Assignment II (Just Lab 9) – Preventing Web Application Vulnerabilities

CPS 499-02/592-02

Software/Language Based Security

Fall 2020

Dr. Phu Phung

Evan Krimpenfort

Task 0: Web Administration – Preparation

a. Database Setup

i. Imported the database and created a new user

```
[11/24/20]seed@VM:~/.../www.myblog.com$ mysql -u krimpenforte1 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| blog               |
+--------------------+
2 rows in set (0.00 sec)
```

Figure 1: The database

ii. Demonstration

```php
<?php

    $dblink = mysqli_connect("localhost", "krimpenforte1", "bobgeorge","blog");
    if (mysqli_connect_errno()) {
        printf("Connect failed: %s\n", mysqli_connect_error());
        exit();
    }

?>
```

Figure 2: classes/db.php

b. Deployment

iii. Using IP Address

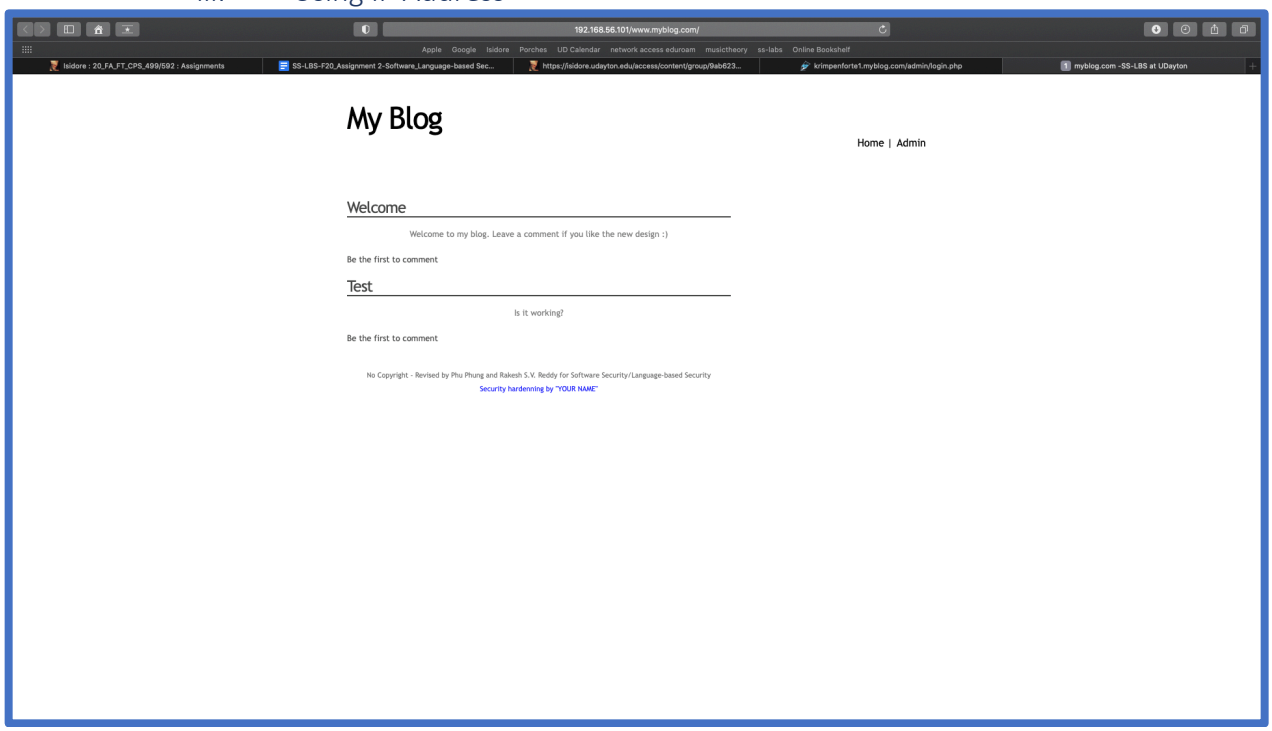

Figure 3: http://192.168.56.101/www.myblog.com/

iv. With local domain name

1. *SEEDVM*

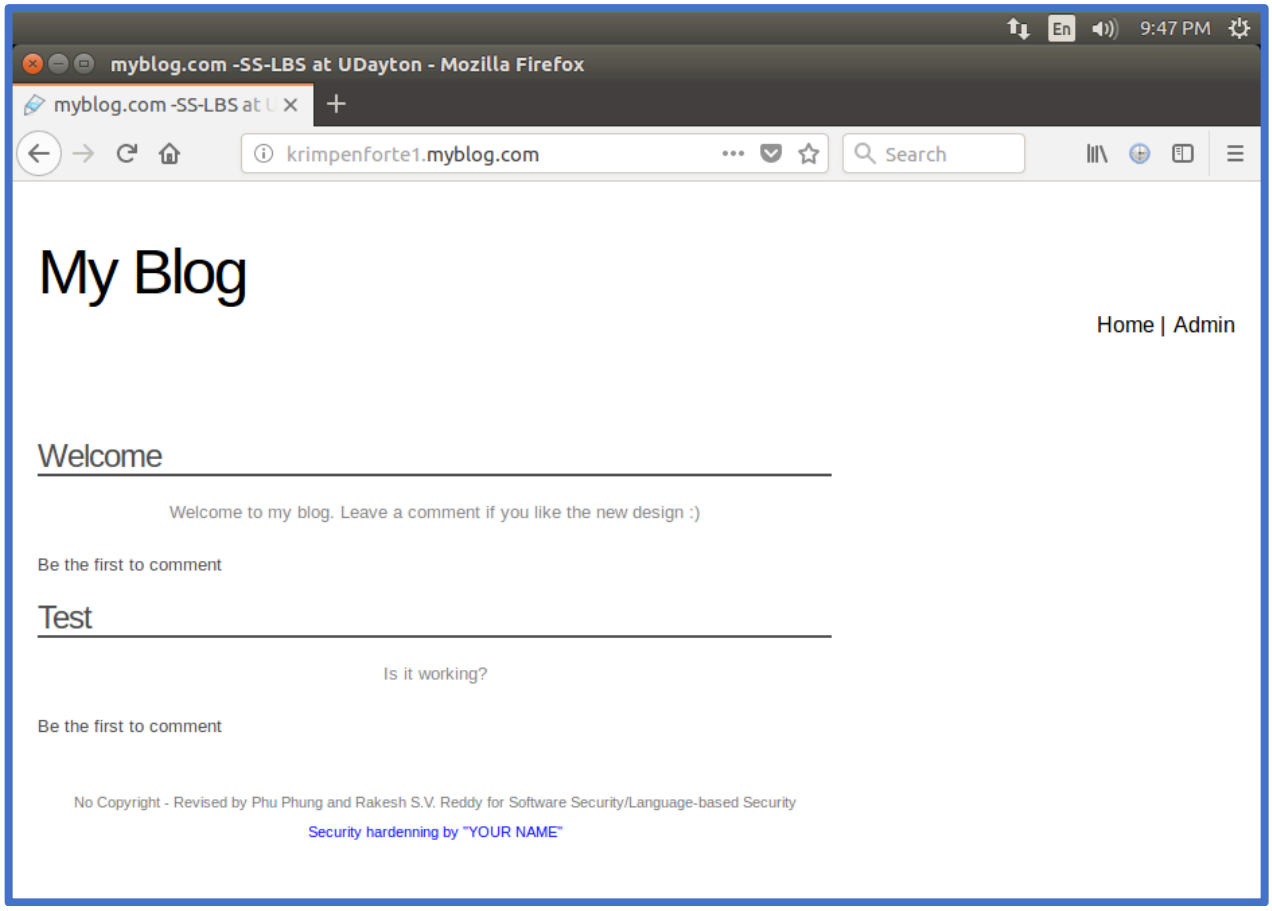

Figure 4: http://krimpenforte1.myblog.com/ on the VM

2. *Personal Computer*

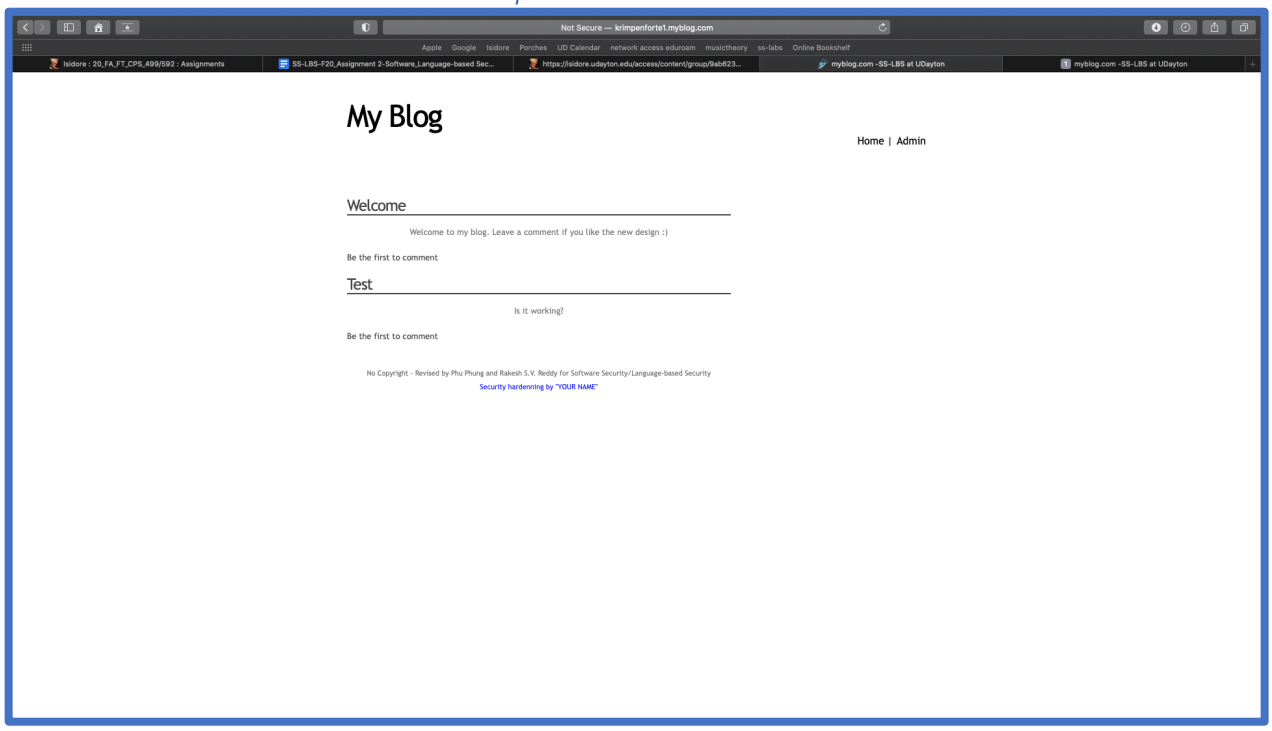

Figure 5: http://krimpenforte1.myblog.com/ on the Mac

c. Misconfiguration Security

v. Deleted the database file (blog.sql)

