emilhem / July 17, 2011 10:45PM
Encrypt password
Please move this topic if it is in the wrong area!

Today I tried to see if I could capture my password in Wireshark when I logged into Phorum and SMF.
Phorum sends the password in clear text! SMF sends the password "encrypted".
Could this feature be added to Phorum?

Maurice Makaay / July 18, 2011 07:11AM
Re: Encrypt password
Why is "encrypted" in quotes here? Is the SMF transport encryption not encryption but something like a basic operation like base64 or so? If yes, then adding that would not provide extra protection. It is just some obfuscation, easily circumvented by an interested hacker.

For real encryption, the system would have to implement a public / private key encryption algorithm. The browser would have to encrypt the password using the public key. The server could decrypt it using the private key. One big drawback of this, is that this implies that the browser should be able to run some code to handle the encryption. You have no guarantee that all browsers that visit your site would be able to make use of this. For example when using javascript for encryption, the encryption would not work for browsers that have javascript blocked or even not implemented at all.

But let's imagine that we'd have some sort of password encryption in place and a user tries to login. The browser would encrypt the password and post that one to the server. Guess what: in plain text! As a hacker I am not directly interested in the exact password. As long as a can grab some bit of data that I can replay, I'm good. I could snif and grab the plain text encrypted password and forge a new request which sends the same encrypted password. The server would not see the difference and happily let me in. This is a flaw that I have seen in quite a few projects. Encryption is useful for making sure that the original contents of a piece of data are not readable. It does not protect against password sniffing.

To really protect the password, other mechanisms need to be in place too. One would have to make sure that there has been no tampering with the data that has been sent to the server and that it is not data that is being replayed. While it should be perfectly possible to completely implement these layers of protection in lets say javascript, things would get quite complicated.

Luckily these is a perfect solution for all issues that we have here. SSL can take care of protecting the data streams to and from your server. If you need to protect transported passwords, then consider getting your site to run als [yoursite.com]. That fully protects the transported passwords.

If you're still interested in "encryption": yes, I think it could be added to Phorum and that it would be possible to fully handle that from a module. It would add some javascript to the login page to handle the obfuscation before posting the form and something like the page_login hook to de-obfuscate the data.

Maurice Makaay
Phorum Development Team
my blog linkedin profile secret sauce

---

emilhem / July 18, 2011 10:43AM
Re: Encrypt password
With "encrypted" I meant that it's JavaScript and a hacker could possibly look into the JavaScript code to reverse the encryption. At least the password isn't clear text.

Now this becomes like a support thread...

Can I make the login pages to SSL while the rest of the forum not SSL?

Maurice Makaay / July 18, 2011 12:55PM

Re: Encrypt password

My point is that if the password is readable on the wire (and somebody has taken the effort to get to that data), then just scambling the data, based on some reversable algorithm, is not useful in terms of protection. Put differently: reversable scrambling equals plain text.

Making only the login page use SSL is definitely possible. But why? As a hacker, I can then grab your cookie from the http request and take over your session. When you're going SSL, then go SSL all the way or you'll most likely break the security scheme.

Maurice Makaay
Phorum Development Team
my blog linkedin profile secret sauce
