

Discourse sending email function exist Server side request forgery SSRF #10509

Merged discoursebuild merged 2 commits into tests-passed from master on Aug 24, 2020

Conversation	0	Commits	2	Checks	0	Files changed	3
--------------	---	---------	---	--------	---	---------------	---

 purple-WL commented on Aug 23, 2020

1、 First, send a new email

← → ↺ [Progress Bar] messages

Brands

[Home](#)

Forum

PowerDraw

Testing Club

Referrals New

Q

Lv0

Email

Country China

Joined 20 hours

Last Post 12 hours

Seen 2 mins

Views 0

Experience Points 20

PowerBucks 10

Summary | Activity | Notifications | **Messages** | Badges | Points&Bucks | Network
| Preferences

 New Message | **Inbox** | Sent | Archive

Adqdq

b_j 19 hours ago

2
1

2. Choose to upload images from a website

Add an image

☐ From my device

☒ From the web

http://2[redacted]o/ssrf.jpg

[link to image](#)

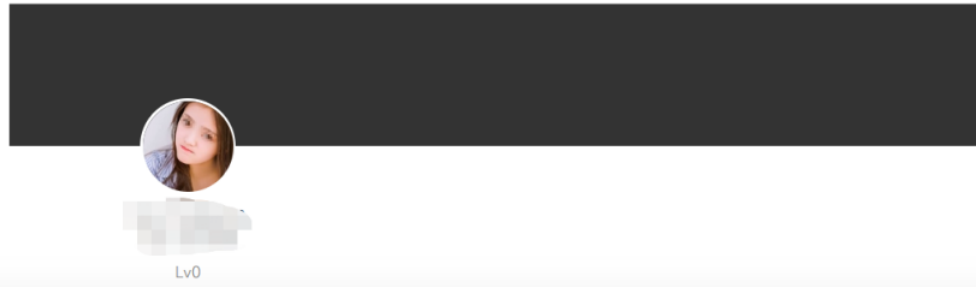
(you can also drag & drop into the editor to upload them)

 Upload


cancel

[show more](#)











3、 send mail




Start a message

19dgarner  Add a user

111111111111111111

 **B** *I*         

 Message cancel

4、 The email has been sent.

[illegible]

5、 Our remote server received a GET request from the site !

ID	Name	Remote Addr	Method	Data	User Agent	Content Type	Created At (UTC+0)
52964	[REDACTED]	[REDACTED]	[REDACTED]		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36		2020-08-12 06:53:13
529642	[REDACTED]	[REDACTED]	[REDACTED]		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36		2020-08-12 06:53:12
5296428	http://27[REDACTED]o/ssrf.jpg	52.89.21.106	GET		Ruby		2020-08-12 06:53:12

6. The vulnerability was tested in both versions 2.3.2 and 2.6

ID	Name	Remote Addr	Method	Data	User Agent	Content Type
548169						
9	http://[redacted].io/3.jpg	72.52.80.4	GET		Ruby	
548168						
1	http://[redacted].io/1.jpg	140.238.29.216	GET		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36	

 FIX: Correct personal_messages:<username> advanced search filter. ...

✓ 4b30799

 **purple-WL** changed the base branch from stable to tests-passed 2 years ago

 Fix lint.

✓ 2f043dc

 **discoursebuild** merged commit **2f043dc** into tests-passed on Aug 24, 2020
1 check passed

[View details](#)

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

3 participants