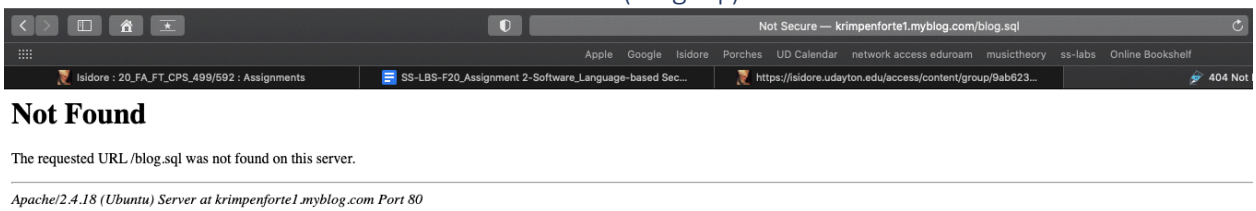

Figure 6: http://krimpenforte1.myblog.com/blog.sql not found

vi. Changed default username and password

```
mysql> select * from users;
+----+---------------------------+----------------------------------+
| id | login                     | password                         |
+----+---------------------------+----------------------------------+
|  1 | admin                     | 2bf802b6cdfb91f2a0863e55c5da5e2e |
|  2 | krimpenforte1@udayton.edu | 2bf802b6cdfb91f2a0863e55c5da5e2e |
+----+---------------------------+----------------------------------+
2 rows in set (0.00 sec)
```

