

Joomla! custom reports using “TinyButStrong”

A “get started” guide: Part 3 – Practical security

Summary

Joomla! Administrators familiar with the database and with SQL can use TinyButStrong (TBS) to present information from the database in web pages without needing to create a module or component. Part 1 of this series looked at simple tables and how to format data in the cells. Part 2 addressed security issues in a theoretical way. This article looks at a practical implementation of the theory.

Background

After reading part 1 and part 2 of this guide, you now realise that the power of TBS brings with it responsibility to give access to information in ways that conform to your security needs. The example given here uses the jos_content table and its close allies. Other Joomla! data sources will almost certainly have similar security features that you will need to discover for yourself.

Data source

The data for the report in this article is taken from the tables jos_content, jos_section and jos_categories in the Joomla! database. Columns used in the example are set out in the table below:

Column name	Sample content	Comment
id	1	primary key for this table
title	Welcome to Joomla!	
sectionid	1	key for jos_sections table; NULL if uncategorised
catid	1	key for jos_categories table; NULL if uncategorised
modified	2008-08-12 10:00:00	date and time last modified
hits	92	number of times article has been read
state	1	1: published; 0: unpublished; -1: archived; -2: deleted
access	0	0: public; 1: registered users; 2: “special”

Table 1: Columns used from jos_content

The columns from table jos_section used in the examples are set out in the table below:

Column name	Sample content	Comment
id	3	primary key for this table
title	FAQs	
published	1	1: published; 0: unpublished
access	0	0: public; 1: registered users; 2: "special"

Table 2: Columns used from jos_section

The jos_categories table is similar in structure:

Column name	Sample content	Comment
id	1	primary key for this table
title	Newsflash	
published	1	1: published; 0: unpublished
access	0	0: public; 1: registered users; 2: "special"

Table 3: Columns used from jos_categories

The "access", "state" and "published" columns contain information that determines if information should be displayed and if so, to whom it should be displayed.

As with the jos_content table, there are other columns that are not used in the examples.

For the purpose of this part of the guide, three new articles have been added to the system:

