NASSCOM® FOUNDATION

Directorate General of Training

Powered by Microsoft

Session2-Explain Cyber

Session2-Explain Cyber Security

Securing website from unauthorized person and third parties

- HTTPS and SSL are used to secure your website.
- Both technologies prevent the data from being read by the man in the middle while sending or receiving the data on the internet.
- HTTPS is the secured version of HTTP protocol that is used by the browser for communication. It uses SSL/TLS for delivering the encrypted data
- On the other hand, SSL is an encryption protocol that is used to encrypt data.

What is HTTPS

- HTTP is the Hypertext Transfer Protocol, which is the most commonly used protocol worldwide.
- The HTTP request is a communication request that is sent by the client(browser) to the webserver.
- The http request and response are in the form of simple text; anyone who is monitoring the session can read the information that is being transferred. Hence it can be a threat as the information can be tempered by man in the middle. To remove this threat, HTTPS was introduced, which is the secured version of HTTP
- It encrypts the data that is retrieved by HTTP protocol and also ensures that data that is being transferred between computers and servers cannot be read by any third person.
- When HTTP is combined with an encryption protocol such as SSL/TLS, it is known as HTTPS.
- HTTPS Stands for Hypertext Transfer Protocol Secure, which is the secure version of the HTTP protocol.

Advantages of HTTPS

- **Secure Communication**: HTTPS protocol transfers data by establishing a secure connection.
- **Data Integrity:** With the help of encryption and authentication, HTTPS provides data integrity between browser and website.
- **Privacy and Security:** It provides privacy and security to prevent the websites from being hacked or passively listen to the communication between browser and server.
- **Faster Performance:** HTTPS enhances the speed of data transfer by reducing the size of data, hence provides faster performance.
- **SEO:** HTTPS is preferred by the search engines as a ranking signal while generating the search results.
- **User Experience:** HTTPS provides a good user experience by increasing the trust of users.

SSL

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- The term cyber security refers to both personal and business devices, mobile computing that are connected to the internet.
- Information security differs from cybersecurity in both scope and purpose.
- Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them.
- The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security.

SSL certificate

what does a SSL certificate contains?

- Name of the domain for which the certificate has been issued.
- Name of the person, organization, or device to which it was provided.
- a certificate authority that issued it
- Digital signature of the certificate authority.
- Associated subdomains
- Issue date of the certificate
- The expiration date of the certificate
- The public key.

Working of SSL

How does SSL work?

SSL encrypts the data that is being transmitted over the internet to make it secure. It means, if a hacker gets the data encrypted with SSL, he will only see the mixed characters, which are nearly impossible to decrypt or read.

Reasons why SSL is mandatory

- For authentication

- To build trust
- To comply with Company Standard

Difference between HTTP and SSL

How HTTPS is different from SSL?

SSL	HTTPS
It is abbreviated as Secure Sockets Layer.	It is abbreviated as Hypertext Transfer Protocol Secure.
It is the first cryptography protocol.	It is the secure version of HTTP, which is a communication protocol between browsers and web servers.
It is used along with HTTP to convert it into HTTPS	HTTPS can be said as the combination of HTTP and SSL.
The main aim of SSL is to provide security and encryption in data transmission.	The main aim of using HTTPS is to increase the security of data transfer, and it is done with the help of cryptography protocols such as SSL/TLS.
There are three versions of SSL, which are SSL1.0, SSL 2.0, SSL 3.0.	There is no other version of HTTPS yet.
Currently, it is considered deprecated and no longer in use. Instead, TLS(Transport Layer Security) protocol is being used widely to provide data security for communication over the internet.	Most of the websites are switching to HTTPS rather than HTTP. If a website does not use HTTPS, browsers flag that site as "Not secure," which also affects the user experience.

List Information Security Vulnerabilities

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. Vulnerabilities mostly happen because if Hardware, Software, Network and Procedural vulnerabilities.