Figure 7: Users available

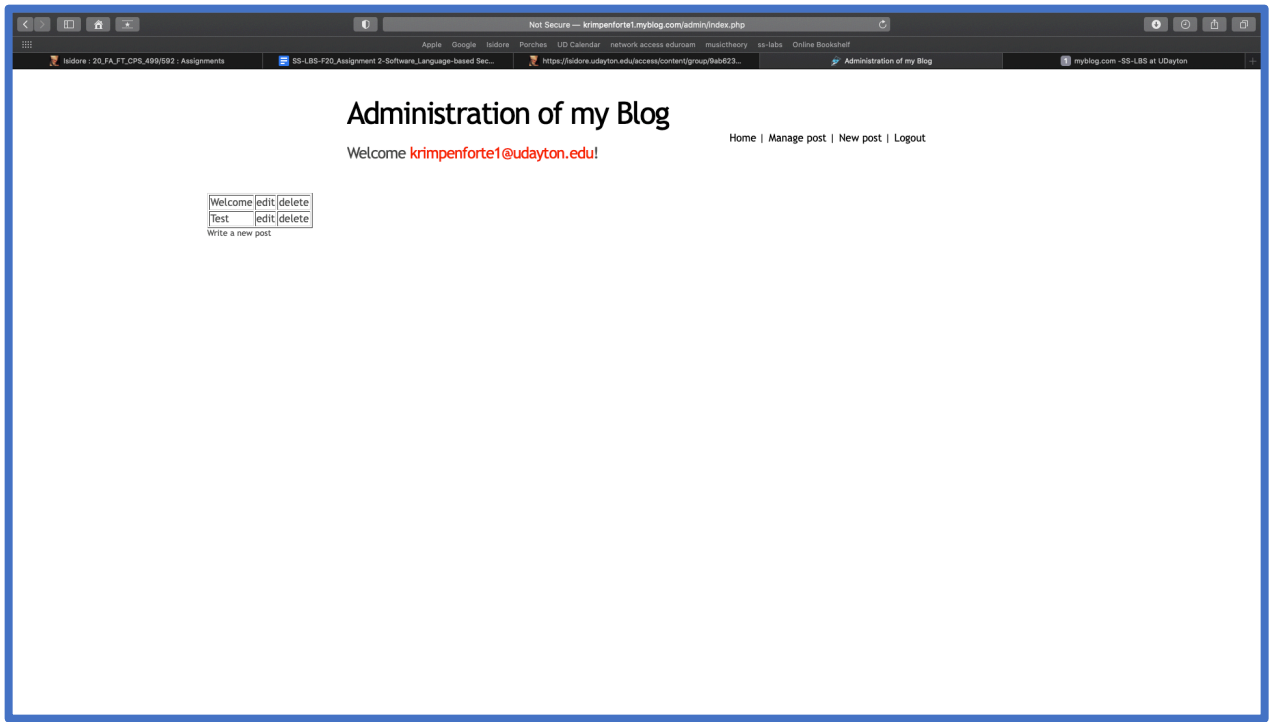

Figure 8: can log in with krimpenforte1@udayton.edu

d. HTTPS Setup