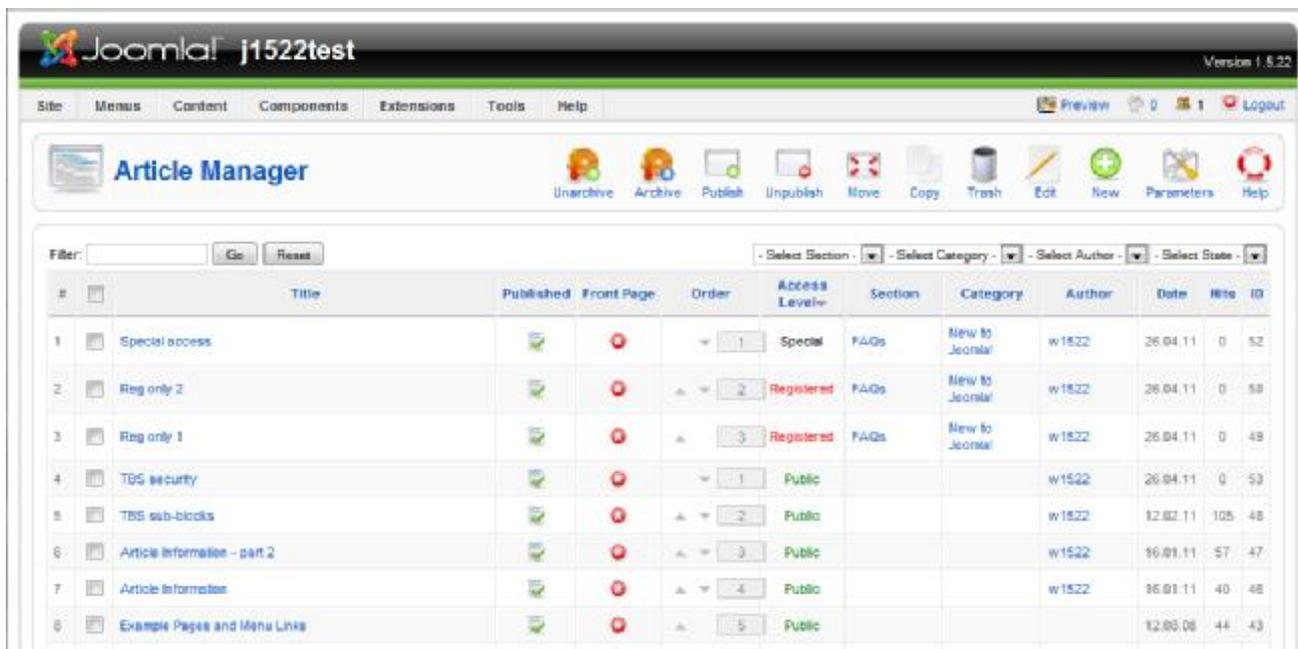


Illustration 1: Three articles with restricted access

In addition, a copy of the "TBS sub-blocks" article was put into the FAQs section and then deleted. It doesn't show in the article manager as can be seen in Illustration 2.

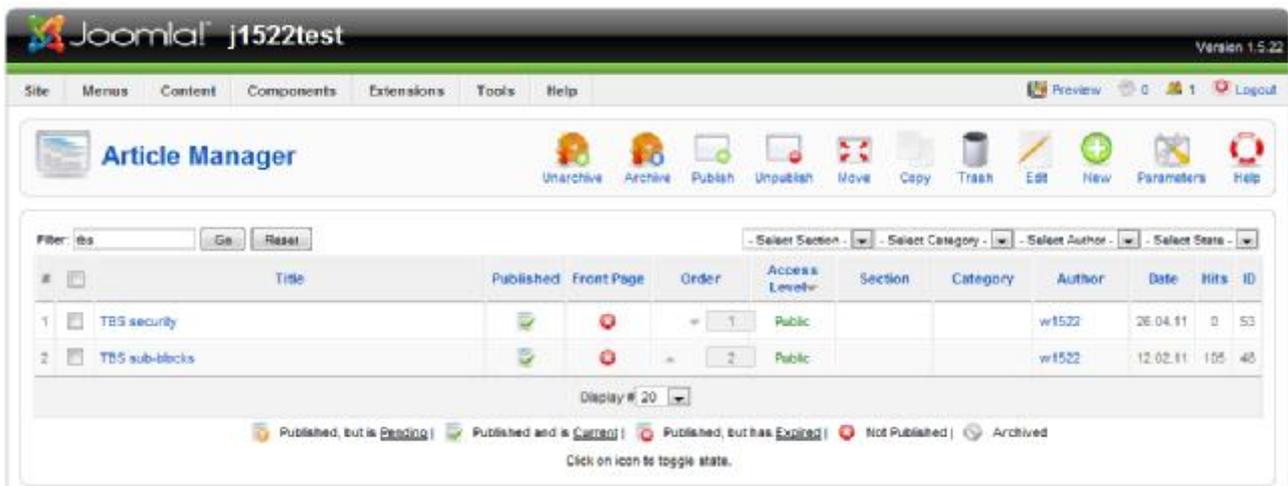


Illustration 2: Only two "TBS" articles visible

If we look at the database with phpMyAdmin, we see the deleted item is still present as in Illustration 3

