**Long Answer Types(5 Marks, 10 Marks)**

1. Explain different session hijacking and fixation techniques. How session hijacking is done?

Ans: Session hijacking is as the term suggests. A user in a session can be hijacked by an attacker and lose control of the session altogether, where their personal data can easily be stolen. After a user starts a session such as logging into a banking website, an attacker can hijack it.

**Cross-site scripting (XSS):** Attackers exploit vulnerabilities within servers or applications to inject client-side Java scripts into the users’ web pages, causing your browser to execute arbitrary code when it loads a compromised page.

**Session side jacking:** By using packet sniffing, an attacker can monitor the traffic within the network and intercept the user's session cookies after they have authenticated it.

* **Session fixation:** Attackers supply a session key and spoof the user into accessing a vulnerable server.

1. Explain GSM security network and its security algorithms.

Ans: GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

GSM uses three different security algorithms called **A3, A5, and A8**. In practice, A3 and A8 are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres.

1. How input injection attack is performed? Explain all methods.

Ans: - An injection attack can expose or damage data and lead to a [denial of service](https://crashtest-security.com/denial-of-service-attack/) or a full webserver compromise. Such attacks are possible due to vulnerabilities in the code of an application that allows for unvalidated user input.

**SQL Injection (SQLi)**

SQL is a query language to communicate with a database. It can be used to perform actions to retrieve, delete and save data in the database.

### ****C****ross-Site Scripting (XSS)

Whenever an application allows user input within the output it generates, it allows an attacker to send malicious code to a different end-user without validating or encoding it. [Cross-Site Scripting (XSS) attacks](https://crashtest-security.com/cross-site-scripting-xss/) take these opportunities to inject malicious scripts into trusted websites.

A text containing malicious code (typically in JavaScript) is inserted i

### Code Injection

In this scenario, an attacker is acquainted with the application code and programming language.

### Command Injection

Sometimes web applications need to call a system command on the web server running them.

### CCS Injection

A [CCS injection](https://crashtest-security.com/prevent-ccs-injection/) exploits a vulnerability found in the ChangeCipherSpec processing in some versions of OpenSSL.

1. How client side scripts help to execute any web application?

Ans:- **1. Client-side scripting :**   
[Web browsers](https://www.geeksforgeeks.org/difference-between-web-browser-and-web-server/) execute client-side scripting. It is used when browsers have all code. Source code is used to transfer from [webserver](https://www.geeksforgeeks.org/web-server-and-its-type/) to user’s computer over the [internet](https://www.geeksforgeeks.org/the-internet-and-the-web/) and run directly on browsers. It is also used for validations and functionality for user events.

It allows for more interactivity. It usually performs several actions without going to the user. It cannot be basically used to connect to databases on a web server. These scripts cannot access the file system that resides in the web browser. Pages are altered on basis of the user’s choice. It can also be used to create “cookies” that store data on the user’s computer.

**Client-side scripting**, like JavaScript, can be embedded into the page on the client’s browser. This script will allow the client’s browser to alleviate some of the burden on your web server when running a web application. Client-side scripting is source code that is executed on the client’s browser instead of the web-server, and allows for the creation of faster and more responsive web applications.

1. Explain different ways to perform session hijacking. How is it mitigated?

Ans:

* **Cross-site scripting (XSS):** Attackers exploit vulnerabilities within servers or applications to inject client-side Java scripts into the users’ web pages, causing your browser to execute arbitrary code when it loads a compromised page. If the server doesn’t set the HTTPOnly in session cookies, injected scripts can gain access to your session key, providing attackers with the necessary information for session hijacking.
* **Session side jacking:** By using packet sniffing, an attacker can monitor the traffic within the network and intercept the user's session cookies after they have authenticated it. If the website takes the cheap route of using [SSL/TLS encryption](https://shop.globalsign.com/en/ssl-tls-certificates) for its login pages only, the attacker can use the session key they have derived from packet sniffing to hijack the user's session and impersonate them to perform actions in the web application. This can usually happen in case of an unsecured WiFi Hotspot in order to gain access to the network, monitor the traffic and set up their own access points to perform the attack.
* **Session fixation:** Attackers supply a session key and spoof the user into accessing a vulnerable server.

