**Security Testing:**

**1.Vulunerability Testing:** It’s used to identify the loopholes in the application.

**2.Penetrtion Testing:** In Penetration testing we not only identify the loopholes, but also we simulates the hackers activity on the application/system to identify to what extent the loop is causing the damage.

**3.Hacking:** Hacking, breaching, intruding (will not teach you identify the security loop holes).

**4.Manual security Testing:** Identifying the security loops holes without using any tools.

**5.Security Testing tools:** Identifying the security loops holes using tools.

**6.CIA Triad:**

**I. Confidentiality:** Information stored should be maintained privately and secured.

**ii. Integrity:** Only authorized people can access and update/edit the information.

**iii. Availability:** Hackers making the system/application unavailable for the intended users by creating false traffic.

**7. Vulnerability vs Threat vs Risk**

**1.Security Risks:**

* **SQL Injection:** Caused to Injecting a SQL query via input data from the client side.

**Cons:** Perform all database operations and manipulates the data.

* **Broken Authentication:** Brute Attack
* **Sensitive Data Exposure:**
* **XML External Entities:**
* **Broken Access Control:**
* **Security Misconfiguration:**
* **Cross-site scripting:**
* **Insecure Deserialization:**
* **Using Components with Known Vulnerability:**
* **Insufficient Logging and Monitoring:**

**2.The of Role Risk Assessments in Security Testing:**

* Database -Asset
* Database connecting to internet -Vulnerability.
* In this case Firewall is a control used to protect asset.

**3.** **Asset Identification**

**4.Security risk assessment techniques:**

1. static application security testing SAST

2. Dynamic application security testing DAST

3.Vulunerability scanning

4.Penetration testing

5.configuration scanning using automation such as Security Content Automation Protocol (SCAP) and

6.Open Vulnerability and Assessment Language (OVAL).

7.OWASP

**8.Security Testing Basics – (HTTP Methods)**

* **Get:** Get is not secure compared to Post Methos.
  + - **Get** sends the request in the form of URL and its parameters.
    - **Get** will retrieve **Http** status code and **Header’s** information along with the **Response.**
* **Post:** Post http methos is used to send the information to server from the client.
  + - **Post** method is more secure as compared to Get.
    - **Post** sends the request in the form of body by encrypting.
* **Head:** Head method is also used to retrieve the data from the sever same as the **Get** method.
  + - Whereas the **Head** method will only retrieve the Http status code and **Header’s** information (Request & Retrieve Headers).
* **Connect:** This method is used to build an end to end tunnel/channel between the client and server.
* **Options:** This http method sends the request from the client to the server, and the server will return all the **http** method supported by the server itself.
* **Trace:** It is used to diagnose the connection between the client and the server.
* **Dangerous/unsafe Http methods:** 
  + - **Put**
    - **Delete**
    - **Options**
    - **Trace**

**9.HTTP Status Codes:**

**i.1xx informational status codes:** 100 and 101, when server sends some information and switching protocols.

**ii.2xx- Success:**

**iii.3xx-Redirection**

**iv.4XX-client side:**

**v.5xx-Server side:**

**10. What is cookie and cookie is related to security testing.**

i. Cookies are small text files placed/stored in our system by the applications we visited.

What cookies can do?

1. Cookies will track our activities and communicate to the server.
2. Cookies will maintain the session id, session id will be provided by the server every time we login to the server.

Every we hit the request to the server, this session id well be attached to the request we send to the server. [Edit this cookie a chrome extension]

1. Back login scenario.

**11. What is a cookie?**

**What is a session ID?**

Every session created will have session ID and these session ID will be stored in the client/pc session Cookie. f

**What is a session?**

When we send a request to server, the request will be processed by the server and compare it with the database, then a session will be created in the server.

**Cookie versus Session**

**Persistent cookies:**

**Cryptography:** Enabling a secrete communication between two parties.

Encryption and decryption of data during the communication btw client and server, with the help of algorithms and Keys.

Cryptography Techniques:

1.Encryption

* Symmetric Key Encryption.
* Asymmetric Key Encryption.

