WRITE UPs CTF #2

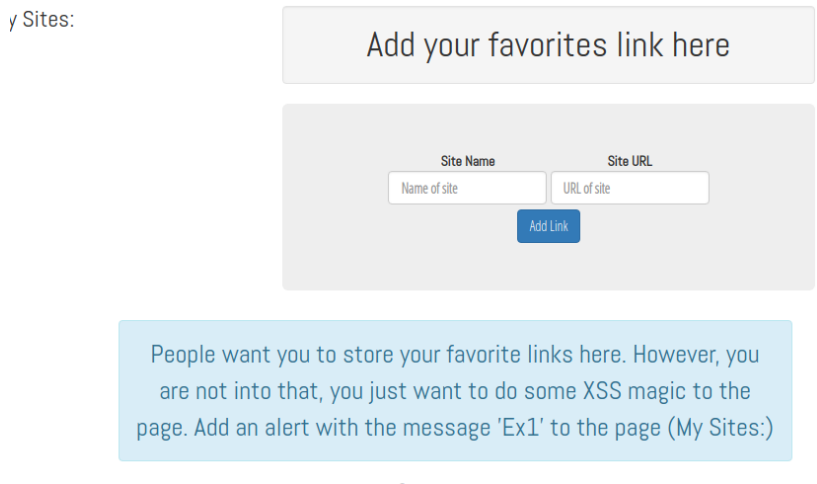
CTF.INFOSECINSTITUTE.COM

Nama : -Marsekal

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

1.1 LEVEL 01

Screenshot Soal :



Deskripsi soal :

kita disuruh manampilkan pesan alert ‘Ex1’ dengan menggunakan teknik XSS.

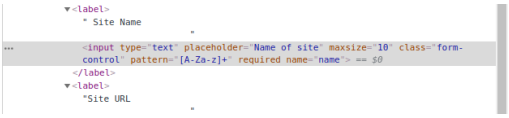
- Marsekal

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.



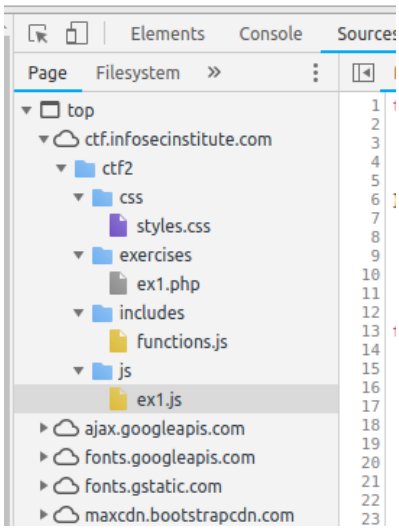
<input type="text" placeholder="Name of site" maxsize="10" class="form-control" pattern="[A-Za-z]+" required="" name="name">

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

Untuk mengakali nya kita bisa menghapus sintax *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* ,

maka XSS tidak berjalan. Saya yakin pasti ada sintax 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 *&lt* dan *&gt* . 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