

# Re: Proposal for Lite Encryption for Login Form without SSL

---

*Source:* <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2007-10/msg00132.html>

---

- *From:* Jerry Stuckle <[jstucklex@xxxxxxxxxxxxxx](mailto:jstucklex@xxxxxxxxxxxxxx)>
  - *Date:* Tue, 02 Oct 2007 06:33:36 -0400
- 

klenwell wrote:

On Oct 1, 6:38 pm, Jerry Stuckle <[jstuck...@xxxxxxxxxxxxxx](mailto:jstuck...@xxxxxxxxxxxxxx)> wrote:

klenwell wrote:

On Oct 1, 2:40 am, "C. (<http://symcbean.blogspot.com/>)" <[colin.mckin...@xxxxxxxxxx](mailto:colin.mckin...@xxxxxxxxxx)> wrote:

On 1 Oct, 06:04, klenwell <[klenw...@xxxxxxxxxx](mailto:klenw...@xxxxxxxxxx)> wrote:

On Sep 30, 9:08 pm, Jerry Stuckle <[jstuck...@xxxxxxxxxxxxxx](mailto:jstuck...@xxxxxxxxxxxxxx)> wrote:

klenwell wrote:

Another request for comments here. I'd like to accomplish something like the scheme outlined at this page here:

Re: Proposal for Lite Encryption for Login Form without SSL

<http://tinyurl.com/3dtcdr>

In  
a  
nutshell,  
the  
form  
uses  
javascript  
to  
hash  
(md5)  
the  
password  
field  
using  
a  
random  
one-time  
salt  
(nonce)  
--  
generated  
by  
php  
and  
pasted  
in  
the  
form  
--  
that  
is  
then  
posted  
with  
the  
hashed  
password  
back  
to  
the  
server.  
This  
way  
the  
password  
is  
not  
sent  
to  
the

Re: Proposal for Lite Encryption for Login Form without SSL

server  
in  
plaintext.  
In  
the  
example  
cited  
above,  
however,  
the  
password  
is  
stored  
unhashed  
back  
at  
the  
server  
(i.e.,  
in  
the  
database)  
and  
it's  
this  
problem  
that's  
been  
tying  
me  
in  
knots  
this  
evening.  
The  
most  
obvious  
way  
it  
seems  
to  
me  
to  
cut  
through  
the  
knot  
is  
to  
simply  
copy

Re: Proposal for Lite Encryption for Login Form without SSL

the  
server-side  
salt  
(sss)  
used  
to  
hash  
the  
pw  
in  
the  
database  
--  
the  
salt  
is  
constant  
--  
within  
the  
javascript  
portion  
of  
the  
form  
so  
that  
that  
client  
would:  
1.  
ssspw  
=  
md5(sss  
+  
pw)  
2.  
nssspw  
=  
md5(nonce  
+  
ssspw)  
3.  
post  
(1)  
nssspw,  
(2)  
nonce,  
(3)  
username  
(in

Re: Proposal for Lite Encryption for Login Form without SSL

plaintext)  
Then  
on  
the  
server  
side,  
php  
would:  
1.  
db\_ldap  
=  
fetch  
hashed  
password  
f