

Batch: __C3_____ Roll No.: 110

Experiment No. 5

Title: XSS using dvwa and burp suite

Objective: To hack dummy websites like dvwa using XSS

Expected Outcome of Experiment:

CO	Outcome
CO3	Identify and analyze web attacks

Books/ Journals/ Websites referred:

<https://portswigger.net/web-security/all-labs>

<https://pentest-tools.com/blog/xss-attacks-practical-scenarios#xss-attack-1-hijacking-the-users-session>

Abstract:-

Cross-site scripting (XSS) is a security vulnerability commonly found in web applications. It occurs when an attacker injects malicious scripts into web pages viewed by other users. These scripts can execute in the context of the user's browser, allowing the attacker to steal sensitive information, hijack sessions, or deface websites. XSS attacks can be categorized as stored, reflected, or DOM-based, depending on how the malicious payload is delivered to the victim. Preventive measures such as input validation, output encoding, and using security mechanisms like Content Security Policy (CSP) are essential for mitigating XSS risks and ensuring the security of web applications.

Related Theory: -

Time left 0:28:24 Hide

Question 1

Not yet answered

Marked out of 1.00

Flag question

What is full form of CAPTCHA ?

Select one:

- ☒ a. Completely Automated Public Turing Test to tell Computers and Humans Apart
- ☐ b. Computer Automated Public Turing Test to tell Computers and Humans Apart
- ☐ c. Completely Automated Private Turing Test to tell Computers and Humans Apart
- ☐ d. Completely Automated Test to tell Computers and Humans Apart

[Clear my choice](#)

Next page

Question 2

Not yet answered

Marked out of 1.00

Flag question

CAPTCHA is used to prevent which type of attack on systems?

Select one:

- ☐ a. Spoofing Attack
- ☐ b. Snooping Attack
- ☐ c. Modification Attack
- ☒ d. Denial of Service Attack

[Clear my choice](#)

Previous page

Next page

Question 3

Not yet
answered

Marked out of
1.00

🚩 [Flag question](#)

Why is CAPTCHA generated randomly?

Select one:

- ☒ a. The attacker cannot guess the next CAPTCHA even if he/she has the program code
- ☐ b. To make the program complex
- ☐ c. to make the program more efficient

[Clear my choice](#)

[Previous page](#)

[Finish attempt ...](#)



I'm not a robot

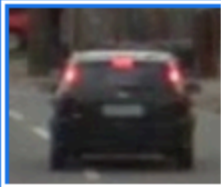


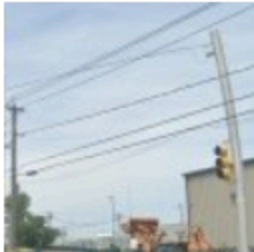


reCAPTCHA
[Privacy](#) - [Terms](#)




submit


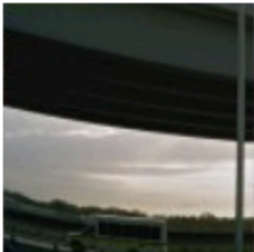

submit




Select all images with
cars













VERIFY



 I'm not a robot



submit

127.0.0.1:5500 says

success

OK

Select all images with
crosswalks



VERIFY

```
<html>

<head>

                                <script
src="https://code.jquery.com/jquery-2.2.4.min.js"></script>

                                <script
src="https://www.google.com/recaptcha/api.js"></script>

</head>

<body>

<form id="myForm" onsubmit="return checkRecaptcha()">

    <input type="text" name="inputField">

    <input type="submit" value="Submit">

                                <div                                class="g-recaptcha"
data-sitekey="6LdIQIkpAAAAAPFqDK00itsJOZ2p8lteEVNskqfA"></div>

</form>

<script>

function checkRecaptcha() {

    var response = grecaptcha.getResponse();

    if (response.length == 0) {

        alert("Please complete the reCAPTCHA challenge.");

    }

}
```



```
        return false; // Prevent form submission

    } else {

        // reCAPTCHA challenge completed, proceed with form
        submission

        return true;

    }

}

</script>

</body>

</html>
```

Conclusion:-

Thus we have implemented google recaptcha in our website. Google reCAPTCHA is a free service provided by Google that helps protect websites from spam and abuse. It uses advanced risk analysis techniques to distinguish between humans and bots, thereby making it harder for bots to submit forms or access restricted areas of a website. **Spam Protection:** One of the primary reasons for using reCAPTCHA is to prevent spam submissions in forms such as contact forms, registration forms, and comment sections. Bots can automatically fill out and submit these forms, flooding the website with spam.