vii. Certificate was made

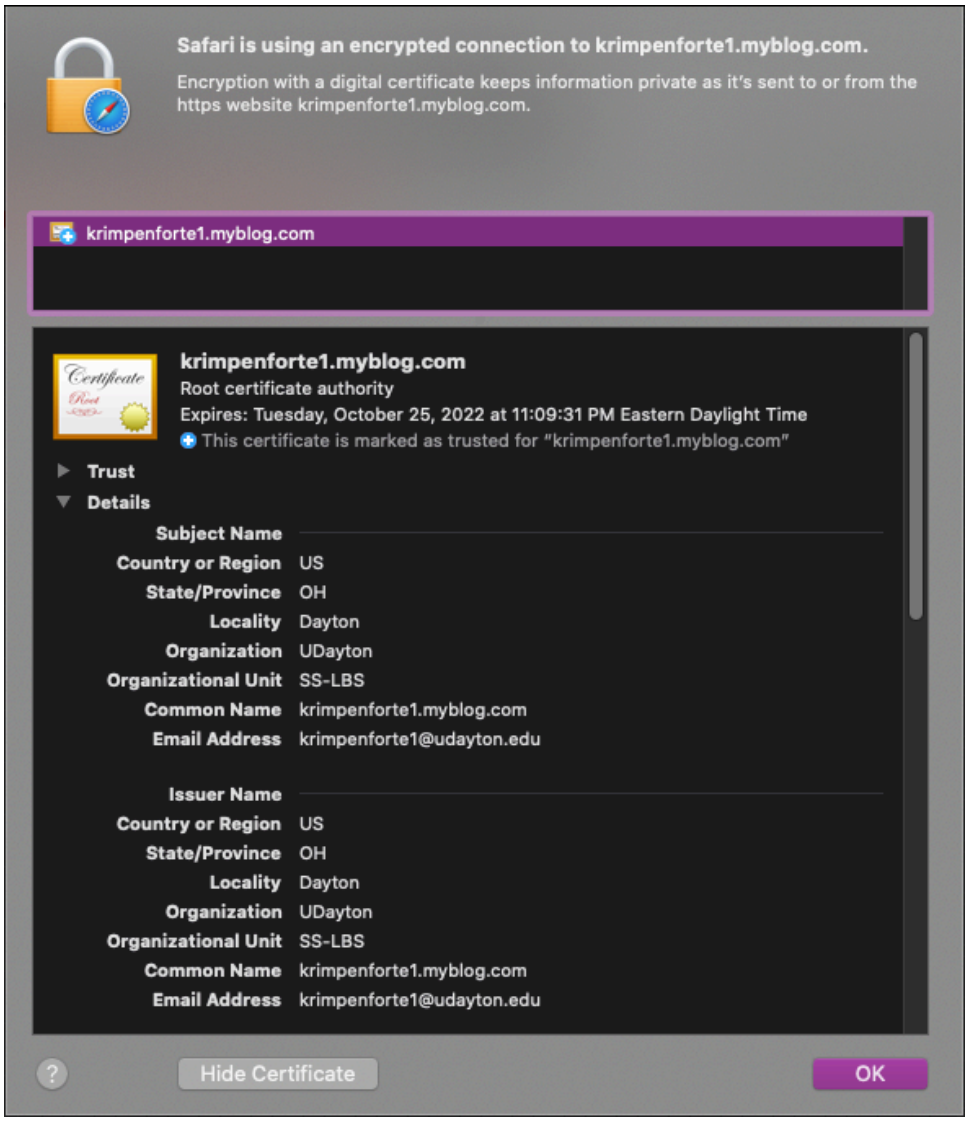

Figure 9: Certificate Details

viii. Deployment was done

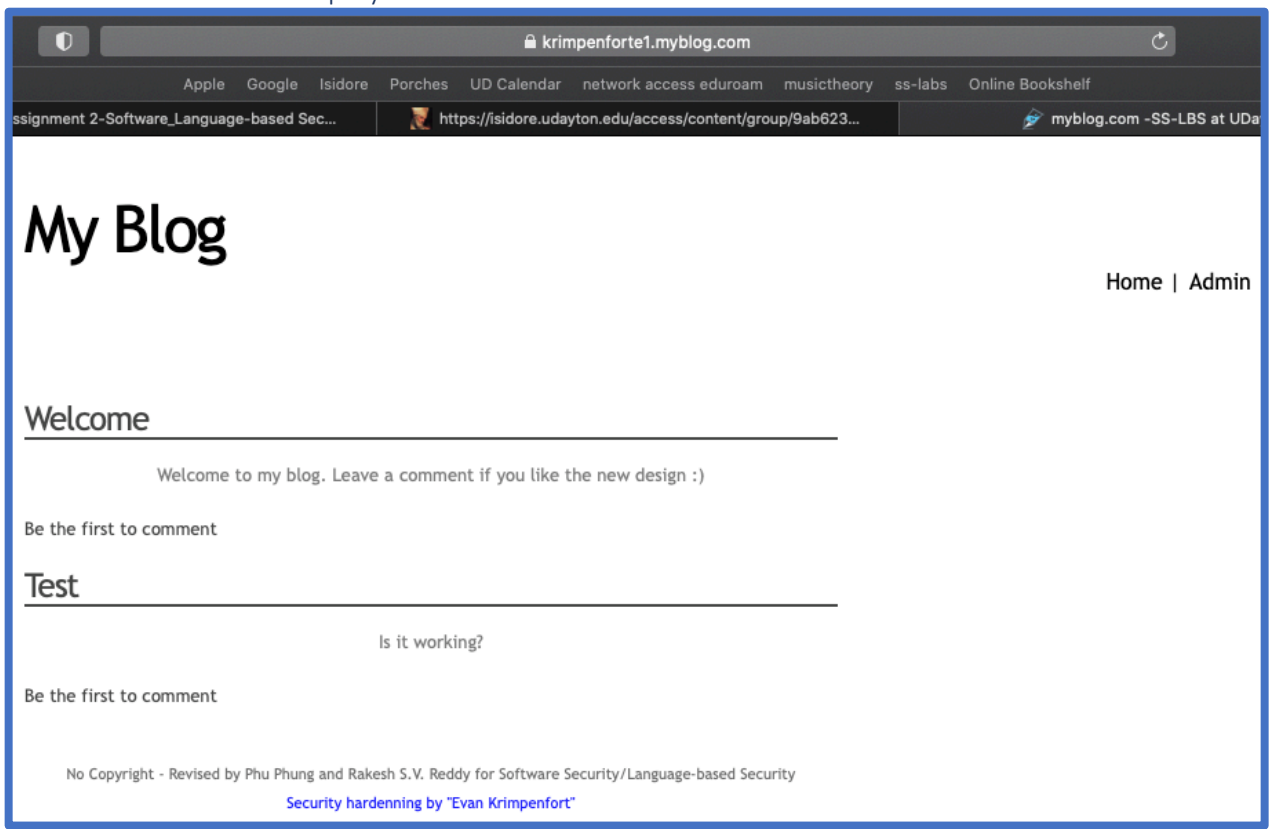

