SQL Injection Attack

|  |
| --- |
| Copyright 2016-2017 Frank Xu, Bowie State University.  The lab manual is adapted from SQL Injection Attack Lab — Using Collabtive, available at http://www.cis.syr.edu/˜wedu/seed/all\_labs.html.  Copyright 2006 - 2013 Wenliang Du, Syracuse University.  The development of this document is/was funded by three grants from the US National Science Foundation: Awards No. 0231122 and 0618680 from TUES/CCLI and Award No. 1017771 from Trustworthy Computing. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy f the license can be found at http://www.gnu.org/licenses/fdl.html. |

1. **Lab Environment setting**
   1. Install Seed Lab Ubuntu image by following the link <http://www.cis.syr.edu/~wedu/seed/lab_env.html>. It has two accounts in the VM. The usernames and passwords are listed in the following:
      1. User ID: root, Password: seedubuntu. Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command **su** to login to the root account.
      2. User ID: seed, Password: dees
   2. Install sqlmp





* 1. Test sqlmp

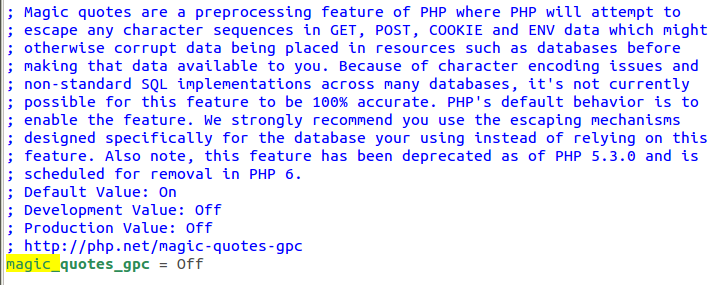


* 1. Turn Off the Countermeasure

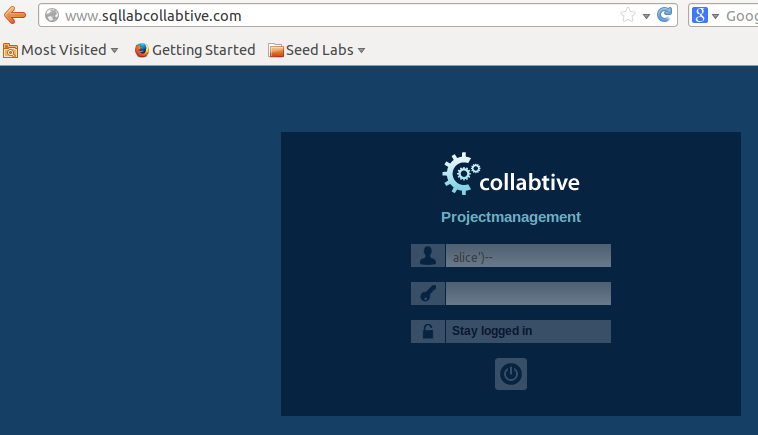
PHP provides a mechanism to automatically defend against SQL injection attacks. The method is called magic quote, and more details will be introduced in Task 3. Let us turn off this protection first (this protection method is deprecated after PHP version 5.3.0).

* + 1. Go to /etc/php5/apache2/php.ini.
    2. Find the line: magic quotes gpc = On.
    3. Change it to this: magic quotes gpc = Off.
    4. Restart the Apache server by running "sudo service apache2 restart".

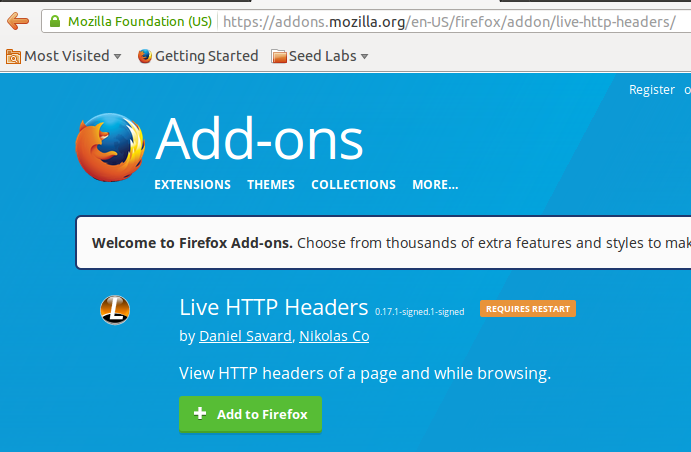




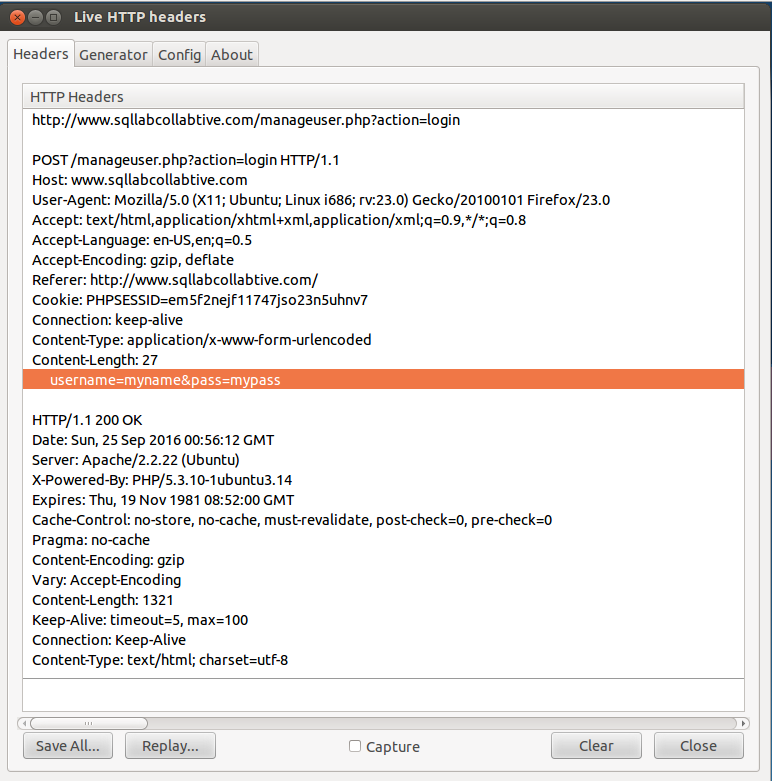
1. **Attack**
   1. Type “alice’)-- ”. Note: You need to add a space after “--”



