ultimatemember / **ultimatemember** Public

Code · **Issues** 188 · Pull requests 18 · Actions · Projects 1 · Wiki · ...

New issue

Jump to bottom

Security issues in URL and social fields #989

Open · 3 tasks done · **yuriinalivaiko** opened this issue on Apr 1 · 0 comments

Assignees

yuriinalivaiko commented on Apr 1 · Contributor

Isolating the problem (mark completed items with an [x]):

- ☑ I have deactivated other plugins and confirmed this bug occurs when only Ultimate Member plugin is active.
- ☑ This bug happens with a default WordPress theme active, or UM Theme.
- ☑ I can reproduce this bug consistently using the steps above.

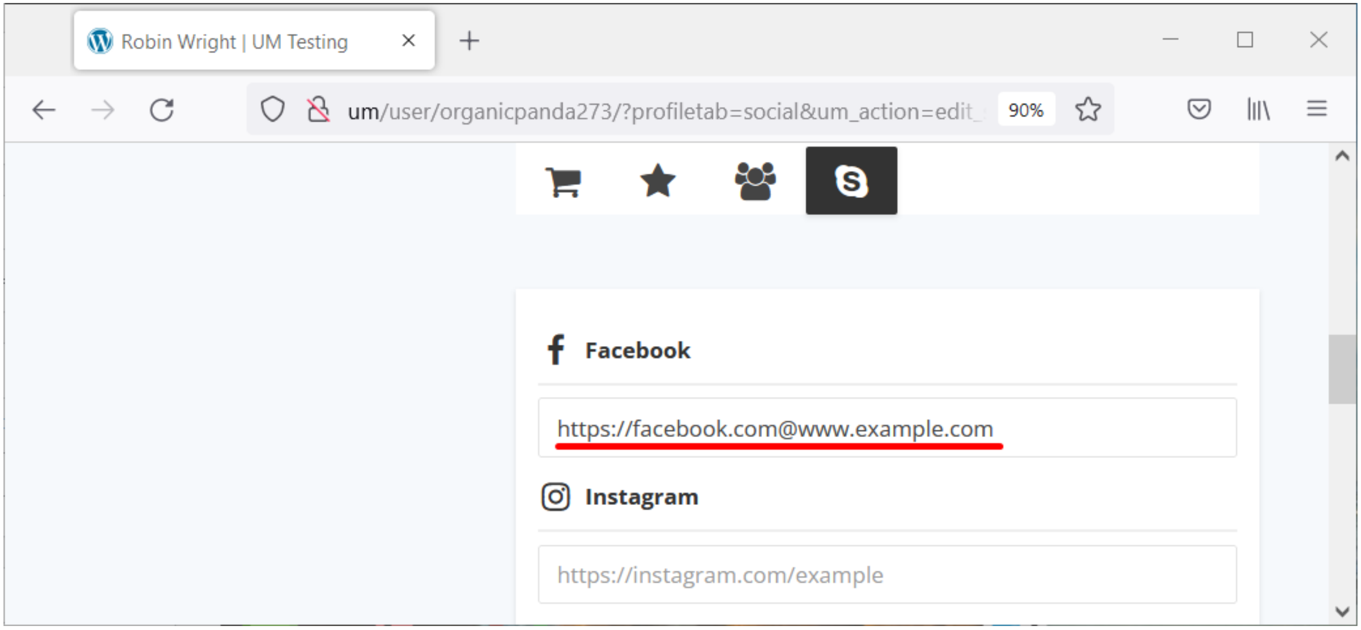
Describe the bug

1. URL redirection issue in some components. @ can be used to bypass the content detection of these components. For example enter a link https://facebook.com@www.example.com into the Facebook field. After updating the profile, the URL is redirected to http://www.example.com. Attackers can redirect these urls to their phishing sites.
2. Considering the domain of wordpress is http://www.example.com and there are two people: Alice and Bob. Alice is an attacker and Bob is a normal user. If the logout page is http://www.example.com/logout, Alice puts this URL into the "Website URL" component or puts https://facebook.com@www.example.com/logout into the "Facebook" component. Then when Bob clicks Alice's Website URL or Facebook link, he will turn to logout and log out the system. The operation of logging out may not cause security issues. However, if the operation is sensitive, it may cause serious security problems.

Expected behavior
Validate social links. Disallow the Logout URL.

