KURS PENTESTERA 22/23

CZYM JEST FRONTEND?

KAROL SŁOMCZYŃSKI, HANNA MARCINIAK

WHITE HATS PWR

GARŚĆ INFORMACJI ORGANIZACYJNYCH

Grupa FB kursu:

https://www.facebook.com/groups/976057843243320

HARMONOGRAM

	LUTY	MARZEC				KWIECIEŃ				MAJ					CZERWIEC				LIPIEC	
PN	27	6 Pn N	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26 Cz P	3	10
WT	28	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27 Pt P	4	11
ŚR	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21 Pn P	28	5	12
CZ	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13
PT	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14
SO	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15
N	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16
P - PARZYSTY N - NIEPARZYSTY	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P

Zajęcia stacjonarne

Zajęcia zdalne

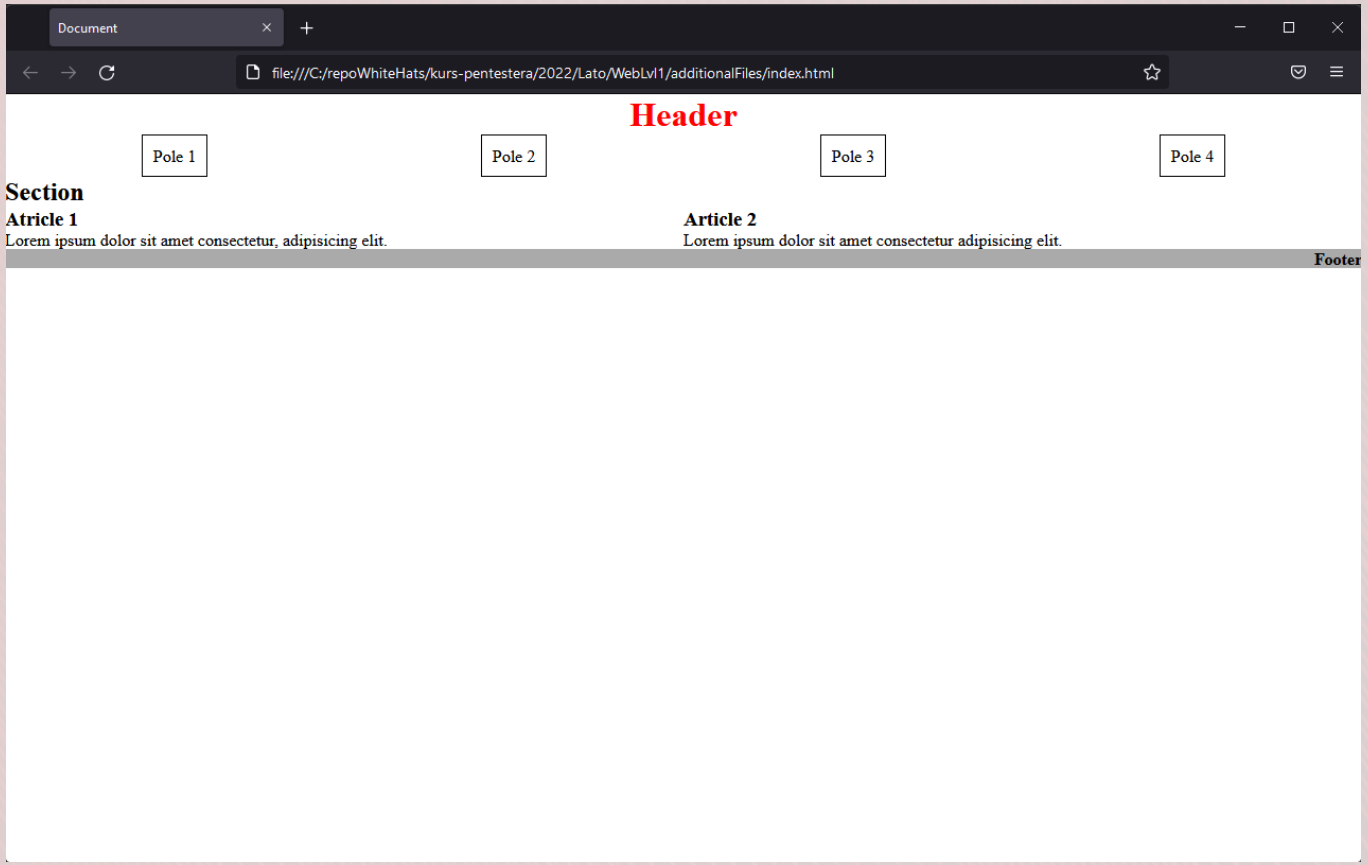
WHITE HATS PWR

JAKIE ASPEKTY PORUSZYMY NA DZISIEJSZYCH ZAJĘCIACH

1. Charakterystyka i rodzaje plików web
2. Narzędzia deweloperskie
3. Pliki cookies
4. Atak Cross-site

WHITE HATS PWR

PRZYKŁADOWA STRONA



PLIKI HTML

Kluczowe elementy

- <head> - znacznik zawierający elementy niewidoczne dla użytkownika,
- <body> - znacznik zawierający elementy widoczne na stronie internetowej.

WHITE HATS PWR

PRZYKŁADOWY KOD

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
    <link rel="stylesheet" href="style.css">
    <style>
        header {
            color: red;
        }
    </style>
</head>
<body>
    <header>
        <h1>Header</h1>
    </header>
    <main>
        <nav>
            <ul>
                <li>Pole 1</li>
                <li>Pole 2</li>
                <li>Pole 3</li>
                <li>Pole 4</li>
            </ul>
        </nav>
```

WHITE HATS PWR

PRZYKŁADOWY KOD

```
        <section>
            <h2>Section</h2>
            <article>
                <h3>Atricle 1</h3>
                    <p>Lorem ipsum dolor sit amet consectetur, adipisicing elit.</p>
            </article>
            <article>
                <h3>Article 2</h3>
                    <a>Lorem ipsum dolor sit amet consectetur adipisicing elit.</a>
            </article>
        </section>
    </main>
    <footer>
        <h4>Footer</h4>
    </footer>
    <script>
        document.getElementById("demo").addEventListener("click", myFunction = () => {
            alert("Hello World!");
        });
    </script>
</body>
</html>
```

PLIKI CSS

Pliki stylu strony, takie jak:

- Tło
- Kolor czcionki
- Odstęp między wierszami
- Pozycjonowanie elementów…

PRZYKŁADOWY KOD

```css
* {
  margin: 0;
  padding: 0;
  box-sizing: border-box;
}
section > h2 {
  width: 100%;
}
section {
  display: flex;
  justify-content: flex-start;
  flex-wrap: wrap;
}
section > article {
  flex: 1;
}
footer {
  background-color: #aaa;
}
```

