

Secure Internet Application Development

CPS 499-63/592-65, Summer 2017

Final Project :: Integrated Chat based Blog System

Designing and Implementation of Blog System:

It is a Web based Secured-Chat integrated Blog system. It is two-level heirarchical system.

The two levels are as follows:

1. Guest Level

Guest can only view the posts and add his comments

It is secured based blog system as we have employed few security measures into it. How my blog

- Login:
log.php

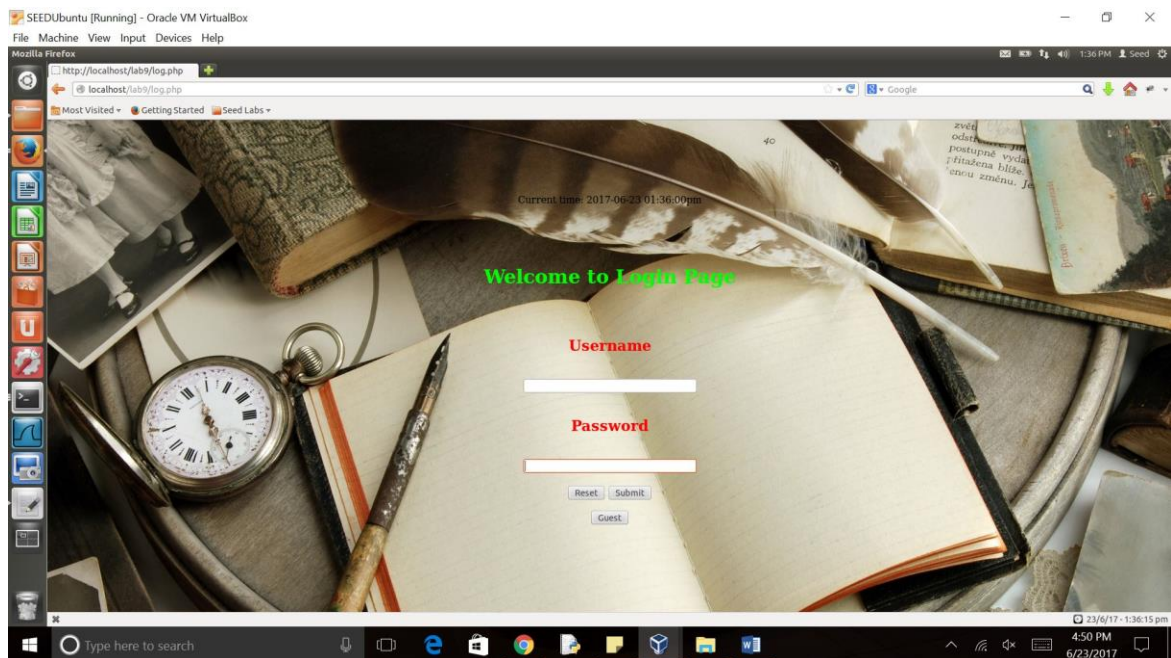


Figure 1: Login page (log.php)

- Guest:

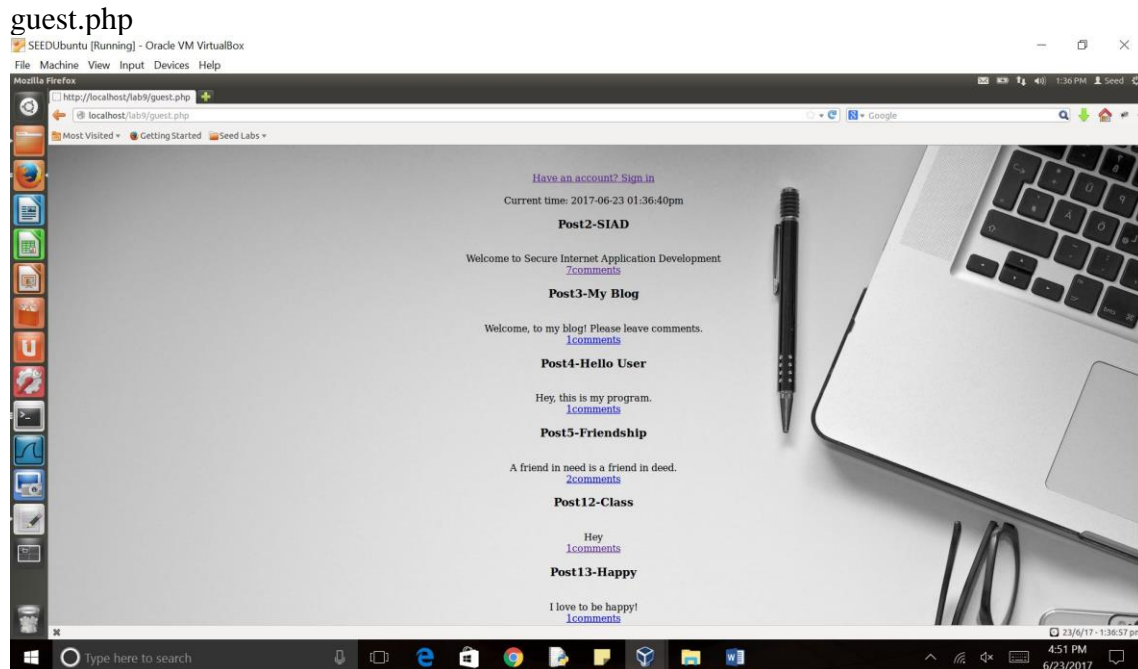


Figure 2: Guest-welcome page (guest.php)

View Comments: guestcomment.php

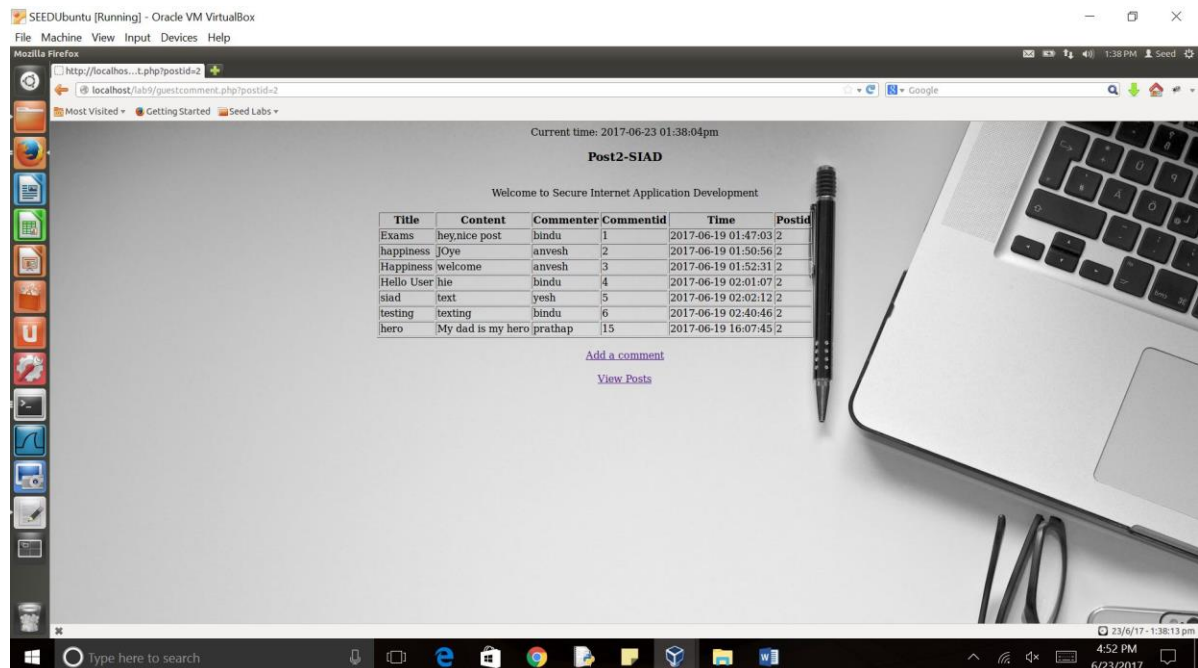


Figure 3: Guest- view comments (guestcomment.php)

