PHISHING

COMPUTER NETWORKING

Time: 60 mins

Introduction

In this class, the students will learn how to clone a website and how phishing attack are created.

New Commands Introduced

● CORS(app)	Enables CORS.
● $.ajax()	Initiates an AJAX request.
● $(document).ready(function() { ... })	Ensures that the code inside the function runs only after the DOM is fully loaded.
● $('#element').append(content)	Appends content to the selected element.
● $("#element").val()	Retrieves the value from the selected element.
● $("{{elementVariable}}")	Inserts the value in the variable.

Vocabulary

- **Phishing** is a cybercrime in which attackers trick individuals into disclosing sensitive information, such as passwords.
- **AJAX** web applications can send and retrieve data from a server asynchronously (in the background) without interfering with the display and behaviour of the existing page.
- **jQuery** is a JavaScript library designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animations, and Ajax.
- The **Document Object Model (DOM)** is a cross-platform and language-independent interface that treats an HTML or XML document as a tree structure wherein each node is an object representing a part of the document.

Learning Objectives

Student/s should be able to:

- ***Recall*** how to send email by SMTP and MIME.
- ***Explain*** how to clone a website and how phishing attack executed.

- ***Demonstrate*** the phishing attack by clonning two websites.

Activities

1. **Class Narrative:** *(3 mins)*

    - Brief the student/s that the disruptive school closure message that caused chaos was sent out sent out by the hackers.

2. **Concept Introduction Activity:** *(4 mins)*

    - Let the student/s undertake the explore-activity to observe how to clone a website and how phishing attack are created.
    - Brief the student of how the large scale cyber attack which affected many US enterprise in 2009 took place.
    - Give examples of the different phishing attacks:
        - **Pop-up phishing** is the technique in which the notification feature of the web browser is used to infect computer.
        - **Image phishing** uses images with malicious files in them meant to help a hacker steal your account info or infect your computer.
        - **Email spoofing** attacks change the apparent source address of an email. This makes the email appear to come from a known address.
        - In **website spoofing**, a hacker creates a fake website that looks legitimate. When you use the site to log in to an account, your info is collected by the hacker.
        - **Vishing** scams take place over the phone or voice messages. In the most common form, the perpetrator poses as a partner firm, vendor or supplier of the target organization.
        - **Smishing** is an attack that uses text messaging or short message service (SMS) to execute the attack.
    - Using the slides, explain that the student/s will learn:
        - to clone the web page.
        - to email the credentials.
        - to clone multiple web pages.

3. **Activity 1: Clone the Web page** *(16 mins)*

    Teacher Activity: *(8 mins)*

    - Explain about CORS, AJAX, and jQuery.
    - Demonstrate how to copy the web page and display the HTML page.
    - Initialize the request and retrieve the HTML content.

    Student Activity: *(8 mins)*

- Guide the student/s to cloned the website by extracting the html content of the website and load the content on the proxy server dynamically using jQuery and AJAX .

4. **Activity 2: Email the Credentials** *(10 mins)*

   Teacher Activity: *(5 mins)*

- Explain how using AJAX the whole page is not reloaded only the required fields are reloaded.
- Demonstrate how to fetch the credentials and send email.

   Student Activity: *(5 mins)*

- Guide the student/s to email the credentials by fetching the credentials from the input fields and sending the email along with the credentials.

5. **Activity 3: Clone Multiple Web pages (***12 mins)*

   Teacher Activity: *(6 mins)*

- Explain how to find IDs on the website component and set the IDs to the users choice.
- Demonstrate how to pass the IDs to the proxy server and receive the IDs on server.

   Student Activity: *(6 mins)*

- Guide the students to add the feature of cloning multiple web pages by setting the ids to the user's choice and updating the ids on the proxy server.

6. **Introduce the Post class project:** *(2 min)*
   - Clone the web page of the toy store and email the credentials of the user.
7. **Test and Summarize the class learnings:** *(5 mins)*
   - Check for understanding through quizzes and summarize learning after respective activities.
   - Summarize the overall class learning towards the end of the class.
   - Give a few tips to protect themselves from phishing.
8. **Additional activities:**
   - Encourage the student/s to add the name of the phishing site as the subject of the email.
   - Encourage the student/s to redirect to the original website after the email with the credentials are sent.

9. **State the Next Class Objective:** *(1 min)*

- In the next class, student/s will learn how keylogger attacks are done.

U.S. Standards:

CSTA: 2-AP-11, 2-AP-12, 2-AP-13, 2-AP-14, 2-AP-19

Links Table		
Activity	**Activity Name**	**Link**
Class Presentation	Phishing	https://s3-whjr-curriculum-uploads.whjr.online/27919466-edbe-4e8e-970f-90eb1cba4997.html
Explore Activity	Phishing	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Activity 1	Clone the Web Page	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS-BP
Teacher Reference: Teacher Activity 1 Solution	Clone the Web Page	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS
Student Activity 1	Clone the Web Page	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Reference: Student Activity 1 Solution	Clone the Web Page	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS
Teacher Activity 2	Email the Credentials	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS-BP
Teacher Reference: Teacher Activity 2 Solution	Email the Credentials	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS
Student Activity 2	Email the Credentials	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Reference: Student Activity 2 Solution	Email the Credentials	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS
Teacher Activity 3	Clone Multiple Web Pages	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS-BP
Teacher Reference: Teacher Activity 3 Solution	Clone Multiple Web Pages	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-TAS
Student Activity 3	Clone Multiple Web Pages	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Reference: Student Activity 3 Solution	Clone Multiple Web Pages	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS
Student's Additional Activity 1	Add a Subject to the Email	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Reference: Student's	Add a Subject to the Email	https://github.com/Tynker-Computer-Ne

Additional Activity 1 Solution		tworks/TNK-M16-C123-SAS
Student's Additional Activity 2	Redirect to the Original Website	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS-BP
Teacher Reference: Student's Additional Activity 2 Solution	Redirect to the Original Website	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-SAS
Post Class Project	Web Page Cloning	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-PCP-BP
Teacher Reference: Post Class Project Solution	Web Page Cloning	https://github.com/Tynker-Computer-Networks/TNK-M16-C123-PCP