

# 22. JavaScript Attack

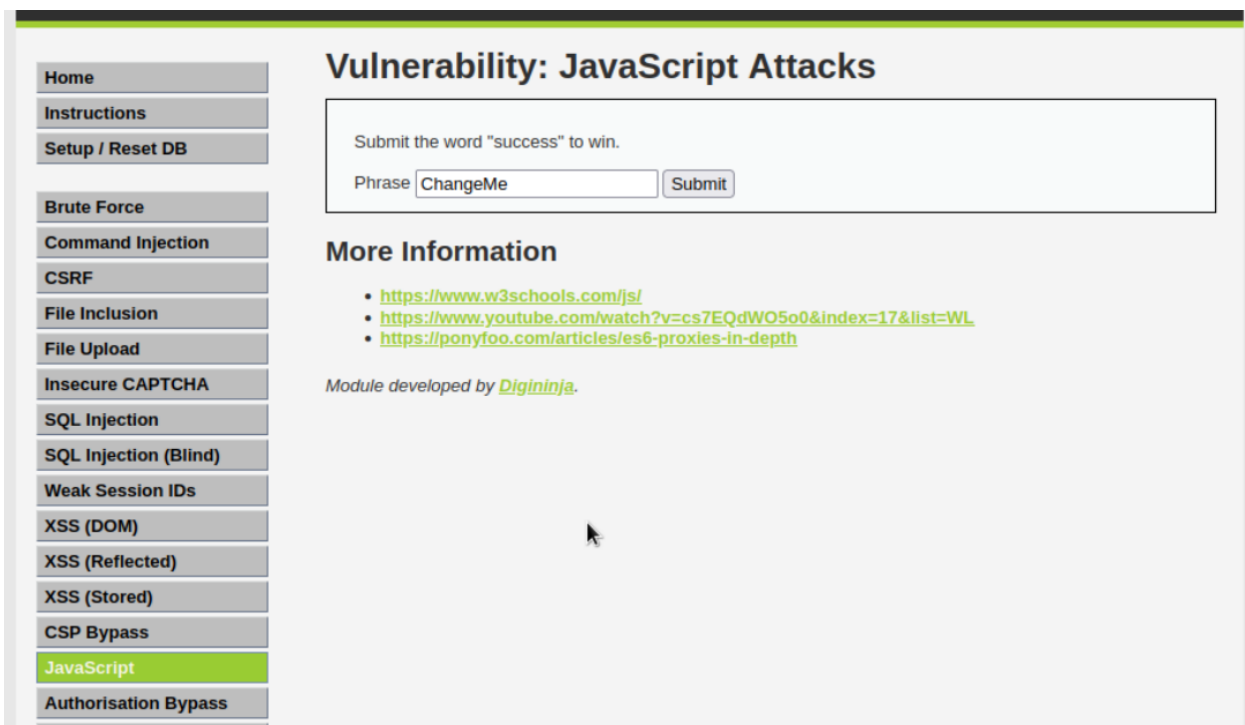
Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafiidh Akbar Sya'bani (akbar@dinustek.com)

## Information Gathering

Pada tampilan awal DVWA klik bagian JavaScript



**Vulnerability: JavaScript Attacks**

Submit the word "success" to win.

Phrase

**More Information**

- <https://www.w3schools.com/js/>
- <https://www.youtube.com/watch?v=cs7EQdWO5o0&index=17&list=WL>
- <https://ponyfoo.com/articles/es6-proxies-in-depth>

Module developed by [Digininja](#).

Tujuan disini adalah untuk menginputkan string yang dianggap "succes"

Menggunakan string default, coba untuk klik Submit

## Vulnerability: JavaScript Attacks

Submit the word "success" to win.

You got the phrase wrong.

Phrase

Muncul bahwa string tersebut salah, muncul status "You got the phrase wrong"  
Coba untuk gunakan kata "success"

## Vulnerability: JavaScript Attacks

Submit the word "success" to win.

You got the phrase wrong.

