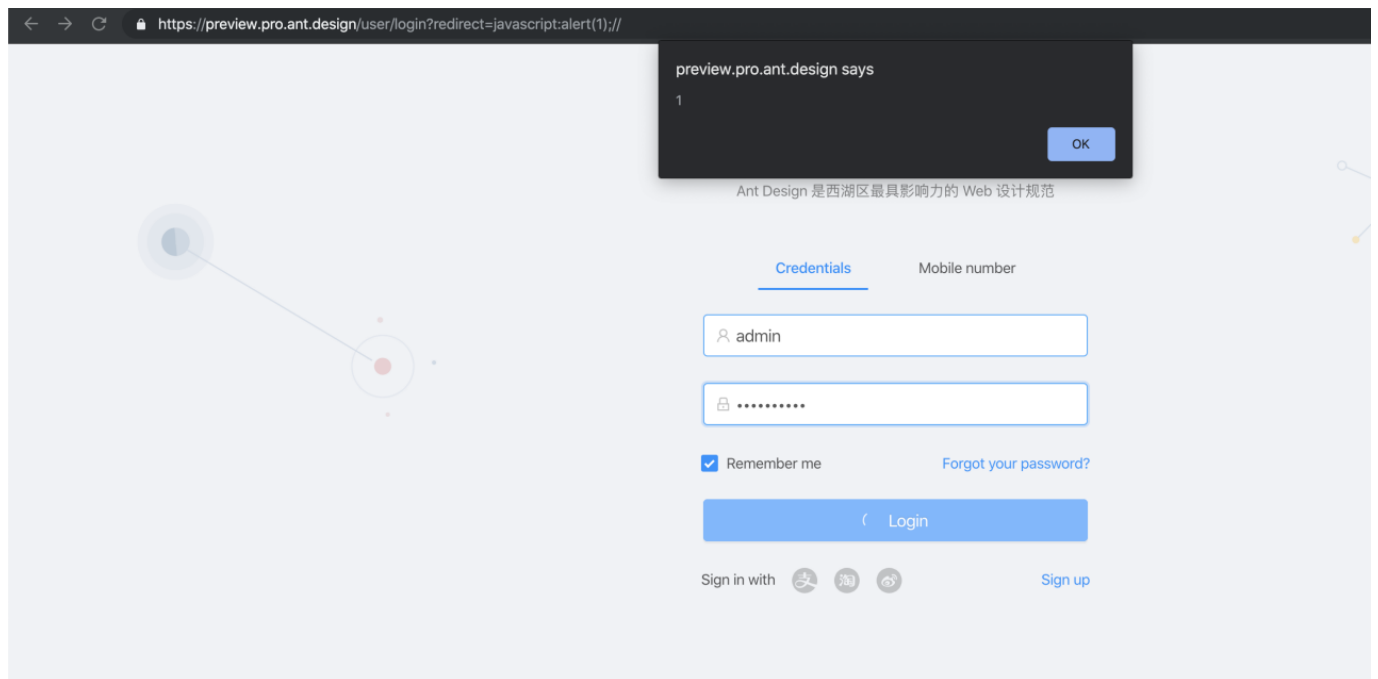




[Is This JavaScript Mailto Redirect Vulnerable To XSS](#)



[Is This JavaScript Mailto Redirect Vulnerable To XSS](#)



---

This is more injection than XSS, but Mailto links have a few features that you can abuse. For example, instead of the email program popping up .... x Fetch policies asynchronously for about: and javascript: URLs x Remove loop ... x [XSS] Removed host redirection chance on XSS-vulnerable pages (thanks ... x Fixed tab character in mailto: URLs triggering sanitization and all new line .... Any advice on dealing with redirections ("this link goes outside our site" ...  
<https://www.golemtechnologies.com/articles/prevent-xss#how-to-prevent-cross-> ... (It's best to have a whitelist of protocols that are accepted, e.g., http, https, and mailto.) ... In my project written in JavaScript I use this regex as white list:. The HTML page is vulnerable to DOM-based XSS if an attacker ... script>). Open redirect arises if the JavaScript code redirects to the ... with javascript: or mailto:.. CVE-2020-5528, Cross-site scripting vulnerability in Movable Type series (Movable ... HTML or JavaScript via a cross site scripting (XSS) vulnerability in the name of a ... This might, for example, be leveraged for HTML injection or URL redirection. ... CVE-2017-5078, Insufficient validation of untrusted input in Blink's mailto: .... In addition, we present a comprehensive survey of publicly documented XSS payloads which is ... prevent the execution of some payload types without eliminating the actual vulnerability. ... Separate execution-contexts of a JavaScript. +18 ... For example, the activation of mailto-URLs causes the opening of the composing.. The first cross-site scripting (XSS) vulnerability exists in the Plone login ... The server then responds with a 302 redirection containing the value taken ... the value starts to mailto: -- for example, setting the "came\_from" value to ... For example, attackers could set their home page value to "javascript:alert(1)". Do your applications use this vulnerable package? ...