Add Comments: guestcform.php

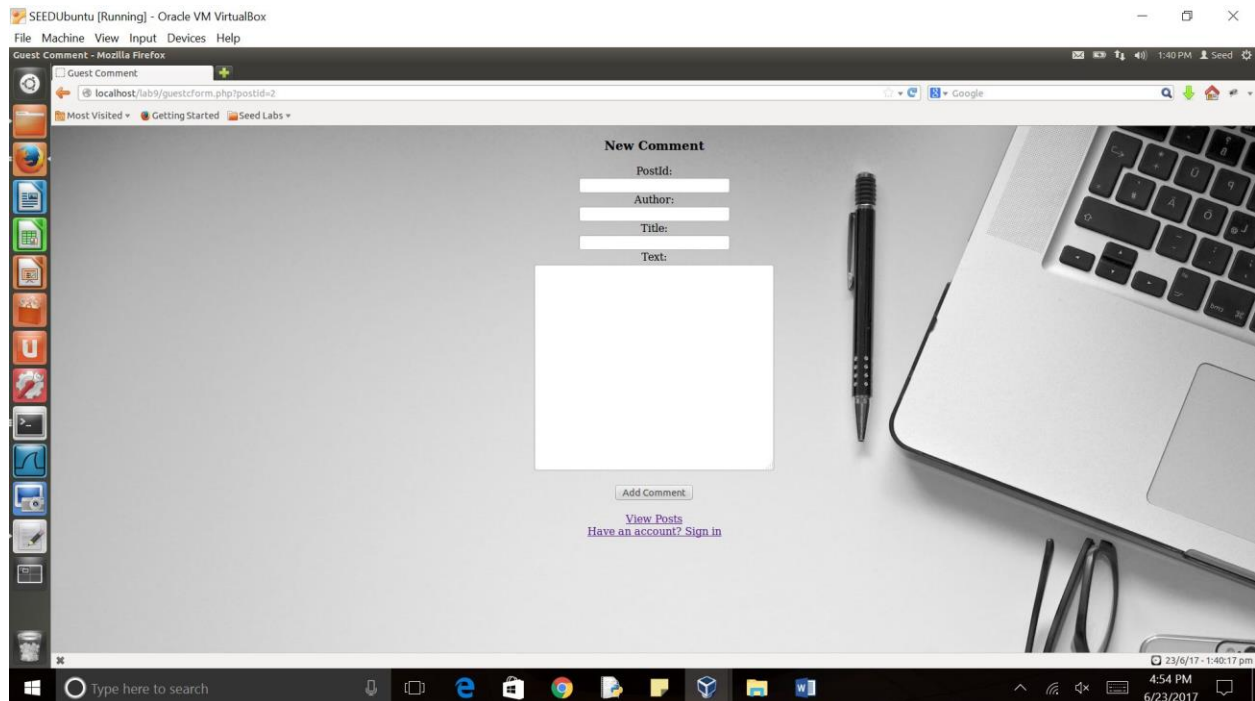


Figure 4: Guest- Add Comment (guestcform.php)

2. User Level

Authentication is required. User can view the posts, edit and delete them. He can scribe comments, edit and delete the comments too.

If user needs any help, he can chat with online users instantly. Chat feature: He can view available online users and chat.

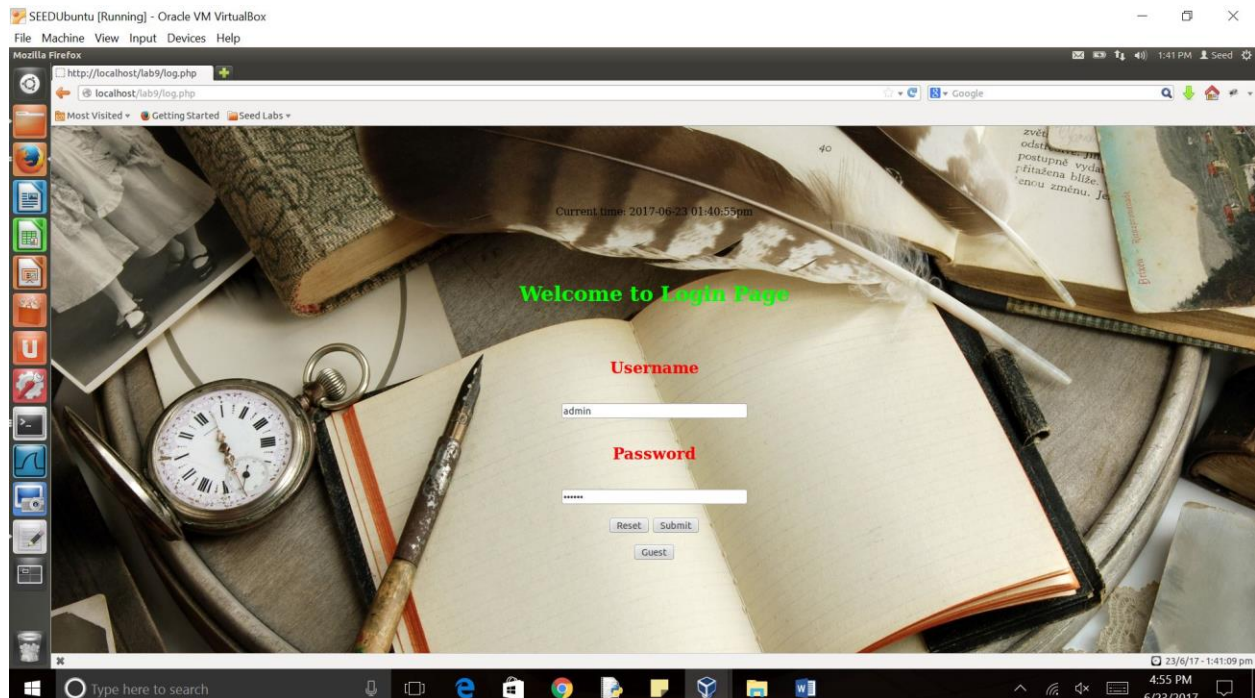


Figure 5: Login with valid credentials

Welcome Page:
(index.php)