```css
nav > ul {
  display: flex;
  flex-direction: row;
  justify-content: space-around;
  list-style: none;
}
ul > li {
  border: 1px solid black;
  padding: 10px;
}
header {
  display: flex;
  justify-content: center;
}
footer {
  display: flex;
  justify-content: flex-end;
}
```

SELEKTORY CSS

Selektory	Przykład	Opis
#id	#special_p	Wybierany jest tylko element z id "special_p"
.class	.few-elements	Wybiera wszystkie elementy z klasą "few-elements"
element.class	div.few-elements	Wybiera tylko z klasą "few-elements"
*	*	Wbiera wszystkie elementy
element	p	Wybiera wszystkie <p>
element,element,..	div, p	Wybiera wszystkie elementy i <p>

JAVA SCRIPT

- Najbardziej znany jako język skryptowy stron internetowych,
- Można go zastosować w pliku HTML jako załącznik <script>,
- Załączanie zewnętrzne jest możliwe, dzięki atrybutowi src.

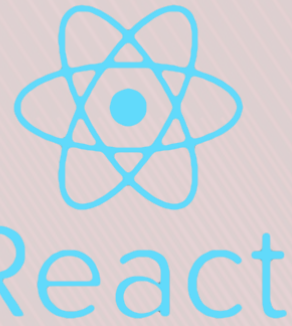
```
const Http = new XMLHttpRequest();
const url='https://jsonplaceholder.typicode.com/posts';
Http.open("GET", url);
Http.send();

