SQL Injection Attack

1. Lab Environment setting

1.1. 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:

1.1.1. 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.

1.1.2. User ID: seed, Password: dees

1.2. Install sqlmp

```
seed@Server(10.0.2.4):~$ sudo apt-get install git
[sudo] password for seed:
Reading package lists... Done
```

```
seed@Server(10.0.2.4):~$ git clone https://github.com/sqlmapproject/sqlmap.git s
qlmap-dev
```

1.3. Test sqlmp

```
seed@Server(10.0.2.4):~$ cd sqlmap-dev/
seed@Server(10.0.2.4):~/sqlmap-dev$ ls
doc    lib      procs      shell         sqlmap.conf  tamper      txt  waf
extra  plugins  README.md  sqlmapapi.py  sqlmap.py    thirdparty  udf  xml
seed@Server(10.0.2.4):~/sqlmap-dev$ sqlmap.py
                          {1.0.9.32#dev}
                          http://sqlmap.org

Usage: python sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --wizard, --update,
--purge-output or --dependencies), use -h for basic or -hh for advanced help
```

1.4. 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).

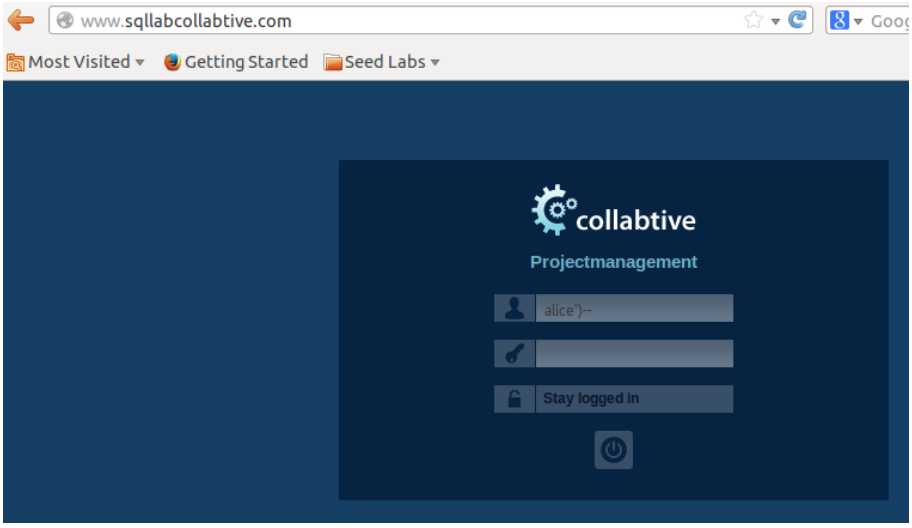
1.4.1. Go to /etc/php5/apache2/php.ini.
1.4.2. Find the line: magic quotes gpc = On.
1.4.3. Change it to this: magic quotes gpc = Off.
1.4.4. Restart the Apache server by running "sudo service apache2 restart".

```
seed@Server(10.0.2.4):/etc/php5/apache2$ sudo gedit php.ini
[sudo] password for seed:
```

```
; Magic quotes are a preprocessing feature of PHP where PHP will attempt to
; escape any character sequences in GET, POST, COOKIE and ENV data which might
; otherwise corrupt data being placed in resources such as databases before
; making that data available to you. Because of character encoding issues and
; non-standard SQL implementations across many databases, it's not currently
; possible for this feature to be 100% accurate. PHP's default behavior is to
; enable the feature. We strongly recommend you use the escaping mechanisms
; designed specifically for the database your using instead of relying on this
; feature. Also note, this feature has been deprecated as of PHP 5.3.0 and is
; scheduled for removal in PHP 6.
; Default Value: On
; Development Value: Off
; Production Value: Off
; http://php.net/magic-quotes-gpc
magic_quotes_gpc = Off
```

