

Forum:[Hack Forums](#)

Thread: [<NEW> Website Vulnerable! Hack it!](#)

Nolann - May 28, 2018, 1:31 pm

Not that anyone cares or anything, but this password recovery page has a vulnerability.

`http s :// bradford. focusschoolsoftware. com/fo cus/auth/index.php?action=recovery` (remove spaces in link!! I'm under 50 posts :c)

If you type

Code ">into the box, and press enter, you will close off the input section of the form, editing the page.

So yes, this is vulnerable. It has been for a while I'm assuming.

If anyone wants to try and hack it, and present the bug to the company "Focus" to gain some kind of bounty, then good luck!

I'd love to see progress posted here in the thread :)

BlindIntruder - June 12, 2018, 3:32 am

Very likely to be nothing more than a POTENTIAL XSS vector. You won't exploit directly the server with this.

DEEPSS - June 12, 2018, 5:00 pm

Hell you couldn't exploit it with sql, it is https most injection tools can't get past https

int - June 12, 2018, 5:28 pm

(Jun 12, 2018 05:00 PM)DEEPSS Wrote: [\[CITE\]](#) Hell you couldn't exploit it with sql, it is https most injection tools can't get past https

Stop spewing bs

the princess - June 12, 2018, 6:36 pm

Playing around with it, i can't seem to get it to run javascript.

`prnt.sc /ju9xbq`

Anybody have any ideas?

DEEPSS - June 12, 2018, 9:10 pm

(Jun 12, 2018 05:28 PM)Jukeboxhook Wrote: [\[CITE\]](#) Stop spewing bs

Dear script kiddie, when you learn about sql and it's protection vectors, come to the big boy table. Most sql tools except for 2 that's I know of can get past https, learn some shit kid. What are you 12?

the princess - June 13, 2018, 12:52 am

(Jun 12, 2018 09:10 PM)DEEPSS Wrote: [\[CITE\]](#) Dear script kiddie, when you learn about sql and it's protection vectors, come to the big boy table. Most sql tools except for 2 that's I know of can get past https, learn some shit kid. What are you 12?

LOL.

Dear script kiddie,

- 1) SQLI has nothing to do with the security of the connection (SSL)
- 2) It's SSL, not https
- 3) The vulnerability is XSS, not SQLI so it's irrelevant to even discuss it

int - June 13, 2018, 3:50 am

(Jun 12, 2018 09:10 PM)DEEPSS Wrote: [\[CITE\]](#) Dear script kiddie, when you learn about sql and it's protection vectors, come to the big boy table. Most sql tools except for 2 that's I know of can get past https, learn some shit kid. What are you 12?

Ok Mr Topp Mirai Rename 24k BotNet Owner

BlindIntruder - June 13, 2018, 11:56 pm

(Jun 12, 2018 05:00 PM)DEEPSS Wrote: [\[CITE\]](#) Hell you couldn't exploit it with sql, it is https most injection tools can't get past https

(Jun 12, 2018 09:10 PM)DEEPSS Wrote: [\[CITE\]](#) Dear script kiddie, when you learn about sql and it's protection vectors, come to the big boy table. Most sql tools except for 2 that's I know of can get past https, learn some shit kid. What are you 12?

A lot of LOLs have been given here.

7teen20nine - June 14, 2018, 2:57 am

Seems fun enough, the other comments are quite carcinogenic, I'll try my best, no promises tho :)

XXXTenacion - June 14, 2018, 3:53 am

Eh it's a school link so im not even touching that.