

Forum:[Hack Forums](#)

Thread: [found blind sql injection vuln on a target - need help to inject sql](#)

thund3r - April 15, 2013, 3:33 am

Hi All

i found a blind sql injection on [this target](#)

How can i inject sql this target and extract data from database?

ajkaro - April 15, 2013, 4:36 am

For blind injection you can use this tutorial <https://hackforums.net/showthread.php?tid=3385306>

SHADOW REALM - April 15, 2013, 4:37 am

Did you use Acunetix? If you did then read this thread

<https://hackforums.net/showthread.php?tid=3402467>

thund3r - April 16, 2013, 2:25 am

Tnx for answer.

I read the topics.

it seems in blind sql injection method we need more time to attack the vulnerable target.

Can Anyone give an example on this target for blind sql injection?

Haki - April 16, 2013, 3:03 am

(Apr 16, 2013 02:25 AM)thund3r Wrote: [\[CITE\]](#) Tnx for answer.

I read the topics.

it seems in blind sql injection method we need more time to attack the vulnerable target.

Can Anyone give an example on this target for blind sql injection?

I believe that Ajkaro did give a rather good tutorial for how to use blind SQLi on a target. But yes blind SQLi does require awful alot of time.

thund3r - April 23, 2013, 5:48 am

(Apr 16, 2013 03:03 AM)Haki Wrote: [\[CITE\]](#) I believe that Ajkaro did give a rather good tutorial for how to use blind SQLi on a target. But yes blind SQLi does require awful alot of time.

Tnx.

But that tutorial has not detailed information about how to use commands and functions like sleep and benchmark and that does not tell how to work with time base bsqli .

in other words, there is no public examples for using bsqli.

ajkaro - April 23, 2013, 2:22 pm

(Apr 23, 2013 05:48 AM)thund3r Wrote: [\[CITE\]](#) Tnx.

But that tutorial has not detailed information about how to use commands and functions like sleep and benchmark and that does not tell how to work with time base bsqli .

in other words, there is no public examples for using bsqli.

Sorry but I don't understand you.

Why do you need time based blind SQLi? You have to much time in your life? ?

Boolean based blind SQLi ([using regexp and binary search](#)) is quicker than waiting for every letter in table/column name like 5 seconds using time based blind SQLi (using sleep or benchmark). Why

are you so attracted by sleep or benchmark? And using binary search with regexp is for sure the most quicker blind SQL injection type. For that type of injection you have full explanation of every possible injection with real case examples (integer based, string based, with magic quotes on or off...). It hardly can be more detailed as it is already (5 parts tutorial) ?

Still remember: doing blind by hand will cost you a lot of time.

Good luck. ?

delwaralam - May 26, 2016, 4:57 pm

find sql injection vulnerability and dump all information
check forum.sqliwiki.com