Suspension process – Moodle

Goals

- Protect the Moodle system from the brute force attack on password
    - The versions of Moodle that don't have this fix are exposed to those kinds of attacks.
        - Moodle check if you failed to login 10 times (value hard coded). If that is the case you need to close your browser to be able to try to login again.
        - In that case it's pretty easy to try breaking a password because there is no limit of attempt.

Solution

- Create a table named login_attempt
    - Log each login attempt (Success or failure)
    - Log IP, agent and the timestamp of the attempt
- Creation of a class login_attempt that manage the process
    - Login status code
        - Status of each login attempt
            - LOGIN_SUCCESS
            - LOGIN_FAILED
        - One new suspension status
            - SUSPENDED_TOO_MANY_ATTEMPT
        - A user that got suspended with the code SUSPENDED_TOO_MANY_ATTEMPT got 3 ways to get unsuspended
            - Login process (UNSUSPENDED_LOGIN_PROCESS)
                - The login process will check if the timeout is reach, if that is the case the user will be able to login again
            - An admin action (UNSUSPENDED_ADMIN)
                - An admin can use the interface for managing user to unsuspended an account
            - cron.php (UNSUSPENDED_CRON)
                - Each time the cron.php will run he will check if there is account that got the status SUSPENDED_TOO_MANY_ATTEMPT and have reach the timeout (suspensiontimeout), if that is the case the account will be unsuspended.
    - Methods :
        - log($loginstatus)
        - get_nb_failed($user)

        - is_suspended_too_many_attempt()
        - static get_all_suspended_too_many_attempt_timeout_reach()
        - is_timeout_reach()
- Modifications of the function authenticate_user_login (lib/moodlelib.php) to use the new login_attempt class
- Modifications of the function update_login_count (lib/moodlelib.php) to use the new login_attempt_class
- Destruction of the function reset_login_count (lib/moodlelib.php) (no use at all)
- Creation of 3 new configuration settings
    - maxfailedloginattempt : After that number of failed login attempts, the account will be suspended for a period specify by the parameter Timeout of suspension.
        - Site administration/Plugins/Authentication/Manage authentication
    - suspensiontimeout : Timeout of suspension for an account that failed to login successfully for a number time greater than Maximum number of failed login attempt.
        - Site administration/Plugins/Authentication/Manage authentication
    - loginattemptlifetime : This specifies the length of time you want to keep the status of the login attempts. Logs that are older than this age are automatically deleted. It is best to keep logs as long as possible, in case you need them, but if you have a very busy server and are experiencing performance problems, then you may want to lower the login attempt status lifetime.
        - Site administration/Server/Cleanup
- Email is send to user when is account suspended because he failed too many time to login
- Email is send to user when is account got unsuspended and that is status was SUSPENDED_TOO_MANY_ATTEMPT

Messages

File : auth.php

$string['maxfailedloginattempt'] = 'Maximum number of failed login attempt';

$string['maxfailedloginattemptdesc'] = 'After that number of failed login attempts, the account will be suspended for a period specifify by the parameter Timeout of suspension.';

$string['minutes'] = 'minutes';

$string['suspensiontimeout'] = 'Timeout of suspension';

$string['suspensiontimeoutdesc'] = 'Timeout of suspension for an account that failed to login succesfully for a number time greater than Maximum number of failed login attempt.';

File : admin.php

$string['configloginattemptlifetime'] = 'This specifies the length of time you want to keep the status of the login attempts. Logs that are older than this age are automatically deleted. It is best to keep logs as long as possible, in case you need them, but if you have a very busy server and are experiencing performance problems, then you may want to lower the login attempt status lifetime.';

$string['configloglifetime'] = 'This specifies the length of time you want to keep logs about user activity. Logs that are older than this age are automatically deleted. It is best to keep logs as long as possible, in case you need them, but if you have a very busy server and are experiencing performance problems, then you may want to lower the log lifetime. Values lower than 30 are not recommended because statistics may not work properly.';

$string['loginattemptlifetime'] = 'Keep status of login attempts for';

File : moodle.php

$string['errortoomanylogins'] = 'Sorry, your account is suspended because you have exceeded the allowed number of login attempts. You will be unsuspended in {$a->minutes} minutes.';

$string['neverdeleteloginattempt'] = 'Never delete status of login attempts';

$string['suspendedtomanyattemptsubj'] = 'Suspension of your account';

$string['suspendedtomanyattempttext'] = 'Hi {$a->firstname},

Your account at \'{$a->sitename}\' has been suspended because you have

exceeded the allowed number of login attempts. You will be unsuspended in

{$a->minutes} minutes.