2.Hashing

3.Encoding

**Information Security Policies and Procedures:**

Policies are guidelines that outline the company’s plans for addressing issues while procedures provide details on how policies will be implemented.

The basis of all security policies should be a security risk assessment that examines specific security threats and how they impact the organization.

**Security Policies and Procedures Examples:**

**1.Acceptable Use:** The policies need to make sure that, who ever the user using the system must be aware of all the policies and make sure to follow.

The policies should cover both acceptable and non-acceptable behaviour of using the network, data, website, etc.

**2.Minimum Access:** This policy defines level of access needed to perform certain tasks.

The goal this policy is preventing the people to access rights in excess of11 what they needed to perform.

**3.Network Access:**

1. This policy defines criteria for accessing the various types of networks such as LAN, WAN, and wireless networks etc.

2.Defines what is Permissible and non-permissible while on this network.

3.Prohibits users to adding unauthorised devices such as routers and hotspots.

**4.Remote Access:**

**5.Internet Access:**

1.This policy defines types of the websites that may or may not be accessed and whether a non-business use of internet is allowed or not.

**6.User Account Management:**

1.This policy defines the creation, maintenance, and deletion of user accounts.

2.This policy as defines the regular auditing of the user accounts to make sure that the accounts are compliance with the policy.

**7.Data Classification:**

1.This policy defines that the sensitive data should be secured.

**a. Public:** Anyone inside or outside the organization can view this data. (Webpages and documents).

**b. Confidential:**

* Any kind of confidential/sensitive information such project reports, business analysis reports, presentations used for internal purpose.
* Non-disclosure agreements are required before sharing to third parties.

**c. Highly confidential:**

* Any sensitive data like trade secrets, product design, and non-public financial data, should only be available for the certain people in the organization.
* This type of data can’t be shared with out explicit permission.

**d. private:**

* This policy defines that the data should be restricted to access until and unless we have the special authority.
* Data like financial, research and development information, merger and acquisition details, as well as customers data like credit card and account information, loss of this can cause huge financial impacts.

**e. secrete:**

* This policy defines the information shared by the third parties, likes consultants working on a new type of technology. Ex: Military research projects.

**8.Configuration and Change Management:**

**i.** This policy defines how configuration and change should be made to the existing resource without any impact.

**ii.** Configuration management defines how the security system is applied to secure devices and application.

**iii.** Any unauthorised changes to the code or application could create a security vulnerability.

**iv.** This policy defines the **standard configuration** need to be used and **approval** process to make the changes and rollback the changes if any problem occurs.

**9.Server Security:**

**i.** This policy defines the responsibility of the owner to provide backup, recovery and limiting active services to those necessary for running application.

**ii.** This policy also defines to follow the industry best practices to install and maintain the services.

**10. Mobile Devices:**

**i. Risk:** Mobiles and laptops are easily stolen and can be loss to companies data.

**ii. Specific rules and precautions:**

* Sensitive data need to be encrypted.
* Installation and maintenance of anti-malware software
* Procedure to reporting lost or stolen devices.

**11. Guest Access:**

* Define separate practices.
* Make sure the reads and accepts the polices before granting access to the network.
* This policy makes sure, that the guests are accessing the network, by following the organizational policies.

**12. Physical Security:**

* This policy defines the controls needed for the physical facilities.
* Natural disasters, fire and natural accidents, power loss, theft and other risks.

**13.Password policy:**

* This policy defines the min. Req. for strong password.
* The min. length of time allowed to change the password.
* Not using the “remember password” option in browsers.

**14. Malware protection:**

* This policy defines a framework of defences and behaviour for preventing, detecting and removing malware.
* This policy restricts the use of USBs.

**15.Incident Response:**

* This policy describes how to report an incident, such as,
* Discovery of malware.
* Unauthorised access to data, by violating the policies.

**16.Audit policies:**

**17. Software Licencing:**

**18.Electronic Monitoring and Privacy:**

**Security Procedures:**

**Analysis of security policies and procedures:**

**Scurity Auditing and its roles in security testing:**

**i.** security auditing is a manual process of identifying the loopholes in organizations security process and infrastructure.

ii.