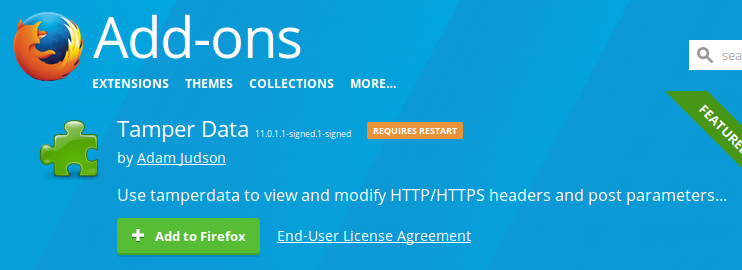
1. **Learn Firefox add-on tools**
   1. Add Livehttpheader add-on to Firefox
      1. Search for the add-on



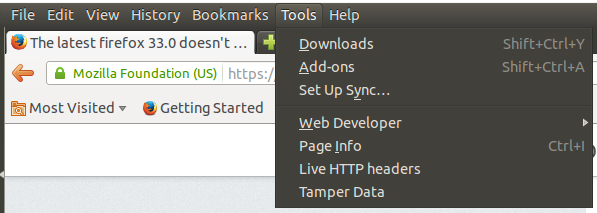
* + 1. Live capture

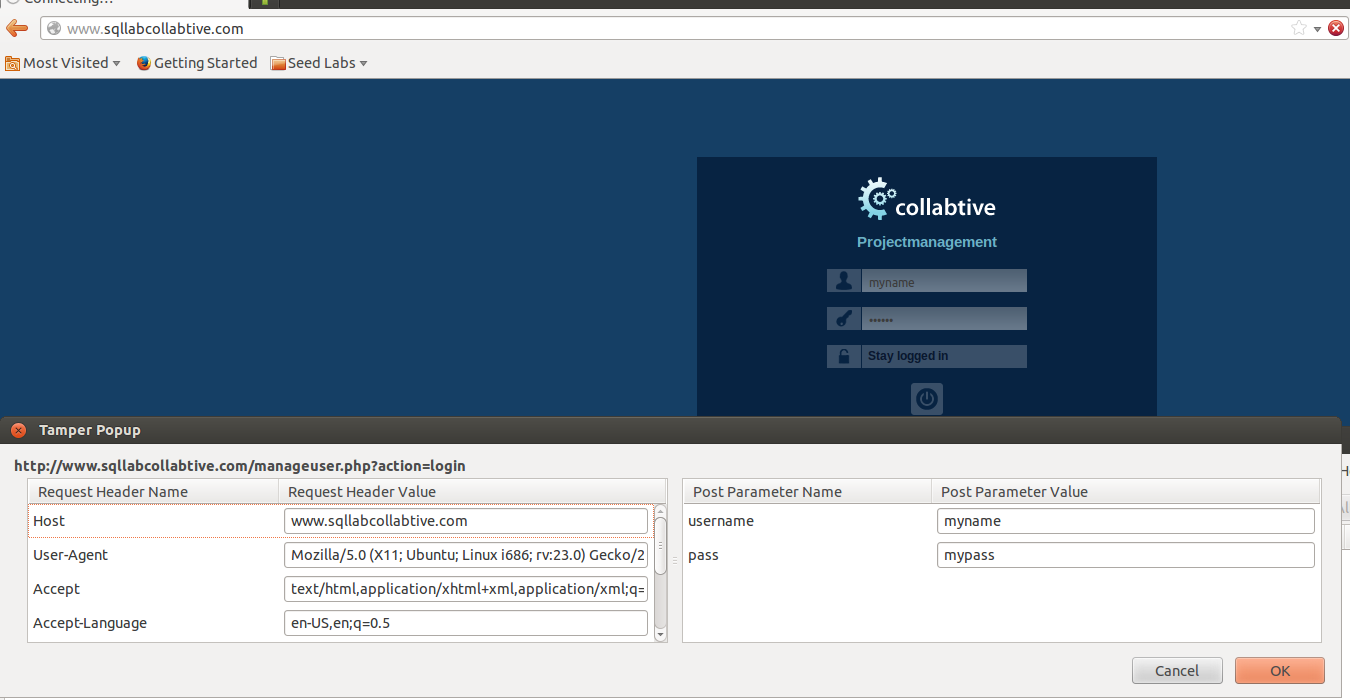


* 1. Add Tamper data addon to Firefox
     1. Search for the addon



* + 1. Tamper data capture screen





1. **Use Firefox add-on tools to capture Http headers. Provide screens here.**
2. **Explain how sqlmp work using an example. You can use an online example. Make sure you provide a link.**

Reference

* http://www.cis.syr.edu/~wedu/seed/lab\_env.html
* <http://www.slideshare.net/helloanand/sql-injection-13537064>
* <http://www.binarytides.com/sqlmap-hacking-tutorial/>