CHANDIGARH UNIVERSITY

UNIVERSITY INSTITUTE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Submitted By:	Submitted To:
Subject Name	WMS Lab
Subject Code	20CSP-338
Branch	BE-CSE
Semester	5th Sem

LAB INDEX

NAME: SUBJECT NAME:

UID: SUBJECT CODE: 20CSP-338

SECTION:

Sr. No	Program	Date	Evaluation				Sign
			LW (12)	VV (10)	FW (8)	Total (30)	

Worksheet Experiment 1

Student Name: UID:

Branch: CSE Section/Group:

Semester: 5th Sem Date of Performance:

Subject Name: WMS Lab Subject Code: 20CSP-338

1. Aim/Overview of the practical:

   Open any website on computer system and identify http packet on monitoring tool like Wireshark.

2. Objective:

   To analyse http traffic.

3. Introduction:

   Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.
   It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

4. Steps/Method:

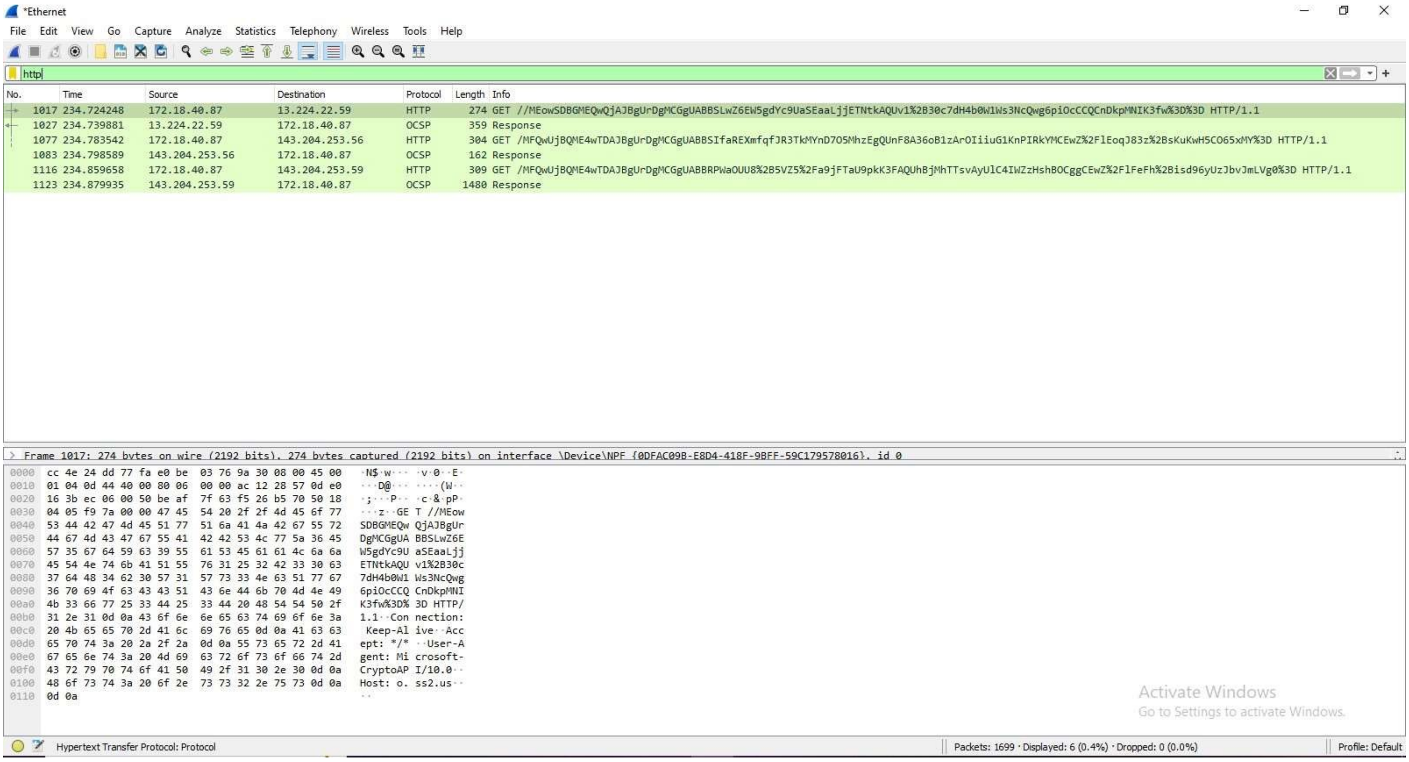
1. Open Wireshark
2. Click on "Capture > Interfaces". A pop-up window will display.
3. You'll start capture traffic that goes through your ethernet driver.