Hardware Vulnerabilities

A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely. Example: Unprotected storage, Unencrypted devices

Software Vulnerabilities

A software error happen in development or configuration such as the execution of it can violate the security policy. Example, Lack of input validation, Unverified uploads, etc.

Network Vulnerabilities

A weakness happen in network which can be hardware or software.Example: Unprotected communication, Social engineering attacks

Procedural Vulnerabilities

A weakness happen in an organization operational methods.Example: Password Procedure, Training Procedure

List of vulnerabilities found.

List of Vulnerabilities		
Complicated user interface	Inadequate physical protection	Lack of or poor implementation of internal audit
Default passwords not changed	Inadequate protection of cryptographic keys	Lack of policy for the use of cryptography
Disposal of storage media without deleting data	Inadequate replacement of older equipment	Lack of procedure for removing access rights upon termination of employment
Equipment sensitivity to changes in voltage	Inadequate security awareness	Lack of protection for mobile equipment
Equipment sensitivity to moisture and contaminants	Inadequate segregation of operational and testing facilities	Lack of systems for identification and authentication
Equipment sensitivity to temperature	Inadequate segregation of duties	Lack of redundancy
Inadequate capacity management	Inadequate supervision of vendors	Location vulnerable to flooding
Inadequate change management	Inadequate training of employees	Poor selection of test data
Inadequate classification of information	Incomplete specification for software development	Uncontrolled download from the Internet
Inadequate control of physical access	Insufficient software testing	Single copy
Inadequate maintenance	Lack of access control policy	Too much power in one person
Inadequate network management	Lack of clean desk and clear screen policy	Uncontrolled copying of data
Inadequate or irregular backup	Lack of control over the input and output data	Uncontrolled use of information systems
Inadequate password management	Lack of internal documentation	Undocumented software
User rights are not reviewed regularly	Unprotected public network connections	Unmotivated employees

Manging the vulnerabilities

How to mange the vulnerabilities

Vulnerability management is the process of identifying, classifying, mitigating, and remediating system vulnerabilities.

Following are the three key steps in managing vulnerabilities:

Identify vulnerabilities is the process of locating and noting exploitable gaps in your network operations.

Evaluate vulnerabilities - Vulnerability assessment allows you to assign risk levels to the identified vulnerabilities so that you can prioritize remediation efforts.

Address vulnerabilities - The different ways you can treat a vulnerability include:

- Remediation
- Mitigation
- Acceptance

Describe Risk Assessment & Management

what is risk assessment?

- Risk assessment is the process of identifying, analyzing, and evaluating risk.
- It is the only way to ensure that the cybersecurity controls you choose are appropriate to the risks you or your organization faces.
- A cybersecurity risk assessment identifies the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets.
- A risk estimation and evaluation is usually performed, followed by the selection of controls to treat the identified risks.

Risk management process

These steps are followed for A risk management programme

- Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
- Analyse the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
- Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
- Prioritise the risks.
- Decide how to respond to each risk. There are generally four options:
- Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.
- Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).

- Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
- Transfer – share the risk with another party, usually by outsourcing or taking out insurance.

____

____

____

____

____

____

____

____

Standards for security risk management in Clause 6.1.2 of ISO 27001

- Risk management is a key requirement of many information security standards and frameworks

Following are some of the standards given for security risk management in Clause 6.1.2 of ISO 27001

- Establish and maintain information security risk criteria;
- Ensure that repeated risk assessments produce "consistent, valid and comparable results";
- "identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system";
- Identify the owners of those risks; and
- Analyse and evaluate information security risks according to the criteria established earlier.

____

____

____

____

____

____

Recap:

- SSL is an encryption protocol that is used to encrypt data.
- HTTPS is the secured version of HTTP protocol
- HTTPS Stands for Hypertext Transfer Protocol Secure
- Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets.
- Risk assessment is the process of identifying, analyzing, and evaluating risk.