spoofing
Threat Description: A software flaw might be used by an attacker to insert malicious code into a server-side application that is running OpenEMR. The attacker might then spoof the identity of the server using the compromised application, giving them the ability to intercept and control communications between the server and other systems or clients. This may provide the attacker the ability to commit a variety of nefarious deeds, such stealing private information or launching denial-of-service assaults. Because the attacker is mimicking the legal OpenEMR server to trick other systems or clients into acting maliciously, this is an illustration of the spoofing danger in STRIDE.
Mitigation Description: Employ strong password policies, multi-factor authentication, and role-based access constraints. Use robust encryption methods, such as SSL/TLS, to protect data exchanges between OpenEMR and other systems or clients. Adopt best practices for software security. Educate users about the risks of spoofing attacks
DREAD Score: 8/10
Damage - 8: The potential damage of a successful Spoofing attack on OpenEMR could be very high, especially if an attacker is able to steal sensitive data or perform denial of service attacks. Therefore, the damage rating is High.
Reproducibility- 8: The likelihood that an attacker can reproduce the Spoofing attack depends on the specific software vulnerability that they are exploiting. However, if the vulnerability is widely known and easily exploitable, the reproducibility rating could be High.
Exploitability - 5: The level of effort required for an attacker to successfully carry out a Spoofing attack depends on the specific software vulnerability that they are exploiting, as well as the security controls in place. However, in general, the exploitability rating is Moderate (5) since attackers may need to perform some initial reconnaissance to identify a suitable vulnerability and develop a payload to inject into the application.
Affected Users - 8: The number of affected users could potentially be very high if a successful Spoofing attack compromises the security of the entire OpenEMR system, including patient data and other sensitive information. Therefore, the affected users rating is High.
Discoverability - 5: The likelihood that a Spoofing attack will be detected by security controls or system administrators depends on the specific attack vector and the sophistication of the attacker. However, in general, the discoverability rating is Moderate (5) since attackers may be able to use evasion techniques to avoid detection.

8. **Threat Category**: Tampering
   Threat Description: An attacker could change a patient's billing information, causing financial hardship.
   Mitigation Description:Implement data encryption and access controls to avoid illegal changes, and verify billing data for discrepancies on a regular basis.
   DREAD Score: 7/10 (Damage potential: 7, Reproducibility:6, Exploitability: 6, Affected Users: 6, Discoverability: 9)
   Damage potential: 7/10 - Billing information tampering can cost patients, providers, and the healthcare company as a whole money. However, the potential harm may be less severe than that of other sorts of tampering, such as tampering with medical data or prescriptions.
   Reproducibility: 6/10 - Tampering with billing information may necessitate some level of insider knowledge or access, making it more difficult to perform than other sorts of attacks. However, if an attacker gains access, it may be quite simple to edit billing information without being detected.
   Exploitability: 6/10 -The exploitability of this threat scenario, like its reproducibility, may be dependent on the attacker's level of access and understanding. However, if an attacker gains access to the system, changing billing information may be a pretty simple operation.
   Affected users: 6/10 - This threat scenario's impact may be confined to patients and providers whose billing information has been tampered with. However, the financial consequences of such manipulation can be enormous.
   Discoverability: 9/10 - Detecting tampering with billing information can be simple, especially if billing data is reviewed on a frequent basis. However, the success of the attack may be determined by the expertise of the attacker and their ability to conceal their trails.

9. **Threat Category:** Repudiation
   Threat Description: An attacker could deny their involvement in modifying or accessing billing information.
   Mitigation Description: Implement audit trails to track user activity and prevent unauthorized access, and ensure all users are accountable for their actions.
   DREAD Score: 5/10 (Damage potential: 3, Reproducibility: 5, Exploitability: 5, Affected users: 5, Discoverability: 7)
   Damage potential: 3/10 Although the modification or access to billing information may not directly affect patient care or have a substantial negative financial or legal consequence, the harm potential for repudiation in this scenario is moderate.
   Reproducibility: 5/10 The attacker may need specialized knowledge or access to the system in order to modify or access the billing information, making it more challenging to repeat the attack. As a result, the reproducibility of this attack is low to medium.
   Exploitability: 5/10 Since an attacker may need access to the system or the data to modify or access the billing information, the exploitability of this attack is moderate to medium.
   Affected users: 5/10 The attack's affected users are moderate because it might only have an effect on a small group of users who are engaged in billing or financial operations within the OpenEMR system.
   Discoverability: 7/10 High audit trails and other security measures can be used to detect any illegal access to or alteration of billing information, and forensic analysis may be used to disprove an attacker's denial of involvement, making this attack highly discoverable.