Phrase

## Vulnerability: JavaScript Attacks

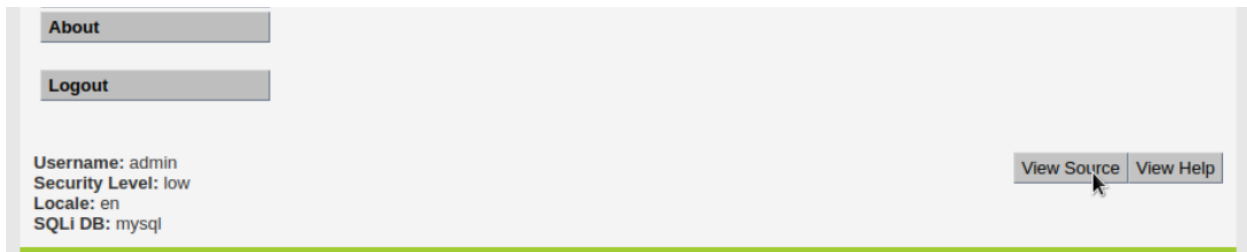
Submit the word "success" to win.

Invalid token.

Phrase

Kata tersebut juga salah, namun status berganti menjadi "Invalid token", ini berarti phrase sudah tepat, namun token masih salah

Coba scroll kebawah dan klik "View Source"

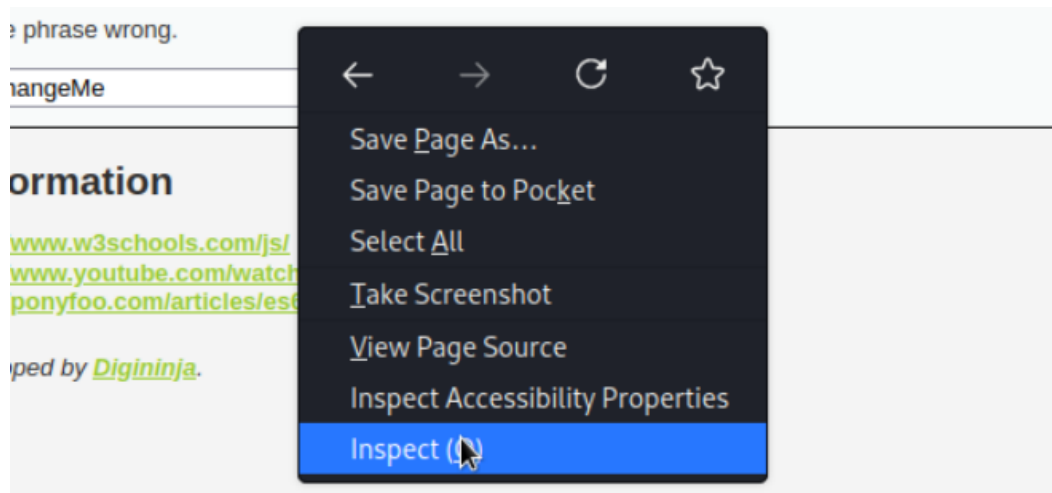


Akan ditampilkan bahwa halaman ini menggunakan kode JavaScript yang ada di `vulnerabilities/javascript/source/medium.js` dengan isi seperti berikut

