

AdventOfCTF-7 Fixed

Challenge

41 Solves

×

07 Fixed

0

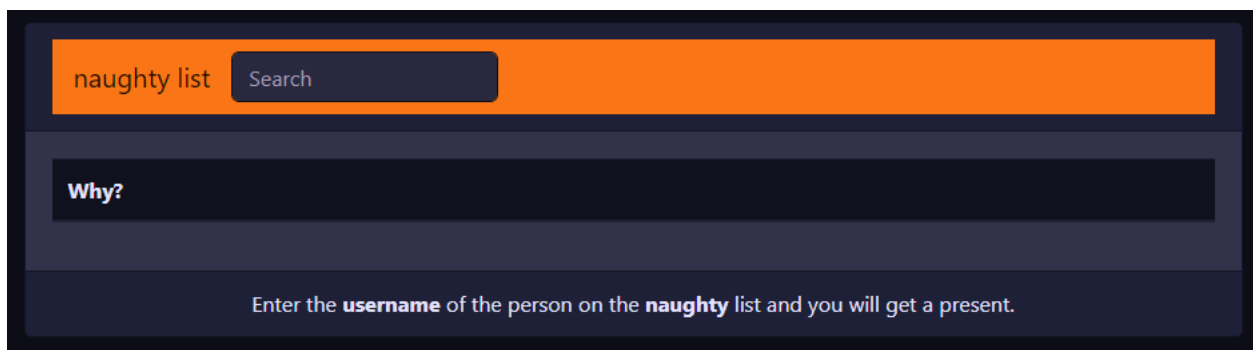
For those that would like to test their blind injection skills this is the fixed version of challenge 7. It removes the feedback to the user in case of wrong SQL and thus it removes the injectionpoint that caused the easy bypass.

The username has been changed, can you find it? Enter the username below.

URL: <https://07-fix.adventofctf.com>

Flag

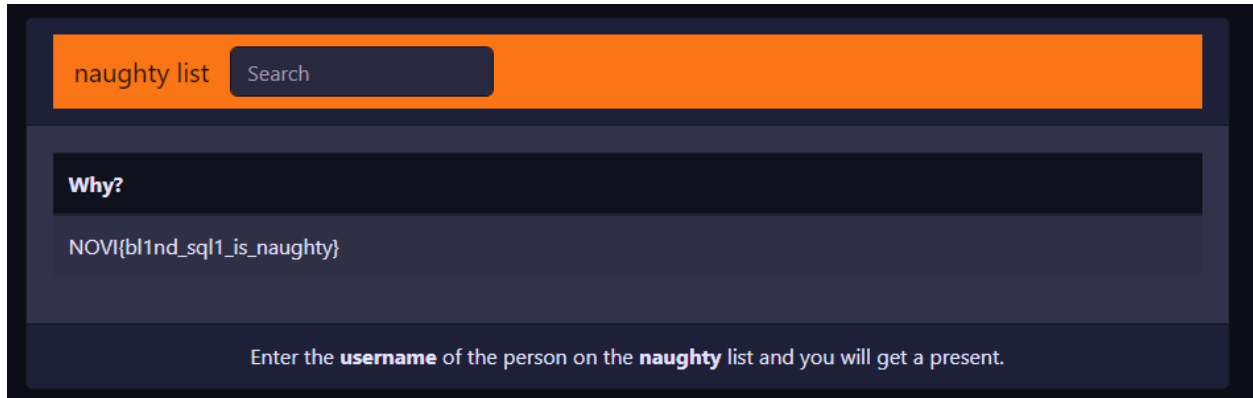
Submit



Using the following query the server will take 5 second to respond, but only if we guess the right letter.

```
' or (select if(mid(username,1,1)='a', sleep(5), 0) from naughty); #
```

So i started sending requests and took note of what characters made the server sleep for 5 seconds and found that the name is: george



The screenshot shows a web application interface with a dark theme. At the top, there is an orange header bar containing the text 'naughty list' and a dark grey search button labeled 'Search'. Below the header, there is a dark grey box with the text 'Why?' in white. Underneath this box, the text 'NOVI{bl1nd_sql1_is_naughty}' is displayed. At the bottom of the interface, a dark grey box contains the instruction: 'Enter the **username** of the person on the **naughty** list and you will get a present.'

To complete the challenge submit the username.