

Forum:[Hack Forums](#)

Thread: [Injecting SQL Vulnerabilitie = HELP](#)

SERPENT@ - January 5, 2018, 10:27 am

Hello. I have found website wilth SQL Injection Vulnerabilitie, by a scanner !

I have tryed to exploit this vulnerabilitie "POST" , with sqlmap but i doing osomething wrong..

Anyone can sucesfully injecct this?

If anyone success, i am able to pay !!

This is Post REQUEST for SQLMAP..

Vuln Parameter: calc_loan_term

SQLMAP FOUND: [INFO] heuristic (XSS) test shows that POST parameter 'calc_loan_amount' might be vulnerable to cross-site scripting attacks

Code [13:25:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[13:25:35] [INFO] target URL appears to be UNION injectable with 10 columns

[13:25:35] [WARNING] applying generic concatenation (CONCAT)

injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n]

PHP Code

<?php

POST / HTTP/1.1

Accept-Encoding: gzip,deflate

Content-Length: 273

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Host: barzakasa.bg

Connection: Keep-Alive

User-Agent: UserAgent

Cookie: PHPSESSID=9d5e41a29655d8fbb3df2707bd2182c0

Cookie2: \$Version=1

calc_loan_amount=400&user_mini_calc_form=product2&calc_loan_term=60%27+AND+1%3D2
+--+&calc_interest_sum=60&user_mini_calc_form=product2&calc_gpr=0&input-agree=on&submit
=%D0%B2%D0%B7%D0%B5%D0%BC%D0%B8+%D0%B7%D0%B0%D0%B5%D0%
BC+%D0%BD%D0%B0+%D0%B2%D0%BD%D0%BE%D1%81%D0%BA%D0%B8

ma_drt - January 8, 2018, 9:58 am

what is the sqlmap command line you have phrased

[BLANK] - January 8, 2018, 2:16 pm

Two things.

First: The information you provided said it may be vulnerable to xss.

Second: If SQLMAP found the sqlinjection, then why not use that? It will provide you with the exact sql injection that you can reproduce manually if you want.

Why do you need other people to do this? Seems like you want someone to break the law for you.

SERPENT@ - January 8, 2018, 10:54 pm

About ur question.. I have found this vulnerabilitie from burp..

I have tryed with sqlmap but they cannot inject this..

If i can inject this i never ask for heelp.. I think this vuln need some skills to inject, so i ask for helping.

And i will pay someone who can inject this POST Vuln , and got databases..

Thanks btw :)

GhoSTBG - January 9, 2018, 12:38 am

There's no SQL Injection in this website m8. SQLMAP is saying "POST parameter 'calc_loan_amount' might be vulnerable to CROSS-SITE SCRIPTING attacks"