vulnerabilities / Ultimate Member <= 2.3.1 - Open Redirect.md

H4de5-7 Create Ultimate Member <= 2.3.1 - Open Redirect.md History

1 contributor

26 lines (13 sloc) | 1012 Bytes ···

Ultimate Member <= 2.3.1 - Open Redirect

Summery

Some URL components (Facebook, Twitter, LinkedIn, Instagram, YouTube, SoundCloud, VKontakte) in user profile exist open redirect vulnerability.

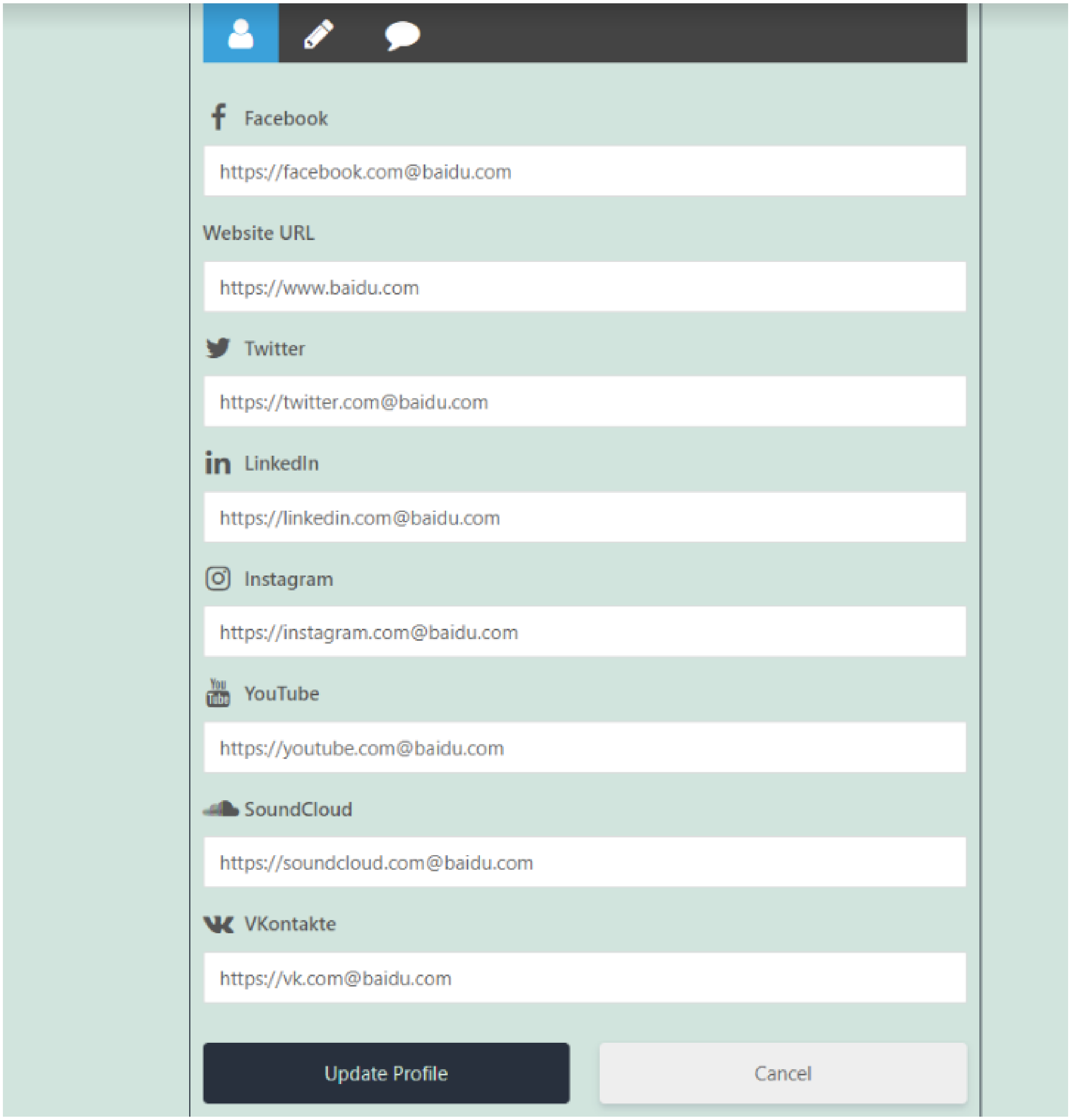
Vulnerability proof

'@' character can be used to bypass the host detection of some URL components.

1.Enter malicious URLs into the components.

For example:

Facebook component checks whether the URL redirects to https://facebook.com or not. Attackers construct malicious URL https://facebook.com@baidu.com and save it.



