Webinar - 7

Topic : Introduction to Web Development for Hackers - Pre-Hacking Assessment

The contents in this pdf has proposed by "PYR RAO" in behalf of NHC.

Note:
This content is prepared only for educational purposes, if somebody misuse it, then the team is not liable for it.

Core components of the Web:

- **HTML** : Hypertext Markup Language is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets (CSS), ruby, php and scripting languages such as JavaScript, python etc. (Latest Version : HTML5).
- **JavaScript** : JavaScript, often abbreviated as JS, is a programming language that conforms to the ECMAScript specification. JavaScript is high-level, often just-in-time compiled, and multi-paradigm. It has curly-bracket, syntax, dynamic typing, prototype-based object-orientation, and first-class functions. And used for server-side manipulation of data.
- **CSS** : Cascade styling script used for designing the web skeleton part or presentation of documents over the html pages. (Latest version : CSS3).

HTML : Hyper Text Markup Language

Extensions : .html or .htm

- HTML is easy to use or implement into the production environment.
- It is the language that can be easily understood and can be modified.
- It provides a more flexible way to design web pages along with the text.
- Links can also be added to the web pages so it helps the readers to browse the information of their interest.

- You can display HTML documents on any platform such as Macintosh, Windows, and Linux, etc.
- Graphics, videos, and sounds can also be added to the web pages which give an extra attractive look to your web pages.

HTML Syntax & tags

Format to design a web page :

```
<!DOCTYPE html>
<html>
    <head>
        <title>NHC Home Page</title>
    </head>
    <body>
        <h1>Heading 1</h1>
        <p>Paragraph</p>
        <a href="link">Hyperlink</a>
    </body>
</html>
```

Save this code in a file with ext. (".html" or ".htm")

Live Example : https://n00b-hack3rs-community.github.io/Webinar-7/

Note : For more details about html tags : HTML Reference

Check for HTML Code sanity :

- For checking html code sanity follow these steps :
- Firstly, visit any web page - > Right Click on the page.
- Click on “**Inspect Element**” -> Now “**Developer Tab”** will open (For Chrome).
- Here you can check html code sanity by hovering over the each tags, elements and layout.
- Also check for the layout, how this layout was built.

Live Example : https://n00b-hack3rs-community.github.io/Webinar-7/

HTML Form :

Syntax : <form action=”/” method=”POST/GET”></form>

```
<!DOCTYPE html>
<html>
<body>
<h1>The form element</h1>
<form action="/action_page.php">
  <label for="fname">First name:</label>
  <input type="text" id="fname" name="fname"><br><br>
  <label for="lname">Last name:</label>
  <input type="text" id="lname" name="lname"><br><br>
  <input type="submit" value="Submit">
</form>
<p>Click the "Submit" button and the form-data will be sent to a page on the server called "action_page.php".</p>
</body>
</html>
```

1. A form tag consists of many elements like <form>, <input>, <label>, <radio>, <button> etc.
2. A form always defined with “form action” like given in the above example, “form action” indicates where the entered data should go!.
3. If a form defines “POST” action over the whole form, which means the data associated with this form will directly go to the web server along with it’s “url” (universal resource locator) via “http” protocol.
4. Vulnerabilities associated with forms : “SSRF”, CSRF”, “Data Tempering” & etc

Note : Remember Never use the "**GET**" method in html form, as it raises the security issue of "**ClearText Data Transformation**" over http or https.

Live Example :
https://n00b-hack3rs-community.github.io/Webinar-7/form/form.html

HTML IFRAME :

Syntax : <iframe src="/" border="0px" width="100" height="100"></iframe>

Framing is the technology to load a webpage inside the parent web page.

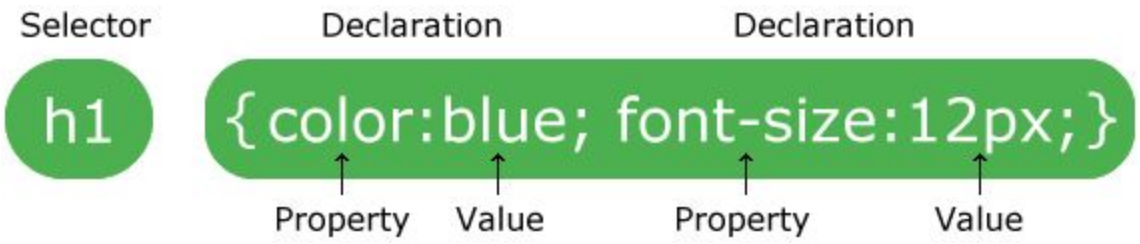
```
<!DOCTYPE html>
<html>
<body>
<center><iframe src="https://evil.com" width=200 height=100
border=0px></iframe></center>
</body>
</html>
```

Live Example :
https://n00b-hack3rs-community.github.io/Webinar-7/iframe/iframe.html

CSS - Cascade Styling Sheet :

Extension : .css & .scss

CSS - SYNTAX :



Source : https://www.w3schools.com

Types of Selector :

Selector	Example	Description
.class	.intro	Selects all elements with class="intro"
#id	#firstname	Select the element with id="firstname"
element	p	Select all <p> elements
*	*	Select all element
element,element,..	Div, p	Selects all elements and all <p> elements

Characteristics of CSS :

Property	Description	Values

color	Sets the color of a text	RGB, hex, keyword
line-height	Sets the distance between lines	normal, *number, length, %*
letter-spacing	Increase or decrease the space between characters	normal, *length*
text-align	Aligns the text in an element	left, right, center, justify
text-decoration	Adds decoration to text	none, underline, overline, line-through
text-indent	Indents the first line of text in an element	*length, %*
text-transform	Controls the letters in an element	none, capitalize, uppercase, lowercase

Javascript - JS :

Extension : .js

- Java is a logical programming language used for html web dynamic functioning.
- Easy to use and implement onto the web world's popular programming language.
- JavaScript is a dynamic computer programming language.
- It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages.
- It is an interpreted programming language with object-oriented capabilities.

Vulnerabilities associated with JS :

- **Third Party Malicious JS Code Injection to Hijacking Session.**
- **XSSI Data Exfiltration.**
- **Click HiJacking.**
- **Cookie - Stealing.**
- **CSRF (Cross-Site Request Forgery -** Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts
- **Cross-Site Scripting –** XSS is a type of attack that can be triggered at server-side as well as client side.

- Types of XSS :
- Reflected
- Dom-Based
- Persistent
- Payload : <script>alert('XSS')</script>.
    - **There're numbers of attacks that can be launched via JS.**

JS XSS Payload :

https://github.com/N00B-HACK3RS-COMMUNITY/Webinar-7/blob/master/XSS_Cheat_Sheet.md

“NHC Learning Material! Please Read it carefully, also helpful for Quiz ASSIGNMENT”

Thanks & Regards

From,

[N00B HACK3RS COMMUNITY], NHC

Founder : Sumit Oneness

Co-Founder : Piyush Kaushik

Community Coordinator : PYR Rao

15-08-2020