

Saturn (web challenge)

URL sanitization

look through files

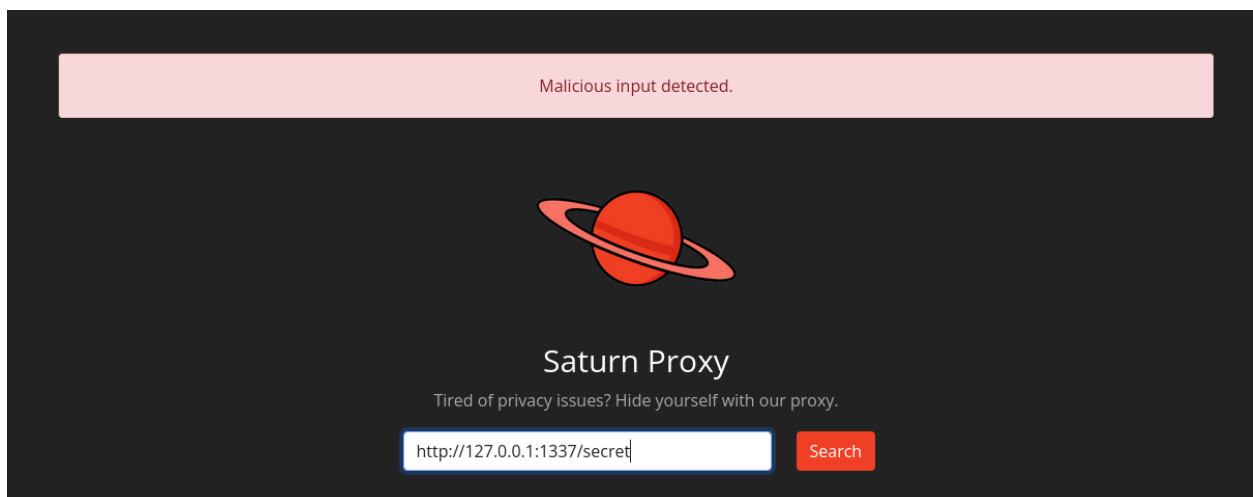
app.py

```
24 @app.route('/secret')
25 def secret():
26     if request.remote_addr == '127.0.0.1':
27         flag = ""
28         with open('./flag.txt') as f:
29             flag = f.readline()
30         return render_template('secret.html', SECRET=flag)
31     else:
32         return render_template('forbidden.html'), 403
33
34
35 if __name__ == '__main__':
36     app.run(host="0.0.0.0", port=1337, threaded=True)
37
```

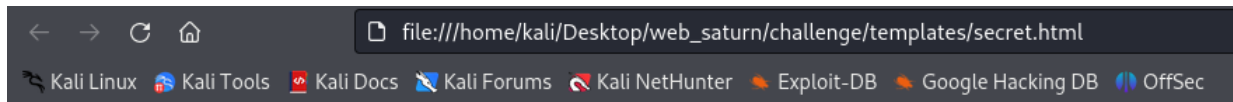
flag.txt is in /secret on localhost (127.0.0.1) on port 1337

input below returns malicious input detected, need to access webpage with different URL input

`http://127.0.0.1:1337/secret`



secret.html



Congratulations!

{{ SECRET }}

```
with open('./flag.txt') as f:
    flag = f.readline()
    return render_template('secret.html', SECRET=flag)
```

webpage returns the flag

need to access through input box but can't because of input sanitization

shorten URL using website to get around input sanitization

<https://cutt.ly/en>

gives shortened/ redirect URL

<https://cutt.ly/LwJAVN9P>

paste into input box on page

gives flag

happy hacking <3