ID:___**640315**_ **Name:**___**สิทธิกร เฉลิมกิตติชัย**____________ **Section :** ________01 ______

Save this answer sheet as " **Lab5-6088xxx.docx**" (Removing all figures will help reduce the file size).
Submit this file to the lab folder in e-learning website according to your session.

Lab 5 : Web Security

Follow Lab 6 document (Lab6.pdf) and answer these questions:

Part I: XSS

Question 1:

1) What is the username you have tested? _____<test>________________________
2) Does the website display correctly? _N____ (Y/N)
3) If not, why does it display incorrectly? _____น่าจะป้องกัน พวกเครื่องที่เป็นคำสั่งต่างๆ____________
4) Does the website print out every character you input? (hint: you might need to "view page source", by pressing Ctrl+u) ___N____ (Y/N)

Question 2:

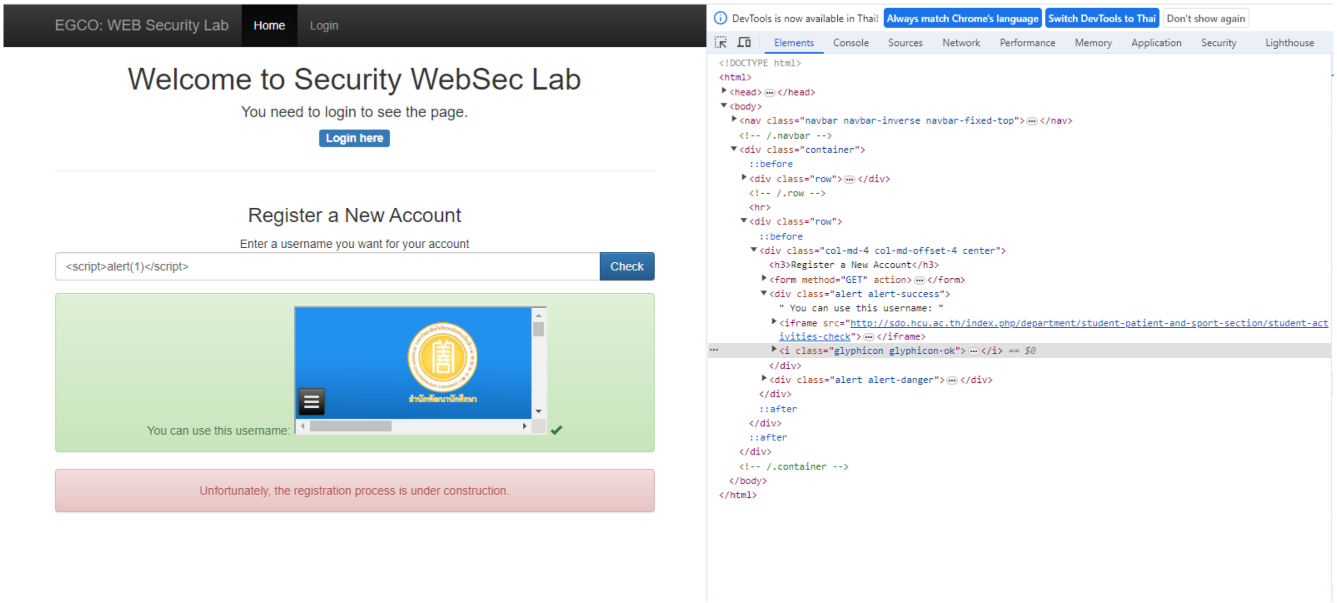
1) Try input "<h1>Hello</h1>", does it displays the word "Hello" in large font? ______Y____ (Y/N)

   Try using tag <iframe> to see if we can include other website into this page. The format is "<iframe src="http://...."></iframe>".

   Choose any website's URL you want.

   (If it displays a blank box, the website you chose might have XSS protection. Try other website.)

2) What is your final input string? _________________<iframe src="http://sdo.hcu.ac.th/index.php/department/student-patient-and-sport-section/student-activities-check"></iframe>________________________
3) Capture the screen of the result.



Welcome to Security WebSec Lab

You need to login to see the page.