4. Visit the URL that you wanted to capture the traffic from.

5. Go back to your Wireshark screen and press Ctrl + E to stop capturing.

6. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.

5. Outcomes:



http

```
No.    Time        Source          Destination     Protocol Length Info
  1017 234.724248  172.18.40.87    13.224.22.59    HTTP      274 GET //MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D HTTP/1.1
  1027 234.739881  13.224.22.59    172.18.40.87    OCSP      359 Response
  1077 234.783542  172.18.40.87    143.204.253.56  HTTP      304 GET /MFQwUjBQME4wTDAJBgUrDgMCGgUABBSIfaREXmfqfJR3TkMYnD7O5MhzEgQUnF8A36oB1zArOIiiuG1KnPIRkYMCEwZ%2FlEoqJ83z%2BsKuKwH5CO65xMY%3D HTTP/1.1
  1083 234.798589  143.204.253.56  172.18.40.87    OCSP      162 Response
  1116 234.859658  172.18.40.87    143.204.253.59  HTTP      309 GET /MFQwUjBQME4wTDAJBgUrDgMCGgUABBRPWaOUU8%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMhTTsvAyUlC4IWZzHshBOCggCEwZ%2FlFeFh%2Bisd96yUzJbvJmLVg0%3D HTTP/1.1
  1123 234.879935  143.204.253.59  172.18.40.87    OCSP     1480 Response
```

```
> Frame 1017: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF_{0DFAC09B-E8D4-418F-9BFF-59C179578016}, id 0
```

```
0000  cc 4e 24 dd 77 fa e0 be  03 76 9a 30 08 00 45 00   ·N$·w···  ·v·0··E·
0010  01 04 0d 44 40 00 80 06  00 00 ac 12 28 57 0d e0   ···D@···  ····(W··
0020  16 3b ec 06 00 50 be af  7f 63 f5 26 b5 70 50 18   ·;···P··  ·c·&·pP·
0030  04 05 f9 7a 00 00 47 45  54 20 2f 2f 4d 45 6f 77   ···z··GE  T //MEow
0040  53 44 42 47 4d 45 51 77  51 6a 41 4a 42 67 55 72   SDBGMEQw  QjAJBgUr
0050  44 67 4d 43 47 67 55 41  42 42 53 4c 77 5a 36 45   DgMCGgUA  BBSLwZ6E
0060  57 35 67 64 59 63 39 55  61 53 45 61 61 4c 6a 6a   W5gdYc9U  aSEaaLjj
0070  45 54 4e 74 6b 41 51 55  76 31 25 32 42 33 30 63   ETNtkAQU  v1%2B30c
0080  37 64 48 34 62 30 57 31  57 73 33 4e 63 51 77 67   7dH4b0W1  Ws3NcQwg
0090  36 70 69 4f 63 43 43 51  43 6e 44 6b 70 4d 4e 49   6piOcCCQ  CnDkpMNI
00a0  4b 33 66 77 25 33 44 25  33 44 20 48 54 54 50 2f   K3fw%3D%  3D HTTP/
00b0  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con  nection:
00c0  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 41 63 63    Keep-Al  ive··Acc
00d0  65 70 74 3a 20 2a 2f 2a  0d 0a 55 73 65 72 2d 41   ept: */*  ··User-A
00e0  67 65 6e 74 3a 20 4d 69  63 72 6f 73 6f 66 74 2d   gent: Mi  crosoft-
00f0  43 72 79 70 74 6f 41 50  49 2f 31 30 2e 30 0d 0a   CryptoAP  I/10.0··
0100  48 6f 73 74 3a 20 6f 2e  73 73 32 2e 75 73 0d 0a   Host: o.  ss2.us··
0110  0d 0a                                              ··
```

Activate Windows
Go to Settings to activate Windows.

```
Hypertext Transfer Protocol: Protocol        Packets: 1699 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)        Profile: Default
```

Learning outcomes (What I have learnt):

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe single small file (e.g., simple html file) request/response behavior and the request/response behavior for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behavior. Observe request/response behavior for a page that needs authentication.

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30

Worksheet Experiment 2

Student Name: UID:

Branch: CSE Section/Group:

Semester: 5th Sem Date of Performance:

Subject Name: WMS Lab Subject Code: 20CSP-338

1. Aim/Overview of the practical:

Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.

