

Forum:[Hack Forums](#)

Thread: [Server Side Template Injections - SSTI](#)

LightOrithm - December 2, 2020, 8:39 am

Hi,

I am currently working on a "website box" and can not for the life of me get past the SSTI section - I dont know how to insert a test code to check if the website is vulnerable to attack.

Where do I insert `{{7*7}}` to check if the website is vulnerable to injection attacks.

All help much appreciated, I have tried google but I think I'm searching the wrong keywords.

Cheers.

caKenpiez - December 4, 2020, 3:51 am

Hey,

So in an essence what you are trying to do is figure out what server side template is in use so you can proceed with the exploit. In order to do that you send your request in whatever user field you can make a request in. However, there is a flow chart you follow to figure out what template is in use by modifying your post request... `{7 * 7}` ... `{{7*7}}` etc and monitoring the output for an answer to your mathematical expression. Try searching for the SSTI crash course on a website called we fourty five dot com. If you have no luck let me know and ill provide more information.

Hey!

Okay so I actually have spent the past hour looking for an answer to your question... First I had to actually understand your question. But try this:

Even if there is no area to actually insert text then modify the url...

So if this is a box challenge it will give you a an address like `xxx.xxx.xx.xxx:xxxxx` and you need to modify it and send your request that way like thus:

```
xxx.xxx.xx.xxx:xxxxx/search={{7*7}}
```

which will return this:

Error 404

The page 'search=49' could not be found

However, this is redundant if this is the box challenge i think it is because the templating engine is already given as Jinja2... I hope you actually log on because i've been working on this lol. So lmk if you need more help :)