This tutorial is for "warleyalex's Delphi for PHP crackme"
Written by *zart*

Tools used: Firebug

Project: Delphi for PHP crackme

Protection in EXE: NONE
This crackme was based on Delphi for PHP project.
PHP is a server-side application script. In this project, i used several languages: php, javascript, html and delphi to compile the crackme.

Imagine you need a valid username and password to enter in that dreamed porn site, but it restricted. My crackme tries to simulate something like this.

Difficulty: 2 - Needs a little brain (or luck)
Platform: Windows
Language: Borland Delphi

Ok what I first did was fire up the olly and search for some strings… I figured it was made in Delphi – how hard could it be? After running it once in Olly you could see it was dumping something call "site.html" to C:\windows\. So I grabbed this and ditched olly and the crackme for right now. It didn't appear that the crackme did much other than dump and shell this file.

Anyway, if you open up the site.html in firefox it presents you with a login. Tried something random – DOH! It's blocking me :\

What do you do? Check out the source, argghhh! Firefox just died because there is so much junk on one line! Ok so I loaded it in notepad and check it out. It's javascript with two huge variables. One is double is actually information and the other is a few function calls that have been escaped twice.

I started to look at the escaped code by dumping it into another file, and doing:

Document.write(unescape(unescape(escaped data here)));

This dumped out what the function was… Nothing about the password in here though – so it must be creating another function that actually checks it.

Anyway – I figured I was making this out to be too hard – use the tools I have! So I fired up firebug (javascript debugger for firefox) and loaded the page.

This shows us that the login form is calling Input(); - now we just need to look for that javascript function! Success we found it!

```
function input()
{pd=document.passwordform.password.value.toUpperCase();
ur=document.passwordform.username.value.toUpperCase();
if
((ur!=ur)||((ur==unescape("%53%45%54%45%4C%41%47%4F%41%53"))&&(
pd==unescape("%47%41%4C%4F")))) {
document.cookie="HTMLPasswordUserID="+ur;document.cookie="HTMLPass
wordPassWD="+pd;passwdok();
}
else
{
alert("Useraccount: "+ur+ " error !");
return false;
};
};
```

Note: This was jumbled on one line, so I added some enters to make it readable.

Ok so what this is doing, is it grabs the username and password we passed to the form and checks it. It takes whatever we get and turns it to uppercase. Next it compares username to: unescape("%53%45%54%45%4C%41%47%4F%41%53") and password to unescape("%47%41%4C%4F").

Drop those into another file and change them to;

```
Document.write(unescape("%53%45%54%45%4C%41%47%4F%41%53"));
Document.write(unescape("%47%41%4C%4F"));
```

Presto! There are the username and password we need;

Username: SETELAGOAS
Password: GALO

Enter this in the page and see the goodboy message! See it was easier than we thought!

> **Congratulations, Dr.Osama challenge was defeated!**
>
> Send me how come you break my security, besides the password and username at warleyalex@yahoo.com.br

Hope you enjoyed this, sorry for the bad English;

+zart

greets to zand and sunbeam @ cheatengine forums