2. Objective:

To test HTML and XSS injection.

3. Steps/Method:

HTML Injection

1. Open website : OWASP Mutillidae II: Web Pwn in Mass Production (URL:http://128.198.49.198:8102/mutillidae/index.php?page=documentation/usageinstructions.php)
2. Now, we'll be redirected to the web page which is suffering from an HTML Injection vulnerability which allows the user to submit his entry in the blog.
3. On the left-hand side, click on OWASP 2017 A1-injection(others) HTML injection Add to your blog
4. Welcome to blog window will appear on the screen. Now, let's try to inject malicious code. Enter the HTML code inside the given text area in order to set up the HTML attack.

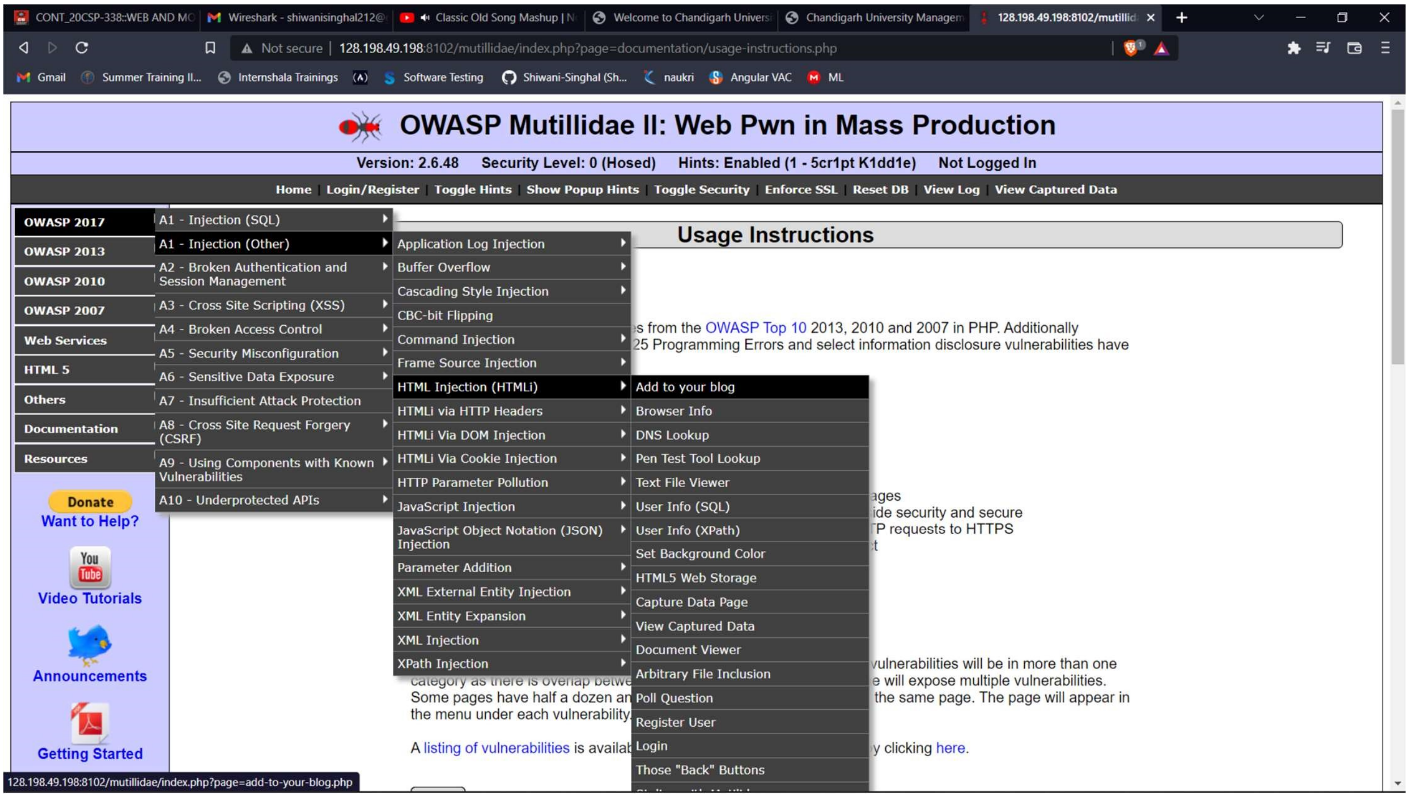
XSS Injection:

1. Open the link https://xss-game.appspot.com/level1 (or Google XSS game website). 2. If the search field is vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script as shown below:
“<script>alert (“Hello”) </script>”

3. Then after clicking on the “Search” button, the entered script will be executed. The script typed into the search field gets executed. This just shows the vulnerability of the XSS attack.

