Yusuf Selaboy

VUG/CSC/21/5772

Cyber security

23rd April, 2024.

1. **Phishing**

Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware such as ransom ware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Center reporting more incidents of phishing than any other type of computer crime.

**Types of Phishing**

1. Email phishing
2. Spear phishing
3. Whaling and CEO fraud
4. Clone phishing
5. Voice phishing
6. SMS phishing
7. Page hijacking
8. Calendar phishing
9. Quishing

**Techniques of Phishing**

**Social Engineering**

Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information. It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account.

An alternative technique to impersonation-based phishing is the use of fake news articles to trick victims into clicking on a malicious link. These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to install malware or present fake "virus" notifications to the victim.

1. **SQL injection**

In computing, SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Example**

var statement = "SELECT \* FROM users WHERE name = '" + userName + "'";

Setting the "userName" variable as:

' OR '1'='1

There are three types of SQL comments

' OR '1'='1' --

' OR '1'='1' {

' OR '1'='1' /\*

Renders one of the following SQL statements by the parent language:

SELECT \* FROM users WHERE name = '' OR '1'='1';

SELECT \* FROM users WHERE name = '' OR '1'='1' -- ';

a';DROP TABLE users; SELECT \* FROM userinfo WHERE 't' = 't

The final SQL statement as follows and specified:

SELECT \* FROM users WHERE name = 'a';DROP TABLE users; SELECT \* FROM userinfo WHERE 't' = 't';

1. **Cross-Site Scripting**

Cross-site scripting (XSS) is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. During the second half of 2007, XSSed documented 11,253 site-specific cross-site vulnerabilities, compared to 2,134 "traditional" vulnerabilities documented by Symantec. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

1. **XML Injection**

XML (Extensible Markup Language) is a markup language used to store and transport data. It is designed to be self-descriptive and allows users to define their own tags, making it highly customizable. XML is commonly used for data storage, configuration files, and web services.

XML Injection is a type of attack that targets web applications that generate XML content. Attackers use malicious code to exploit vulnerabilities in XML parsers to manipulate the content of an XML document. This can result in unauthorized access to sensitive data, denial of service, and other potential risks to the application and its users.

**XPath Vulnerable Code**

import lxml.etree as ET

# User input (usually obtained through a web form)

username = input("Enter your username: ")

password = input("Enter your password: ")

# Construct the XPath query with user input

query = "/users/user[username/text()='" + username + "' and password/text()='" + password + "']"

# Parse the XML file

tree = ET.parse("users.xml")

root = tree.getroot()

# Attempt to find a user with the given credentials

user = root.xpath(query)

# Check if the user was found

if user:

print("Authentication successful. Welcome, " + username + "!")

else:

print("Authentication failed. Invalid username or password.")

1. **LDAP injection**

In computer security, LDAP injection is a code injection technique used to exploit web applications which could reveal sensitive user information or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores. LDAP injection exploits a security vulnerability in an application by manipulating input parameters passed to internal search, add or modify functions. When an application fails to properly sanitize user input, it is possible for an attacker to modify an LDAP statement.

String filter = “(&(USER = ” + user\_name + “) (PASSWORD = “ + user\_password + “))”;

1. **Using Logs to Investigate – SQL Injection Attack Example**

A log file is an extremely valuable piece of information that is provided by a server. Almost all servers, services, and applications provide some sort of logging. A log file records events and actions that take place during the run time of a service or application.

Log files provide us with a precise view of the behavior of a server as well as critical information like when, how, and by whom a server is being accessed. This kind of information can help us monitor the performance, troubleshoot and debug applications, as well as help forensic investigators unfold the chain of events that may have led to malicious activity.