In most mail programs, this should appear as a blue link

which you can just click on. If that doesn\'t work,

then cut and paste the address into the address

line at the top of your web browser window.

Cheers from the \'{$a->sitename}\' administrator,

{$a->signoff}';

$string['unsuspendedtomanyattemptsubj'] = 'Unsuspention of your account';

$string['unsuspendedtomanyattempttext'] = 'Hi {$a->firstname},

Your account at \'{$a->sitename}\' has been unsuspended.

To try to login again, please use this link :

  {$a->link}

In most mail programs, this should appear as a blue link

which you can just click on. If that doesn\'t work,

then cut and paste the address into the address

line at the top of your web browser window.

Cheers from the \'{$a->sitename}\' administrator,

{$a->signoff}';

Example of email

Suspension

Subject: Your Moodle: Suspension of your account

Hi Luke Skywalker,

Your account at 'Your Moodle' has been suspended because you have
exceeded the allowed number of login attempts. You will be unsuspended in
5 minutes.

In most mail programs, this should appear as a blue link
which you can just click on. If that doesn't work,
then cut and paste the address into the address
line at the top of your web browser window.

Cheers from the 'Your Moodle' administrator,

Support
support-your-moodle@yourschool.com

Unsuspension

Subject: Your Moodle: Unsuspension of your account

Hi Like Skywalker,

Your account at 'Your Moodle' has been unsuspended.

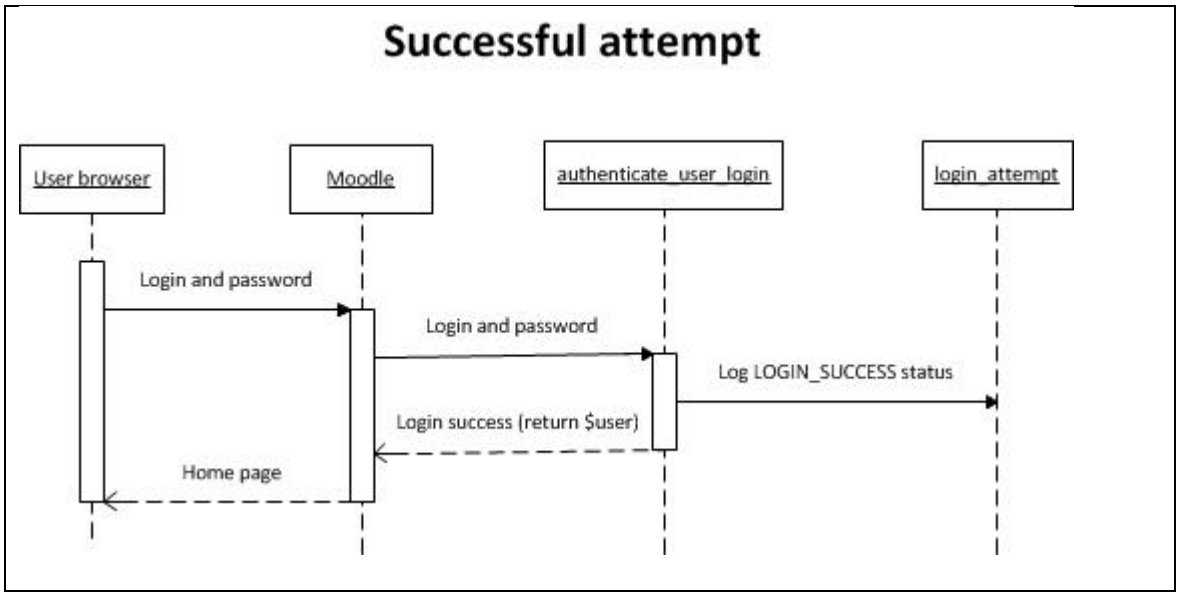
To try to login again, please use this link :
https://yourmoodle.yourschool.com/login/