**Pillars of security auditing:**

**1.Assessments**

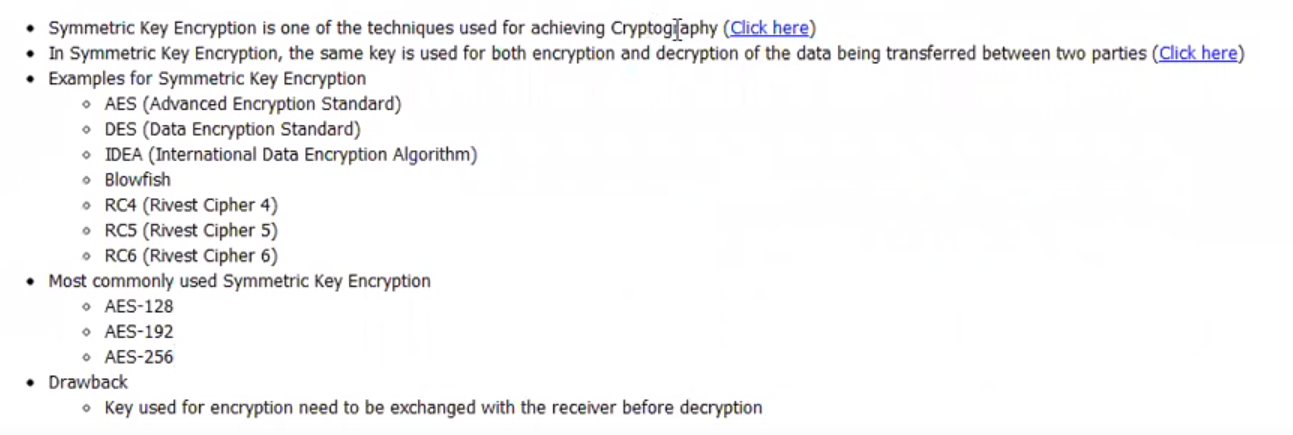
**2.Prevention**

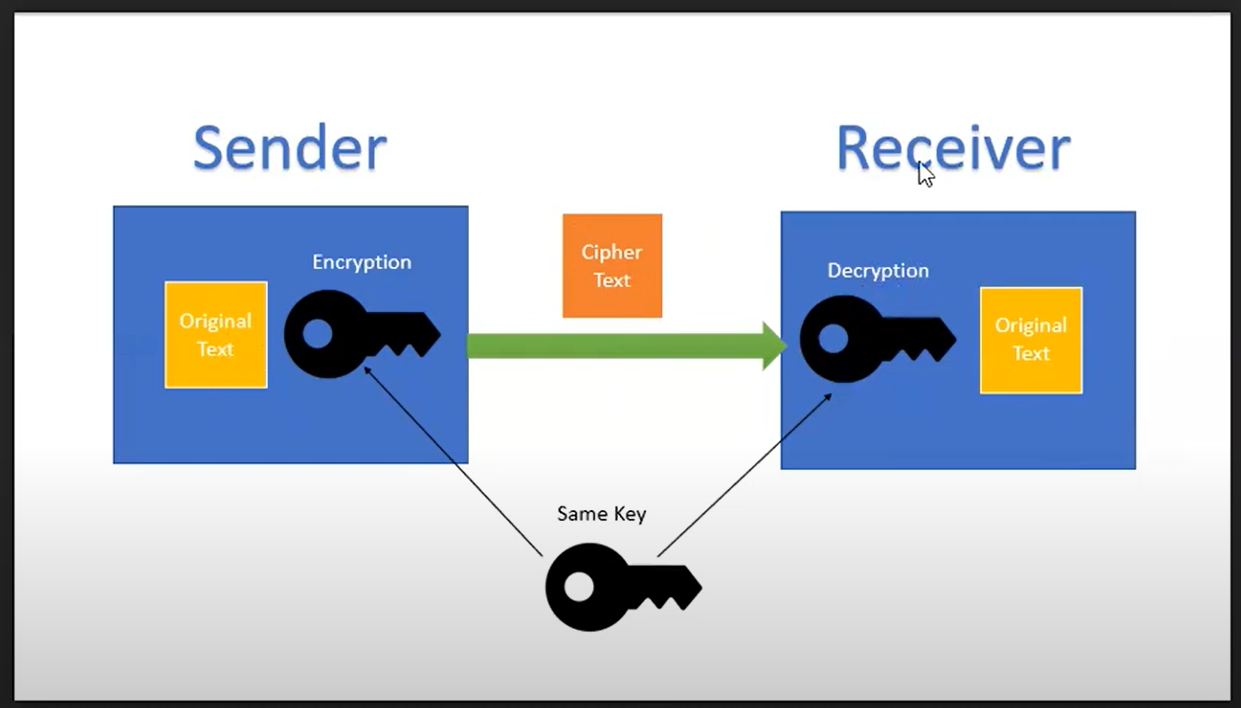