We can mitigate this by these prevention techniques

**HTTPS:** The use of HTTPS ensures that there is [SSL/TLS encryption](https://www.globalsign.com/en/blog/maximum-ssltls-certificate-validity-now-one-year) throughout the session traffic.

**HTTPOnly:** Setting up an HTTPOnly attribute prevents access to the stored cookies from the client-side scripts.

**System Updates:** Install [reputable antivirus software](https://www.attack-secure.com/norton-vs-mcafee/) which can easily detect viruses and protect you from any type of malware

* **Session Management:** In order to offer sufficient security, website operators can incorporate web frameworks, instead of inventing their own session management systems.

**Session Key:**It is advised to regenerate session keys after their initial authentication.

**Identity Verification:** Perform additional identity verification from the user beyond the session key.

* **Public Hotspot:** Avoid using public WiFi to protect the integrity of your sessions and opt for secure wireless networks.

1. Explain network topologies along with advantages and disadvantages.
2. How android and IOS security is maintained? Explain with their layer architecture.
3. Explain Creaser cipher with an example.

Ans:- In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a **Caesar cipher**, also known as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known [encryption](https://en.wikipedia.org/wiki/Encryption) techniques. It is a type of [substitution cipher](https://en.wikipedia.org/wiki/Substitution_cipher) in which each letter in the [plaintext](https://en.wikipedia.org/wiki/Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](https://en.wikipedia.org/wiki/Alphabet). For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after [Julius Caesar](https://en.wikipedia.org/wiki/Julius_Caesar), who used it in his private correspondence.[[1]](https://en.wikipedia.org/wiki/Caesar_cipher#cite_note-1)

1. Explain encryption and decryption process of Monoalphabetic cipher with an example

Ans:- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

1. Discuss polyalphabetic algorithm with example.

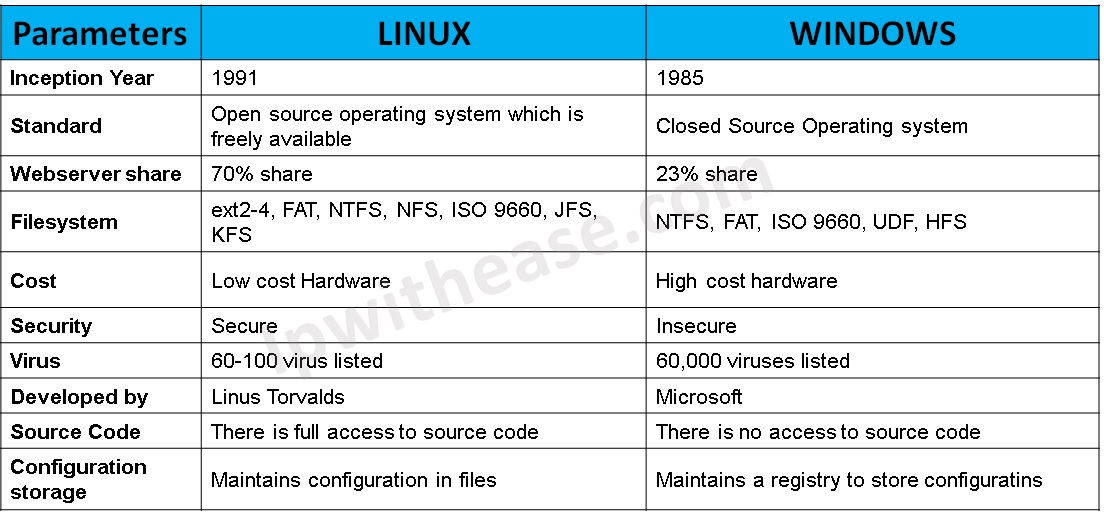
Ans:- A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.

For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle. The polyalphabetic ciphers have the benefit of hiding the letter frequency of the basic language. Therefore attacker cannot use individual letter frequency static to divide the ciphertext.

1. What types of attacks are performed on remote server? Explain each with their countermeasures.
2. Explain the working of CAPTCHA program.