4. Outcomes:

HTML Injection



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.48 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Usage Instructions

...s from the OWASP Top 10 2013, 2010 and 2007 in PHP. Additionally ...25 Programming Errors and select information disclosure vulnerabilities have

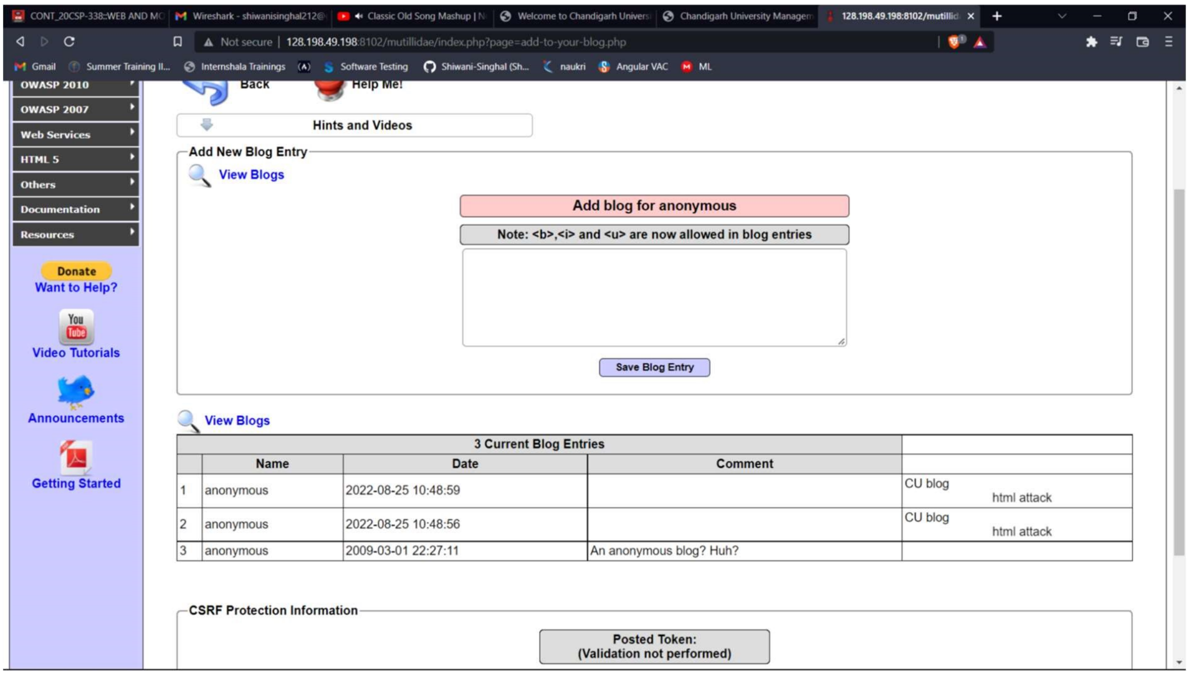
...ages ...ide security and secure ...P requests to HTTPS

...category as there is overlap betw... ...vulnerabilities will be in more than one ...e will expose multiple vulnerabilities. Some pages have half a dozen an... ...the same page. The page will appear in the menu under each vulnerability...

A listing of vulnerabilities is availab... ...y clicking here.

128.198.49.198:8102/mutillidae/index.php?page=add-to-your-blog.php

CONT_20CSP-338::WEB AND MC
Wireshark - shiwanisinghal212@
Classic Old Song Mashup | N
Welcome to Chandigarh Univers
Chandigarh University Managem
128.198.49.198:8102/mutillid
Not secure | 128.198.49.198:8102/mutillidae/index.php?page=documentation/usage-instructions.php
Gmail
Summer Training Il...
Internshala Trainings
Software Testing
Shiwani-Singhal (Sh...
naukri
Angular VAC
ML
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Announcements
Getting Started
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Broken Access Control
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Insufficient Attack Protection
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Underprotected APIs
Application Log Injection
Buffer Overflow
Cascading Style Injection
CBC-bit Flipping
Command Injection
Frame Source Injection
HTML Injection (HTMLi)
HTMLi via HTTP Headers
HTMLi Via DOM Injection
HTMLi Via Cookie Injection
HTTP Parameter Pollution
JavaScript Injection
JavaScript Object Notation (JSON) Injection
Parameter Addition
XML External Entity Injection
XML Entity Expansion
XML Injection
XPath Injection
Add to your blog
Browser Info
DNS Lookup
Pen Test Tool Lookup
Text File Viewer
User Info (SQL)
User Info (XPath)
Set Background Color
HTML5 Web Storage
Capture Data Page
View Captured Data
Document Viewer
Arbitrary File Inclusion
Poll Question
Register User
Login
Those "Back" Buttons