**3.Detection**

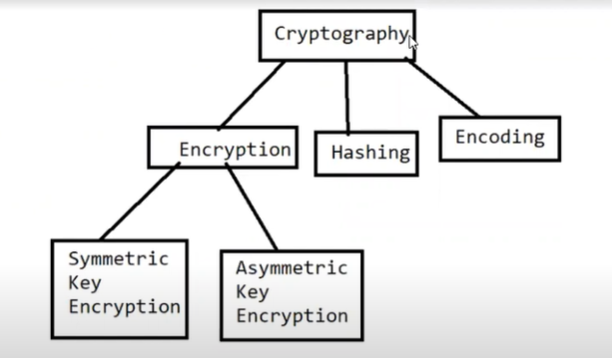
**4.Reaction**

**5.Recovery**

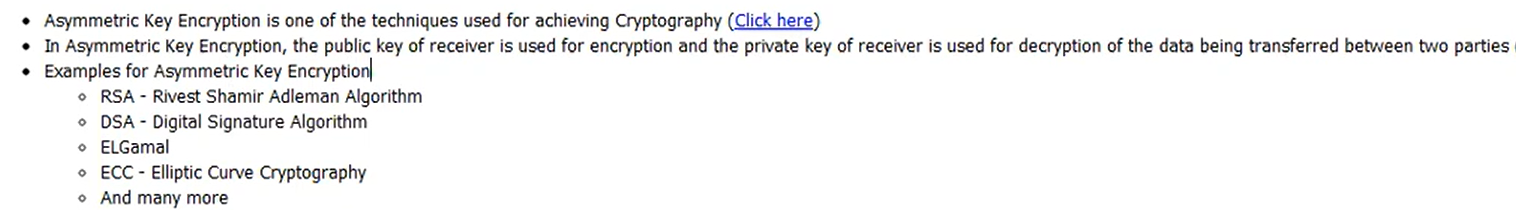
**Symmetric Key Encryption**:

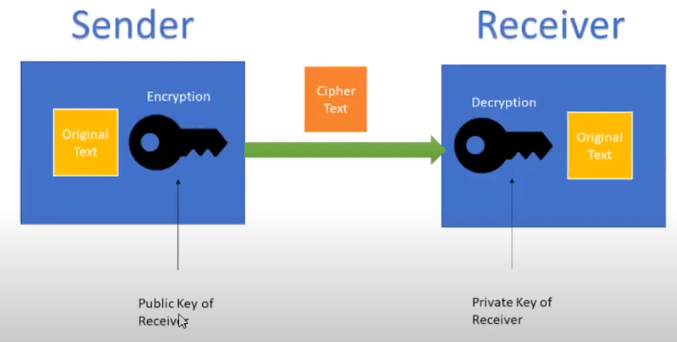




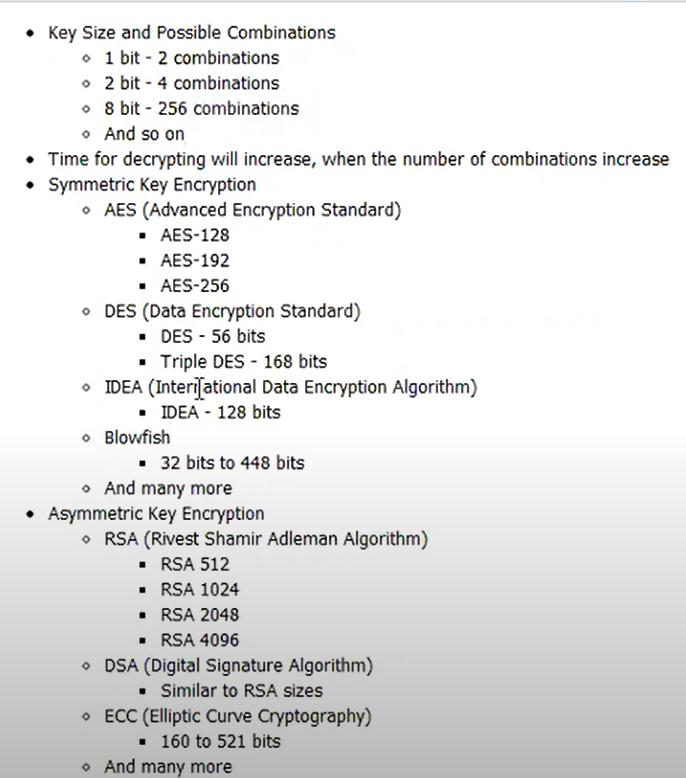


**Asymmetric Ket encryption:**

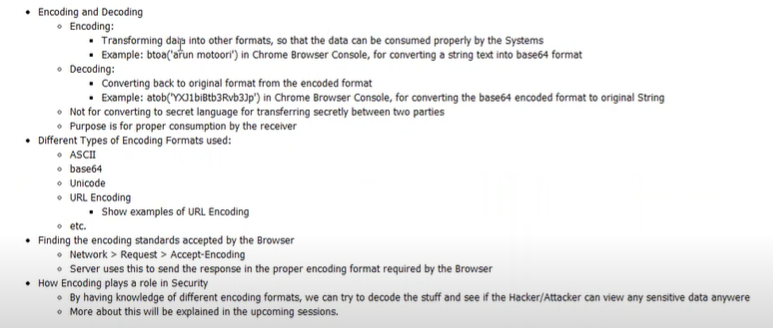
****

****

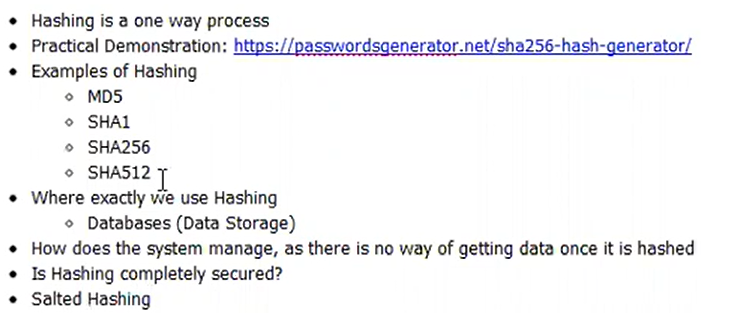
**Symmetric and Asymmetric Keys size:**

****

**Encoding and Decoding:**

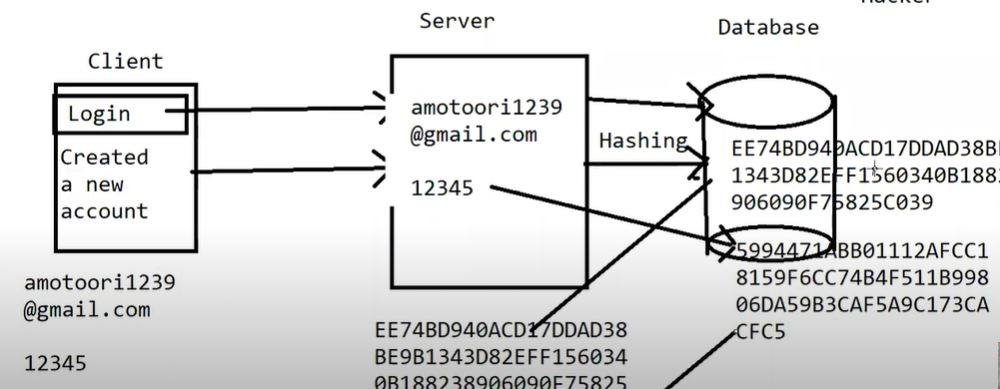
****

**Security Testing Basics – Hashing**

****

**Ex: Online Hash Converter.**

[**https://passwordsgenerator.net/sha256-hash-generator/**](https://passwordsgenerator.net/sha256-hash-generator/)

