

Forum:[Hack Forums](#)

Thread: [I have question about Cross Site Scripting](#)

Fisher - February 16, 2019, 2:40 am

Hello dear hackforum members.

I wanted to ask what I could do if I found this gap that then i enter this code in the search bar

Code `";alert(3)//--></SCRIPT>`

`<SCRIPT>alert("Hey");</SCRIPT>`

Code successfully executes and alert box pop up.

I'm thinking maybe somehow i can use this gap and get usernames;passwords of users.

Any ideas will be accepted. Thank you.

This is example how website url looks after execute search button

Code

`/index.php?do=search&subaction=search&search_start=0&full_search=&result_from=1&story="%3Balert(3)%2F%2F--><%2FSCRIPT>+<SCRIPT>alert("Hey")%3B<%2FSCRIPT>&dosearch=Search`

Abruptum - February 16, 2019, 7:14 am

(Feb 16, 2019 03:40 AM)Trojanisches Pferd Wrote: [\[CITE\]](#) Hello dear hackforum members.

I wanted to ask what I could do if I found this gap that then i enter this code in the search bar

Code `";alert(3)//--></SCRIPT>`

`<SCRIPT>alert("Hey");</SCRIPT>`

Code successfully executes and alert box pop up.

I'm thinking maybe somehow i can use this gap and get usernames;passwords of users.

Any ideas will be accepted. Thank you.

This is example how website url looks after execute search button

Code

`/index.php?do=search&subaction=search&search_start=0&full_search=&result_from=1&story="%3Balert(3)%2F%2F--><%2FSCRIPT>+<SCRIPT>alert("Hey")%3B<%2FSCRIPT>&dosearch=Search`

Most of the time xss-attacks are used to steal sessions and you then swap the password with your own after you applied the targets cookie on your script/browser.