1110111011011

1001100

110011001100

10101010101010

00011001001

HTML

Ataki webowe

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Co to phishing?
2. Czym jest FTP?

Przypomnienie

1. Co to phishing?
   metoda oszustwa, polegająca na podszywaniu się pod inną osobę bądź instytucję (np. bank / wnuczek – ktoś zaufany) w celu wyłudzenia pewnych informacji, np. danych wrażliwych – wykorzystując socjotechniki

2. Czym jest FTP?

Przypomnienie

1. Co to phishing?
   metoda oszustwa, polegająca na podszywaniu się pod inną osobę bądź instytucję (np. bank / wnuczek – ktoś zaufany) w celu wyłudzenia pewnych informacji, np. danych wrażliwych – wykorzystując socjotechniki

2. Czym jest FTP?
   ***File Transfer Protocol*, protokół pozwalający na zdalny dostęp do plików na serwerze poprzez przesył plików (port 20 - serwer) oraz stosowanie poleceń dla serwera (21 – klient)**

Czy HTML to język programowania?

Czy HTML to język programowania?

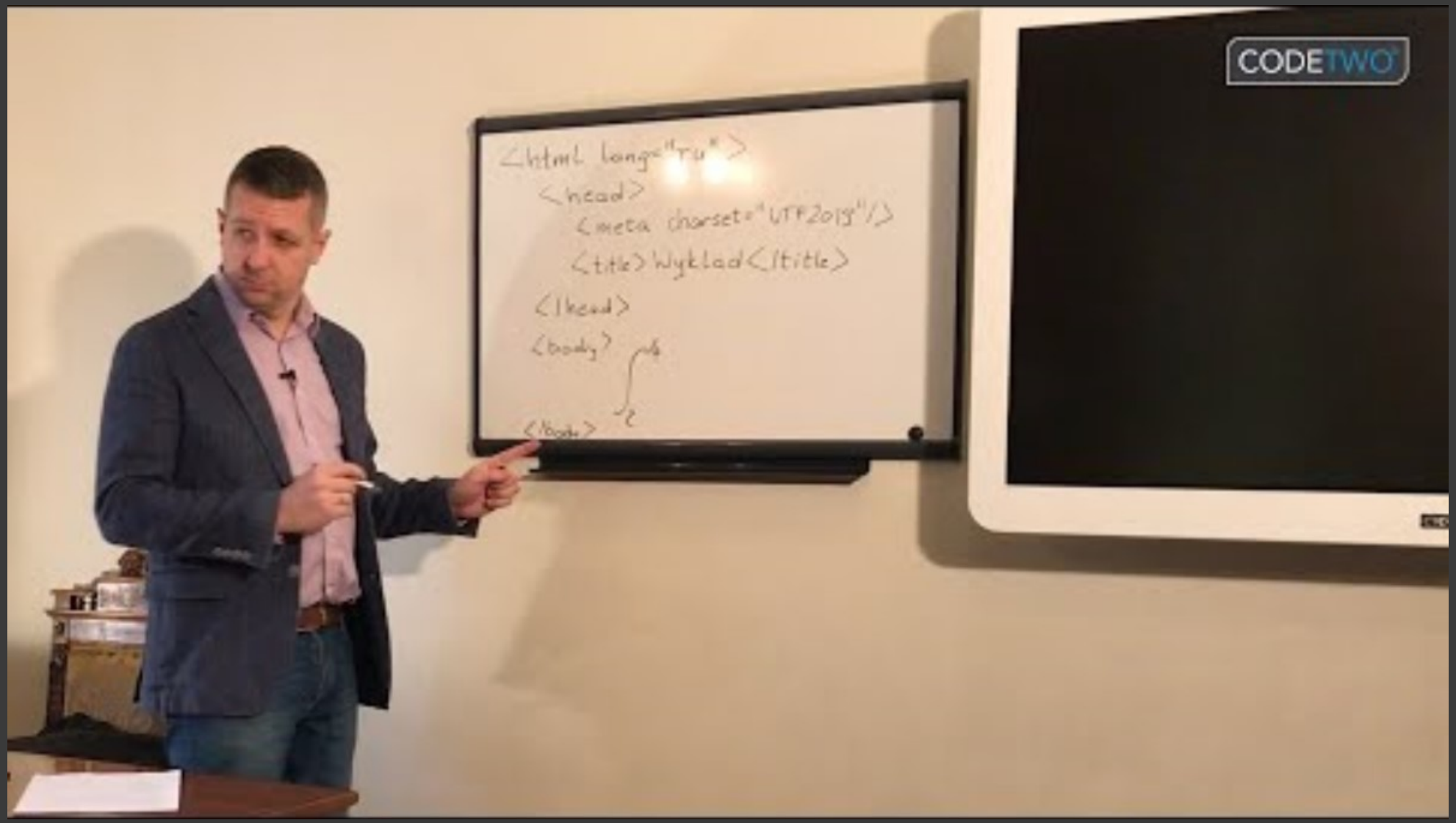
NIE!!!!