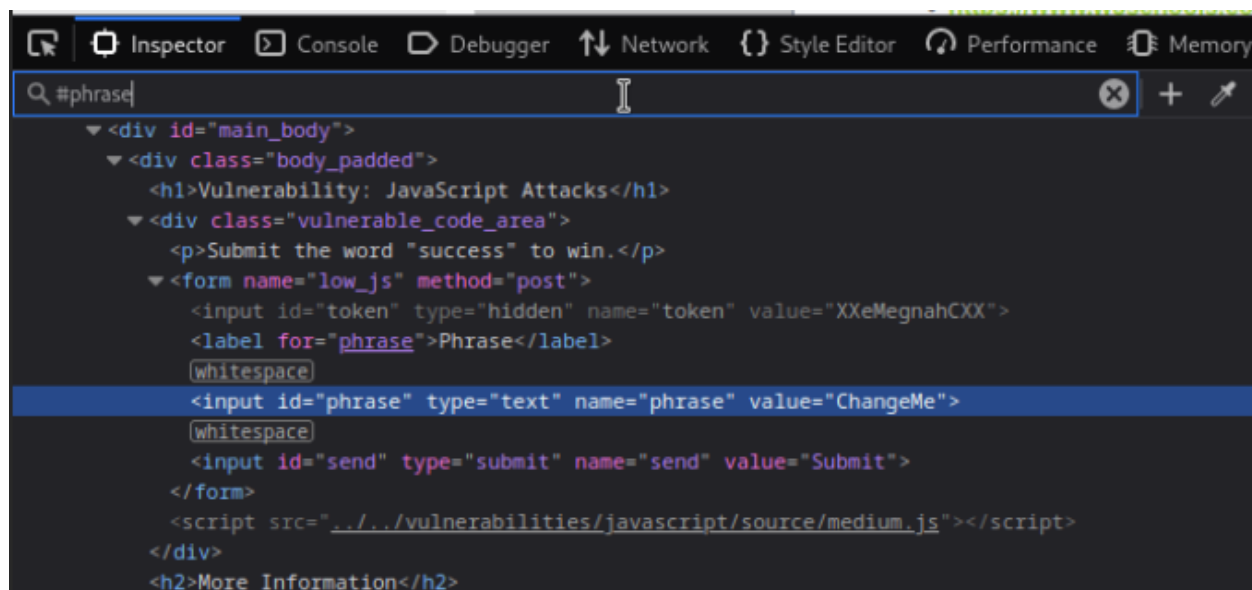
```
function do_something (e) {
  for (var t = '', n = e.length - 1; n >= 0; n--)
    t += e[n];
  return t;
}
setTimeout (function () {
  do_elsesomething ('XX');
}, 300);
function do_elsesomething (e) {
  document.getElementById ('token').value = do_something (
    e + document.getElementById ('phrase').value + 'XX'
  );
}
```

Terdapat 2 fungsi yaitu `do_something` dan `do_elsesomething`, fungsi `do_something` mengubah nilai string parameter menjadi string terbalik, seperti saat string 'ChangeMe' dimasukkan, fungsi ini akan membalik string per karakter sehingga menjadi 'eMegnahC'. Lalu fungsi `do_elsesomething` berfungsi untuk mengubah elemen dengan ID `token` yang berasal dari elemen dengan ID `phrase` dan menambahkan string 'XX' pada bagian belakang dan string parameter `e` di bagian depan lalu dibalik urutan karakternya menggunakan fungsi `do_something`.

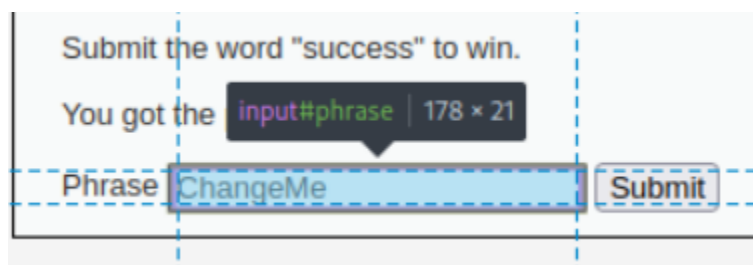
Pada browser Firefox, klik kanan dimana saja lalu pilih "Inspect"