Figure 10: Site has https and the footer has been changed

e. Repository

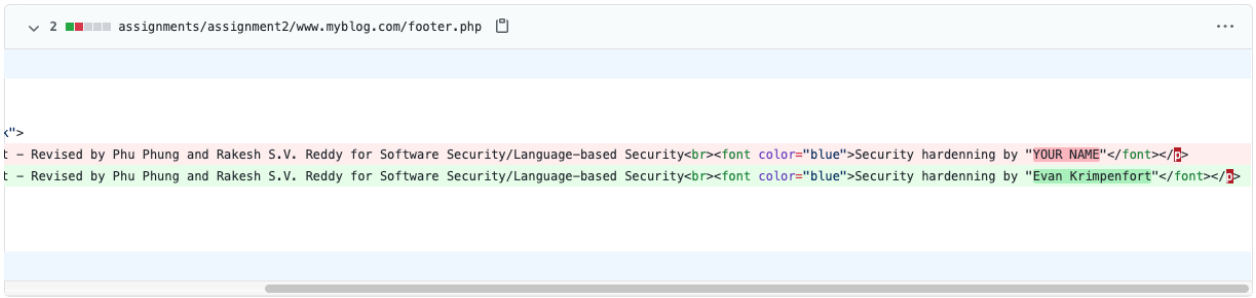

Figure 11: Footer was changed