HTML

Hypertext Markup Langugage

*(lub też **z angielska…** „hipertekst markap languaż” ~ prof. Zbigniew JSON, HRejeterzy 2020)*

język opisowy, stanowiący szkielet do budowy strony internetowej. Określa zależności między poszczególnymi elementami na stronie poprzez tzw. tagi / encje, zapisywane pomiędzy „< … >xyz </…>” lub „<…>”.



https://www.youtube.com/watch?v=BAju0_IS-ns

Przykładowa struktura strony

```
<!DOCTYPE html>
<html lang="en">
<head>

<meta charset="UTF-8">
<title>Welcome, welcome</title> <!- tytuł strony -->
</head>
<body>
    <h1>Hello World!</h1> <!- największy nagłówek  -->

    <p>Lorem ipsum dolor sit amet, consectetur
adipisicing elit. Nostrum consequuntur tempora
accusamus commodi a sint, quas nihil esse molestias
nesciunt explicabo accusantium corporis, odit
repellat ut, blanditiis unde ex facilis.</p>
<!-- akapit - dłuższy zbiór tekstu  -->
</body>
</html>
```

DEKLARACJA DOKUMENTU W FORMACIE HTML 5

Tag html -> wskazanie początky pliku w HTML'u (zakończone jako </html>. Atrybut *lang* określa język dla przeglądarki, aby odpowiednio dostosowywała swoje wbudowane funkcje, np. autotłumaczenie strony czy dla robotów indeksujących

Kodowanie znaków z obsługą polskich znaków (typ utf-8)

SEKCJA <HEAD>/HEAD> *GŁOWA STRONY*

Zawiera tzw. metdane, czyli informacje konfiguracyjne dla przeglądarki, powiązania z innymi plikami itd. // ta sekcja jest niewidoczna w przeglądarce

SEKCJA <BODY>/BODY> *CIAŁO STRONY*

Zawartość strony // ta sekcja jest widoczna w przeglądarce

Przykładowe elementy na stronie

```html
<h1>Nagłówek 1</h1>
<h2>Nagłówek 2</h2>
<h3>Nagłówek 3</h3>
<h4>Nagłówek 4</h4>
<h5>Nagłówek 5</h5>
<h6>Nagłówek 6</h6>
```

NAGŁÓWKI

```html
<a href="https://cybersec.michcia.online">Zobacz materiały</a>
```

HIPERŁĄCZA (linki)

```html
<img src="./img/baner.png"/>
```

OBRAZEK

```html
<form method="POST" action="">
    <label for="text">Wpisz login</label>
    <input type="text" name="text">
    <label for="password">Wpisz hasło</label>
    <input type="password" name="password">
    <input type="submit" name="send„ value="wyślij">
</form>
```

FORMULARZ

Przykładowe elementy na stronie

```
    <div>
        <table style="border: 1px solid #000;  border-collapse: collapse;">
            <tr style="border: 1px solid #000;  border-collapse: collapse;">
                <th style="border: 1px solid #000;  border-collapse: collapse;">L.p</th><th style="border: 1px solid #000;  border-
collapse: collapse;">Imię i nazwisko</th>
            </tr>
            <tr style="border: 1px solid #000;  border-collapse: collapse;">
                <th style="border: 1px solid #000;  border-collapse: collapse;">1</th><th style="border: 1px solid #000;  border-
collapse: collapse;"s>Jan Kowalski</th>
            </tr>
        </table>
    </div>
```