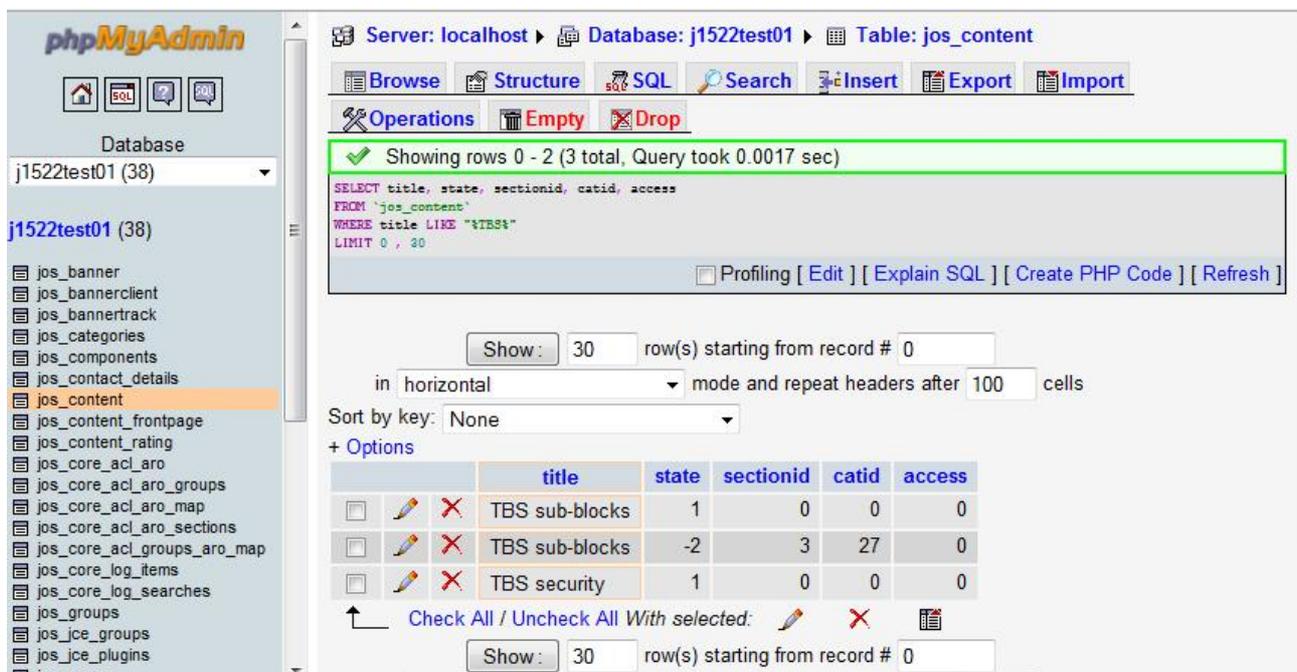


Illustration 3: Deleted item has state of -2

This should alert us to the need to filter the data carefully before presenting it. We don't want outsiders seeing the material we have discarded.

For the purpose of this example, the sample data has been modified: the section/category FAQs/Current Users access level has been set to "Registered" and FAQs/Languages access level set to "Special" so that data can be filtered by category as well as by article. To reduce the amount of data presented, only articles with sectionid=3 (FAQs) are shown. The effect of using phpMyAdmin to run the SQL below on the database is shown in Illustration 4.

```
SELECT content.title, sec.title AS section, cat.title AS category,
sec.published AS secpub, sec.access AS secacc, cat.access AS
```

```

catacc, cat.published AS catpub, content.access AS artacc,
content.state AS artpub FROM jos_content AS content LEFT JOIN
jos_sections AS sec ON sectionid = sec.id LEFT JOIN jos_categories
AS cat ON catid = cat.id WHERE sectionid=3 ORDER BY section,
category

