

- Marsekal

Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

WRITE UPs CTF #2

CTF.INFOSECINSTITUTE.COM

Nama : -Marsekal

Team : iL7Team, Sulawesi I.T Security, & Medan Cyber Security

1.1 LEVEL 01

Screenshot Soal :

My Sites:

Add your favorites link here

Site Name	Site URL
<input type="text" value="Name of site"/>	<input type="text" value="URL of site"/>
<input type="button" value="Add Link"/>	

People want you to store your favorite links here. However, you are not into that, you just want to do some XSS magic to the page. Add an alert with the message 'Ex1' to the page (My Sites:)

Deskripsi soal :

kita disuruh menampilkan pesan alert 'Ex1' dengan menggunakan teknik XSS.

- Marsekal

Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

Writeups :

Mari kita lakukan teknik XSS seperti pada umumnya.



Terlihat ada notifikasi bahwa format yang kita masukkan salah.



```
<input type="text" placeholder="Name of site" maxsize="10" class="form-control"
pattern="[A-Za-z]+" required="" name="name">
```

Tentu saja inputan kita salah, jika kita lihat kodingannya sang dev memfilter inputan dengan menggunakan syntax `pattern="[A-Za-z]+"` yang mana inputan berupa huruf A sampai Z dan a sampai z.

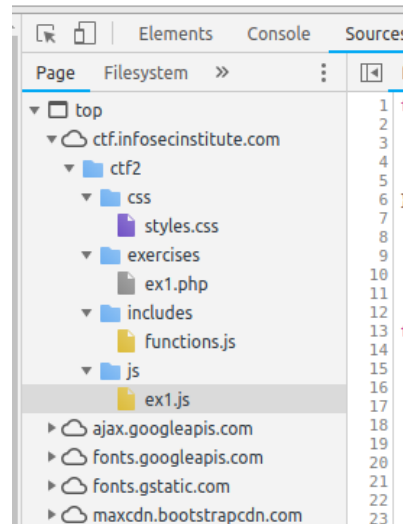
Untuk mengakali nya kita bisa menghapus syntax `pattern` atau menambahkan huruf apa yang bisa kita masukkan. Seperti ini : `pattern="[A-Za-z<>()'/0-9]+"`

Seharusnya ini berjalan dengan lancar, Tapi jika kita submit klik *button Add links* ,

- Marsekal

Team : [iL7Team](#), [Sulawesi I.T Security](#) & [Medan Cyber Team](#)

maka XSS tidak berjalan. Saya yakin pasti ada syntax untuk memfilter lagi setiap inputan kita. Mari kita lihat kumpulan source code yang tersedia.



Terlihat ada file *ex1.js* yang mencurigakan. Mungkin saja dev nya menaruh code filter di file *ex1.js* dan curiga saya benar teletak di baris 18 yang mana memfilter inputan kita.

```
var siteName = $(".ex1 input[type='text']").val().trim().replace(/</g, "&lt;").replace(/>/g, "&gt;");  
var siteURL = $(".ex1 input[type='url']").val().trim().replace(/</g, "&lt;").replace(/>/g, "&gt;");
```

Ada method `.replace()` jika kita sadari bahwa method ini mengganti inputan kita dengan `<` dan `>` . jadi kita cukup hanya menghapus method `replace()`

```
evt.preventDefault();  
var siteName = $(".ex1 input[type='text']").val().trim();  
var siteURL = $(".ex1 input[type='url']").val().trim().replace(/</g, "&lt;").replace(/>/g, "&gt;");
```

Jangan lupa disimpan dengan `ctrl+s` lalu lihat hasil nya.

- Marsekal

Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

ctf.infosecinstitute.com/ctf2/exercises/ex1.php

Website Hacking

My Sites:

ctf.infosecinstitute.com says
Ex1

OK

Site Name	Site URL
<input type="text" value="<script>alert('Ex1');</script>"/>	<input type="text" value="http://google.com"/>
<input type="button" value="Add Link"/>	

You made it to exercise 2. You will be redirected to it in 10 seconds.