Http.onreadystatechange = (e) => {
  console.log(Http.responseText)
}
```

```
document.getElementById("demo").addEventListener("click", myFunction = () => {
            alert("Hello World!");
        });
```


WHITE HATS PWR

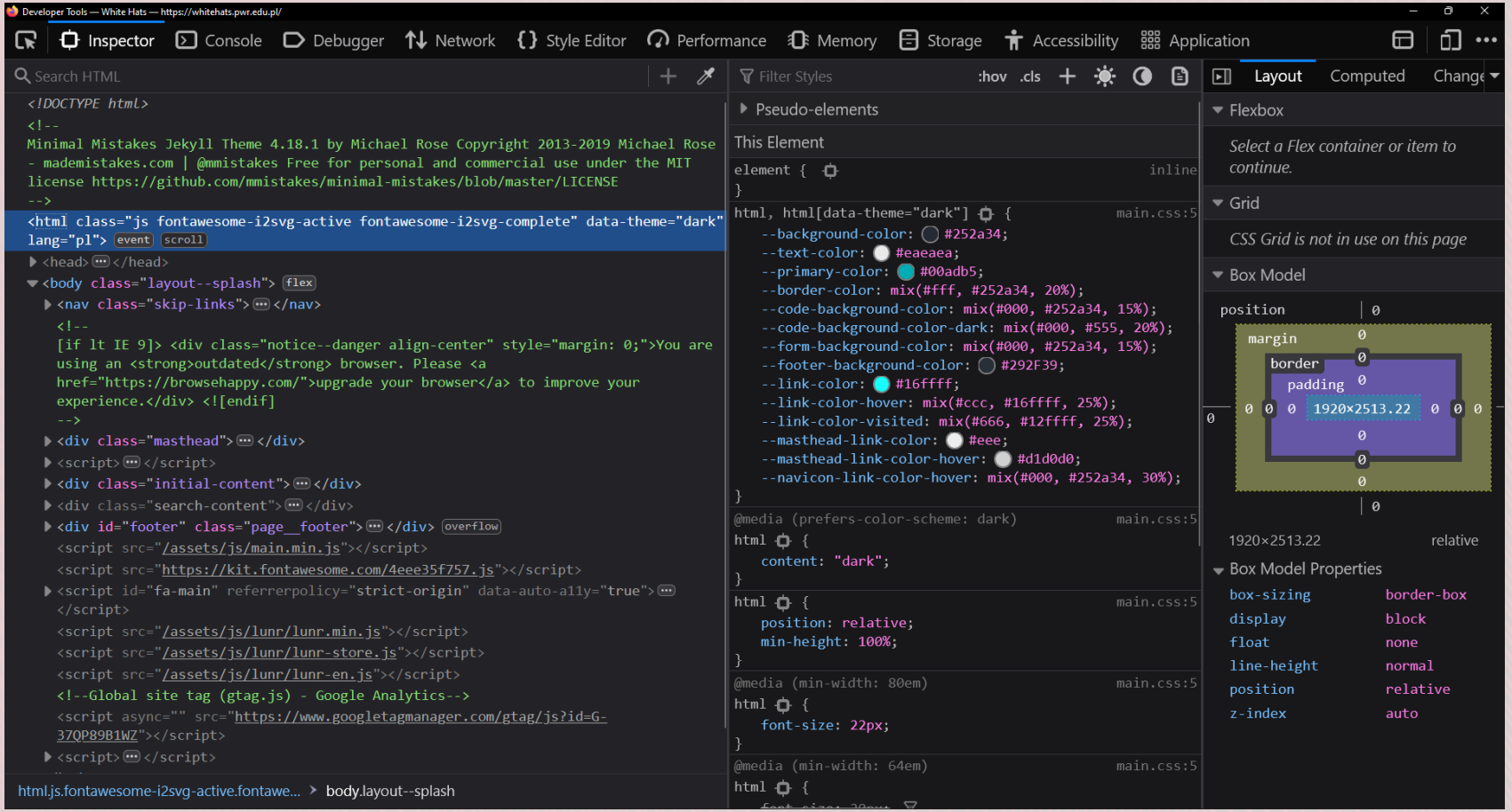
FRAMEWORKI

- Framework to biblioteka wstępnie napisanego kodu JavaScript, która umożliwia łatwiejsze tworzenie aplikacji opartych na JavaScript, zwłaszcza dla technologii AJAX i innych technologii internetowych.



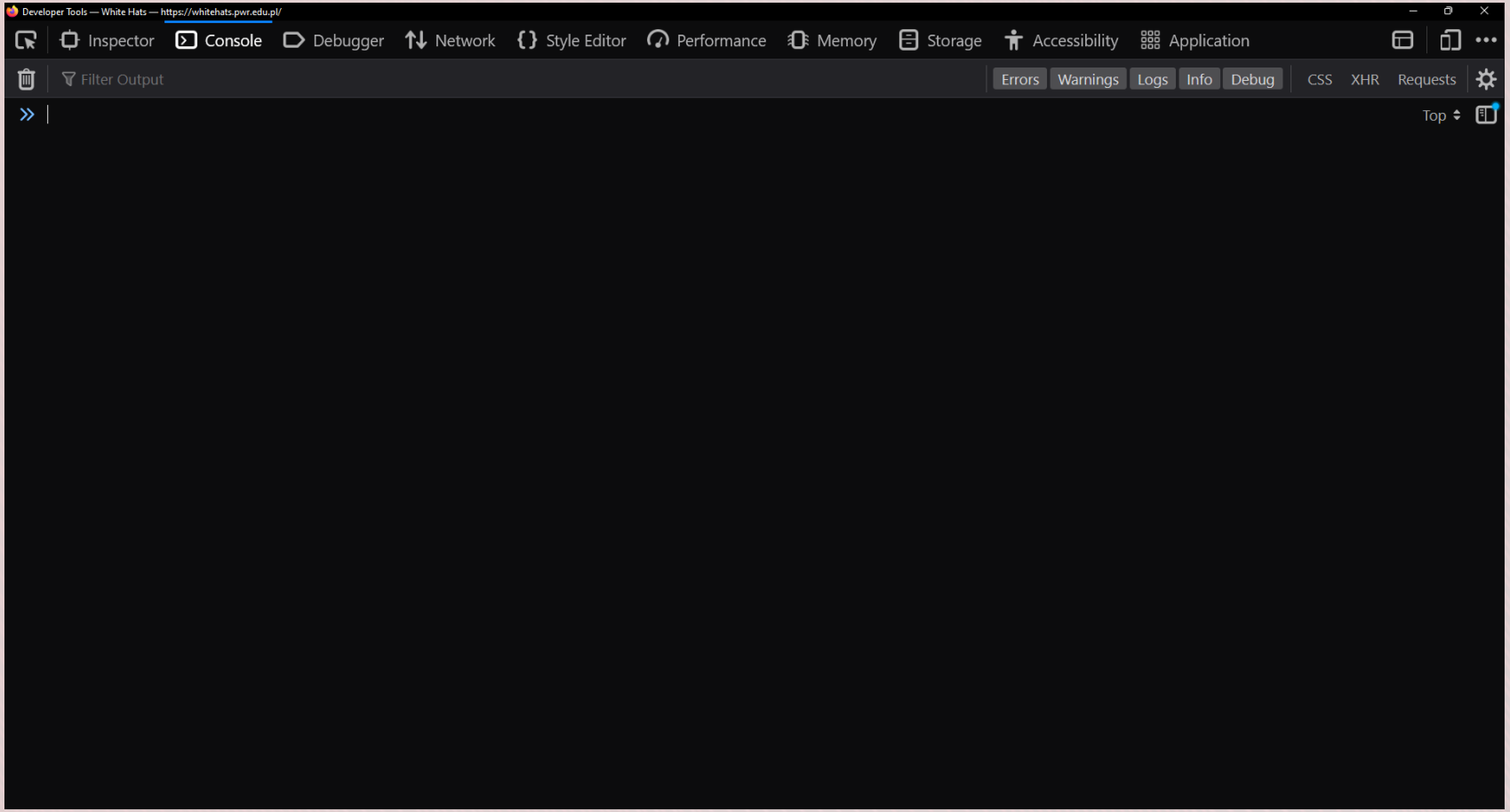
NARZĘDZIA DEWELOPERSKIE