```

title	section	category	secpub	secacc	catacc	catpub	artacc	artpub
How do I upgrade to Joomla! 1.5 ?	FAQs	Current Users	1	0	1	1	0	1
What happened to the locale setting?	FAQs	Current Users	1	0	1	1	0	1
Only one edit window! How do I create "Read more.....	FAQs	Current Users	1	0	1	1	0	1
Where is the Static Content Item?	FAQs	Current Users	1	0	1	1	0	1
Where did the Installers go?	FAQs	Current Users	1	0	1	1	0	1
Where did the Mambots go?	FAQs	Current Users	1	0	1	1	0	1
Why does Joomla! 1.5 use UTF-8 encoding?	FAQs	General	1	0	0	1	0	1
What is the FTP layer for?	FAQs	General	1	0	0	1	0	1
Can Joomla! 1.5 operate with PHP Safe Mode On?	FAQs	General	1	0	0	1	0	1
My MySQL database does not support UTF-8. Do I hav...	FAQs	General	1	0	0	1	0	1
What are the requirements to run Joomla! 1.5?	FAQs	General	1	0	0	1	0	1
How do I install Joomla! 1.5?	FAQs	General	1	0	0	1	0	1
What is an Uncategorized Article?	FAQs	General	1	0	0	1	0	1
Is it possible to change A Menu Item's Type?	FAQs	General	1	0	0	1	0	1
How do I localise Joomla! to my language?	FAQs	Languages	1	0	2	1	0	1
What is the purpose of the collation selection in ...	FAQs	Languages	1	0	2	1	0	1
What languages are supported by Joomla! 1.5?	FAQs	Languages	1	0	2	1	0	1
Does the PDF icon render pictures and special char...	FAQs	Languages	1	0	2	1	0	1
I installed with my own language, but the Back-end...	FAQs	Languages	1	0	2	1	0	1
Is it useful to install the sample data?	FAQs	New to Joomla!	1	0	0	1	0	1
How do I remove an Article?	FAQs	New to Joomla!	1	0	0	1	0	1
What is the difference between Archiving and Trash...	FAQs	New to Joomla!	1	0	0	1	0	1
Reg only 1	FAQs	New to Joomla!	1	0	0	1	1	1
Reg only 2	FAQs	New to Joomla!	1	0	0	1	1	1
TBS sub-blocks	FAQs	New to Joomla!	1	0	0	1	0	-2
Special access	FAQs	New to Joomla!	1	0	0	1	2	1

Illustration 4: Articles and their attributes as displayed by phpMyAdmin

The special values of the Access field in jos_categories and of the access and state field in jos_content are highlighted in Illustration 4 in the columns catacc, artacc and artpub respectively. Using phpMyAdmin to test SQL can be a real timesaver as it enables you to move tested SQL into TBS and then concentrate on the use of TBS as a display tool.

In part two of this series, it was noted that the SQL query used should make available only that information that can safely be exposed. It is therefore necessary to amend the SQL so that only published articles with public access are visible. The following WHERE clause conditions should achieve this:

```

sec.published=1 AND cat.published=1 AND content.state=1 AND
sec.access=0 AND cat.access=0 AND content.access=0

```

The revised SQL statement is now

```

SELECT content.title, sec.title AS section, cat.title AS category,
sec.published AS secpub, sec.access AS secacc, cat.access AS
catacc, cat.published AS catpub, content.access AS artacc,
content.state AS artpub FROM jos_content AS content LEFT JOIN
jos_sections AS sec ON sectionid = sec.id LEFT JOIN jos_categories
AS cat ON catid = cat.id WHERE sectionid=3 AND sec.published=1 AND
cat.published=1 AND content.state=1 AND sec.access=0 AND

```

```
cat.access=0 AND content.access=0 ORDER BY section, category
```

Now that the data extracted from the database is properly filtered, we can construct a TBS report that can safely be shown to the public. The SQL is identical to that above except for the addition of “hits” as an extra column. It is now stored in a script directory outside the web root, as explained in part 2 of the series. The script is shown in the Appendix.

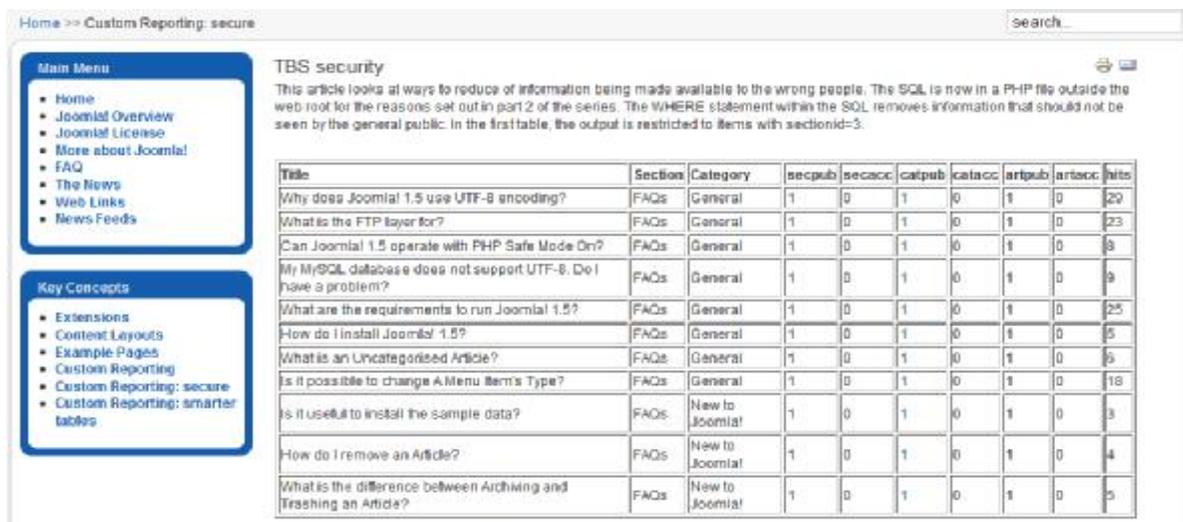
It is invoked by a TBS statement such as

```
{tbs}script=tbs3a.php{/tbs}
```