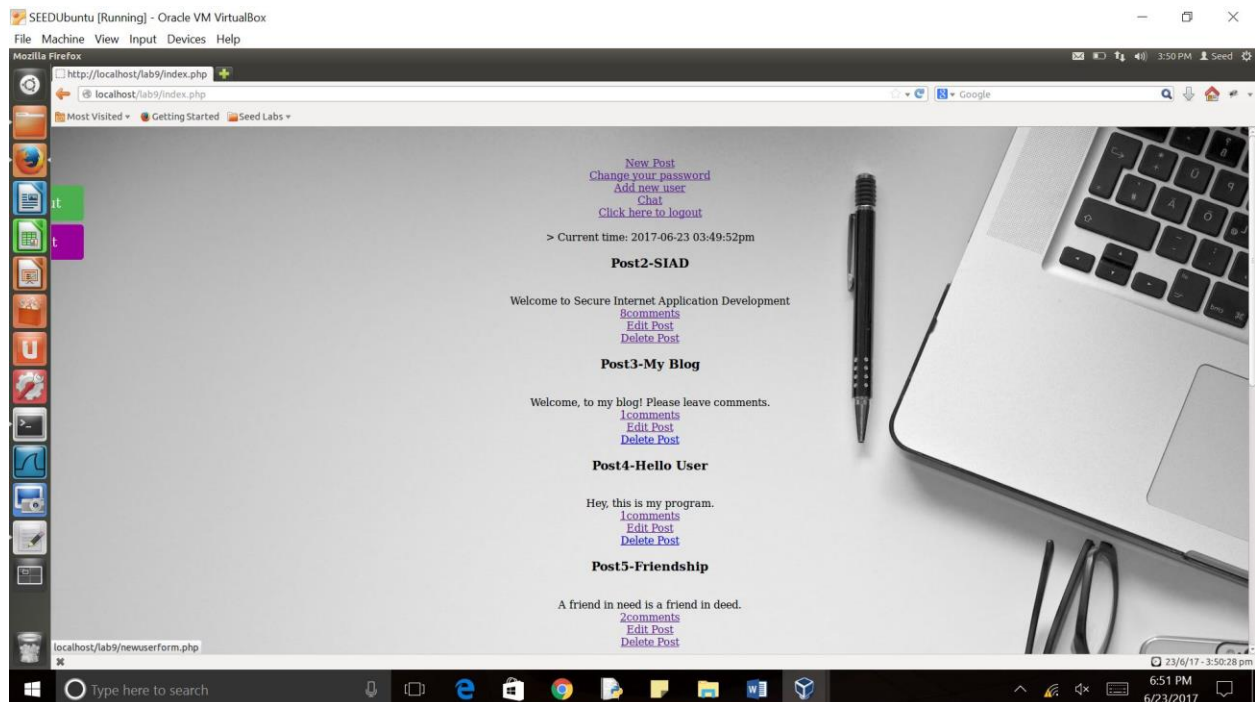


Figure 6 : Welcome page

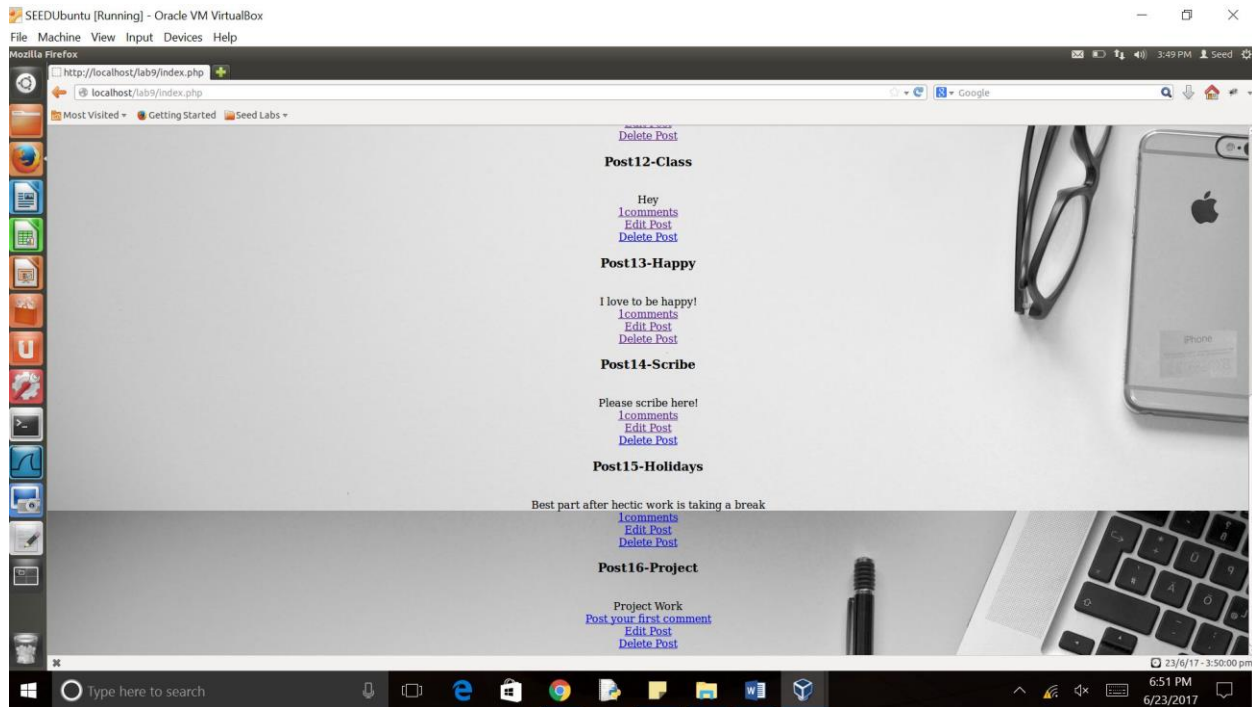


Figure 7 : Welcome page 1.1

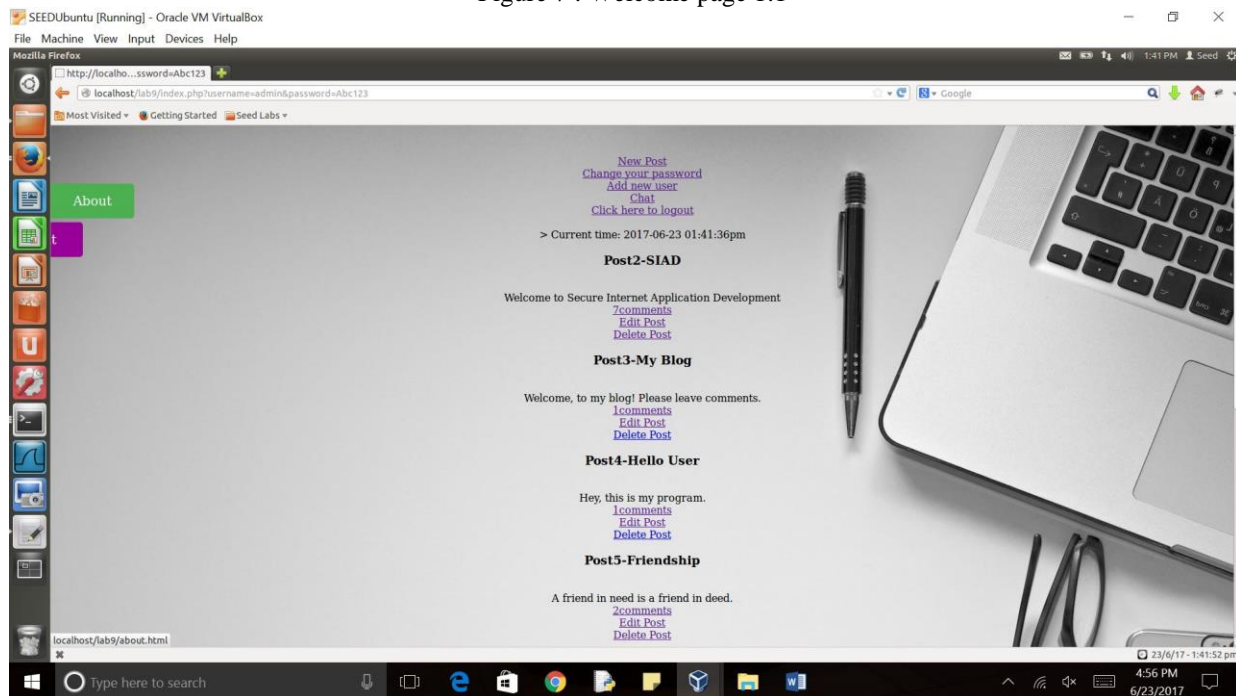


Figure 8: Welcome page 1.2

About Page: (about.html)