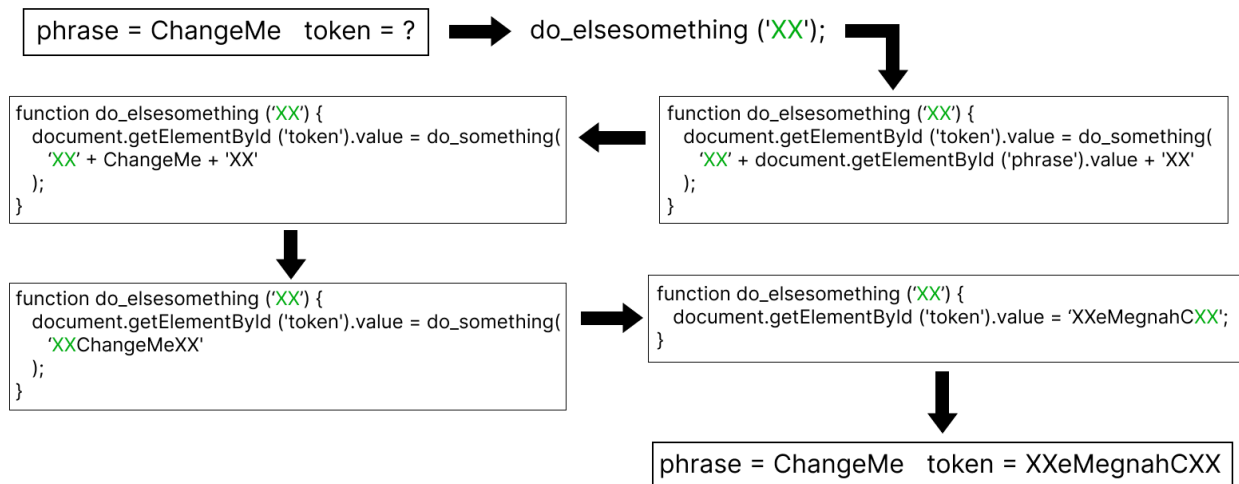
Pada kolom pencarian, ketikkan “#phrase” lalu enter



Maka akan tampak bahwa ID “phrase” digunakan pada kolom string yang diinputkan pada field Phrase



Perhatikan pada elemen input, disana terdapat attribute `value="ChangeMe"`, yang mana ini membuat string "ChangeMe" menjadi default value, jadi setiap kali halaman dibuka, yang akan digunakan pada `document.getElementById ('phrase').value` di fungsi `do_elsesomething()` adalah string "ChangeMe"

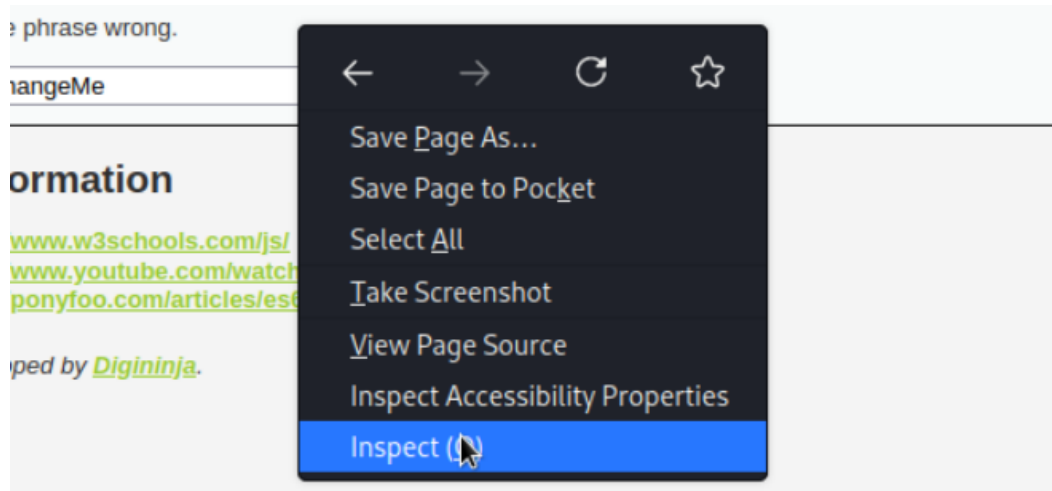


Dari alur diatas didapatkan token dari phrase `ChangeMe` adalah `XXeMegnahCXX`, token dan phrase ini akan terus dipakai selama halaman JavaScript Attack dibuka.