The template HTML follows:

```
<tr>
  <td>[tbs3a.title]</td>
  <td>[tbs3a.section]</td>
  <td>[tbs3a.category]</td>
  <td>[tbs3a.secpub]</td>
  <td>[tbs3a.secacc]</td>
  <td>[tbs3a.catpub]</td>
  <td>[tbs3a.catacc]</td>
  <td>[tbs3a.artpub]</td>
  <td>[tbs3a.artacc]</td>
  <td>[tbs3a.hits;block=tr]</td>
</tr>
```

The “block=tr” code is within the “hits” template element to demonstrate that it doesn't need to come on the first item in the template. The output is shown in Illustration 5.



Home >> Custom Reporting: secure

search

TBS security

This article looks at ways to reduce of information being made available to the wrong people. The SQL is now in a PHP file outside the web root for the reasons set out in part 2 of the series. The WHERE statement within the SQL removes information that should not be seen by the general public. In the first table, the output is restricted to items with sectionid=3.

Title	Section	Category	secpub	secacc	catpub	catacc	artpub	artacc	hits
Why does Joomla! 1.5 use UTF-8 encoding?	FAQs	General	1	0	1	0	1	0	29
What is the FTP layer for?	FAQs	General	1	0	1	0	1	0	23
Can Joomla! 1.5 operate with PHP Safe Mode On?	FAQs	General	1	0	1	0	1	0	8
My MySQL database does not support UTF-8. Do I have a problem?	FAQs	General	1	0	1	0	1	0	9
What are the requirements to run Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	25
How do I install Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	5
What is an Uncategorized Article?	FAQs	General	1	0	1	0	1	0	5
Is it possible to change A.Menu Item's Type?	FAQs	General	1	0	1	0	1	0	18
Is it useful to install the sample data?	FAQs	New to Joomla!	1	0	1	0	1	0	3
How do I remove an Article?	FAQs	New to Joomla!	1	0	1	0	1	0	4
What is the difference between Archiving and Trashing an Article?	FAQs	New to Joomla!	1	0	1	0	1	0	5

Illustration 5: Data as shown by TBS for sectionid=3

Before cheerfully signing this off as “job done”, let's take off the selection by sectionid to see how it works with the full set of data. The WHERE clause now reads:

```
WHERE sec.published=1 AND cat.published=1 AND content.state=1 AND
sec.access=0 AND cat.access=0 AND content.access=0
```