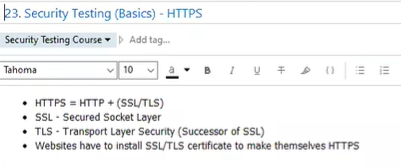


**Security Testing Basics – HTTP is Stateless:**

****

****

**Security Testing Basics – HTTPS:**

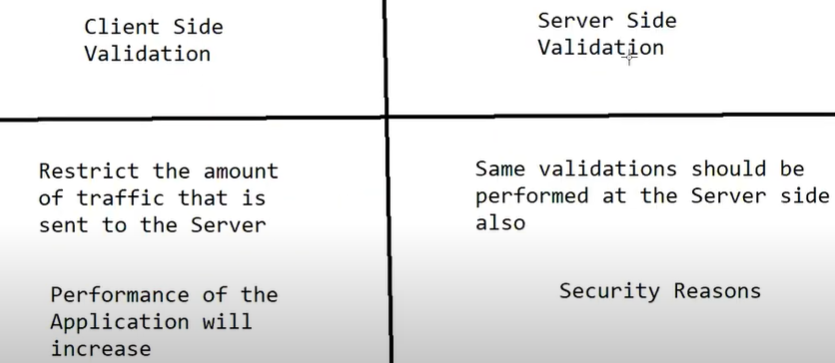
****

**Security Testing Basics – Input validation and Output Encoding:**

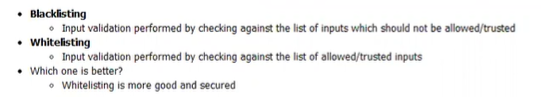
****

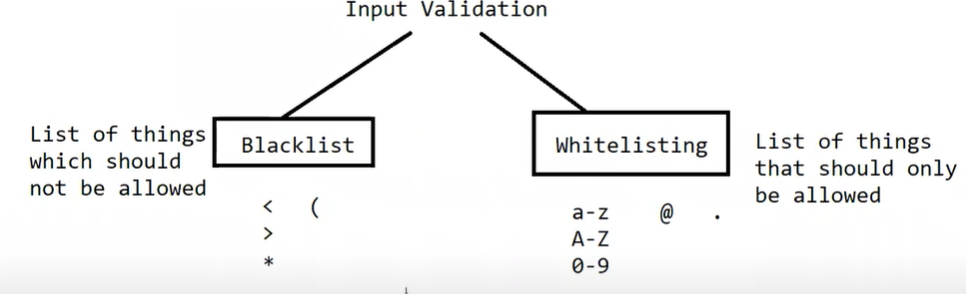
**Security Testing Basics – Client-side validation vs Server-side validation:**

Client-side validation can be bypassed.