INSPECTOR



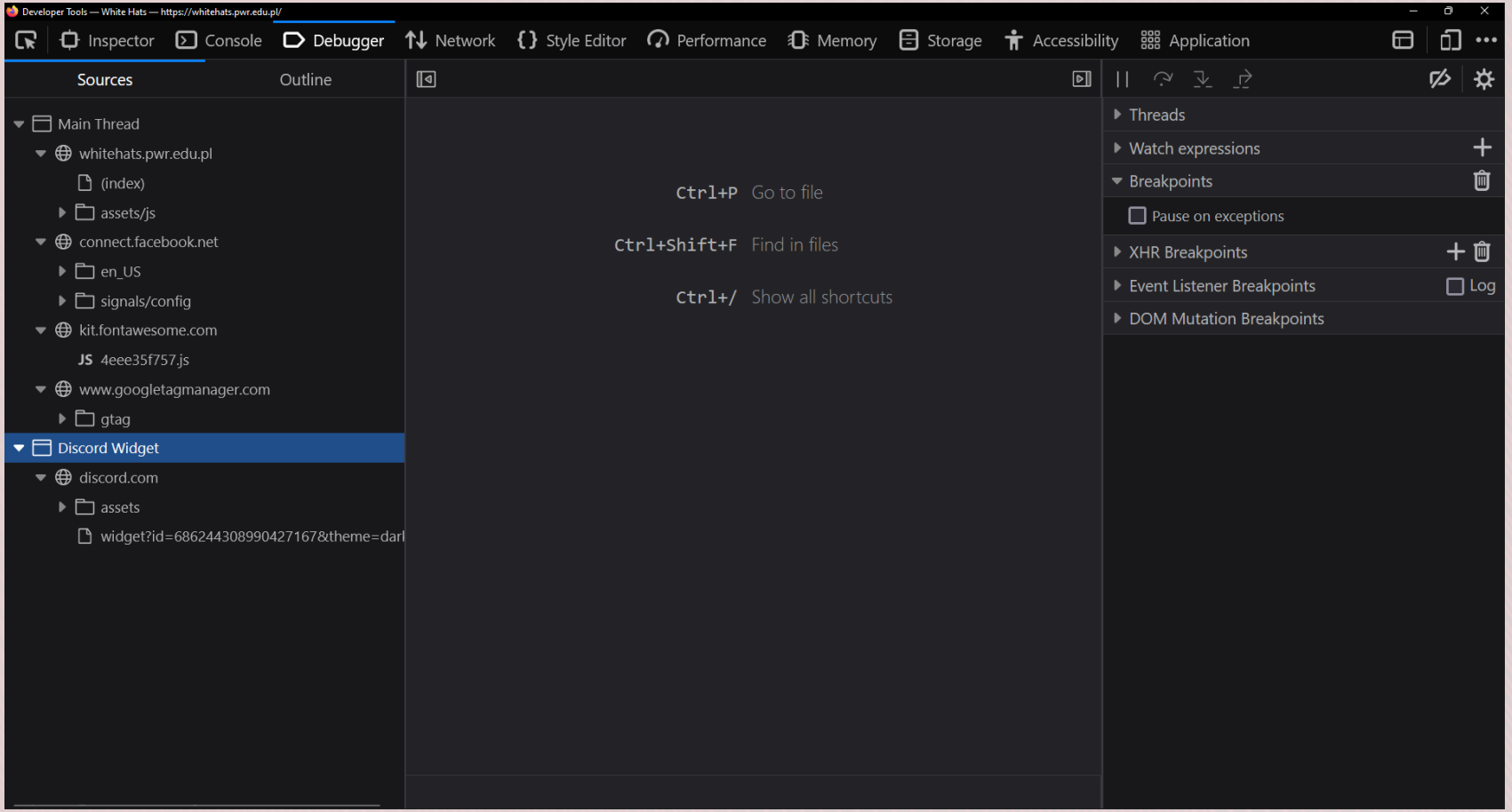
WHITE HATS PWR

WEB CONSOLE



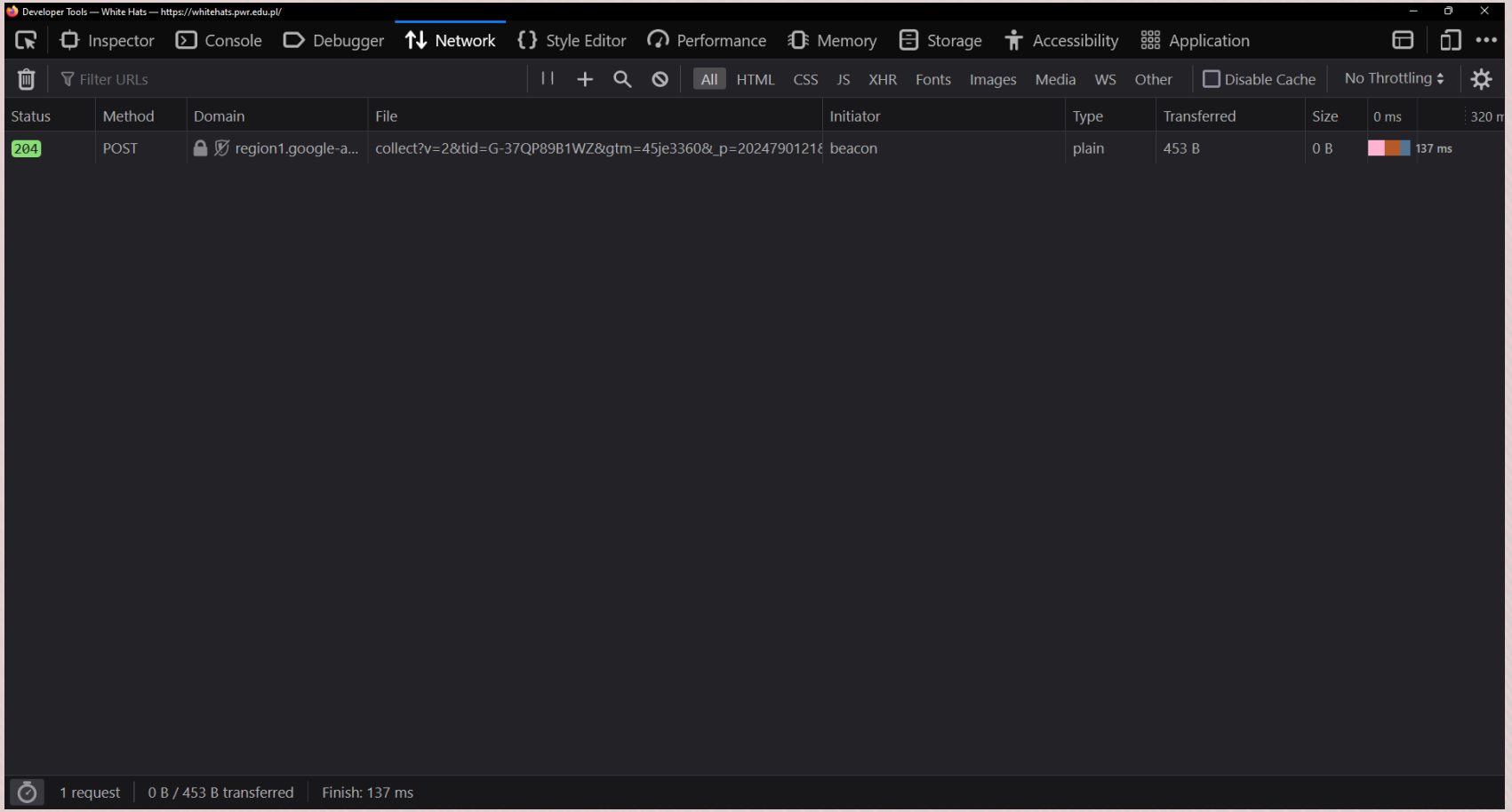
WHITE HATS PWR

DEBUGGER



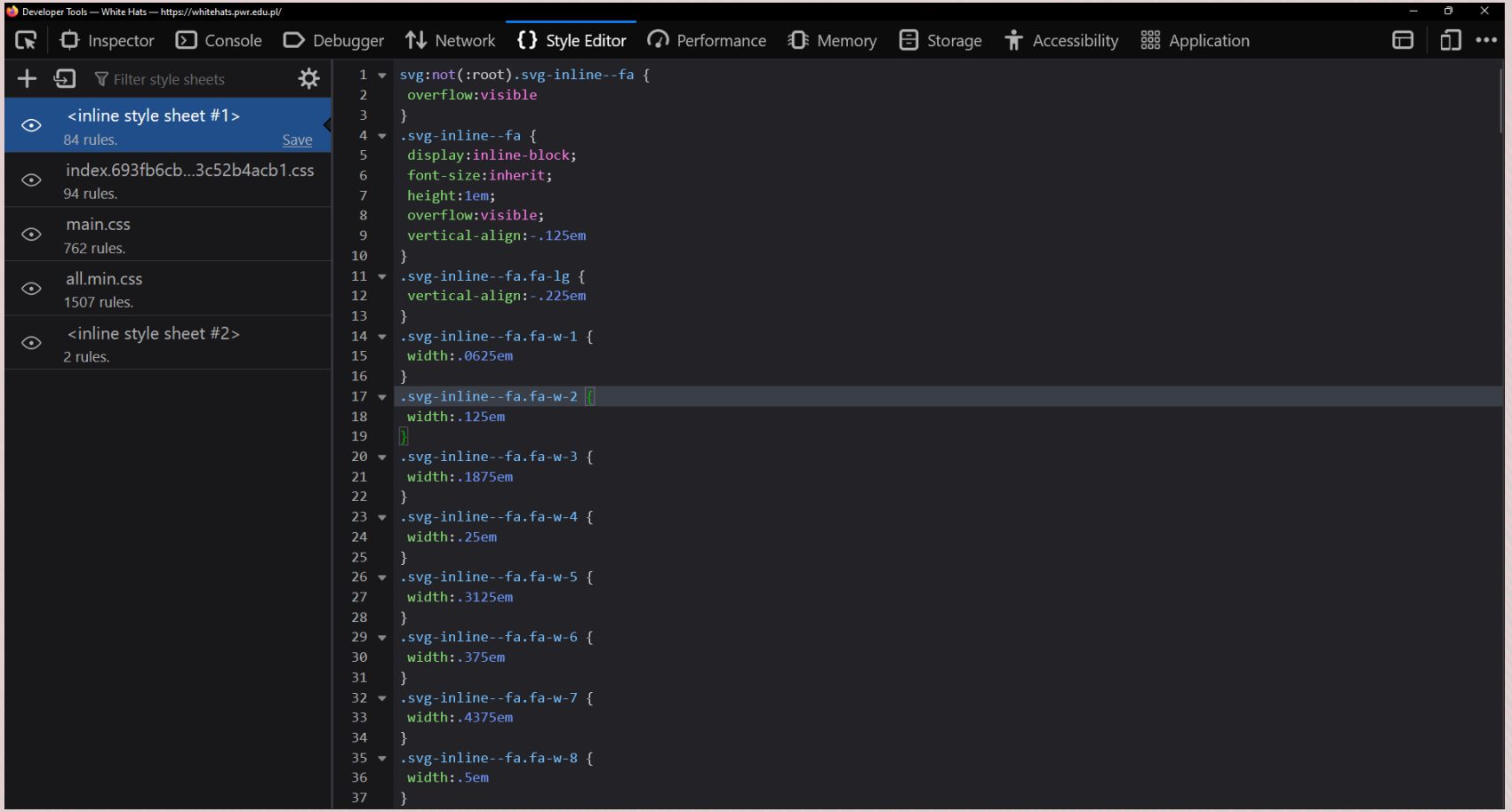
WHITE HATS PWR

NETWORK



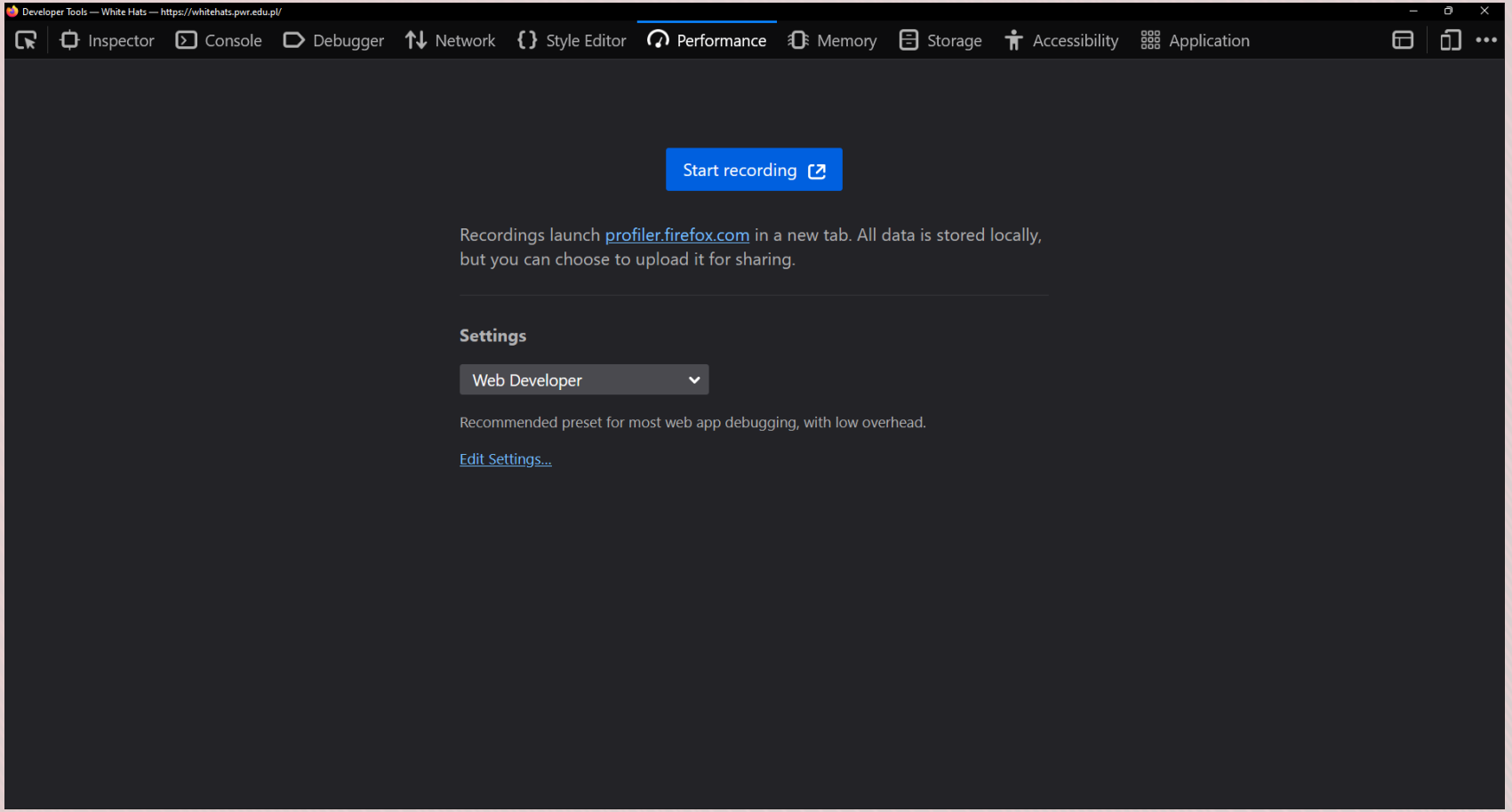
WHITE HATS PWR

STYLE EDITOR



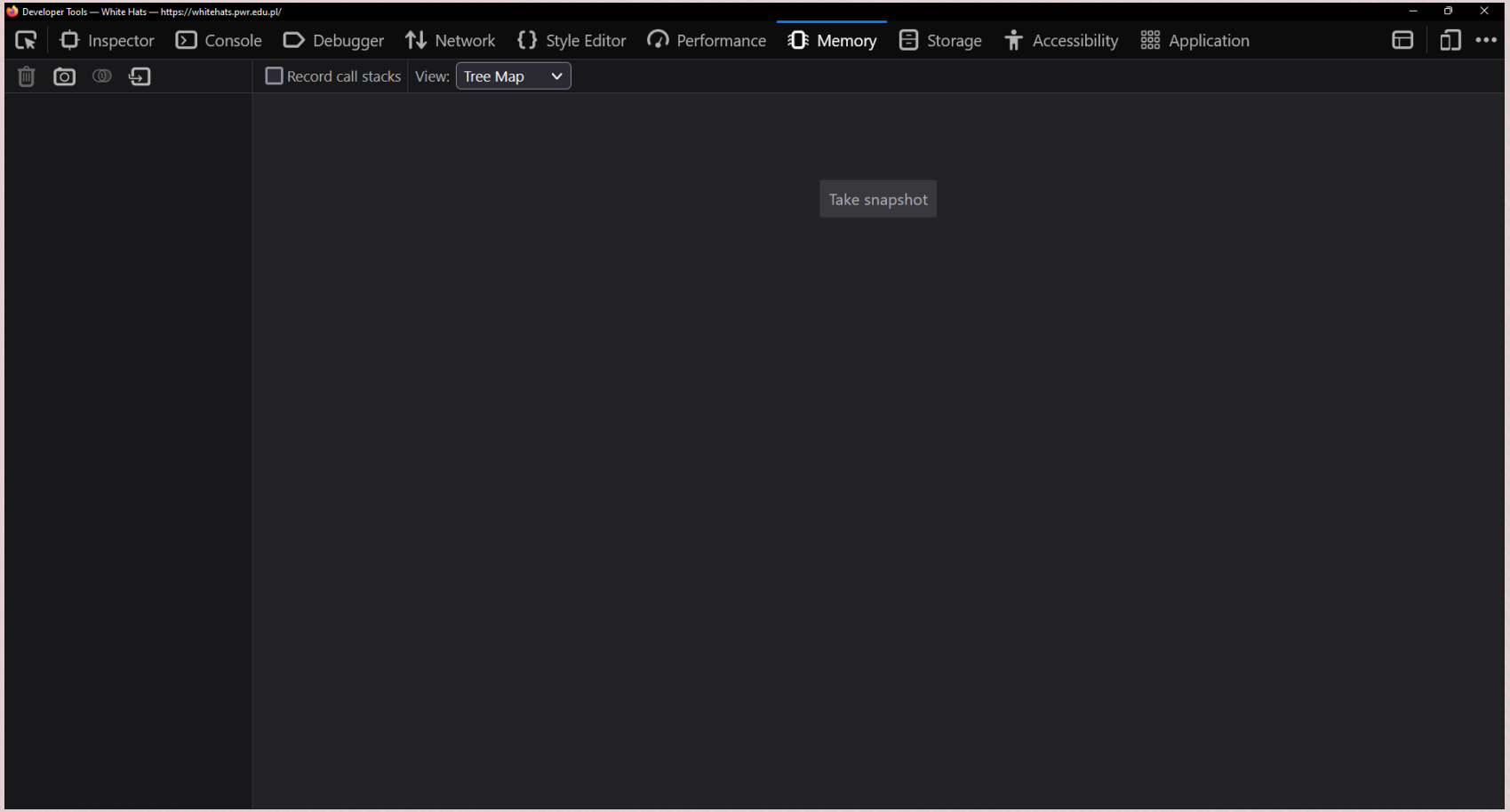
WHITE HATS PWR

PERFORMANCE



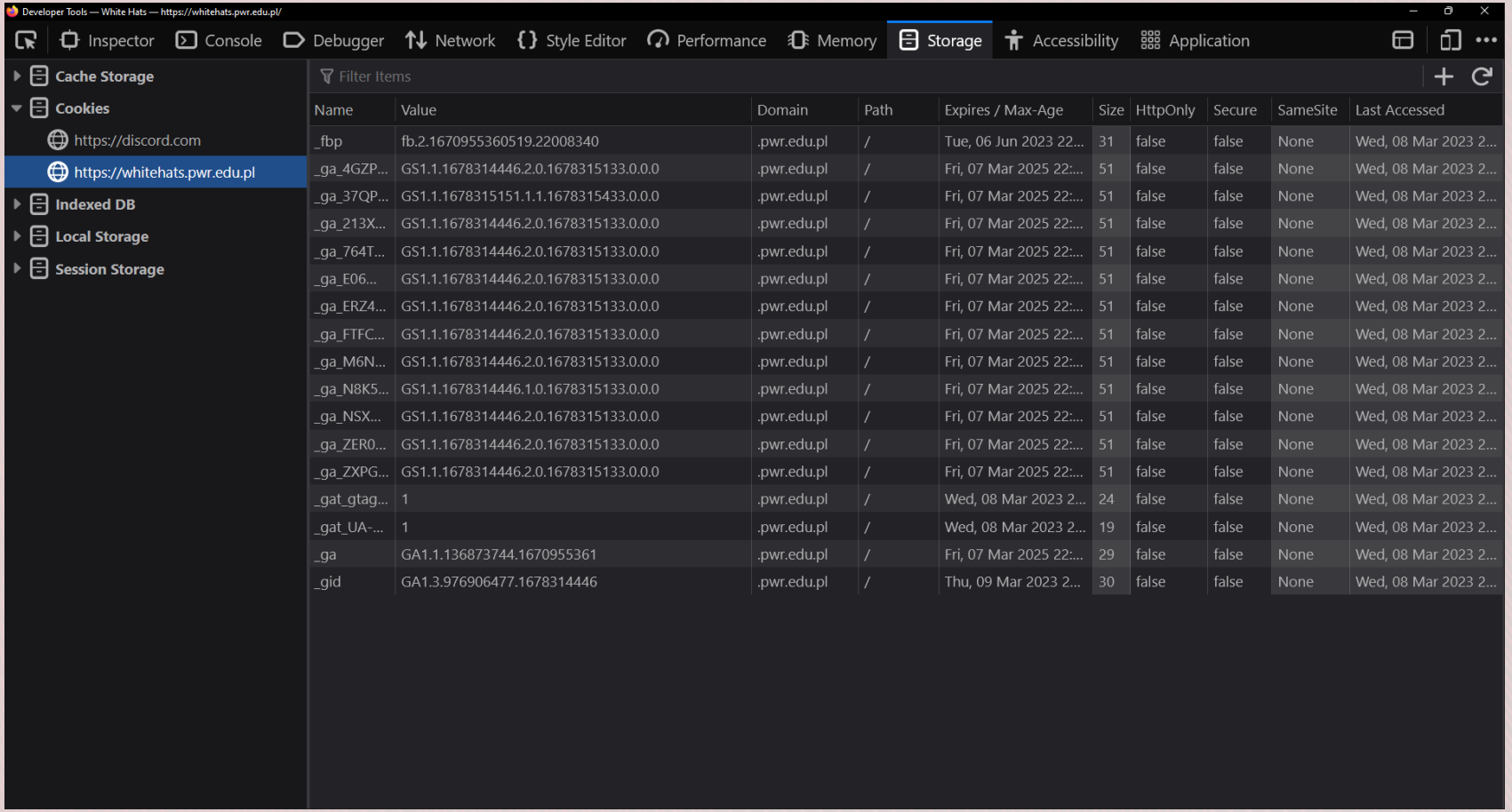
WHITE HATS PWR

MEMORY



WHITE HATS PWR

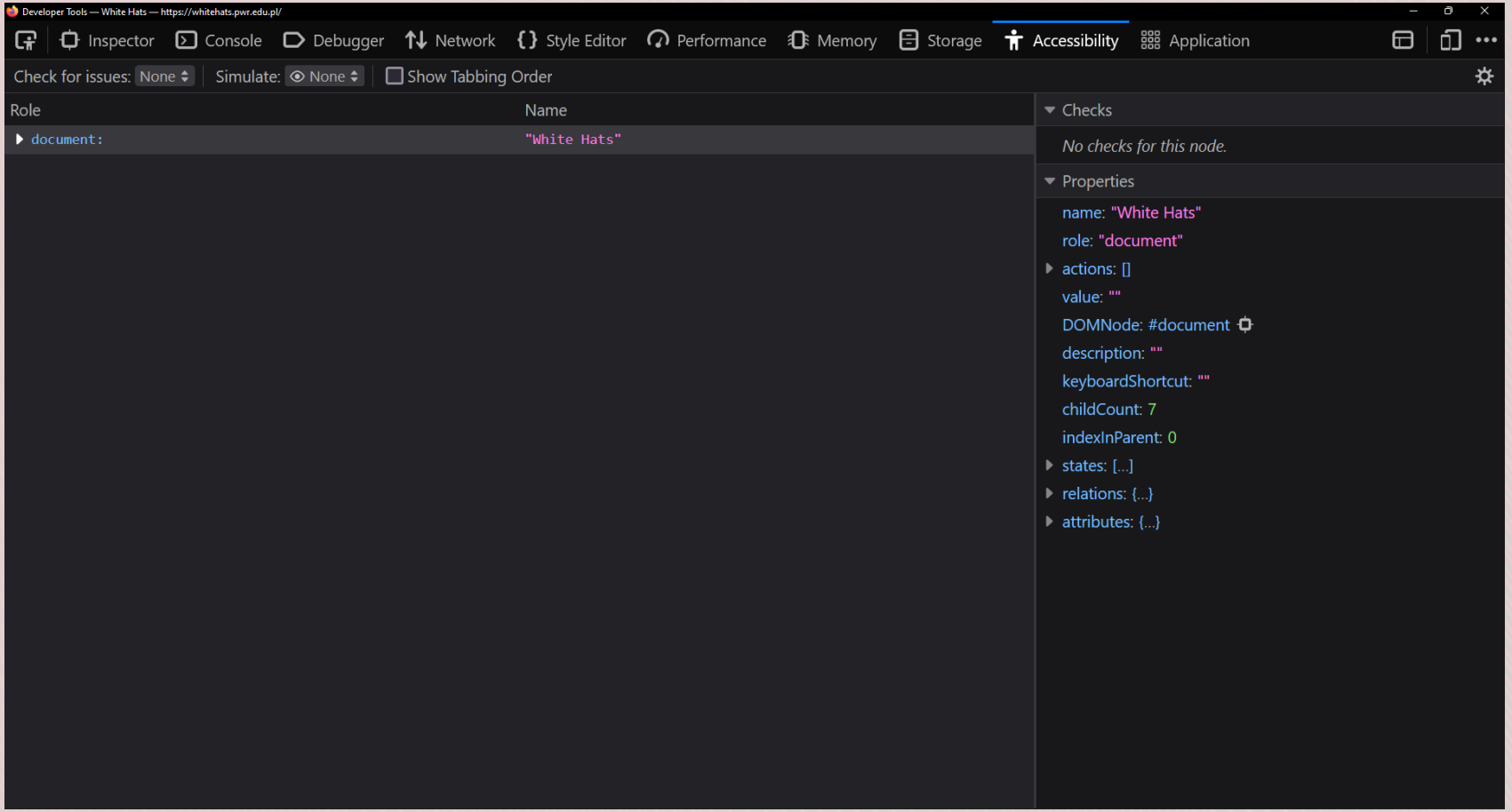
STORAGE



