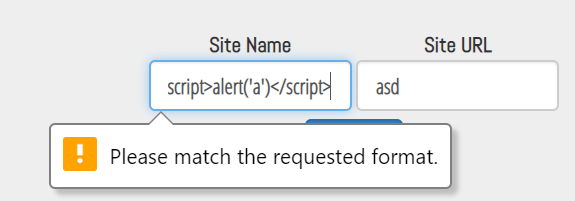
When one tries to insert something malicious one will receive the following error:



The cause for this is that a certain pattern is requested in the html form:



The allowed pattern is letters only (and maxsize of 10).

So what?

Let’s modify it:

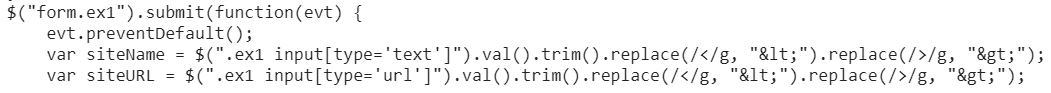


Now we ought to have enough room and be able to insert every character due to the fact that we changed the pattern to be- .\*

When we try again now it doesn’t seem to work either.

So let’s check what happens when the form is sent:

We can see the following function which runs on form submission



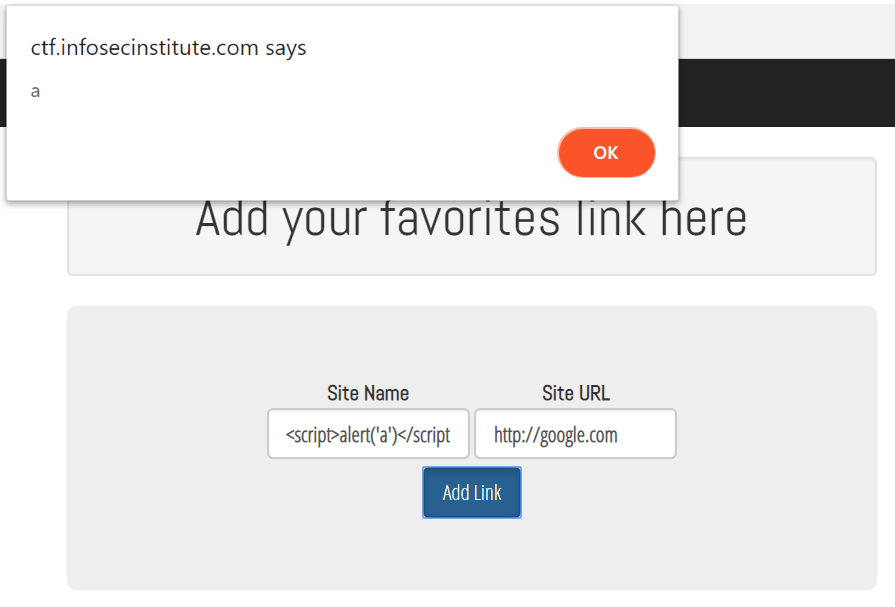
As we can the form’s values are edited before being sent:

the characters “<” and “>” are being replaced with “&lt;” and “&gt;” .

Hence, we can simply erase that part:



Now, we try again:



Yay!