The output from this is shown in Illustration 6

Now without the sectionid=3 constraint

Title	Section	Category	secpub	secacc	catpub	catacc	artpub	artacc	hits
Joomla! Features	About Joomla!	The CMS	1	0	1	0	1	0	59
Joomla! Overview	About Joomla!	The CMS	1	0	1	0	1	0	151
What's New in 1.5?	About Joomla!	The CMS	1	0	1	0	1	0	92
Content Layouts	About Joomla!	The CMS	1	0	1	0	1	0	70
Extensions	About Joomla!	The CMS	1	0	1	0	1	0	103
Joomla! Facts	About Joomla!	The Community	1	0	1	0	1	0	50
The Joomla! Community	About Joomla!	The Community	1	0	1	0	1	0	52
Joomla! License Guidelines	About Joomla!	The Project	1	0	1	0	1	0	100
Support and Documentation	About Joomla!	The Project	1	0	1	0	1	0	6
Platforms and Open Standards	About Joomla!	The Project	1	0	1	0	1	0	11
What is an Uncategorized Article?	FAQs	General	1	0	1	0	1	0	6
Is it possible to change A Menu Item's Type?	FAQs	General	1	0	1	0	1	0	18
Why does Joomla! 1.5 use UTF-8 encoding?	FAQs	General	1	0	1	0	1	0	29
What is the FTP layer for?	FAQs	General	1	0	1	0	1	0	23
Can Joomla! 1.5 operate with PHP Safe Mode On?	FAQs	General	1	0	1	0	1	0	8
My MySQL database does not support UTF-8. Do I have a problem?	FAQs	General	1	0	1	0	1	0	9
What are the requirements to run Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	25
How do I install Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	5
Is it useful to install the sample data?	FAQs	New to Joomla!	1	0	1	0	1	0	3
How do I remove an Article?	FAQs	New to Joomla!	1	0	1	0	1	0	4
What is the difference between Archiving and Trashing an Article?	FAQs	New to Joomla!	1	0	1	0	1	0	5
Welcome to Joomla!	News	Latest	1	0	1	0	1	0	92
We are Volunteers	News	Latest	1	0	1	0	1	0	54
Millions of Smiles	News	Latest	1	0	1	0	1	0	23
Joomla! Security Strike Team	News	Latest	1	0	1	0	1	0	0
Joomla! Community Portal	News	Latest	1	0	1	0	1	0	5
Newsflash 1	News	Newsflash	1	0	1	0	1	0	1
Newsflash 2	News	Newsflash	1	0	1	0	1	0	0

Illustration 6: Output without the sectionid=3 constraint (a couple of “Newsflash” items are not shown)

Unfortunately, if we compare this with the equivalent report at illustration 13 in article 1, there are some missing items. These are the “Uncategorised” items that have sectionid=NULL in the database. Our select phrase

```
sec.published=1 AND cat.published=1 AND content.state=1 AND
sec.access=0 AND cat.access=0 AND content.access=0
```

subtly eliminates these items as the LEFT JOIN will result in sec.published and sec.access being

NULL for these items rather than zero. The WHERE clause must therefore be extended to cope with this situation:

```
WHERE (sec.published=1 OR ISNULL(sec.published)) AND
(cat.published=1 OR ISNULL(cat.published)) AND content.state=1 AND
(sec.access=0 OR ISNULL(sec.access)) AND (cat.access=0 OR
ISNULL(cat.access)) AND content.access=0
```

When this clause is used, the output is consistent with the output seen in Illustration 11 of article 1. The “ifempty” parameter has not been used in the template, so where the section or category name is “Uncategorised”, the appropriate cell is empty.

Title	Section	Category	secpub	secacc	catpub	catacc	artpub	artacc	hits
Example Pages and Menu Links							1	0	44
Article Information							1	0	42
Article Information - smarter tables							1	0	67
TBS sub-blocks							1	0	109
TBS security							1	0	28
Content Layouts	About Joomla!	The CMS	1	0	1	0	1	0	70
Extensions	About Joomla!	The CMS	1	0	1	0	1	0	103
Joomla! Features	About Joomla!	The CMS	1	0	1	0	1	0	59
Joomla! Overview	About Joomla!	The CMS	1	0	1	0	1	0	151
What's New in 1.5?	About Joomla!	The CMS	1	0	1	0	1	0	92
The Joomla! Community	About Joomla!	The Community	1	0	1	0	1	0	52
Joomla! Facts	About Joomla!	The Community	1	0	1	0	1	0	50
Platforms and Open Standards	About Joomla!	The Project	1	0	1	0	1	0	11
Joomla! License Guidelines	About Joomla!	The Project	1	0	1	0	1	0	100
Support and Documentation	About Joomla!	The Project	1	0	1	0	1	0	6
What are the requirements to run Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	25
How do I install Joomla! 1.5?	FAQs	General	1	0	1	0	1	0	5
What is an Uncategorized Article?	FAQs	General	1	0	1	0	1	0	6
Is it possible to change A Menu Item's Type?	FAQs	General	1	0	1	0	1	0	18
Why does Joomla! 1.5 use UTF-8 encoding?	FAQs	General	1	0	1	0	1	0	29
What is the FTP layer for?	FAQs	General	1	0	1	0	1	0	23
Can Joomla! 1.5 operate with PHP Safe Mode On?	FAQs	General	1	0	1	0	1	0	8
My MySQL database does not support UTF-8. Do I have a problem?	FAQs	General	1	0	1	0	1	0	9
Is it useful to install the sample data?	FAQs	New to Joomla!	1	0	1	0	1	0	3