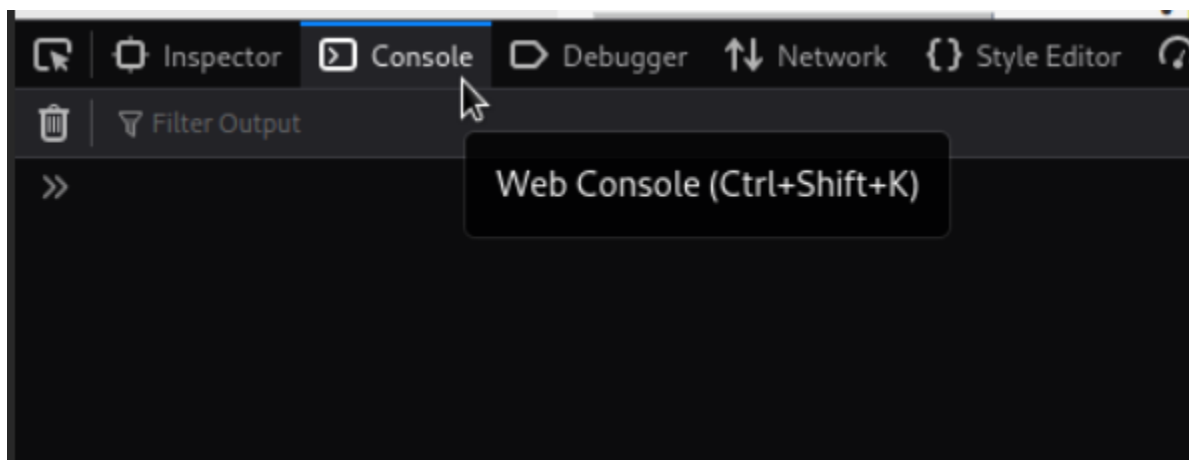
## JavaScript Attack

Kelas ini bertujuan sama seperti JavaScript Attack level low sebelumnya, yaitu memunculkan teks "Well done!" dengan submit phrase dan token yang tepat. Dari paparan sebelumnya, phrase yang tepat untuk kelas ini adalah "success" namun token yang benar belum diketahui.

Pada browser Firefox, klik kanan dimana saja lalu pilih "Inspect"