Ans:- Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again. Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages. The idea is that a computer program such as a bot will be unable to interpret the distorted letters, while a human being, who is used to seeing and interpreting letters in all kinds of contexts – different fonts, different handwritings, etc. – will usually be able to identify them.

1. Differentiate between Window and Linux.

Ans: 

1. Explain security measures of WI-FI attacks.

Ans:- **Change default passwords.** Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup.

**Restrict access.** Only allow authorized users to access your network.

**install a firewall.** Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall).

**Maintain antivirus software.**Install antivirus software and keep your virus definitions up to date.

**Connect using a Virtual Private Network (VPN).**Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office

1. How SQL injection is performed? Explain methods and solutions.

Ans:- SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

To make an SQL Injection attack, an attacker must first find vulnerable user inputs within the web page or web application. A web page or web application that has an SQL Injection vulnerability uses such user input directly in an SQL query. The attacker can create input content. Such content is often called a malicious payload and is the key part of the attack. After the attacker sends this content, malicious SQL commands are executed in the database.

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

1. How HTML injection is performed? Explain methods and solutions.

Ans:- In order to perform this type of injection, firstly, the malicious user should find vulnerable parts of the website. As it was mentioned, vulnerable parts of the website may be data input fields and website’s link.

Malicious HTML code can get into the source code by innerHTML. Let’s remember, that innerHTML is the property of DOM document and with innerHTML, we can write dynamic HTML code. It is used mostly for data input fields like comment fields, questionnaire forms, registration forms, etc. Therefore those elements are most vulnerable to HTML attack.

#### **#1) Stored HTML Injection:**

The main difference between those two injection types is that stored injection attack occurs when malicious HTML code is saved in the web server and is being executed every time when the user calls an appropriate functionality.

#### **#2) Reflected HTML Injection:**

**This can be again divided into more types:**

* Reflected GET
* Reflected POST
* Reflected URL

Reflected Injection attack can be performed differently according to the HTTP methods i.e, GET and POST. I would remind, that with POST method data is being sent and with GET method data is being requested.

Prevention

There are no doubts, that the main reason for this attack is the developer’s inattention and lack of knowledge. This type of injection attack occurs when the input and output are not properly validated. Therefore the main rule to prevent HTML attack is appropriate data validation.

Every input should be checked if it contains any script code or any HTML code. Usually it is being checked, if the code contains any special script or HTML brackets – <script></script>, <html></html>

1. How CSS and CSRF are performed? Explain methods and solutions.

Ans:

CSS

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.

Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

## **What are the types of XSS attacks?**

There are three main types of XSS attacks. These are:

* [Reflected XSS](https://portswigger.net/web-security/cross-site-scripting#reflected-cross-site-scripting), where the malicious script comes from the current HTTP request.
* [Stored XSS](https://portswigger.net/web-security/cross-site-scripting#stored-cross-site-scripting), where the malicious script comes from the website's database.
* [DOM-based XSS](https://portswigger.net/web-security/cross-site-scripting#dom-based-cross-site-scripting), where the vulnerability exists in client-side code rather than server-side code.

Preventing cross-site scripting is trivial in some cases but can be much harder depending on the complexity of the application and the ways it handles user-controllable data.

In general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

* **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
* **Encode data on output.** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
* **Use appropriate response headers.** To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
* **Content Security Policy.** As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

CSRF

[Cross-site Request Forgery](https://www.invicti.com/learn/cross-site-request-forgery-csrf/), also known as CSRF, Sea Surf, or XSRF, is an attack whereby an attacker tricks a victim into performing actions on their behalf. There are two main parts to executing a Cross-site Request Forgery attack. The first one is tricking the victim into clicking a link or loading a page. This is normally done through social engineering and malicious links. The second part is sending a crafted, legitimate-looking request from the victim’s browser to the website. The request is sent with values chosen by the attacker including any cookies that the victim has associated with that website

## A CSRF Attack Example Using a GET Request

HTTP GET is by its very nature meant to be an idempotent request method. This means that this HTTP method should not be used to perform state changes. Sending a GET request should never cause any data to change. However, some web apps still use GET instead of the more appropriate POST to perform state changes for operations such as changing a password or adding a user.