Register a New Account

Enter a username you want for your account

<script>alert(1)</script>

You can use this username: ✓

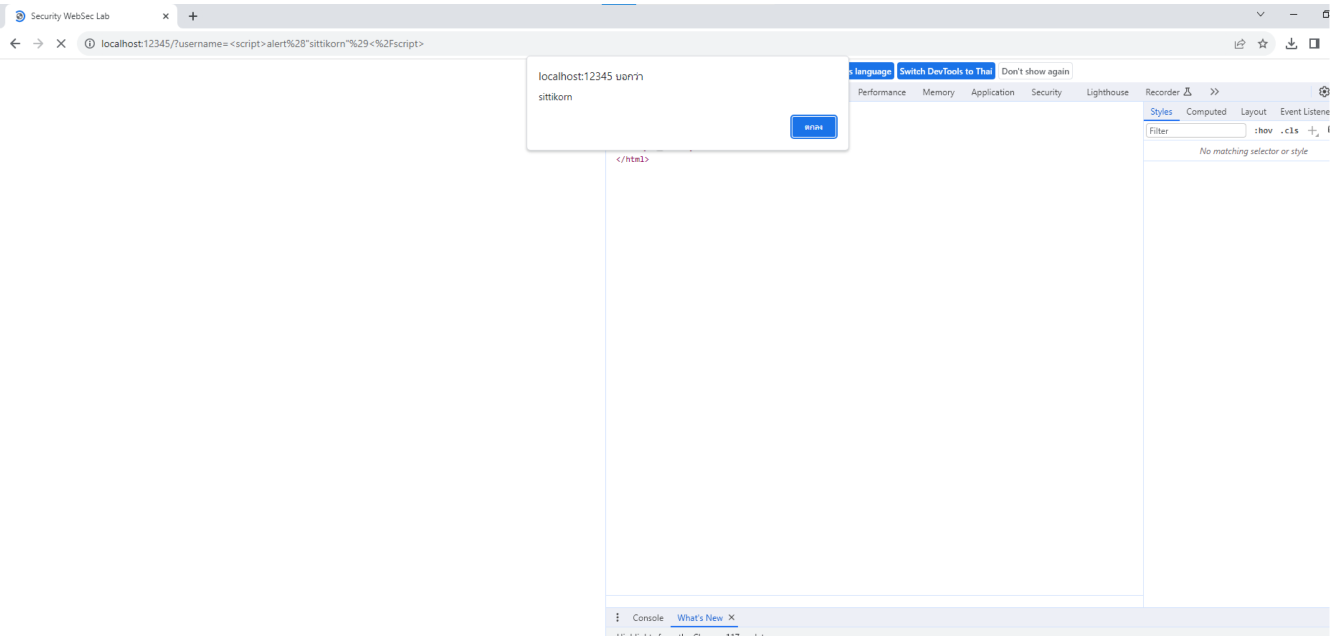
Unfortunately, the registration process is under construction.

```
<!DOCTYPE html>
<html>
 ▶<head> … </head>
 ▼<body>
   ▶<nav class="navbar navbar-inverse navbar-fixed-top"> … </nav>
    <!-- /.navbar -->
   ▼<div class="container">
      ::before
     ▶<div class="row"> … </div>
      <!-- /.row -->
      <hr>
     ▼<div class="row">
        ::before
       ▼<div class="col-md-4 col-md-offset-4 center">
          <h3>Register a New Account</h3>
         ▶<form method="GET" action> … </form>
         ▼<div class="alert alert-success">
            " You can use this username: "
           ▶<iframe src="http://sdo.hcu.ac.th/index.php/department/student-patient-and-sport-section/student-activities-check"> … </iframe>
           ▶<i class="glyphicon glyphicon-ok"> … </i> == $0
          </div>
         ▶<div class="alert alert-danger"> … </div>
        </div>
        ::after
      </div>
      ::after
    </div>
    <!-- /.container -->
  </body>
</html>
```

Question 3:

1) Try input this username: “<script>alert(1)</script>” (without quote).
   What does it show? ____________1____________________________________

2) Change the input above to display your name, and capture screen the result.



localhost:12345/?username=<script>alert%28"sittikorn"%29<%2Fscript>

localhost:12345 บอกว่า

sittikorn

Let’s try this input and answer what it displays.

3) <script>alert(document.title)</script> → ________Security WebSec Lab________

4) <script>alert(document.location)</script> →
   http://localhost:12345/?username=%3Cscript%3Ealert%28document.location%29%3C%2Fscript%3E____________________

5) <script>alert(document.referrer)</script> →

______http://localhost:12345/?username=%3Cscript%3Ealert%28document.location%29%3C%2Fscript%3E__________________________

6) <script>alert(document.cookie)</script> → _____username=anonymous________

Question 4:

In a real situation, a victim would NOT manually type javascript code and hit "Check" button himself.

1) Do you think how an attacker makes a victim executes the javascript code? ______ ___________Get data and change content text page in website__________________
____
____
____
2) If the trustworthy websites (such as Google, Facebook, Apple) have this vulnerability, you think what could be the worst thing that happen to their users? _ ________________________________Cheat and steal___________________________
____

Part II: Cookie

Question 5:

To change a cookie value, type this in the developer tools panel **document.cookie="username=alice"** , then enter.

1) Try viewing the cookie value again. Does the value change? __Y____ (Y/N
If yes, what is the new value? _______Username=alice__________________________

Press F5 to reload the page.

2) Do you still on the same page? _____N____ (Y/N)
If no, then what is the URL of the page? ___http://localhost:12345/user.php______
3) Under what user, you have logged in as? ________alice____________

Question 6:

Open a new tab in the browser, and go to the same URL.
http://muict.securitylab.ninja/websec/

1) Are you still logged in? _N_____ (Y/N)

Now, close every tabs of Firefox and also exit Firefox browser. Then, open Firefox again.