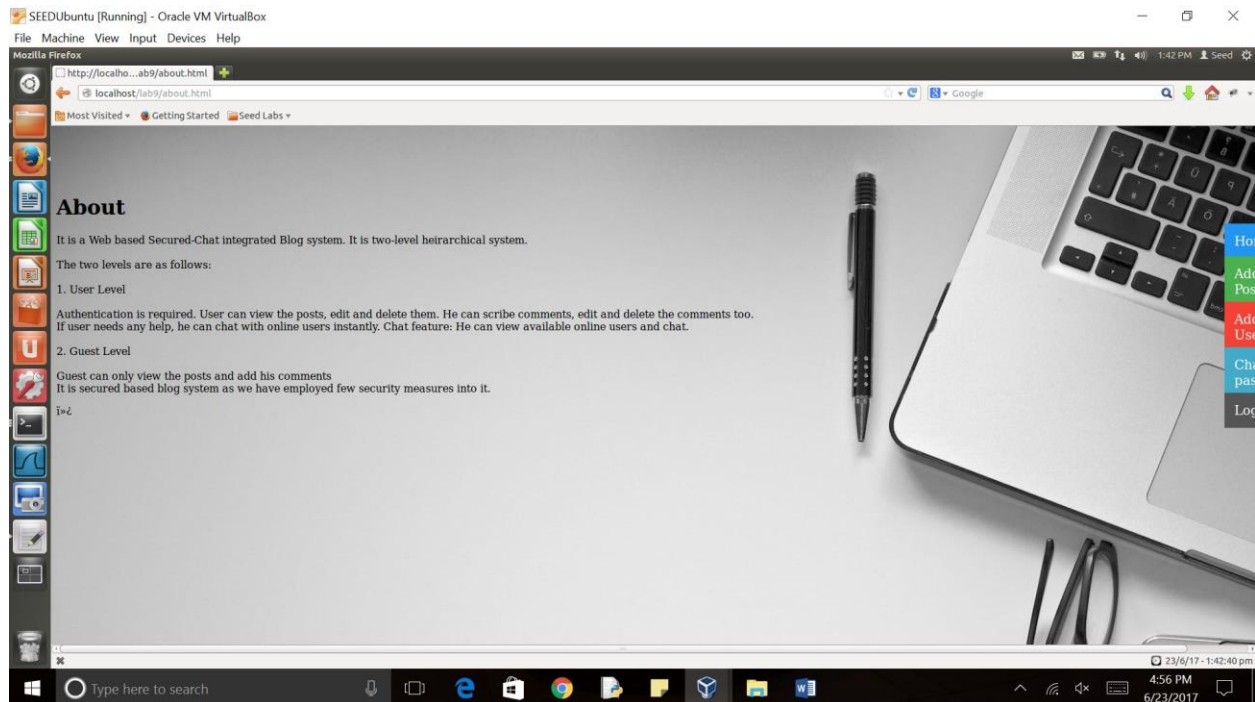


Figure 9: About page

Chat: (websocketchat1.php)