128.198.49.198:8102/mutillidae/index.php?page=add-to-your-blog.php

Add New Blog Entry

Add blog for anonymous

Note: <b>,<i> and <u> are now allowed in blog entries

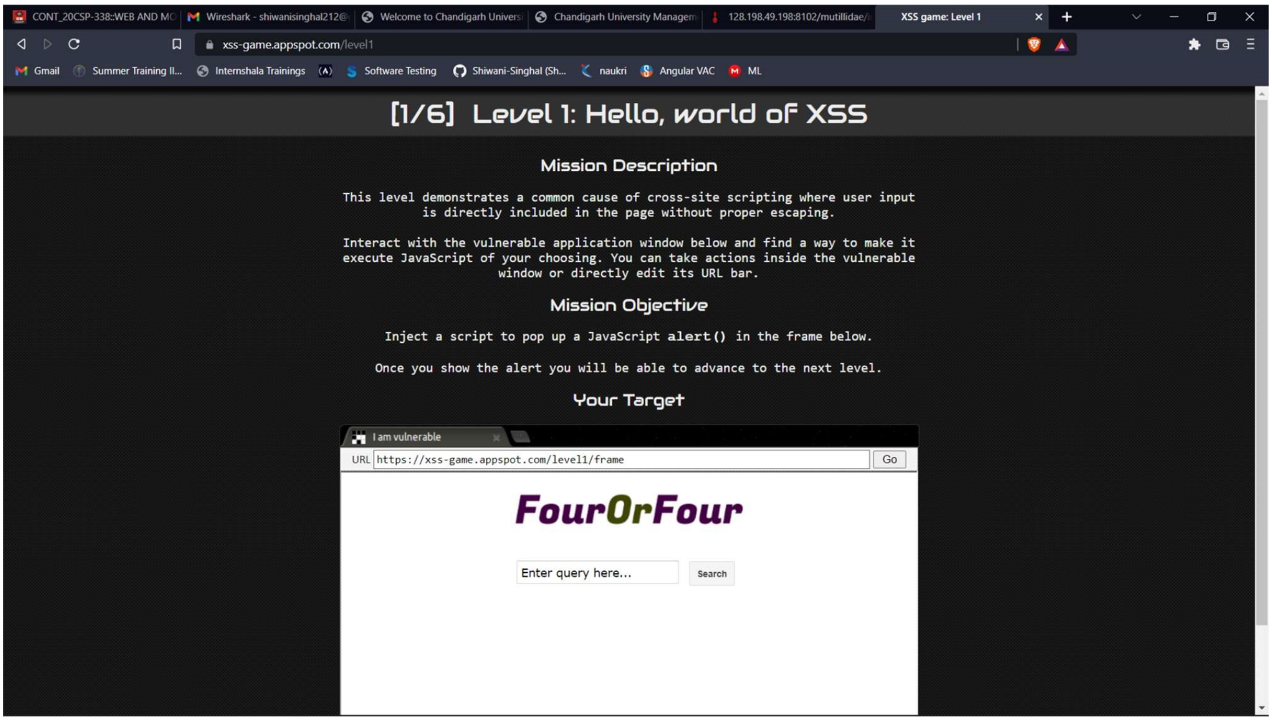
View Blogs

3 Current Blog Entries				
	Name	Date	Comment	
1	anonymous	2022-08-25 10:48:59		CU blog html attack
2	anonymous	2022-08-25 10:48:56		CU blog html attack
3	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?	