2) If you go to the same URL, are you still logged in? _____N_____ (Y/N)
3) Try refresh the page about 3 times. Are you still logged in? ___N____ (Y/N)

Part III: SQL Injection

Question 7:

Try login again by appending a single quote (’) to the username, such that it becomes **alice'** , and with the same password.

1) What is the SQL query now? You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'pass'' at line 1select * from users where username='alice'' and password='pass'
2) Did it run correctly (without error) ? _N_____ (Y/N)
   If not, you think why the input caused an error? ‘ ไม่ครบคู่

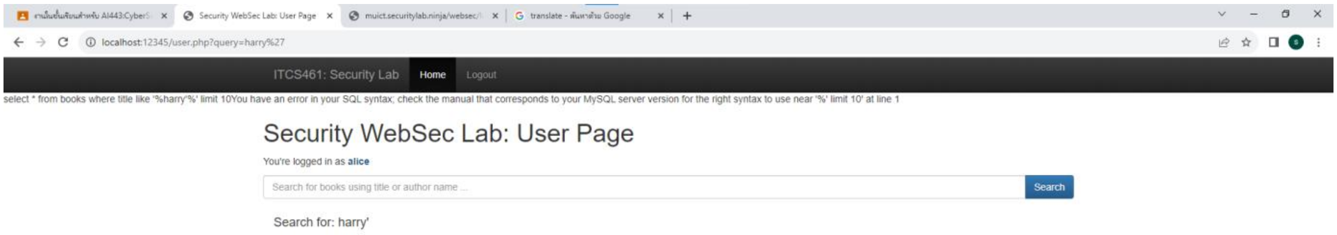
   If using double dash (--) in SQL statement means commenting until the end of the line.
3) What do you think will happen if you use username as “**alice' --** ” (with a space at the end) ? comment all after – and then I can login it.

   Try it

Question 8:

Checking if this form (user.php) is vulnerable to SQL injection. (hint: make it causes an error.)

1) What is the input you use to make it errors?
   select * from books where title like '%harry'%' limit 10You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' limit 10' at line 1
2) Capture a screenshot of when it errors.


งานเริ่มต้นเรียนสำหรับ AI443:CyberS
Security WebSec Lab: User Page
muict.securitylab.ninja/websec/
translate - ค้นหาด้วย Google
localhost:12345/user.php?query=harry%27
ITCS461: Security Lab
Home
Logout
Search for books using title or author name ...
Search

select * from books where title like '%harry'%' limit 10You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' limit 10' at line 1

Security WebSec Lab: User Page

You're logged in as alice

Search for: harry'

3) What would happen if we use the trick like in question 7, by entering just "' -- " (single-quote, space, dash, dash, space)? ___Show all data______________________
____

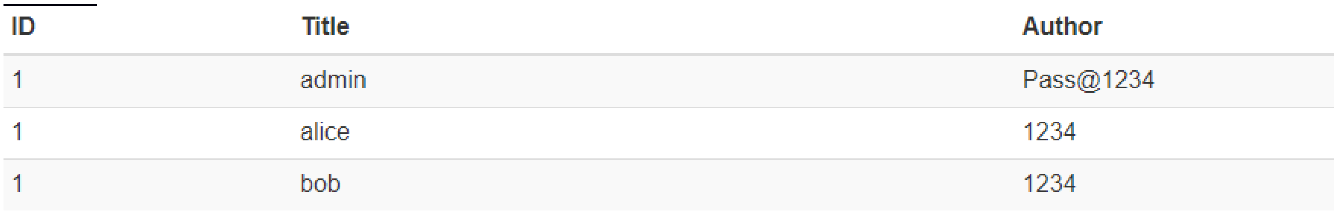
Question 9:

From SQL query displayed in the login page (in Question 7). Look closely what we can learn from this query.

1) What is the table's name used in login page? _____users _________________
2) What are the two column's names used in login page? ________Username___ and ______password_________

Question 10:

1) What is the final input after replacing column and table name? ________________ ________________________' and false UNION SELECT 1, username, password FROM users --____
2) How many users in the system? _____3_____
3) What are their usernames and passwords? _________________________________ _______________________ ______



ID	Title	Author
1	admin	Pass@1234
1	alice	1234
1	bob	1234

Part IV: Command Injection

Question 11:

1) Did the web page show the result of the command “ls”? ______Y____ (Y/N)
   If yes, then you would know all the files in current directory.
2) What are the file names in this directory? (list only .php file) __________________
   ______admin.php
   config.php
   index.php
   login.php
   logout.php
   user.php____
3) In one of the .php files, it contains usernames and passwords to connect to MySQL database. Find out what file it is? _______config.php___________________
   ______
4) What are the usernames and passwords for connecting database? _______________
   ___________username = lab9 passwords = MUICTCTFPassword_______________
   __________________________database = lab0________