KONTENER (div) Z TABELĄ

L.p	Imię i nazwisko
1	Jan Kowalski

Przykładowe elementy na stronie

NIEZALECANY SPOSÓB! RYZYKO ATAKU XSS (*Cross-site scripting*)

```
<iframe src="https://www.onet.pl" height="400px" width="600px"></iframe>
```

OSADZENIE TREŚCI

```
<embed src="https://www.onet.pl" height="400px" width="600px"></embed>
```

OSADZENIE TREŚCI

Przykładowe pola formularza

- Tag wyboru koloru `<input type="color" name="kolor">`
- Tag wyboru daty `<input type="date" name="data">`
- Tag dołączenia pliku `<input type="file" name="plik">`
- Tag resetujące wpisane wartości `<input type="reset">`
- Tag pola liczbowego `<input type="number">`
- Tag zakresu liczbowego (suwak)`<input type="range">`. Dla tego typu są jeszcze atrybuty min oraz max, np `<input type="range" min ="0" max="100">`
- Tag opcji wyboru (radiobutton): `<input type="radio" name="opcja 1" value="1">` Opcja pierwsza. Radiobutton pozwala na wybranie tylko JEDNEJ opcji w zakresie RadioButtonow o tej samej nazwie. UWAGA: Wartość value mówi o wartości, która zostanie przesłana do serwera po zatwierdzeniu formularza.

WIĘCEJ RODZAJÓW PÓL FORMULARZA
https://www.w3schools.com/html/html_form_input_types.asp

WYZWANIE NR 1

Stwórz stronę, która będzie wysyłała dane z pola tekstowego o nazwie „imie” na adres https://giganci.cytr.us/

Metody formularza:
GET – przekazuje dane w sposób jawny, w URL
POST – przekazuje dane niejawnie (Form Data)

WYZWANIE NR 1 - rozwiązanie

metoda: GET

```html
<!DOCTYPE html>
<html lang="pl">
<head>
<meta charset="UTF-8">
<title>Wyzwanie nr 1</title>
</head>
<body>
    <form action="https://giganci.cytr.us" method="get">
        <input type="text" name="imie" id="imie" placeholder="Podaj imię" />
        <input type="submit" value="Wyślij">
    </form>
</body>
</html>
```

WYZWANIE NR 1 - rozwiązanie

metoda: POST

```
<!DOCTYPE html>
<html lang="pl">
<head>
<meta charset="UTF-8">
<title>Wyzwanie nr 1</title>
</head>
<body>
    <form action="https://giganci.cytr.us" method=„post">
        <input type="text" name="imie" id="imie" placeholder="Podaj imię" />
        <input type="submit" value="Wyślij">
    </form>
</body>
</html>
```

EVENTY

Korzystając z możliwości języka JavaScript (JS), możemy tworzyć różne mechanizmy na stronie, wykonywane tylko po stronie klienta. Jednym z nich są tzw. *eventy*.

Eventy są wykonywane przez atrybut HTML: onclick=„” – w środku podajemy wydarzenie, które ma się wykonać po kliknięciu, np. w przycisk

Inne metody wywoływania:
onload -> wykonanie zdarzenia podczas ładowania
onerror -> wykonanie zdarzenia, jeżeli wystąpi jakiś błąd
onselect -> wykonanie zdarzenia po zaznaczeniu czegoś, np. tekstu

Więcej metod: https://www.w3schools.com/tags/ref_eventattributes.asp

WYZWANIE NR 2

Stwórz event, który będzie wywoływał okienko (alert) o treści *click, click... done!* po kliknięciu przycisku

Okienko w JS'ie wywołujemy poprzez funkcję:
alert(...)

WYZWANIE NR 2 - rozwiązanie

```
<button onclick="alert('click, click… done!');">Kliknij tutaj!</button>
```

Czym jest atak XSS?