2. **Attack**

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

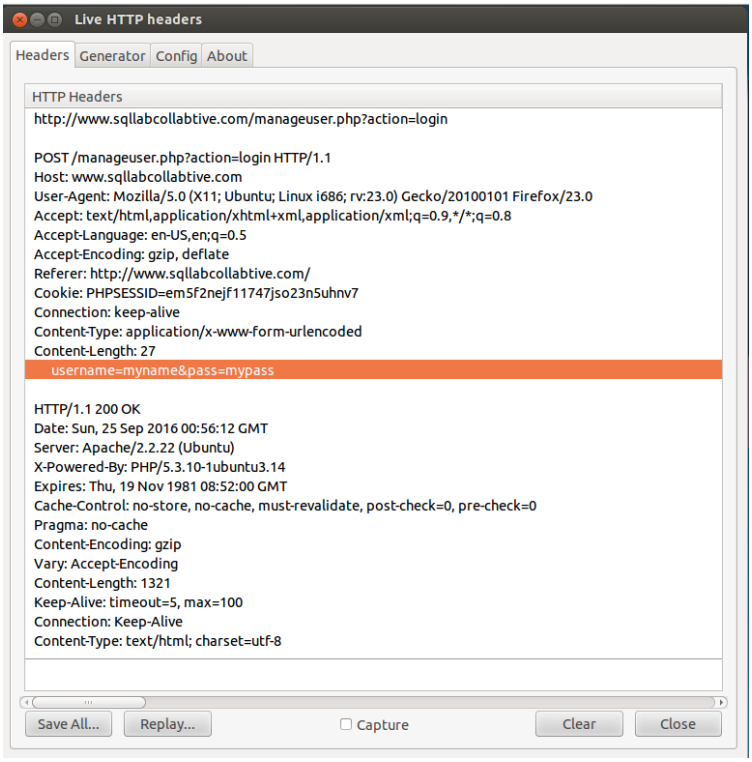


3. **Learn Firefox add-on tools**

3.1. Add Livehttpheader add-on to Firefox

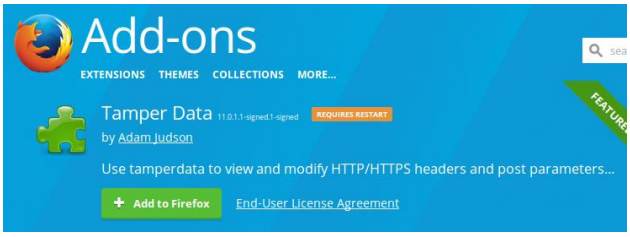
3.1.1. Search for the add-on

3.1.2.Live capture

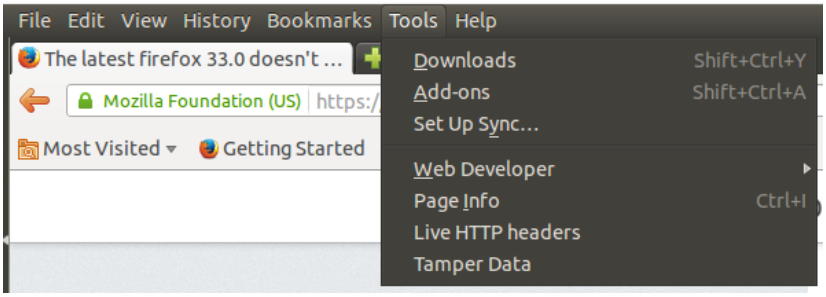


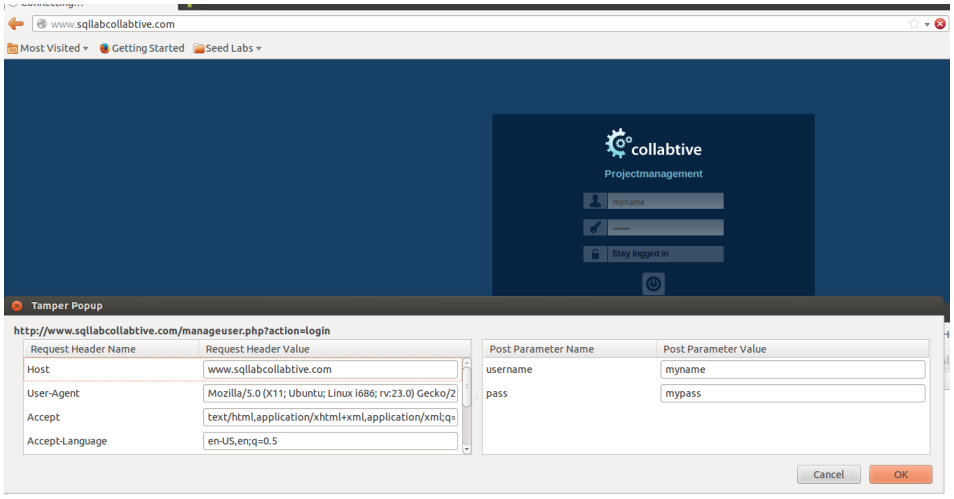
3.2. Add Tamper data addon to Firefox

3.2.1.Search for the addon



3.2.2.Tamper data capture screen





4. Use Firefox add-on tools to capture Http headers. Provide screens here.

5. 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/