Advanced SQL Injection

Bypass Blacklists

Bypass Blacklists

- Bypass SQL Injection blacklist protection in following SQLi Labs lessons
- We recommend working on these three lessons using both black box and white box testing

Try white box testing

Try black box testing

ZDResearch

Bypass Blacklists - Solution

- We have talked about blacklists, that they can [mostly] be bypassed, I hope you are not disappointed during your testing process
- In Lesson 25, SQLi Lab removes all the 'AND' and 'OR' keywords in the input. Is there any equivalent for 'AND' and 'OR'?
  - If you look at the blacklisted items you will figure out case insensitive:
    - AND
    - OR
- If you check logical operators in MySQL manual you will find out '&&' and '||' are the equivalents
- But in Lesson 25 we can not use '&&' easily because it used as a parameter separator in HTTP GET requests
  - You can solve this problem by URL Encoding (& => %26)

Bypass Blacklists - Solution - Contd.

- Alright! Our final payload is %27%26%261=0--+
  - %27 means ‘
  - %26%26 means &&
  - 1=0 is our condition
  - --+ comment further parts of query (+ is the URL encoded equivalent of space)
- Check the solution on the online lab:

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com