XSS

Cross-Site Scripting

atak na strony WWW, polegający na osadzeniu szkodliwej treści, np. złośliwego kodu, w serwisie bez zgody twórcy. Skrypt oparty o metodę XSS może doprowadzić do wycieku danych czy uzyskania dostępu do czyjegoś konta, nawet bez potrzeby znajomości hasła. Podatność na ataki XSS wynikają zazwyczaj ze słabych zabezpieczeń kodu strony, np. brak walidacji formularzy

WYZWANIE NR 3*

Napisz stronę, która będzie prostą sekcją komentarzy. Plik ze stylem CSS znajdziesz tutaj: https://pastebin.com/fXcD8Bzw : stwórz plik z rozszerzeniem .css, a następnie załącz do pliku z rozszerzeniem .html w sekcji *head*: `<link rel="stylesheet" type="text/css" href="style.css">`

Szablon pliku .html : https://pastebin.com/aaqZds9j

1. W tagu formularza o id *commentForm* dodaj pole tekstowe (input z typem *text*) o id commentInput oraz przycisk typu submit
2. W kontenerze (div) o id „comments" dodaj nagłówek 2. stopnia z napisem „Komentarze"
3. W tagu <script> dodaj trzy zmienne stałe (const *nazwa = ...*) *i przypisz do nich elementy o następujących id: commentForm, commentInput oraz comments*
4. Wklej pod spodem następującą funkcję Listenera: https://pastebin.com/wzMpS5hY i sprawdź działanie (Wklej do pola formularza osadzenie jakiegoś filmiku z youtube'a, np. rickroll). *Co się wydarzyło po kliknięciu przycisku?*
5. Teraz podmień powyższy kod następującym: https://pastebin.com/ijvtFj9n *Jakie zmiany dostrzegasz? Jak myślisz, jak wpływa to na bezpieczeństwo strony?*

WYZWANIE NR 3*
rozwiązanie + wyjaśnienie

Pełny kod (niezabezpieczony):
https://pastebin.com/jfgadU3d

Pełny kod (zabezpieczony):
https://pastebin.com/Y6k1AZj6

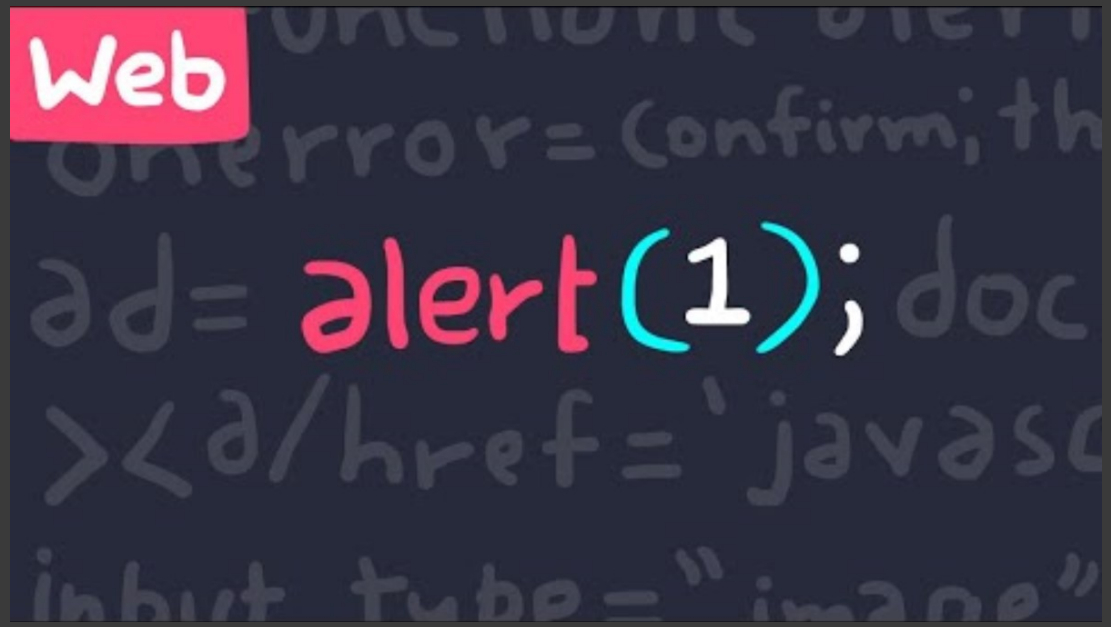
WYJAŚNIENIE:
Podatność na atak zawdzięczamy metodzie „innerHTML", która bezpośrednio wstawia zawartość podaną w polu formularza, nie konwertując jej na prosty tekst. Pozwala to w ten sposób wstawiać różne skrypty, które przeglądarka wykrywa i wykonuje.

