Subject: Security upgrades need on API
Posted by mctrivia on Fri, 14 Oct 2011 15:21:21 GMT
View Forum Message <> Reply to Message

I need a way to access any shop through the API without the shops password but only if shops have given me access.

Ideal method: you have a api page where users can check what api's are allowed to access there account. Then I can log in to any account that has checked it using my username and password. Also each API should be restricted in what they can do. I would tell you what I need access to, you would list this on the API access page in bold so people can chose to give access to that or not.

Less ideal but easier to implement. Provide each shop with a 64byte api password. I can sha1 there password with my api code(not my password) and store this in my database and log on using my username and the combined password. In this way if I get hacked the password is only good until my api code is changed, there is no way to get the users api code and they can invalidate my access by changing theres, or if I am found to be unreliable you can shut my access off by deleting mine.

The current method opens up a lot of security risks. I need to store real passwords which means if someone hacks me they have full access to peoples accounts.