XSS

Typowa strona WWW

(w latach 90 :P)

- HTML - od 1993
- CSS - od 1996
- Java - od 1996...

Typowa strona WWW

(w latach 90 :P)

- po drodze jest kilka różnych rozwiązań, które mają dodać "wodotryski" (szeroko pojętą interaktywność)
- Adobe Flash Player
- Javę wypiera JavaScript (z czasem)...

Jak dodać kod JS w HTML?

- <script src="myScript.js"></script>
- <script src="/js/myScript.js"></script>
- <script src="https://www.w3schools.com/js/myScript.js"></script>

za: W3schools

Jak dodać kod JS w HTML?

- <script></script> w sekcji head (<head></head>)
- <script></script> w sekcji... body (<body></body>)

za: W3schools

Jak dodać kod JS w HTML?

```
<!DOCTYPE html>
<html>
<body>

<h2>Demo JavaScript in Body</h2>

<p id="demo">A Paragraph</p>
<button type="button" onclick="myFunction()">Try it</button>

<script>
function myFunction() {
  document.getElementById("demo").innerHTML = "Paragraph changed.";
}
</script>

</body>
</html>
```

A gdzieś indziej?...

- ... np. w znaczniku <input /> ?
- ... albo w polu tekstowym?

Co może pójść nie tak? O_O

Jak działa XSS?

- podatna strona zwraca użytkownikowi złośliwy kod JS
- kod wykonuje się w przeglądarce ofiary

za: Portswigger

Czemu ten błąd jest taki straszny?

- może wpłynąć na interakcję między użytkownikiem a podatną aplikację
- atakujący może podszyć się pod użytkownika...
- ... wykonać działania, które on może wykonać...
- ... albo wykraść jego dane.

za: Portswigger

Rodzaje XSS

- Reflected XSS - przez żądanie HTTP
- Stored XSS - przez kod znajdujący się w bazie danych
- DOM-based XSS - przez kod po stronie klienta (nie serwera)

za: Portswigger

Proof of concept: metoda alert

<script>alert(0);</script>

(windows.alert(x));

Advanced Proof of concept

<script>print();</script>

za: Portswigger

Koniec laby, czas na laby!

Reflected XSS

- dane od użytkownika wyświetlone w kodzie źródłowym, bez modyfikacji
- aplikacja może być podatna, jeśli przetwarza różne znaczniki HTML od użytkownika
- warto się przyjrzeć, jak łączą się z istniejącym kodem

Reflected XSS

Lab:
https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

Stored XSS

- dodajemy treść, która będzie przechowana w bazie danych (np. komentarz)
- alert() nie wykona się od razu
- musimy wejść na podstronę, gdzie się wyświetli nasza treść
- uwaga na encje :)

Stored XSS

Lab: https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded

DOM XSS

- atak wykonuje się bezpośrednio w przeglądarce
- nie wszystkie funkcje w JS są "bezpieczne"
- document.write

--

DOM XSS dla document.write

Lab: https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink

Ściągawka:

```
<img src="x" onerror="alert(1)" />
<img width="600px" height="400px" onclick="alert(1);" />
onmouseover...
```