Illustration 7: Articles with NULL sectionid and categoryid now appear

The example above shows that when checking the output it is important to look both at the things that do appear and at the things that don't appear. The latter are much more difficult to check.

Conclusion

To ensure that data cannot be seen by the wrong people you need to look at the database contents carefully so that you understand how restricted access is indicated. Once you have this knowledge, you can create SQL statements that filter the data appropriately. You can then concentrate on using TBS to display the data in the way that best suits your audience. You can also safely let others develop TBS templates using the same data.

Acknowledgement

Thanks to Skrol29 for his efforts in developing TBS.

CheshireCat

1 Jul 2011

Appendix

Example 1 – selected by sectionid

The script filters out data that should not be seen by the general public.

Script

The script below can be pasted into a good text editor (e.g. Notepad++) and then saved as a .php file in your scripts directory.

```
<?php
$TBS->MergeBlock('tbs3a','mysql','SELECT content.title, sec.title
AS section, cat.title AS category, sec.published AS secpub,
sec.access AS secacc, cat.access AS catacc, cat.published AS
catpub, content.access AS artacc, content.state AS artpub,
content.hits AS hits FROM jos_content AS content LEFT JOIN
jos_sections AS sec ON sectionid = sec.id LEFT JOIN jos_categories
AS cat ON catid = cat.id WHERE sectionid=3 AND sec.published=1 AND
cat.published=1 AND content.state=1 AND sec.access=0 AND
cat.access=0 AND content.access=0 ORDER BY section, category ');
?>
```

HTML

The HTML text below can be pasted into the HTML editing window of Joomla Content Editor.

```
<p>This article looks at ways to reduce of information being made
available to the wrong people. The SQL is now in a PHP file
outside the web root for the reasons set out in part 2 of the
series. The WHERE statement within the SQL removes information
that should not be seen by the general public.</p>
```

```
<p> </p>
```

```
<p>{tbs} script=tbs3a.php{/tbs}</p>
```

```
<p> </p>
```

```
<table border="1">
```

```
  <tbody>
```

```
    <tr>
```

```
      <td><strong>Title</strong></td>
```

```
      <td><strong>Section</strong></td>
```

```
      <td><strong>Category</strong></td>
```

```
      <td><strong>secpub</strong></td>
```

```
      <td><strong>secacc</strong></td>
```

```
      <td><strong>catpub</strong></td>
```

```
      <td><strong>catacc</strong></td>
```

```
      <td><strong>artpub</strong></td>
```

```
      <td><strong>artacc</strong></td>
```

```
      <td><strong>hits</strong></td>
```

```
    </tr>
```

```
</tbody>
```

```
</table>
```

```

        <td>[tbs3a.title]</td>
        <td>[tbs3a.section]</td>
        <td>[tbs3a.category]</td>
        <td>[tbs3a.secpub]</td>
        <td>[tbs3a.secacc]</td>
        <td>[tbs3a.catpub]</td>
        <td>[tbs3a.catacc]</td>
        <td>[tbs3a.artpub]</td>
        <td>[tbs3a.artacc]</td>
        <td>[tbs3a.hits;block=tr]</td>
    </tr>
</tbody>
</table>

