i censored/took a lot of shit so you don't own my school too easily :D
I gave a more explicit copy to my comp teacher at school...

Security on the MPS Webserver (ftp.milwaukee.k12.wi.us)

Problems:
-PHF cgi is exploitable
/usr/local/bin/ph -m alias=x/bin/cat /etc/shadow

After I had the unshadowed passwd file i could run it through programs that encrypt words and compare them to the encrypted words in the file.

-The passwords are badly picked
Examples:
login: mps
password: ###
login: grants
password: ###
login: project_stay
password: ###

All of those are VERY easily guessed. To get those passwords we ran the "passwd" file throuhg a password cracking program. Here are all of them that we've found:

mps ###
project_stay ###
grants ###
washington ###
kuryladj ###

We also found to accounts where the password was "abc123" but the computer crashed before it printed the login.

I've decided to stop working on the system and give my information to you so it can be fixed. If someone with more malicious intents worked on the MPS server they could have gotten root easily (with a few hours/days trying to decrypt the password. I am guessing that the pass for root is more secure). Then they would have the power to modify/delete files on the server.