## CSRF Attacks Using POST Requests

Most state-changing requests are done using HTTP POST requests. This means that web apps are more likely to accept POST instead of GET when a state change is involved. In the case of POST, the user’s browser sends parameters and values in the request body and not the URL as in the case of a GET request.

Security experts propose many CSRF prevention mechanisms. This includes, for example, using a referer header, using the HttpOnly flag, sending an X-Requested-With custom header using jQuery, and more. Unfortunately, not all of them are effective in all scenarios. In some cases, they are ineffective and in other cases, they are difficult to implement in a particular application or have side effects.

1. Explain different types of mobile malwares and security practices.

Ans:- Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones and tablets, with the goal of gaining access to private data.

## Types of Mobile Malware

* **Remote Access Tools (RATs)** offer extensive access to data from infected victim devices and are often used for intelligence collection. RATs can typically access information such as installed applications, call history, address books, web browsing history, and sms data. RATs may also be used to send SMS messages, enable device cameras, and log GPS data.
* **Bank trojans** are often disguised as legitimate applications and seek to compromise users who conduct their banking business — including money transfers and bill payments — from their mobile devices. This type of trojan aims to steal financial login and password details.
* [**Ransomware**](https://www.crowdstrike.com/cybersecurity-101/ransomware/)is a type of [malware](https://www.crowdstrike.com/cybersecurity-101/malware/) used to lock out a user from their device and demand a “ransom” payment — usually in untraceable Bitcoin. Once the victim pays the ransom, access codes are provided to allow them to unlock their mobile device.
* **Cryptomining Malware** enables attackers to covertly execute calculations on a victim’s device – allowing them to generate cryptocurrency. Cryptomining is often conducted through Trojan code that is hidden in legitimate-looking apps.
* **Advertising Click Fraud** is a type of malware that allows an attacker to hijack a device to generate income through fake ad clicks.

**Mobile Device Security Best Practices**

* Enable user authentication.
* Always run updates.
* Avoid public wifi.
* Use a password manager.
* Enable remote lock.
* Cloud backups.

1. What types of attacks are performed through Bluetooth connection? Explain.

Ans:- There are different types of hacking such as **Bluejacking, Bluesnarfing, Bluebugging, Bluetoothing, Blueprinting** etc. The purpose of this entire Bluetooth hacking is to hack your phone and your privacy. Bluetooth hacking takes place because of security lacking in Bluetooth technology.

## **Bluejacking**

### Description

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field to another Bluetooth-enabled device via the OBEX protocol.

## **Bluesnarfing**

### Description

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

## **Bluebugging**

### Description

Bluebugging is a form of Bluetooth attack often caused by a lack of awareness. It was developed after the onset of bluejacking and bluesnarfing.

1. Explain Attacks and countermeasures for common web authentication.
2. What attacks are performed on VoIP? How is it made secure? Explain

Ans:- VoIP hacking is a type of attack that a person uses to infiltrate your business phone system. They can listen in on calls, rack up expensive bills, and steal sensitive information–both about your business and your customers.

### 1. Unauthorized use

This type of attack is when hackers use your business’ phone system to make phone calls.

### 2. Toll fraud

Toll fraud occurs when hackers make international calls to other devices. Toll charges for these long-distance phone numbers can be expensive and will be billed from your account. A staggering **$27 billion** is lost due to toll fraud, according to [Trend Micro](https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/toll-fraud-irsf-criminals-monetize-hacked-phones-iot-devices-telecom-fraud).

### 3. Caller ID spoofing

When your phone rings and the caller ID appears, do you trust the number shown?  
Caller ID isn’t always a reliable way to verify the person calling you. Attackers can use fake caller IDs and leverage them in coordination with another attack, like social engineering.

### 4. Eavesdropping

Eavesdropping is only possible when the connection is unencrypted or the local network itself is breached. Insecure Wi-Fi networks—those without Transport Layer Security (TLS) and Real-time Transport Protocol (SRTP) — can invite attackers to monitor the network.

### 5. Social engineering

Social engineering is used by attackers because they prey on the fact that people genuinely want to be nice. It’s uncomfortable to say no when someone asks for something—especially if you’ve got no reason to doubt who they say they are.