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_fbp	fb.2.1670955360519.22008340	.pwr.edu.pl	/	Tue, 06 Jun 2023 22...	31	false	false	None	Wed, 08 Mar 2023 2...
_ga_4GZP...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_37QP...	GS1.1.1678315151.1.1.1678315433.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_213X...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_764T...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_E06...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_ERZ4...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_FTFC...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_M6N...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_N8K5...	GS1.1.1678314446.1.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_NSX...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_ZER0...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_ga_ZXPG...	GS1.1.1678314446.2.0.1678315133.0.0.0	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	51	false	false	None	Wed, 08 Mar 2023 2...
_gat_gtag...	1	.pwr.edu.pl	/	Wed, 08 Mar 2023 2...	24	false	false	None	Wed, 08 Mar 2023 2...
_gat_UA-...	1	.pwr.edu.pl	/	Wed, 08 Mar 2023 2...	19	false	false	None	Wed, 08 Mar 2023 2...
_ga	GA1.1.136873744.1670955361	.pwr.edu.pl	/	Fri, 07 Mar 2025 22:...	29	false	false	None	Wed, 08 Mar 2023 2...
_gid	GA1.3.976906477.1678314446	.pwr.edu.pl	/	Thu, 09 Mar 2023 2...	30	false	false	None	Wed, 08 Mar 2023 2...

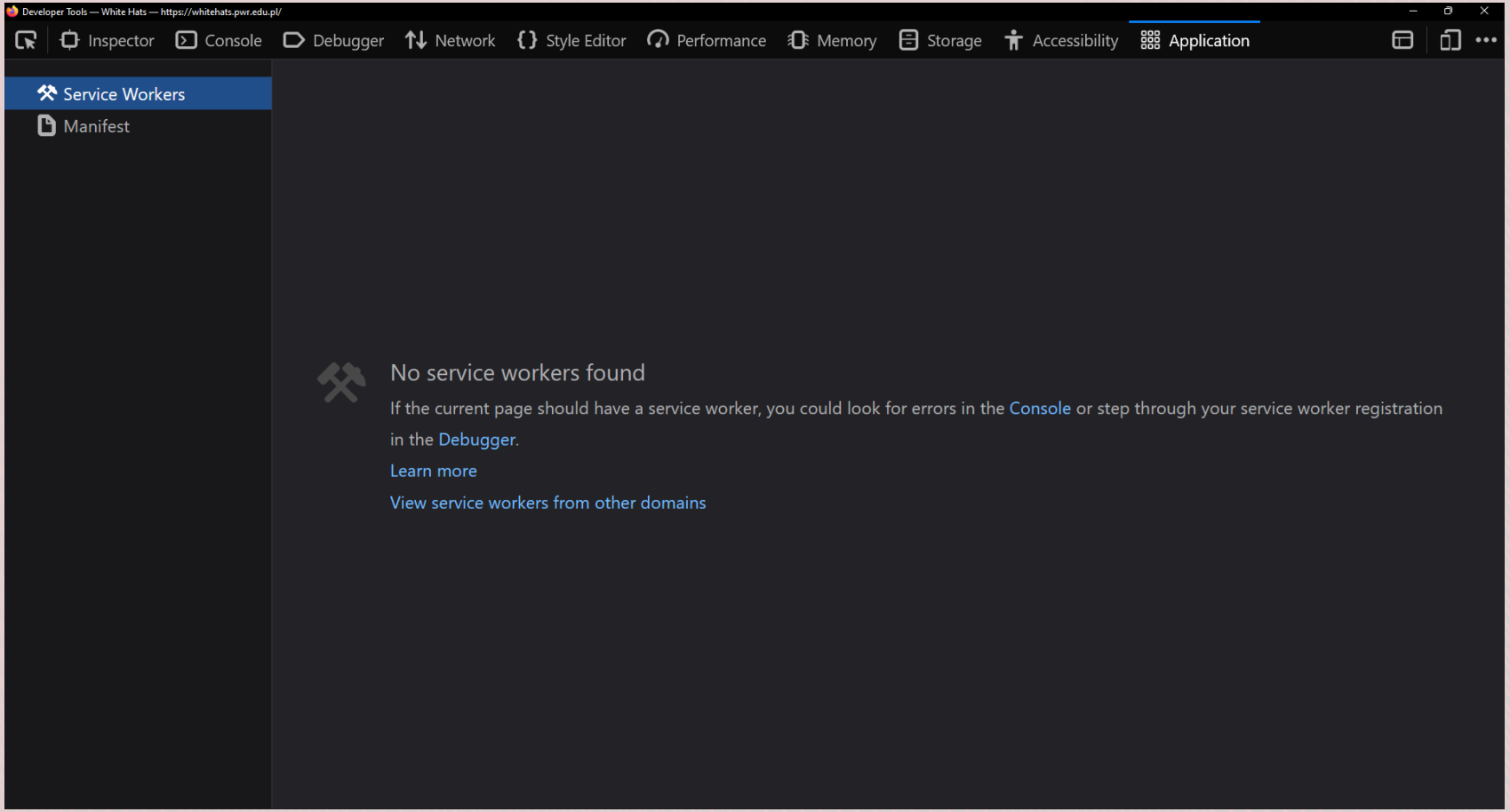
WHITE HATS PWR

ACCESSIBILITY



WHITE HATS PWR

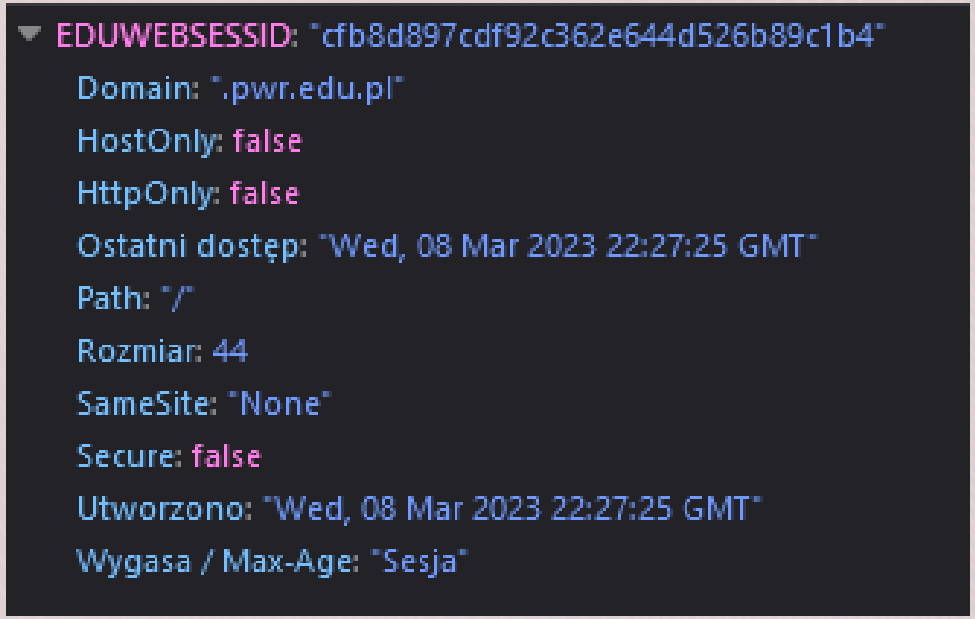
APPLICATION



WHITE HATS PWR

PLIKI COOKIES

Są to małe pliki tekstowe umieszczane przez witrynę internetową na komputerze użytkownika.



WHITE HATS PWR