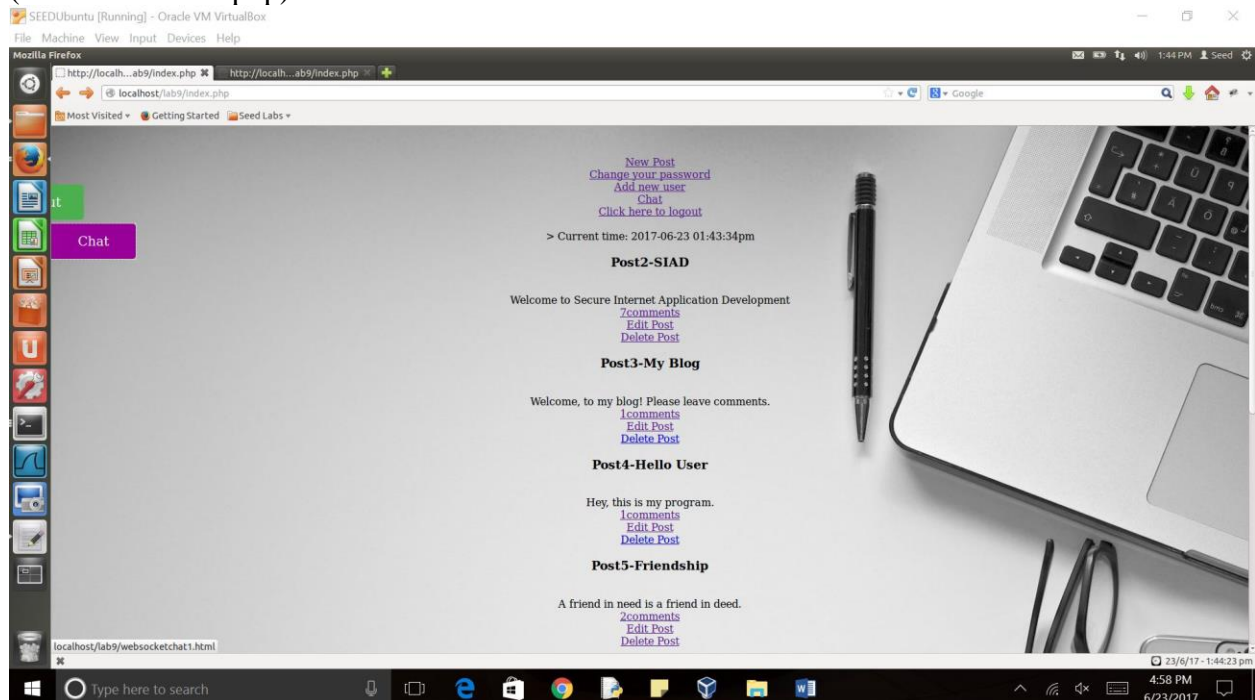


Figure 10: Chat

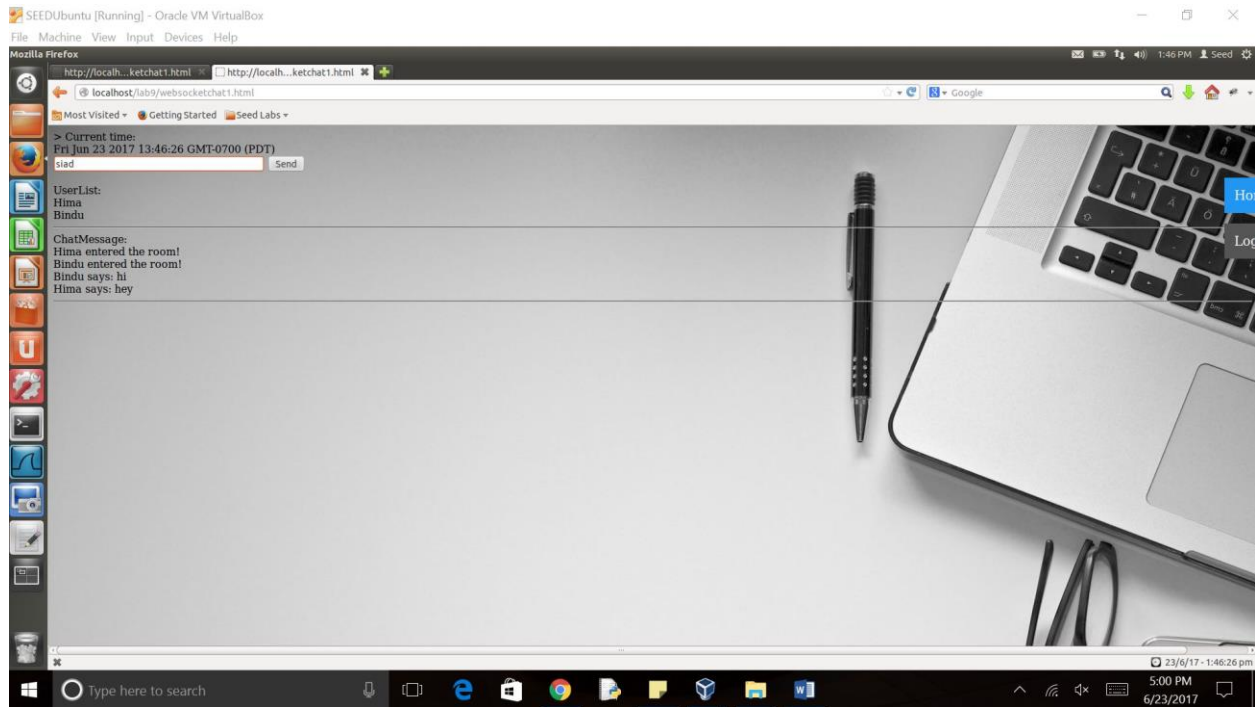


Figure 11: Chat

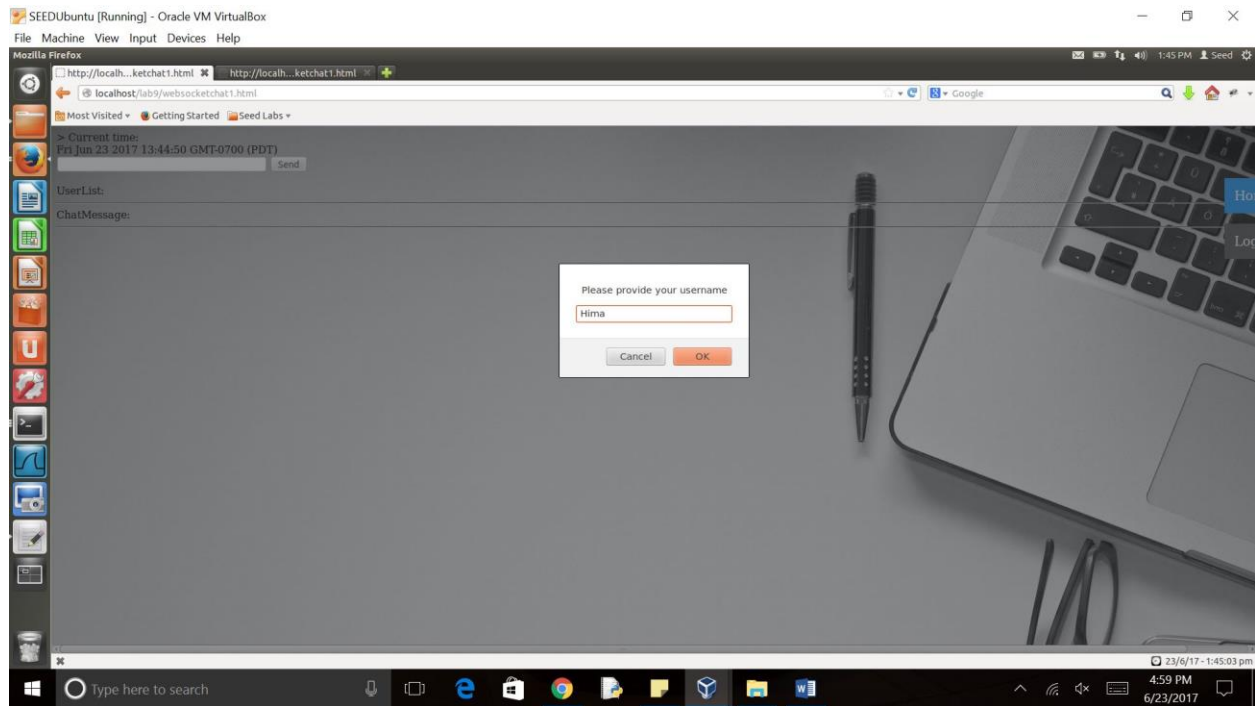


Figure 12 Chat- enter name

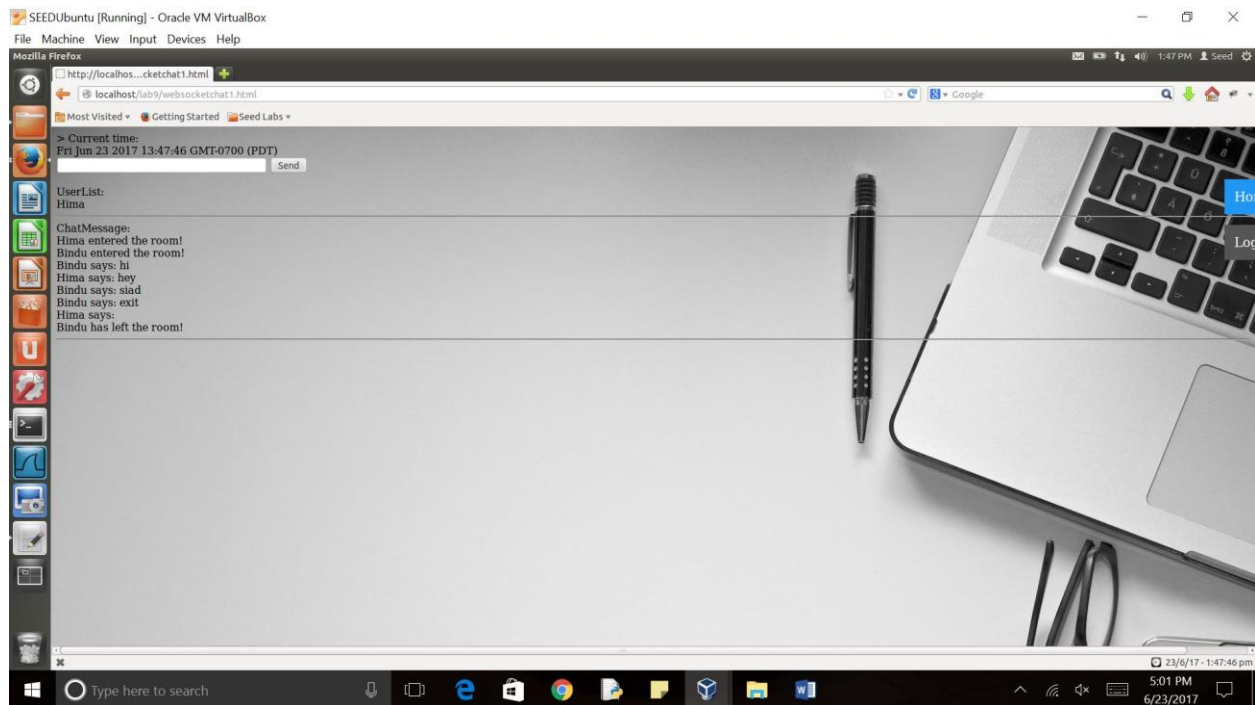


Figure 13: Chat close

Change Password Form:

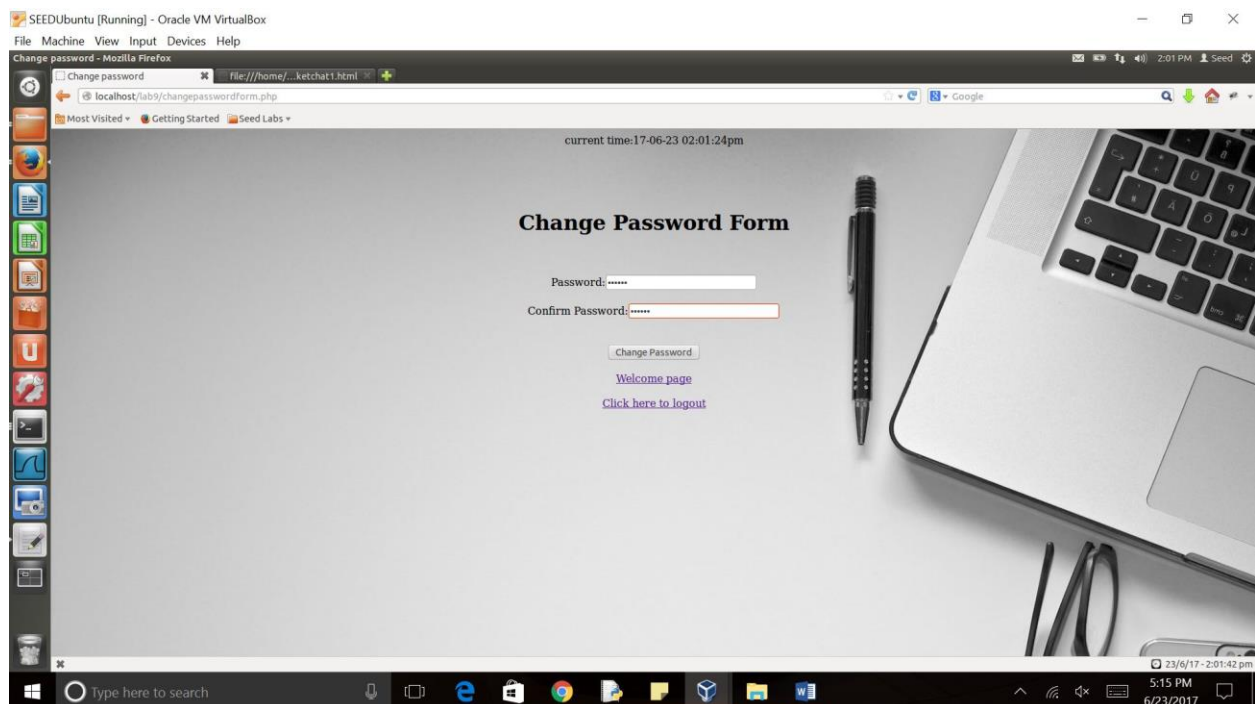


Figure 14: Change Password Form

Add Post :