Screenshots

Image 01 - Edit mode

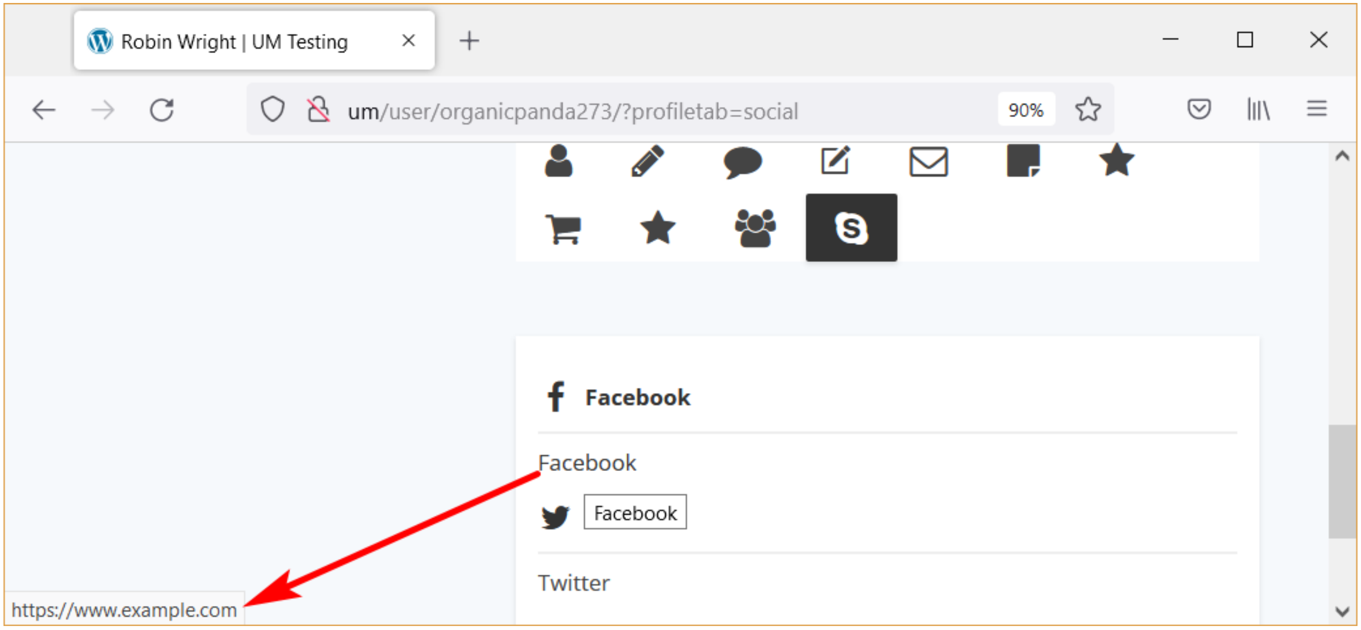


um/user/organicpanda273/?profiletab=social&um_action=edit_

https://facebook.com@www.example.com

https://instagram.com/example

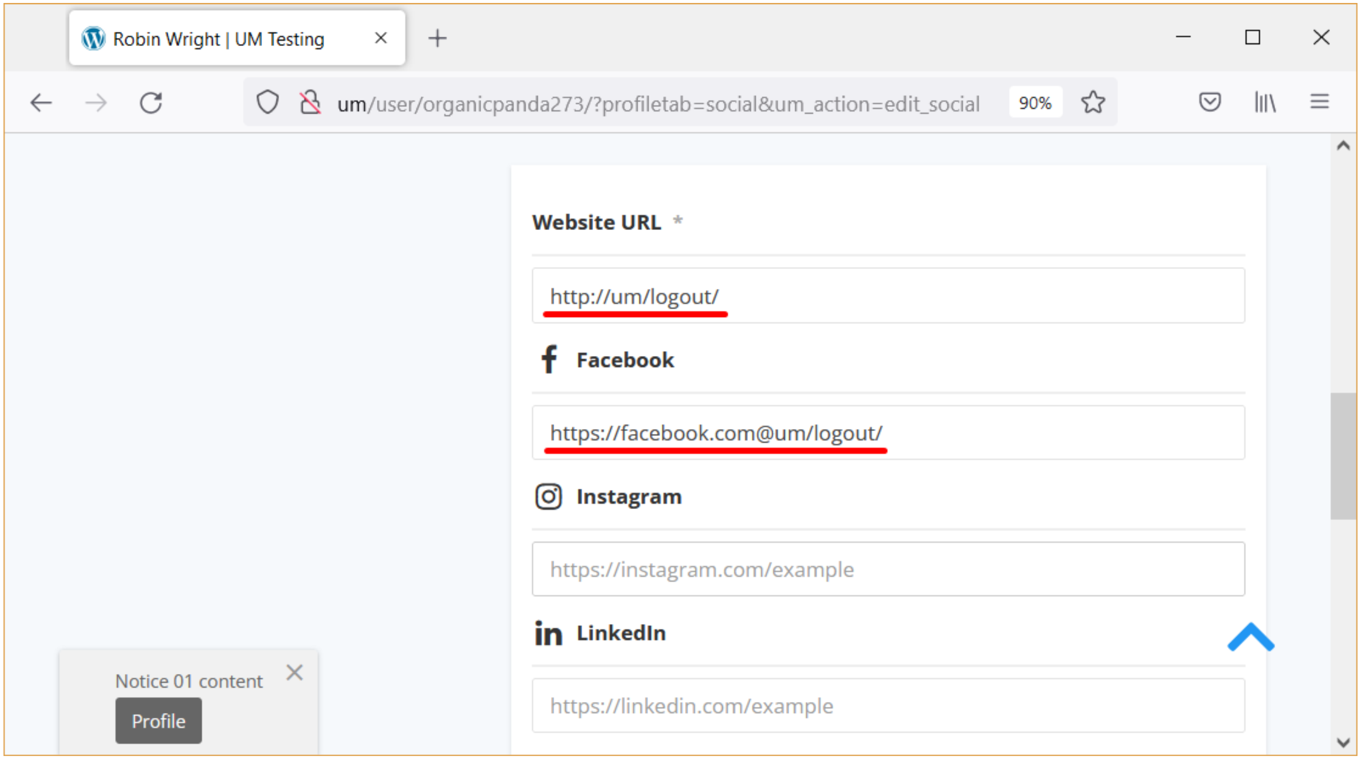
Image 02 - View mode



um/user/organicpanda273/?profiletab=social

https://www.example.com

Image 03 - Edit mode



um/user/organicpanda273/?profiletab=social&um_action=edit_social

Website URL *

http://um/logout/

Facebook

https://facebook.com@um/logout/

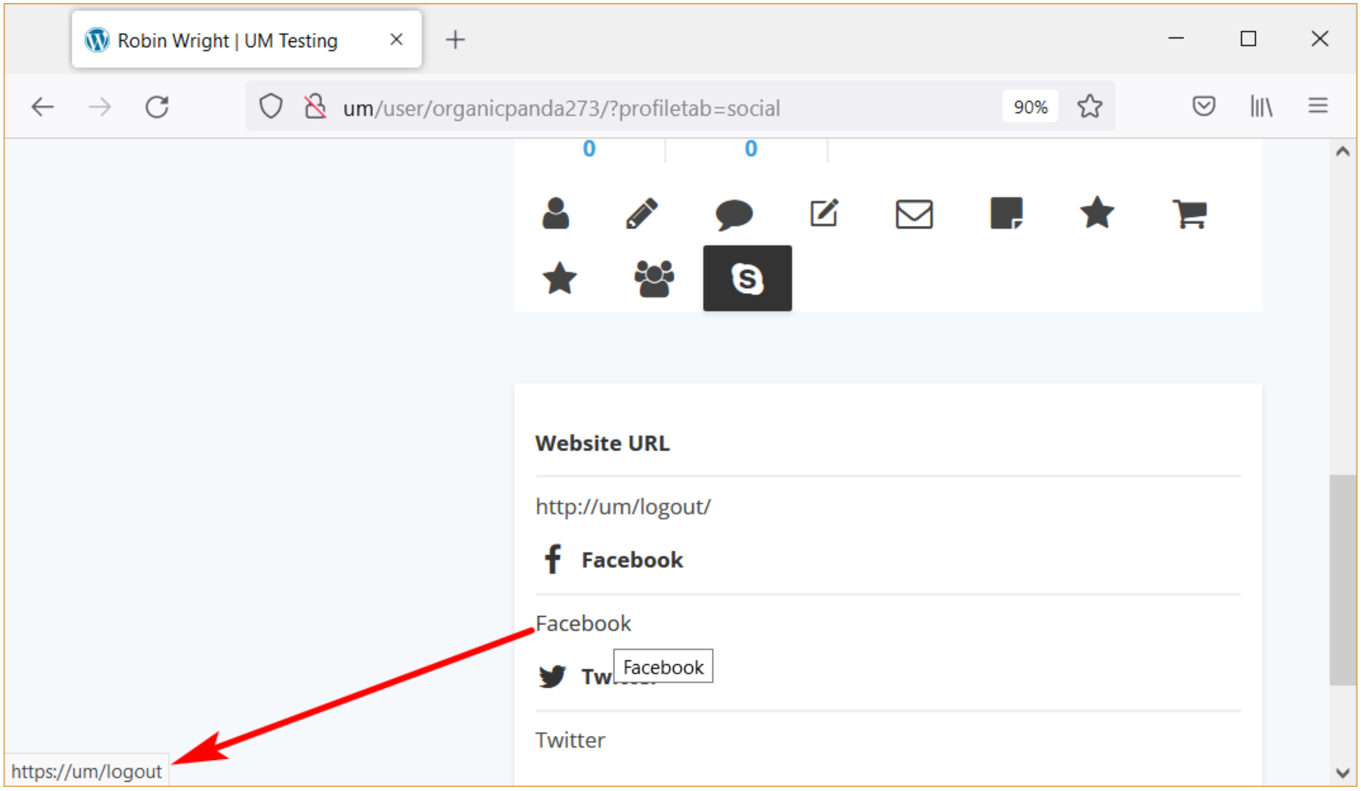
Instagram

https://instagram.com/example

LinkedIn

https://linkedin.com/example

Image 04 - View mode



um/user/organicpanda273/?profiletab=social

Website URL

http://um/logout/

Facebook

Facebook

Twitter

Twitter

https://um/logout

yuriinalivaiko self-assigned this on Apr 1

yuriinalivaiko linked a pull request on Apr 1 that will close this issue

Security issues in URL and social fields #990

Closed

Assignees

yuriinalivaiko

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Security issues in URL and social fields
ultimatemember/ultimatemember

1 participant