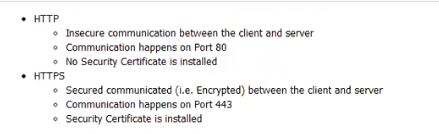


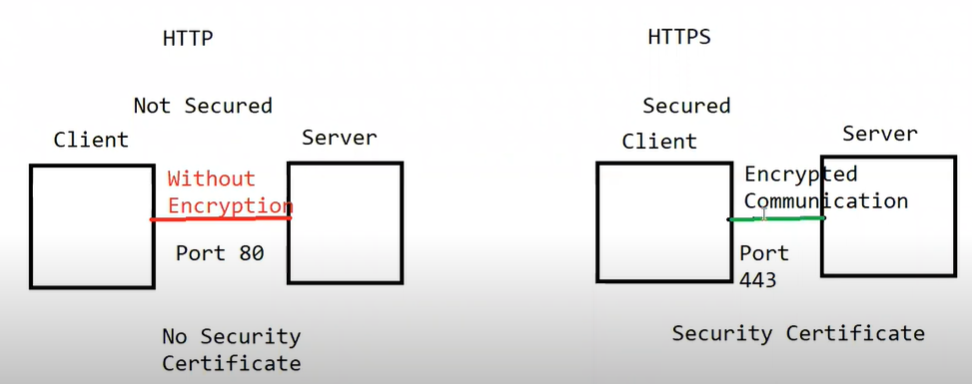
**Security Testing Basics – Blacklisting vs Whitelisting:**





**Security Testing Basics – HTTP vs HTTPS:**





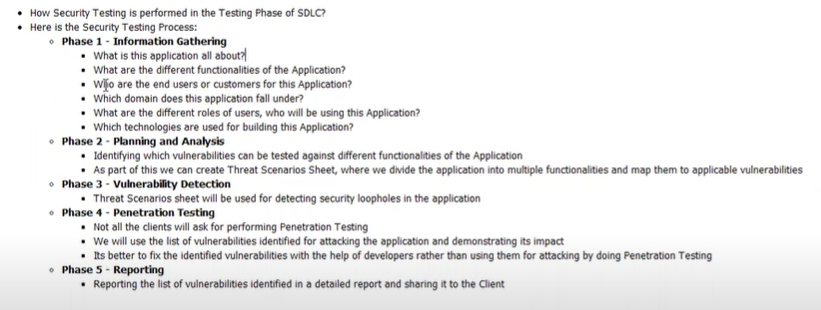
**Security testing terminology – Payload and Malicious input:**

****

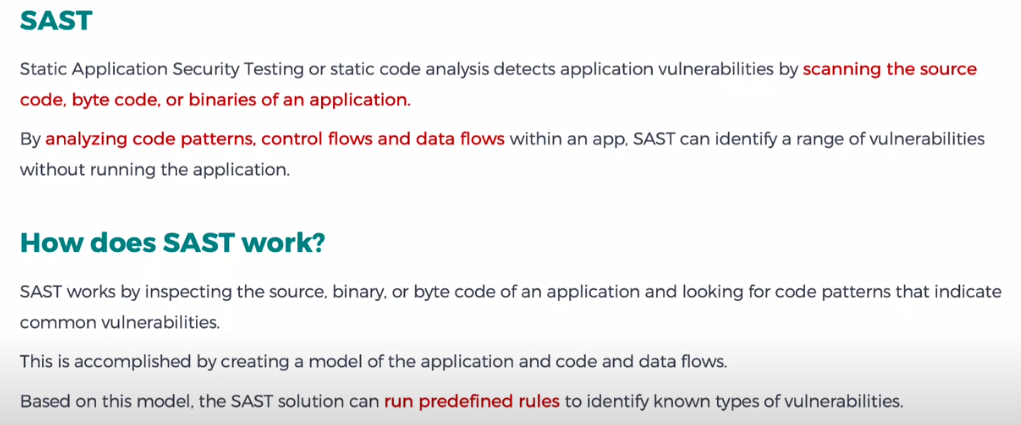
**Security testing terminology – DAST:**

**DAST** stands for Dynamic Application Security testing, it’s a black box security testing techniques performed on running application using the UI.

