

Forum:[Hack Forums](#)

Thread: [Question about defacing a web site!](#)

BeggFoMercy - December 9, 2011, 8:00 am

Hi guys.!

I have been trying to deface a web site for 5 days :S

i have SQLI more than 133 site all i get is the admin id and pw but cant find admin link to login

or when i find the login link the pw would be a md5 and doesnt get decyrpted on any sites.w.e leme get this to deface a web site i have to find the admin user,pw and admin login link and after accessing the cp

then upload a shell and edit the index.html

and put my defaced code in and save and thats it right ? if im saying some thing wrong warn me please and thanks !

bckslsh - December 9, 2011, 8:12 am

Uhm, to deface a site you don't HAVE to be a dick and edit the index, but you can. Or you can just upload your deface. This is all you would need to do, unless it has read only privileges or something, then you would need to go deeper.

If your MD5 doesn't get decrypted, try this.

1. After trying all usual sites, try hashchecker.de, it will test it on like 40 sites.
2. If that still fails, google the hash. You might find it come up in a request thread on some forums, or in an MD5 database.
3. Crack manually.

And you don't have to find the admin user/password. There are ways of using loadfile to find out info about the OS, and other sensitive data. Though this can get advanced.

<http://kaoticcreations.blogspot.com/2011/08/sql-injection-how-to-use-load-file-into.html>

And here are a couple of tips to find the login -

1. Run it through a couple different admin page finders, like the built in one on Havij, or a script. (adminfinder.pl - <http://pastebin.com/0AAMFUVD>)
2. Use dorks. like site:site.com inurl:admin OR control OR cms etc.
3. Check if the login works with the cpanel/ftp, normally it wont, but you may get lucky. For cpanel - site.com/cpanel - site.com/kpanel - site.com:2082. For ftp, just put the site as a host in an FTP client such as filezilla or cufteft. Most browsers have built in ftp support, too.

Good luck ;)

BeggFoMercy - December 9, 2011, 8:22 am

(Dec 9, 2011 09:12 AM)?Dan Wrote: [\[CITE\]](#) Uhm, to deface a site you don't HAVE to be a dick and edit the index, but you can. Or you can just upload your deface. This is all you would need to do, unless it has read only privileges or something, then you would need to go deeper.

If your MD5 doesn't get decrypted, try this.

1. After trying all usual sites, try hashchecker.de, it will test it on like 40 sites.
2. If that still fails, google the hash. You might find it come up in a request thread on some forums, or in an MD5 database.
3. Crack manually.

And you don't have to find the admin user/password. There are ways of using loadfile to find out info about the OS, and other sensitive data. Though this can get advanced.

<http://kaoticcreations.blogspot.com/2011/08/sql-injection-how-to-use-load-file-into.html>

And here are a couple of tips to find the login -

1. Run it through a couple different admin page finders, like the built in one on Havij, or a script. (adminfinder.pl - <http://pastebin.com/0AAMFUVD>)
2. Use dorks. like site:site.com inurl:admin OR control OR cms etc.
3. Check if the login works with the cpanel/ftp, normally it wont, but you may get lucky. For cpanel - site.com/cpanel - site.com/kpanel - site.com:2082. For ftp, just put the site as a host in an FTP client such as filezilla or cufteft. Most browsers have built in ftp support, too.

Good luck ;)

Lol okai ill try what u said wish me luck i didnt think that its that hard w.e Thanks bro!