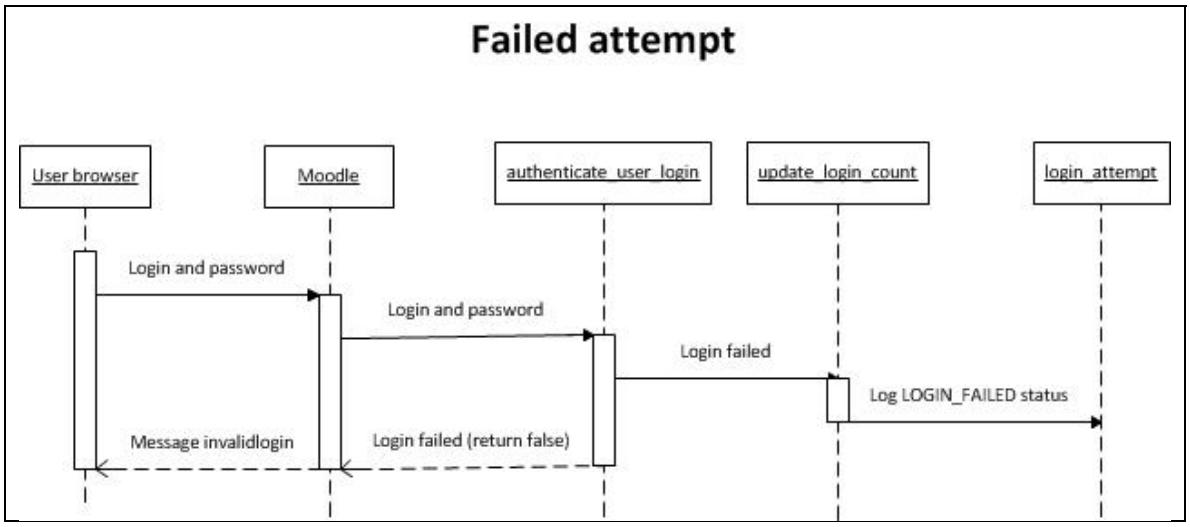
In most mail programs, this should appear as a blue link
which you can just click on. If that doesn't work,
then cut and paste the address into the address
line at the top of your web browser window.

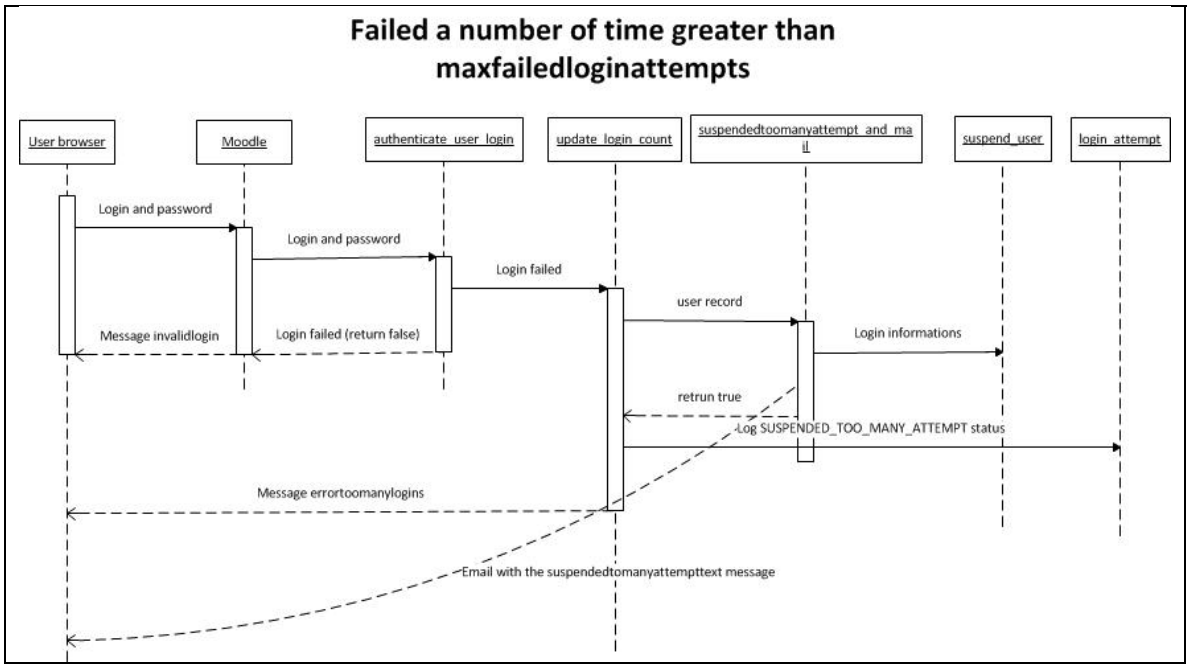
Cheers from the 'Your Moodle' administrator,

Support
support-your-moodle@yourschool.com

Sequences diagrams






Failed a number of time greater than maxfailedloginattempts
User browser
Moodle
authenticate_user_login
update_login_count
suspendedtoomanyattempt_and_mail
suspend_user
login_attempt
Login and password
Login and password
Login failed
user record
Login informations
Message invalidlogin
Login failed (return false)
retrun true
Log SUSPENDED_TOO_MANY_ATTEMPT status
Message errortoomanylogins
Email with the suspendedtomanyattempttext message