Exercises Lecture 3-4: Hacking beyond, Detection

July 16, 2020

1 Blind sql injection - natas15

The challenge can be accessed at: natas15
Username = natas
Password = AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J
This challenge is similar to natas 14, which you did in the last exercise session, since it is also a kind of sql injection. It does however differ since this is a blind sql incetion. As with he previous natas chalenges, your objective is to get the password to the next level, i.e. natas 16.

Like with natas 14 you are able to get the site into a debug mode by modifying the url. This can be accessed by using this as the url instead natas15.natas.labs.overthewire.org/index.php?debug=true&username=natas15, where you may replace natas15 with whatever you would normally have typed in the username field. By doing this you can at least see what query you end up running on the server.

Note: The password is exactly 32 characters long, so you might want make a small program/ script to get it, once you figure out the right syntax for getting a character from the password. This can either be done with a shell script, or in a programming language of your choice.