**Security Testing process in SDLC phases:**



**SAST vs DAST:**



A screenshot of a computer

Description automatically generated

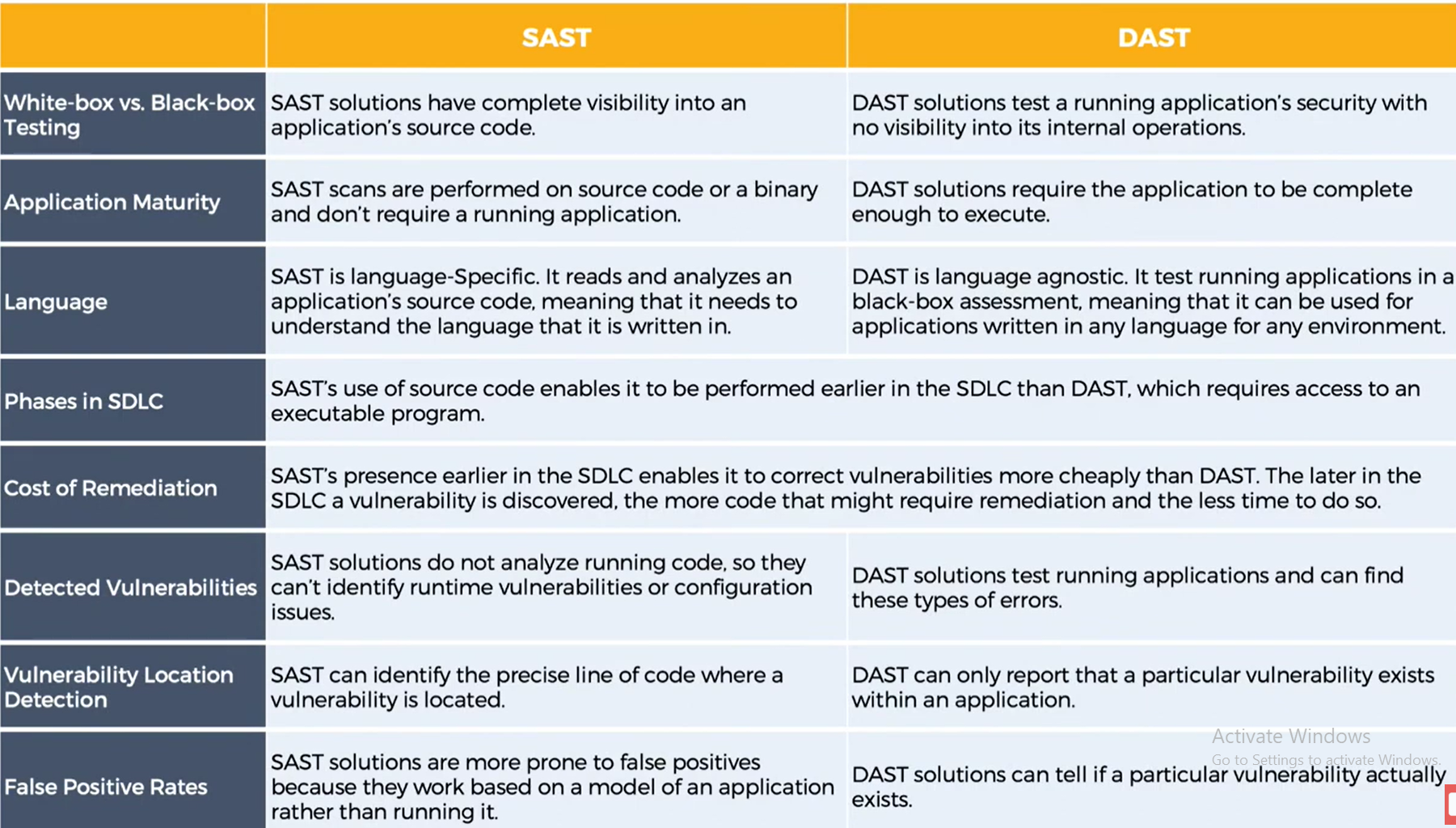
1.How to spot vulnerabilities in web application.

2.Reports manually

3.What type of attacks do security testing companies generally do on mobile/web application.

4.Exploring ZAP Tool features.

5.

****

**Risk Identification, Assessment and Mitigation:**

Risk assessment models:

Risk Models defines the risk factors to be assessed and relationship among those factors.

NIST publications 800-30.

Guide for conducting Risk assessments [NIST 800-30]

OWASP Risk rating methodology [OWASP2]

**Typical Risk Factors Include:**

1.Threat

2.Vulnerability

3.Impact

4.Likelyhood

5.Predosposing condition