ATAKI NA COOKIES

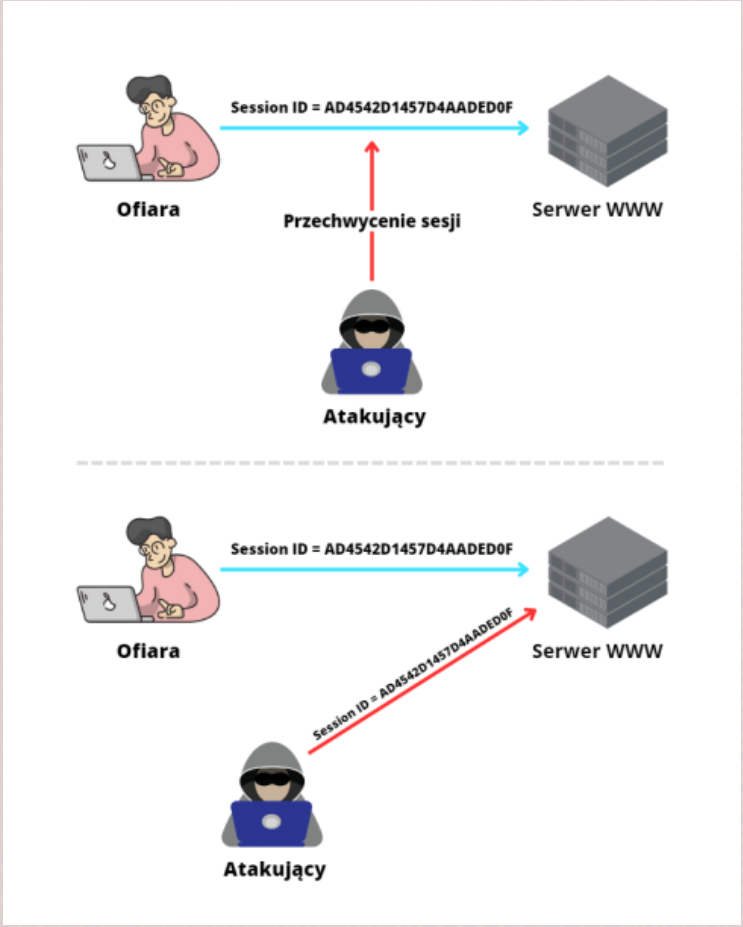
Sposoby na przejęcie tokenu sesji (Session Hijacking):

- Przewidywalny token sesji
- Session Sniffing
- Client-side attacks
- Man-in-the-middle
- Man-in-the-browser

WHITE HATS PWR

SESSION SNIFFING

Atakujący przejmuje token sesji, a następnie podszywa się pod ofiarę.



WHITE HATS PWR

ATAK CROSS-SITE SCRIPT

Polega na spreparowaniu linku do witryny, wykonującego kod od strony klienta. Umożliwia on przejęcie session token znajdujący się w plikach cookie.

WHITE HATS PWR

DZIĘKUJĘ ZA UWAGĘ!