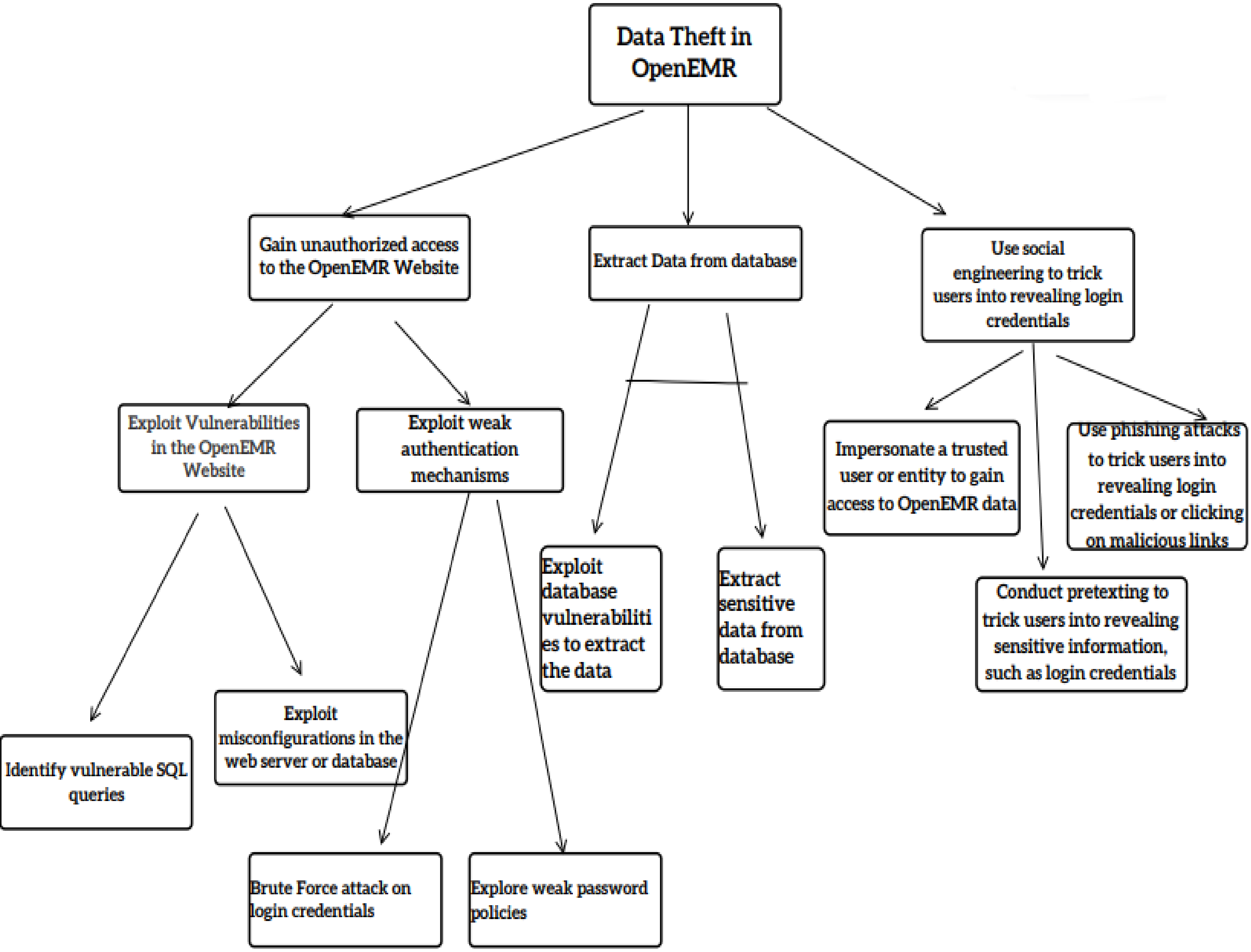
10. **Threat Category**: Information Disclosure