CSRF Protection Information

Posted Token:
(Validation not performed)

<u>XSS Injection</u>


CONT_20CSP-338::WEB AND MC
Wireshark - shiwanisinghal212@
Welcome to Chandigarh Univers
Chandigarh University Managem
128.198.49.198:8102/mutillidae/
XSS game: Level 1
xss-game.appspot.com/level1
Gmail
Summer Training II...
Internshala Trainings
Software Testing
Shiwani-Singhal (Sh...
naukri
Angular VAC
ML

[1/6] Level 1: Hello, world of XSS

Mission Description

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

Mission Objective

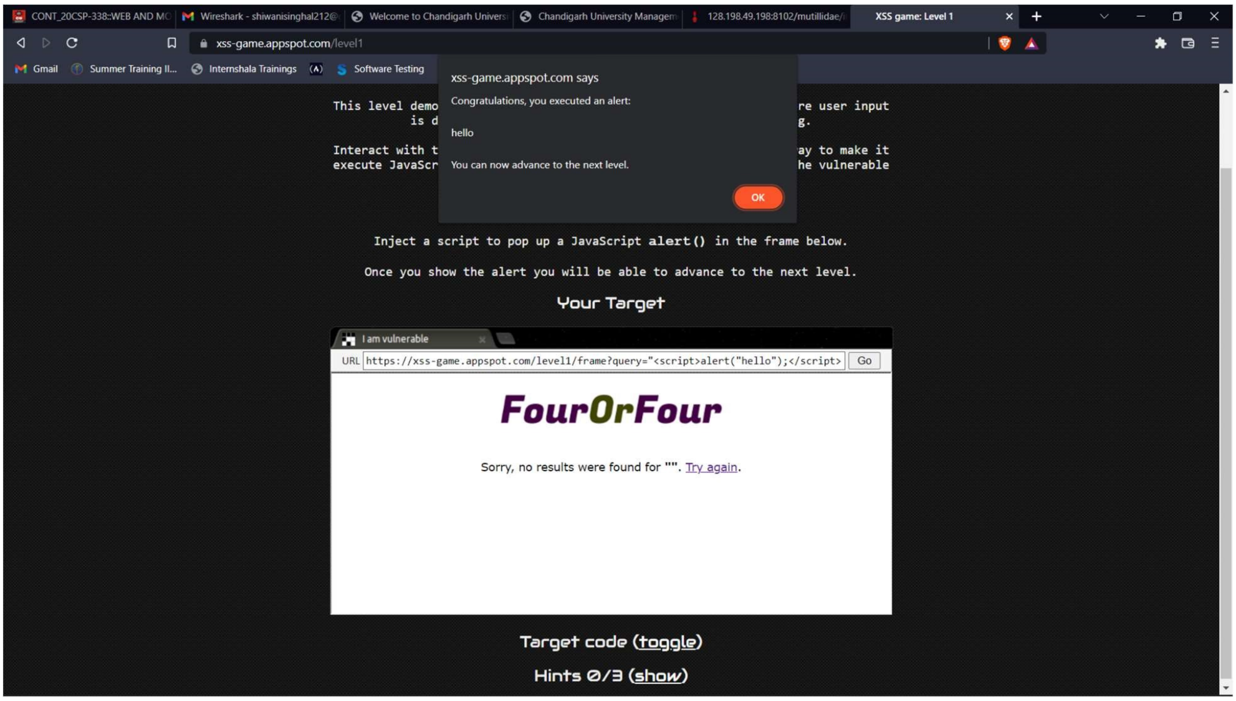
Inject a script to pop up a JavaScript **alert()** in the frame below.

Once you show the alert you will be able to advance to the next level.

Your Target

URL https://xss-game.appspot.com/level1/frame Go

FourOrFour
Enter query here...
Search


CONT_20CSP-338::WEB AND MC
Wireshark - shiwanisinghal212@
Welcome to Chandigarh Univers
Chandigarh University Managem
128.198.49.198:8102/mutillidae/
XSS game: Level 1
xss-game.appspot.com/level1
Gmail
Summer Training II...
Internshala Trainings
Software Testing

xss-game.appspot.com says

Congratulations, you executed an alert:

hello

You can now advance to the next level.

This level demo… re user input is d… g.

Interact with t… ay to make it execute JavaScr… he vulnerable

Inject a script to pop up a JavaScript **alert()** in the frame below.

Once you show the alert you will be able to advance to the next level.

Your Target

URL https://xss-game.appspot.com/level1/frame?query="<script>alert("hello");</script> Go

Sorry, no results were found for "". Try again.

Target code (toggle)

Hints 0/3 (show)

Learning outcomes (What I have learnt):

We have learned what HTML injection is and XSS injection. An overview of how these attacks is constructed and applied to real system. If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system. As a result, the attacker can steal the user's active session cookie and can be the harmful for the website.

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30