

Forum: [Hack Forums](#)

Thread: [SQL injection in POST-Content](#)

~flexen - December 23, 2014, 4:44 am

Hi,
I got a quick question.

Theres an exploit where you add an SQL-query to the post content with HTTP Live Headers
It looks like this:

Code &cat[0]=1) UNION SELECT concat(.....What does the Code &cat[0]=1) part exactly do?
And is there a way to generally determine when to inject via the post content method?

Thanks. ?

benzi - December 23, 2014, 5:21 am

well, the parameter is 'cat', and the injection point is inside ()'s.

the query probably looks like that-

SELECT.... WHERE cat_id IN (1,2,3,4\$injection)