Aby zapobiec temu atakowi, podmieniliśmy tę metodę inną – „textContent", która z góry traktuje to co otrzyma jako zwykły tekst i tak też to przeglądarka interpretuje.

Podsumowanie

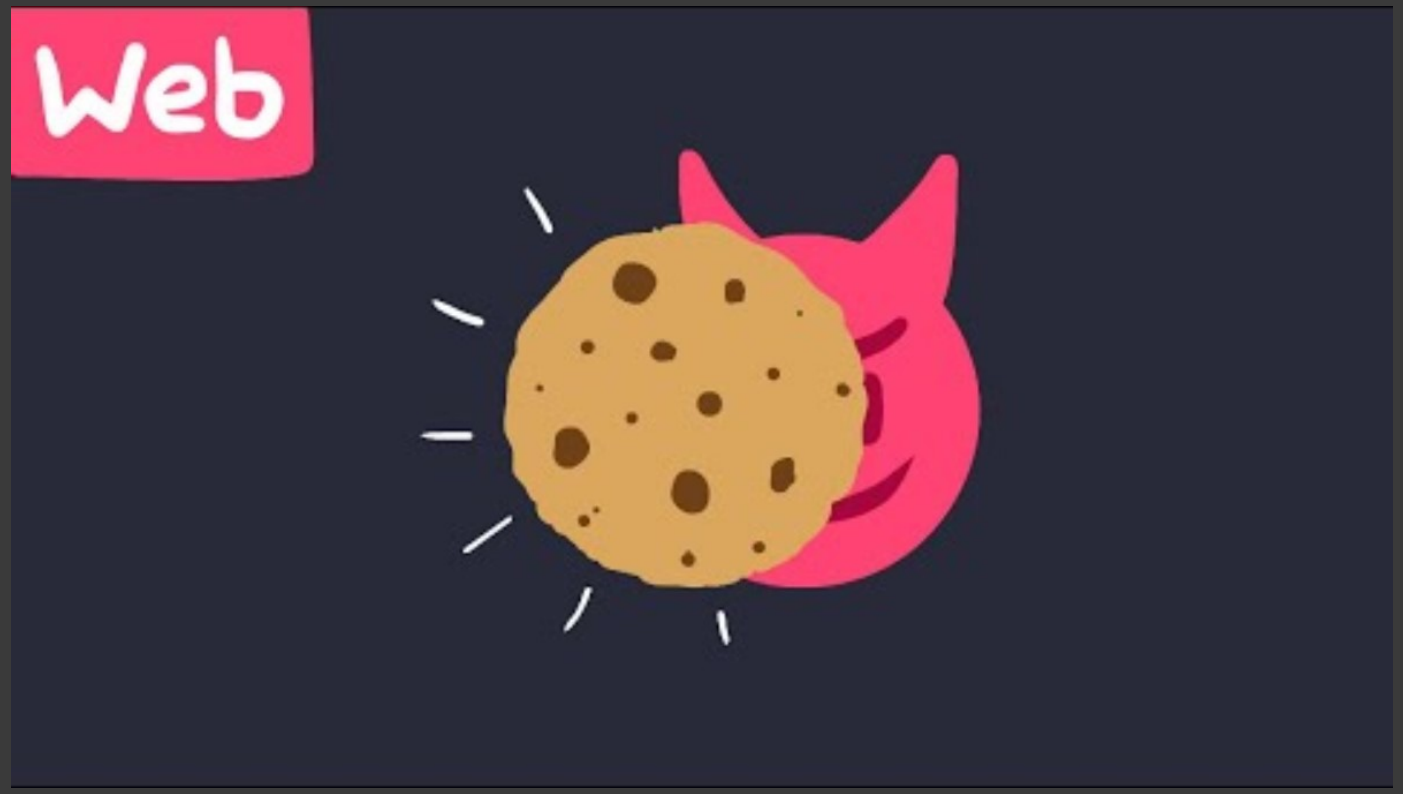
1. Czym jest język HTML?
2. Jakie są podstawowe znaczniki?
3. Co to są formularze?

Polecam!



ŹRÓDŁO:
https://www.youtube.com/watch?v=EoaDgUgS6QA

Polecam!



ŹRÓDŁO:
https://www.youtube.com/watch?v=eWEgUcHPle0

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=9G3jWs1gcf4