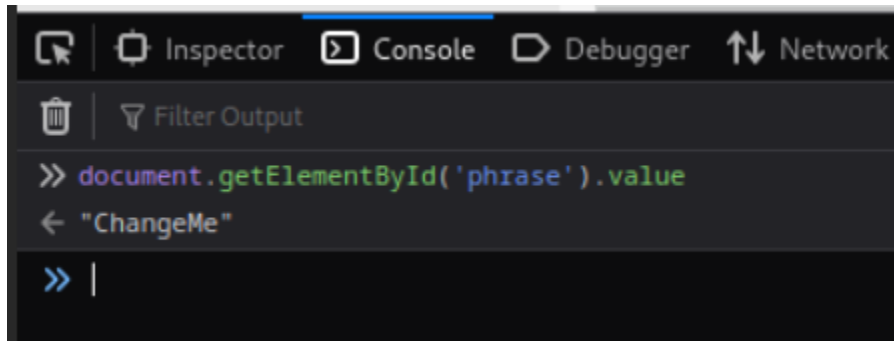


Masuk ke tab Console



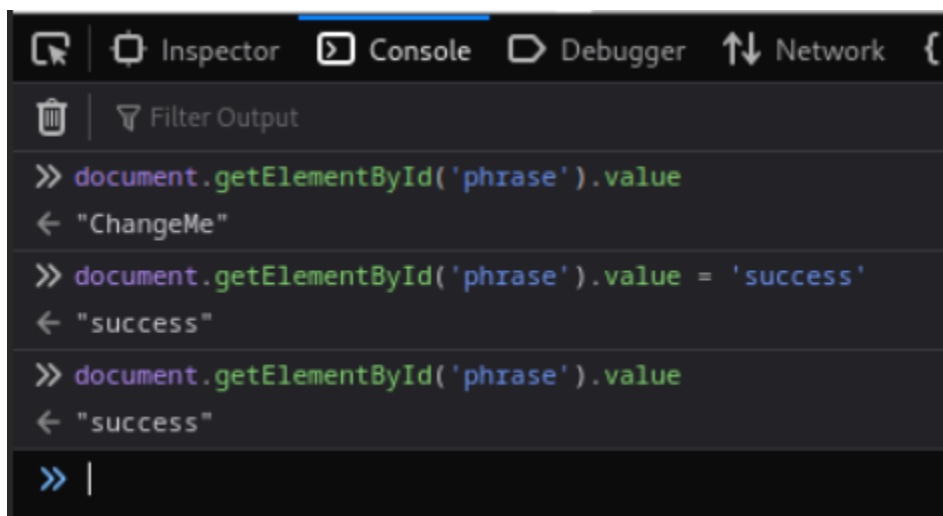
Disini perintah JavaScript dapat dieksekusi, coba untuk print phrase yang sedang digunakan dengan perintah berikut

```
document.getElementById('phrase').value
```



Maka akan muncul phrase yang sedang digunakan saat ini adalah “ChangeMe”, ubah phrase ini menjadi phrase yang benar yaitu “success” menggunakan perintah berikut

```
document.getElementById('phrase').value = 'success'
```



## Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Phrase

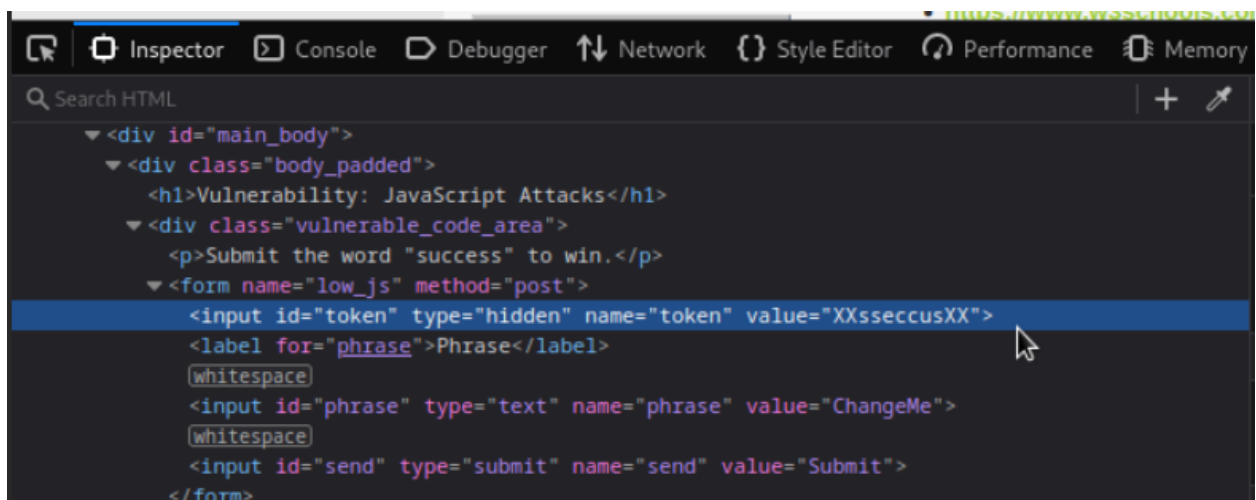
Dengan perintah diatas phrase sudah berganti menjadi “success”. Pada tahap ini phrase sudah tepat, selanjutnya eksekusi fungsi `do_elsesomething('XX')` untuk generate

token.

```
do_elsesomething('XX')
```

```
>> do_elsesomething('XX')
← undefined
>>
```

Di tahap ini jika tab Inspector dibuka lalu lihat pada element dengan ID token, valuenya akan berubah menjadi `XXsseccusXX`



Selanjutnya klik Submit

## Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Phrase





Maka akan muncul teks “Well done!” karena kombinasi phrase dan token sudah benar  
 Dari langkah langkah diatas, alurnya kurang lebih seperti berikut