```

Example 2 – without selection by sectionid

Script

The only change in the script below is the removal of the sectionid=3 constraint

```

<?php
$tBS->MergeBlock('tbs3b','mysql','SELECT content.title, sec.title
AS section, cat.title AS category, sec.published AS secpub,
sec.access AS secacc, cat.access AS catacc, cat.published AS
catpub, content.access AS artacc, content.state AS artpub,
content.hits AS hits FROM jos_content AS content LEFT JOIN
jos_sections AS sec ON sectionid = sec.id LEFT JOIN jos_categories
AS cat ON catid = cat.id WHERE sec.published=1 AND cat.published=1
AND content.state=1 AND sec.access=0 AND cat.access=0 AND
content.access=0 ORDER BY section, category ');
?>

```

HTML

The only alterations in the script below are to the name of script file and the name of the mergeblock:

```

<p>{tbs} script=tbs3b.php{/tbs}</p>
<p>Now without the sectionid=3 constraint:</p>
<table border="1">
    <tbody>
        <tr>
            <td><strong>Title</strong></td>
            <td><strong>Section</strong></td>
            <td><strong>Category</strong></td>
            <td><strong>secpub</strong></td>
            <td><strong>secacc</strong></td>
            <td><strong>catpub</strong></td>
            <td><strong>catacc</strong></td>
            <td><strong>artpub</strong></td>
            <td><strong>artacc</strong></td>

```

```

        <td><strong>hits</strong></td>
    </tr>
    <tr>
        <td>[tbs3b.title]</td>
        <td>[tbs3b.section]</td>
        <td>[tbs3b.category]</td>
        <td>[tbs3b.secpub]</td>
        <td>[tbs3b.secacc]</td>
        <td>[tbs3b.catpub]</td>
        <td>[tbs3b.catacc]</td>
        <td>[tbs3b.artpub]</td>
        <td>[tbs3b.artacc]</td>
        <td>[tbs3b.hits;block=tr]</td>
    </tr>
</tbody>
</table>

```

Example 3 – without selection by sectionid but with correct handling of *NULL* fields

Script

Articles with *NULL* values for some fields are accepted:

```

<?php
$TBS->MergeBlock('tbs3c','mysql','SELECT content.title, sec.title
AS section, cat.title AS category, sec.published AS secpub,
sec.access AS secacc, cat.access AS catacc, cat.published AS
catpub, content.access AS artacc, content.state AS artpub,
content.hits AS hits FROM jos_content AS content LEFT JOIN
jos_sections AS sec ON sectionid = sec.id LEFT JOIN jos_categories
AS cat ON catid = cat.id WHERE (sec.published=1 OR
ISNULL(sec.published)) AND (cat.published=1 OR
ISNULL(cat.published)) AND content.state=1 AND (sec.access=0 OR
ISNULL(sec.access)) AND (cat.access=0 OR ISNULL(cat.access)) AND
content.access=0 ORDER BY section, category ');
?>

```

Note that this example is for MySQL.

HTML

As in example 2, the only alterations in the script below are to the name of script file and the name of the mergeblock:

```

<p>{tbs} script=tbs3c.php{/tbs}</p>
<p>Now without the sectionid=3 constraint but with the corrected
treatment for NULL values</p>
<table border="1">
    <tbody>
        <tr>

```

```
<td><strong>Title</strong></td>
<td><strong>Section</strong></td>
<td><strong>Category</strong></td>
<td><strong>secpub</strong></td>
<td><strong>secacc</strong></td>
<td><strong>catpub</strong></td>
<td><strong>catacc</strong></td>
<td><strong>artpub</strong></td>
<td><strong>artacc</strong></td>
<td><strong>hits</strong></td>
</tr>
<tr>
<td>[tbs3c.title]</td>
<td>[tbs3c.section]</td>
<td>[tbs3c.category]</td>
<td>[tbs3c.secpub]</td>
<td>[tbs3c.secacc]</td>
<td>[tbs3c.catpub]</td>
<td>[tbs3c.catacc]</td>
<td>[tbs3c.artpub]</td>
<td>[tbs3c.artacc]</td>
<td>[tbs3c.hits;block=tr]</td>
</tr>
</tbody>
</table>
<p> </p>
<p>End of custom report</p>
```