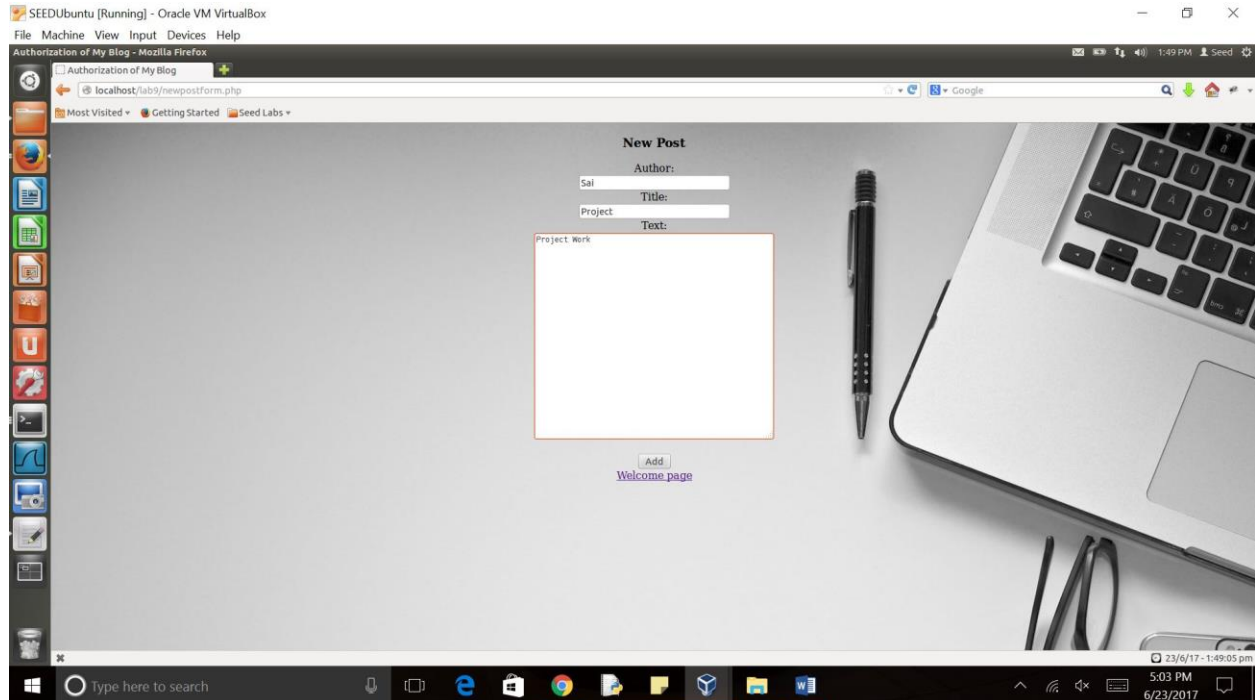
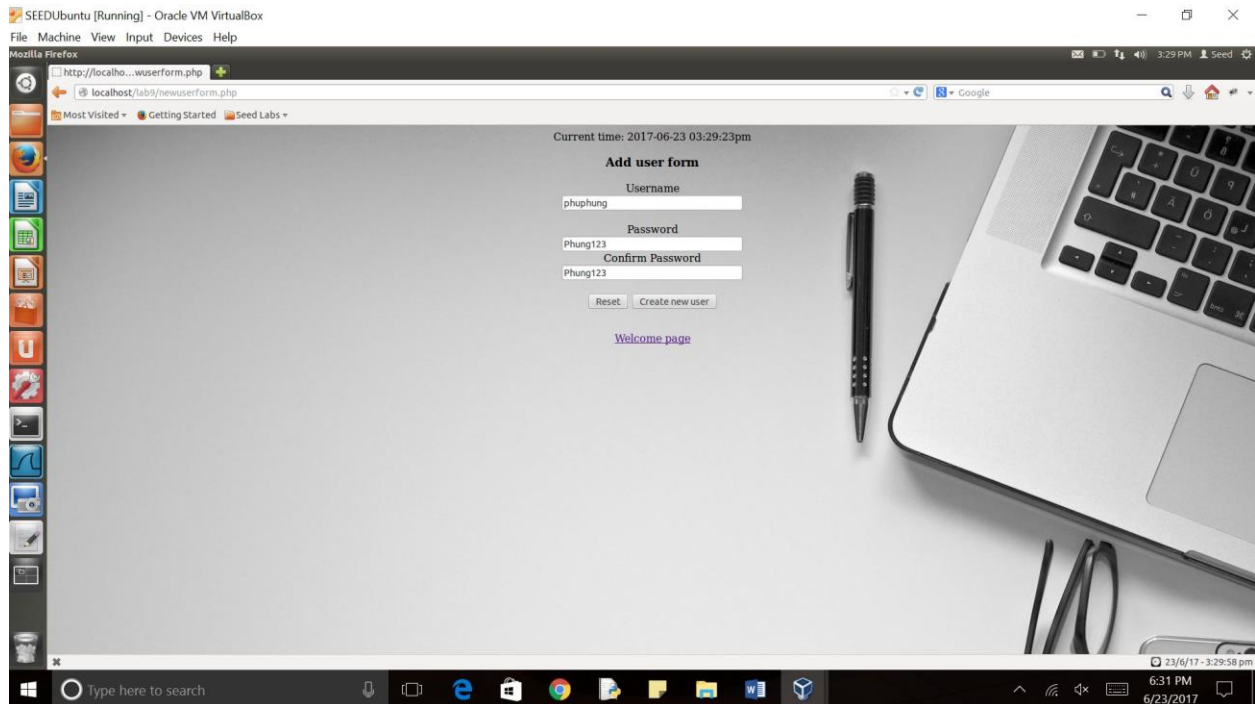
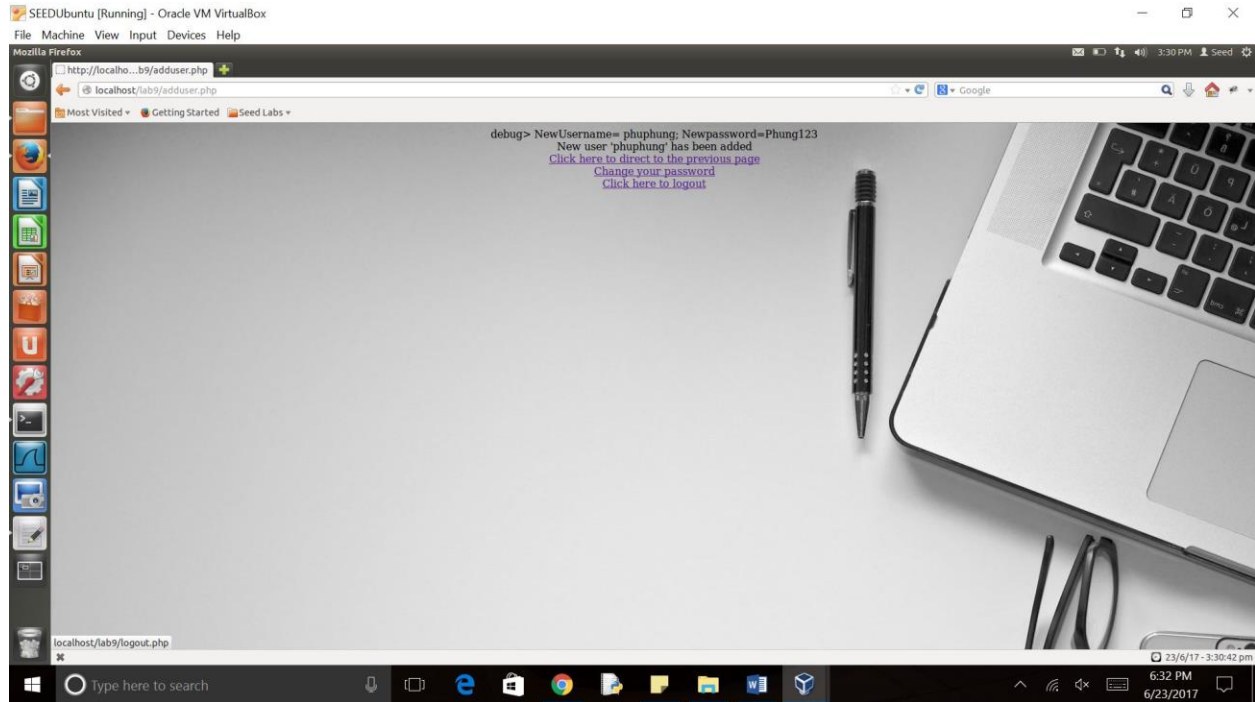


Figure 15: Add new post

Add user form





Add Comment form

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Add a Comment - Mozilla Firefox

localhost/lab9/commentpost.php

Most Visited Getting Started Seed Labs

New Comment

PostId:

Author:

Title:

Text:

[Welcome page](#)

New comment 'Life' has been added

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Add a Comment - Mozilla Firefox

localhost/lab9/commentpost.php?postId=2

Most Visited Getting Started Seed Labs

New Comment

PostId:

Author:

Title:

Text:

[Welcome page](#)

View Comments:

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Mozilla Firefox

http://localhost...t.php?postId=2

localhost/lab9/comment.php?postId=2

Most Visited Getting Started Seed Labs

Current time: 2017-06-23 03:33:34pm

Post2-SIAD

Welcome to Secure Internet Application Development

Title	Content	Commenter	Commentid	Time	Postid
Exams	hey,nice post	bindu	1	2017-06-19 01:47:03	2
happiness	Joye	anvesh	2	2017-06-19 01:50:56	2
Happiness	welcome	anvesh	3	2017-06-19 01:52:31	2
Hello User	hie	bindu	4	2017-06-19 02:01:07	2
siad	text	yesh	5	2017-06-19 02:02:12	2
testing	texting	bindu	6	2017-06-19 02:40:46	2
hero	My dad is my hero	prathap	15	2017-06-19 16:07:45	2

[Add a comment](#)
[Edit a comment](#)
[Delete a comment](#)
[Welcome page](#)

23/6/17 - 3:33:43 pm

6:35 PM
6/23/2017

Delete Comments

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Enter the commentid that you want to delete:

31

Submit

Commentid	Title	Content	Owner	Postid
1	Exams	hey,nice post	bindu	2
2	happiness	JOye	anvesh	2
3	Happiness	welcome	anvesh	2
4	Hello User	hie	bindu	2
5	siad	text	yesh	2
6	testing	texting	bindu	2
15	hero	My dad is my hero	prathap	2
30	Life	Life is all about learning	Swaroop	2
31	Life	Life is all about learning	Swaroop	2

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sql = Delete from comments where commentid='31'; Comment '31' has been deleted

[Welcome page](#)

Edit Comments

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Enter the commentid that you want to edit:

Enter the content that you want to edit:

Submit

commentid	title	content	commenter	postid
1	Exams	hey,nice post	bindu	2
2	happiness	JOye	anvesh	2
3	Happiness	welcome	anvesh	2
4	Hello User	hie	bindu	2
5	siad	text	yesh	2
6	testing	texting	bindu	2
15	hero	My dad is my hero	prathap	2
30	Life	Life is all about learning	Swaroop	2
31	Life	Life is all about learning	Swaroop	2

23/6/17 - 3:38:48 pm

6:40 PM
6/23/2017

Edit Post

SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Mozilla Firefox
http://localhost...php?postid=17
localhost/lab9/updateform.php?postid=17
Most Visited Getting Started Seed Labs

Edit Post
Enter POSTID that you want to edit:
Enter TITLE that you want to edit:
Enter CONTENT that you want to edit:

postid	title	content	owner
17	Project	Project Work	Sal

23/6/17 - 3:45:51 pm
6:47 PM
6/23/2017

SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Mozilla Firefox
http://localhost/lab9/edit.php
localhost/lab9/edit.php
Most Visited Getting Started Seed Labs

```
debug> Postid= 17; Title= Project Work Submission; Content=Project Work Submission  
sql = update posts set content = 'Project Work Submission',title='Project Work Submission' where  
postid=17; post '17' has been updated
```

[Welcome page](#)

23/6/17 - 3:48:20 pm
6:49 PM
6/23/2017

Editing Post

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Mozilla Firefox

http://localhost:8080/php/postid=17

localhost/lab9/updateform.php/postid=17

Most Visited Getting Started Seed Labs

Edit Post

Enter POSTID that you want to edit:
17

Enter TITLE that you want to edit:
Project Work Submission

Enter CONTENT that you want to edit:
Project Work Submission

Submit

postid	title	content	owner
17	Project	Project Work	Sai

23/6/17 - 3:47:24 pm

Type here to search

6:48 PM 6/23/2017

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Mozilla Firefox

http://localhost:8080/php/postid=17

localhost/lab9/delete.php/postid=17

Most Visited Getting Started Seed Labs

sql = Delete from posts where postid="17";
Post '17' has been deleted

[Welcome page](#)

23/6/17 - 3:49:15 pm

Type here to search

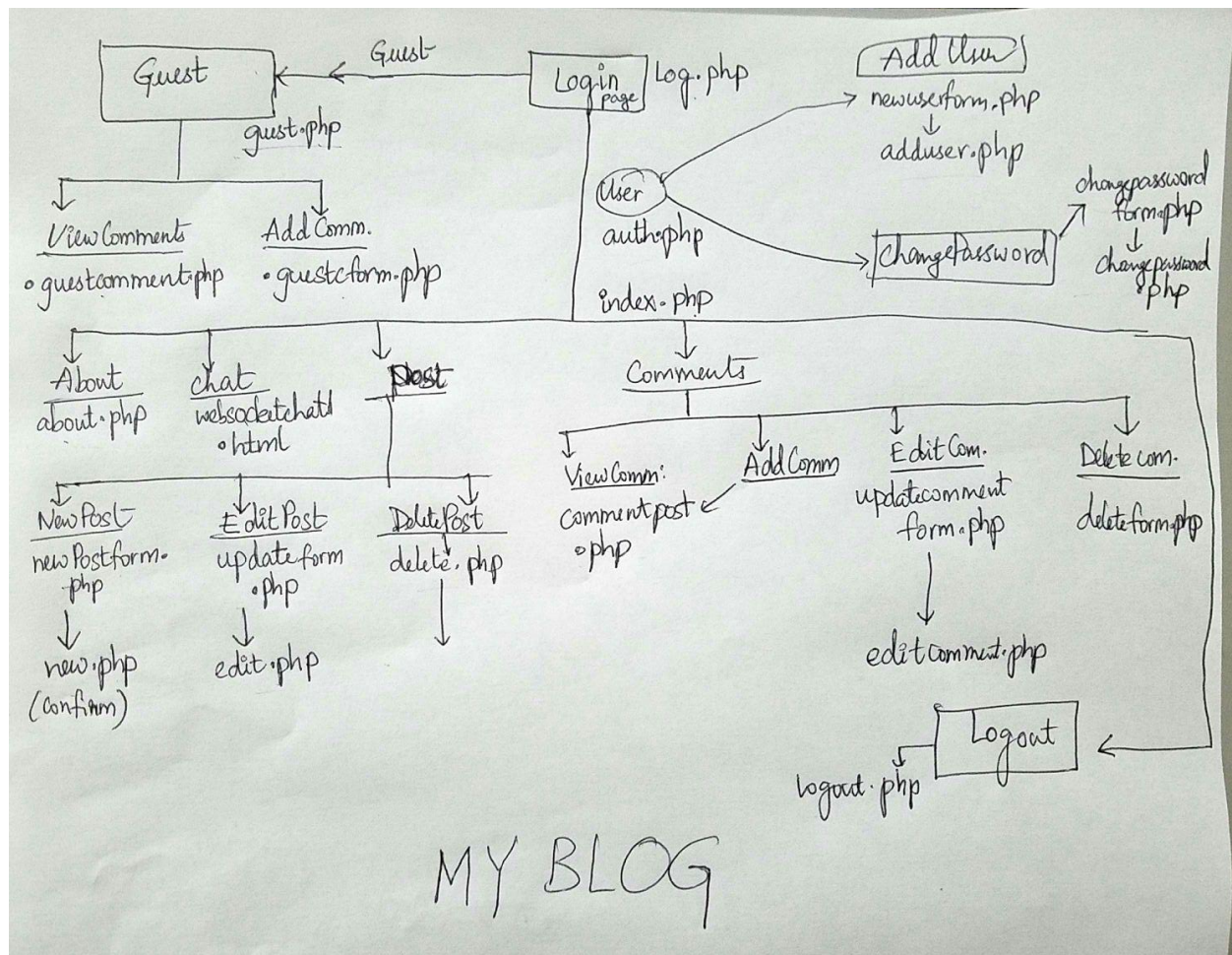
6:50 PM 6/23/2017

File Management System

- Authorization:
auth.php
- About:
about.php
- Login:
log.php
- Guest:
guest.php
View Comments: guestcomment.php
Add Comments: guestcform.php
- Welcome page:
index.php
- Chat:
websocketchat1.php
- Add User
Newuserform.php
Adduser.php
- Change Password
Changepasswordform.php
Changepassword.php
- Add Post
Newpostform.php
New.php
- Edit Post
Updateform.php
Edit.php
- Delete Post
Delete.php
- Add Comment
Commentpost.php
- Edit Comment

Updatecommentform.php
Editcomment.php

- Delete Comment
Deleteform.php
- Logout:
logout.php



File Management System

Potential Risks and preventions adopted:

Common Security risks are: "NEVER TRUST USER INPUT"

1. Session hijacking

Avoid:

- a. set session cookies parameters
- b. store more information about the browser (HTTP_USER_AGENT, REMOTE_ADDR, HTTP_ACCEPT, HTTP_ACCEPT_LANGUAGE)
- c. re-authenticate if there is any change in the database
- d. while user request is to change password, ask for current password too

2. SQL Injection Attacks

Avoid:

- a. user database platform dependent APIs- eg. mysql_real_escape_string
- b. use prepared statements
- c. escaping all user supplied input

3. Cross-site Request Forgery

Avoid:

- a. server needs to re-authenticate
- b. generate secret token to link between the webpages
- c. validating referrer

4. Cross-site Scripting Attack

Avoid:

- a. use HTML entities
- b. use HTML attributes