LinHES - Bug # 406: Password change fails for many characters

Status:	Closed	**Priority:**	Normal
Author:	alien	**Category:**	
Created:	06/21/2009	**Assignee:**	jams
Updated:	12/25/2011	**Due date:**	12/31/1969

Description:

Passwords with @, $, *, (or) do not work when set from the menus.

This happens for userIDs on setup and on the web interface password. I almost was locked out of root when I first did this but then discovered I can sudo password from another userID. I except not everyone will think of this recovery.

I almost made this critical because it appears that the passwords are being executed by the shell in certain circumstances. See the last example below where I caused a "ls -l /home" to be executed. The following: <code>"x;sudo rm -rf /</code>would be really *really* bad.

Examples (from running mythinstall -s webuser from the command line):

Password: x$$x
Result: adding webUSERNAME mythtv with pass x20767x

Password: *x*
Result: adding webUSERNAME mythtv with pass appletrailer.xml

Password: x(x)
Result: sh: -c: line 0: syntax error near unexpected token `('
sh: -c: line 0: `sudo myth_user_call -c web -umythtv -p x*x('

Password: x;ls -al /home
Result:
<code>Running program to make the changes for web password
adding webUSERNAME mythtv with pass x
total 16
drwxr-xr-x 4 root root 4096 2009-06-20 11:48 .
drwxr-xr-x 22 root root 4096 2009-06-20 17:08 ..
drwx------ 5 allen allen 4096 2009-06-21 09:04 allen
drwxr-xr-x 6 mythtv mythtv 4096 2009-06-21 09:13 mythtv
i should save my settings(2)
Europe/Berlin
c save
t syssettings
template is syssettings
d localhost
0
[mythtv@violet home]$ </code>

History

06/21/2009 05:46 am - alien

Just to add to this. Adding various quotes to the script probably won't help. There is always risk that the user will accidentally close the quotes in their password. I'm not sure it is possible to write a safe password changing program that uses a script or makes any shell calls to commands like htpasswd.

I just checked and lighttpd doesn't do PAM authentication, so we can't use that to get around the problem.

07/05/2009 04:10 pm - jams

Special character check is now enforced or escaped out.

A person would now need to try a bit harder to erase thier harddrive with the web security module.

Although anybody using ;rm -rf / as a password needs to have their head examined.

12/25/2011 03:10 pm - jams

- Target version changed from 8.0 to 6.00.04