Facebook

https://facebook.com@baidu.com

Website URL

https://www.baidu.com

Twitter

https://twitter.com@baidu.com

LinkedIn

https://linkedin.com@baidu.com

Instagram

https://instagram.com@baidu.com

YouTube

https://youtube.com@baidu.com

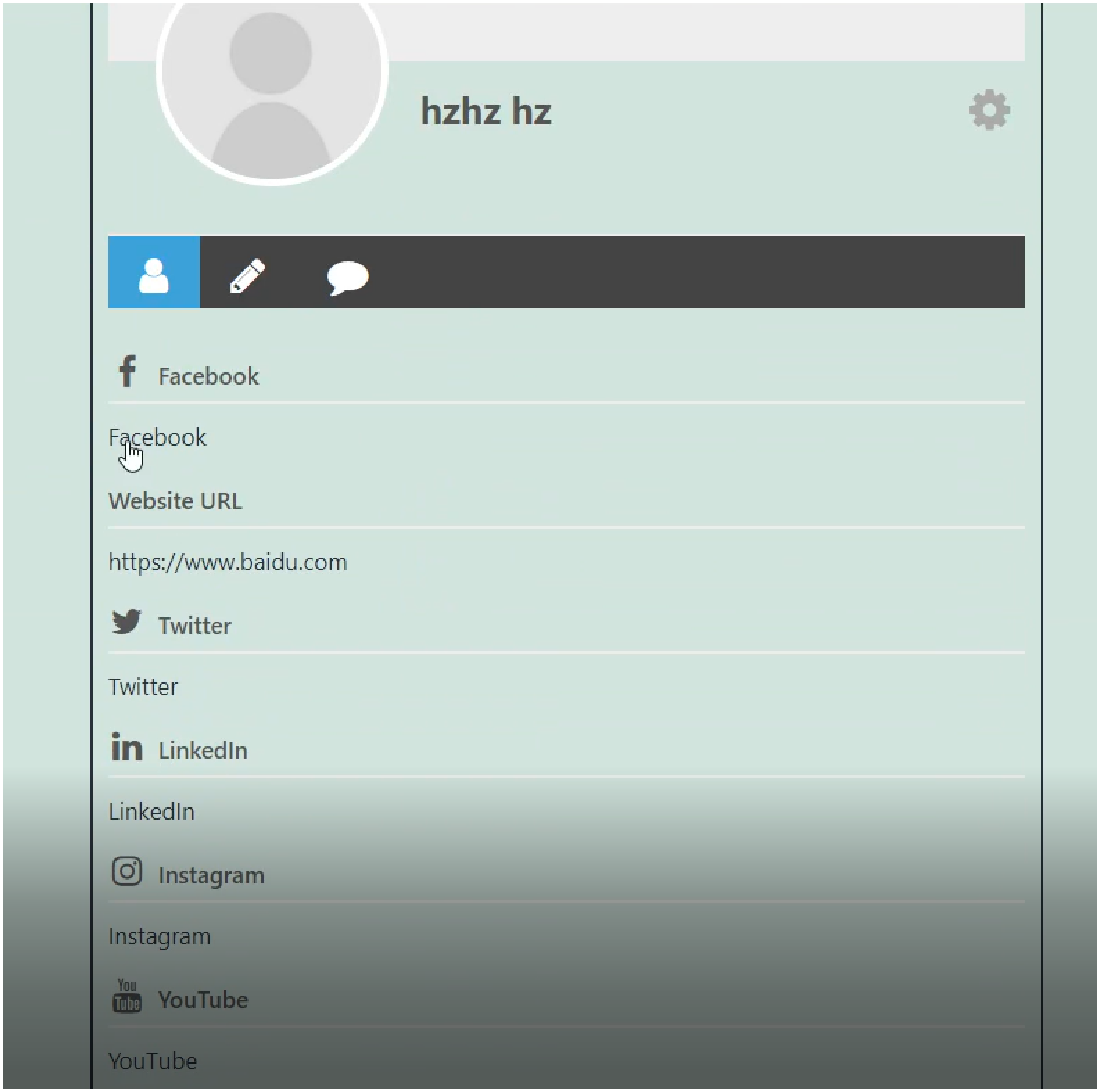
SoundCloud

https://soundcloud.com@baidu.com

VKontakte

https://vk.com@baidu.com

2.Reload the user profile and click "Facebook" component.



hzhz hz

Facebook

Facebook

Website URL

https://www.baidu.com

Twitter

Twitter

LinkedIn

LinkedIn

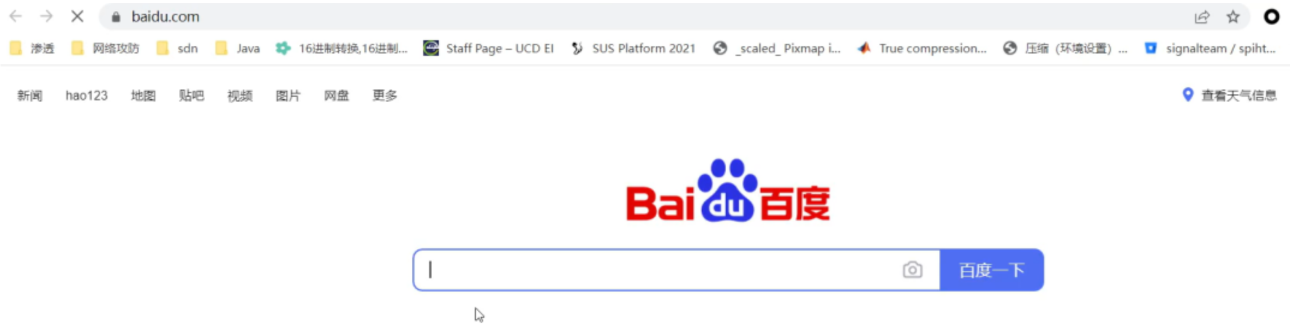
Instagram

Instagram

YouTube

YouTube

3.When people click the "Facebook" URL, website will redirects to https://baidu.com.



baidu.com