Subject: Re: Safe web authentication
Posted by dolik.rce on Sun, 22 Feb 2015 11:05:35 GMT
View Forum Message <> Reply to Message

mirek wrote on Sun, 22 February 2015 11:20First things first: It would be nice to have google login integrated with this (possible even others, but google is essential).
It should not be hard to add option to login using Google, Facebook or other service. I guess most of them use oauth, right?

mirek wrote on Sun, 22 February 2015 11:20As for safety, I guess 'standard' is to send salt (random string) from server (server remembers it), append password to this salt in client and send back hash of whole (I am afraid that means using javascript and having some safe has library available - I guess SHA1 is not considered safe anymore, so perhaps first step is to find some nice new hash, perhaps SHA256, add it to Core, find javascript library...)

It is not a problem to implement pretty much anything in javascript (e.g.: I saw an RSA implementation just yesterday :) ). The real problem with this approach is that it means the password is stored on the server in plaintext. It could be hashed, but that solves only part of the problem (the case when your database is compromised).

I'd prefer to use an approach where server doesn't know the password at all. As far as I know, the only way to do this is using asymmetric cryptography, where server has only public key of the client and the private key never leaves the clients computer.

Honza