

Forum:[Hack Forums](#)

Thread: [How can I report a website vulnerability, by the vulnerability being I guessed the PW](#)

Ciroc - October 25, 2015, 3:31 pm

Hey guys,

Any ideas on how can I report a website vulnerability to the company, by the means of I guessed the admin password.

I have a couple hundred retail sites, which are admin:admin/1/123/etc

You can't really say "hey your sites vuln i guessed the password". I mean I'm trying to be legit and earn through bounties and generous feedback from companies.

Would it be worth just implementing an actual vulnerability in to the site? And then just reporting that specific vulnerability. Hey if they pay up I can always rinse and repeat.

Thanks in advance, any advice is appreciated.

Royal Crowd - October 25, 2015, 3:33 pm

"Would it be worth just implementing an actual vulnerability in to the site? And then just reporting that specific vulnerability. Hey if they pay up I can always rinse and repeat."

It is pretty BlackHat, but you could probably make some profit ;)

You could even possibly "find" a few vulns, no?

Have a nice day! ?

Possession - October 25, 2015, 4:02 pm

If its shopping website get hold of database it might contains data which could generate you income.

Ciroc - October 25, 2015, 5:14 pm

(Oct 25, 2015 03:33 PM)Authix Wrote: [\[CITE\]](#) "Would it be worth just implementing an actual vulnerability in to the site? And then just reporting that specific vulnerability. Hey if they pay up I can always rinse and repeat."

It is pretty BlackHat, but you could probably make some profit ;)

You could even possibly "find" a few vulns, no?

Have a nice day! ?

I've had a look on a few of the sites and I haven't found any vulnerabilities that the Company would deem severe, e.g (slqi/csrf/etc)

I'm not going to bother looking for something mild on each e.g cross site scripting, as no one even bothers to reply to my disclosures when I do so.

(Oct 25, 2015 04:02 PM)Possession Wrote: [\[CITE\]](#) If its shopping website get hold of database it might contains data which could generate you income.

I have done so on quite a few of the sites, I've shelled too and it's been un-noticed. I have, on estimate from 1 site 10k> "things that could be sold"

But that's not my game any more, I'm more in to helping Company's and hoping for a kind gesture back from them. However I don't want to contradict myself, I will reap once I see a reward in sight. But I'm not in the 'deep' I guess, line of hacking/fraud any more.

Thanks for the replies :)

Viktory - October 26, 2015, 3:00 am

what makes you think weak passwords are not a serious vulnerability? it's like putting all your cash in a safe with a toothpick as a key.

many a big corps have had their dbs leaked over some sysadmin reusing same weak passwords.

besides, I doubt you're gonna get a reply at all. no company worth their salt has "admin" as a password...

Sharkky - October 26, 2015, 6:26 am

(Oct 26, 2015 03:00 AM)Viktory Wrote: [\[CITE\]](#) no company worth their salt has "admin" as a password...

Honestly, you'd be surprised.

Glubz - October 26, 2015, 7:09 am

Contact them via their admin email (www.who.is) and see what they say.

qExecute - October 26, 2015, 1:07 pm

My school had the the district number as password for website, grades and just about everything else

limainfinita - October 26, 2015, 5:03 pm

just send them a email saying

"hey i guessed your password, please change it and make it better, more dificult/impossible to guess and hey if you dont mind a donation would be apreciated"

bascily you guessed the pass
and now you want to report it
but you also want to earn something like everybody does

the correct way to do it is that

other than that you are making "not-the-good-choice choices"

but it is your call so.. good luck

(Oct 26, 2015 03:00 AM)Viktory Wrote: [\[CITE\]](#) what makes you think weak passwords are not a serious vulnerability? it's like putting all your cash in a safe with a toothpick as a key.

many a big corps have had their dbs leaked over some sysadmin reusing same weak passwords.

besides, I doubt you're gonna get a reply at all. no company worth their salt has "admin" as a password...

agree