1. Elaborate the countermeasures or mitigations for SQL INJECTION attack.
2. Discuss the countermeasures or mitigations for wifi attack.
3. How VPN is used to provide security in public network? Explain.

Ans:- VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

### What should a good VPN do?

**Encryption of your IP address:**

**Encryption of protocols**

**Kill switch**

**Two-factor authentication:**

1. How hashing is different from encryption? Explain.

Since encryption is two-way, the data can be decrypted so it is readable again. Hashing, on the other hand, is one-way, meaning the plaintext is scrambled into a unique digest, through the use of a salt, that cannot be decrypted. Technically, hashing can be reversed, but the computational power needed to decrypt it makes decryption infeasible.

|  |  |  |
| --- | --- | --- |
|  | **Encryption** | **Hashing** |
| **Definition** | A two-way function that takes in plaintext data, and turns it into undecipherable ciphertext. | A one-way method of hiding sensitive data. Using a hashing algorithm, hashing turns a plaintext into a unique hash digest that cannot be reverted to the original plaintext, without considerable effort. |
| **Reversible or Irreversible?** | Reversible | Irreversible |
| **Variable or Fixed Length Output?** | Variable Length | Fixed Length |
| **Types** | Asymmetric and Symmetric | Hashing |
| **Common Algorithms** | AES, RC4, DES, RSA, ECDSA | SHA-1, SHA-2, MD5, CRC32, WHIRLPOOL |

1. Explain the working process of session hijacking using Burpsuite.
2. Discuss the working of Digital Signatures.

Ans:- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender ([authenticity](https://en.wikipedia.org/wiki/Authentication)), and that the message was not altered in transit ([integrity](https://en.wikipedia.org/wiki/Data_integrity)).[[1]](https://en.wikipedia.org/wiki/Digital_signature#cite_note-Vtkl8-1)

Digital signatures are a standard element of most [cryptographic protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol) suites, and are commonly used for software distribution, financial transactions, [contract management software](https://en.wikipedia.org/wiki/Contract_management_software), and in other cases where it is important to detect forgery or [tampering](https://en.wikipedia.org/wiki/Tampering_(crime)).

1. What security practices are applied to keep your Mobile phone safe?
2. Why IOS is more secure than android? Explain.

Ans: Apple’s mobile devices and their operating systems are inseparable, giving them far more control over how they work together. While iOS device features are more restricted than an Android device, the iPhone’s integrated design makes security vulnerabilities far less frequent and harder to find.

Android’s open nature means it can be installed on a wide range of devices. Depending on the manufacturer and the model, this can be a good thing or a bad thing. Some mobile devices integrate perfectly with Android while others leave significant security vulnerabilities.

**Security patch and updates:** **Apple updates are easier to control across devices, promising consistent security.**

Android and iOS software updates and security updates are some of the main ways that Apple and Google can keep their devices secure. Because Apple strictly controls the devices in its ecosystem, updates are easier to create and distribute. This also means that Apple can usually keep iOS devices updated for longer, generally withdrawing official support after 5 years.

1. Explain the security countermeasures for Android and IOS.
2. How to ensure security of window phone?

ANS: **Set PINs and passwords**. To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone’s home screen as a first line of defense in case your phone is lost or stolen

**Do not modify your smartphone’s security settings**. Do not alter security settings for convenience. Tampering with your phone’s factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

**Only install apps from trusted sources**. Before downloading an app, conduct research to ensure the app is legitimate.

**Be smart on open Wi-Fi networks**. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals.

**Wipe data on your old phone before you donate, resell or recycle it**. Your smartphone contains personal data you want to keep private when you dispose your old phone.

1. Explain the following in detail(types, methods and solutions):
2. Wi-fi Security
3. ASP.net and PHP attacks
4. Apache and IIS server attacks
5. Admin misconfiguration attack
6. Security of Mobile VoIP Communications.
7. Elaborate following: (methods and mitigations)
8. LTE network security
9. Stealth-encoding techniques
10. Emerging Trends in Mobile Security-Mobile Geo-location
11. XSS Attack
12. XML injection attacks