Threat Description: An attacker could gain unauthorized access to financial information, such as bank account details or insurance data.
Mitigation Description: Implement data encryption, access controls, and regular security updates to prevent unauthorized access, and monitor for any suspicious activity.
DREAD Score: 9/10
Damage potential: 10 - A successful information disclosure assault against OpenEMR might cause a great deal of harm, especially if private financial data, such bank account information or insurance information, is exposed.
Reproducibility: 7 - The possibility that an attacker may use a given vulnerability or flaw to launch an Information Disclosure attack relies on what they are attacking. Nevertheless, the repeatability grade might be higher if the vulnerability is well-known or simple to exploit.
Exploitability: 7 - Depending on the exact vulnerability or weakness that is being exploited and the security measures in place, the amount of work needed for an attacker to effectively execute an information disclosure assault will vary. But generally speaking, the exploitability grade ranges from Moderate to High.
Affected users: 8 - The number of affected users could potentially be significant
Discoverability: 10 - Attackers might be able to employ covert methods to escape detection.

Part 2:

Attack Tree

Attack Goal: Data Theft In OpenEMR website


Data Theft in OpenEMR
Gain unauthorized access to the OpenEMR Website
Extract Data from database
Use social engineering to trick users into revealing login credentials
Exploit Vulnerabilities in the OpenEMR Website
Exploit weak authentication mechanisms
Impersonate a trusted user or entity to gain access to OpenEMR data
Use phishing attacks to trick users into revealing login credentials or clicking on malicious links
Exploit database vulnerabilities to extract the data
Extract sensitive data from database
Conduct pretexting to trick users into revealing sensitive information, such as login credentials
Exploit misconfigurations in the web server or database
Identify vulnerable SQL queries
Brute Force attack on login credentials
Explore weak password policies

Part 3:
Design principles from Saltzer & Schroeder:

1. **Economy of Mechanism:** This design guideline highlights the importance of keeping security measures as basic as possible to limit the likelihood of errors or undesired behavior. This is especially critical in complicated systems such as OpenEMR, which have numerous components and possible attack routes. The danger of misconfiguration or misuse is decreased when security mechanisms are designed to be simple and easy to comprehend, which can help prevent security vulnerabilities. Access control policies, for example, can be designed to be simple and easy to implement, and encryption keys can be managed automatically to limit the danger of human error.

2. **Complete Mediation**: According to this design principle, every access to a resource should be validated against the security policy. This means that in the context of OpenEMR, any access to patient data, user accounts, or system settings should be checked against the necessary access control regulations to ensure that only authorized individuals have access to critical information. This approach contributes to ensuring that security regulations are consistently applied throughout the system, lowering the risk of unwanted access or data breaches. For example, rather than checking rights at the level of entire records or modules, access control methods can be built to check permissions at the granularity of particular data fields or system functions.

3. **Open Design:** The need for transparency and documentation in security measures is emphasized by this design philosophy. Security specialists can more easily audit and verify the system's security if security procedures are transparent and well-documented. In the context of OpenEMR, this means that the system's security mechanisms should be open and well-documented, allowing security experts to examine them for potential flaws or weaknesses. This philosophy also encourages the use of open standards and open source software, which can help to ensure that the system's security procedures are widely known and tested by the security community as a whole.

Design principles from IEEE:

1. **Defense in Depth:** This principle underlines the significance of layering security systems in order to provide numerous levels of resistance against various sorts of attacks. The concept is that if one layer of security fails, the system is still protected by other layers. Multiple layers of security, such as firewalls, access controls, encryption, and intrusion detection systems, can be built with OpenEMR. Each of these layers can aid in the prevention of various types of attacks, such as network-based attacks, user authentication attacks, and data theft.

2. **Least Privilege**: This principle asserts that users should only be granted the least amount of access required to do their tasks. This means that with OpenEMR, user accounts should be configured with the least amount of permission required to perform their jobs, decreasing the risk of unauthorized access or data theft. The danger of accidental or intentional data breaches can be reduced by restricting user access to only what is required. A receptionist who just needs to access patient data, for example, should not be granted the authority to alter or delete patient data.

3. **Separation of Duties:** This principle highlights the need of delegating diverse responsibilities to different people in order to avoid any one person from wielding too much power or influence over the system. Different roles and duties should be assigned to different users in OpenEMR, such as those who can see patient data, those who can alter patient data, and those who can configure system settings. This division of roles can lessen the possibility of insider threats or errors produced by people who have too much power over the system. A system administrator, for example, should not be given the authority to edit patient data or billing information, since this could lead to a conflict of interest and raise the risk of data breaches.