**Task 1:**

1. [SQL injection vulnerability in WHERE clause allowing retrieval of hidden data](https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data)

A screenshot of a computer

Description automatically generated

I have performed the basic SQL attack in the where clause

A screenshot of a computer

Description automatically generated

1. SQL injection vulnerability allowing login bypass

A screenshot of a computer

Description automatically generated

I have performed the SQL attack and got the admin access

A screenshot of a computer

Description automatically generated

1. [Reflected XSS into HTML context with nothing encoded](https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded)



I have performed the basic scripting attack using the alert function

A screenshot of a search box

Description automatically generated

1. [Stored XSS into HTML context with nothing encoded](https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded)

A pair of christmas stockings

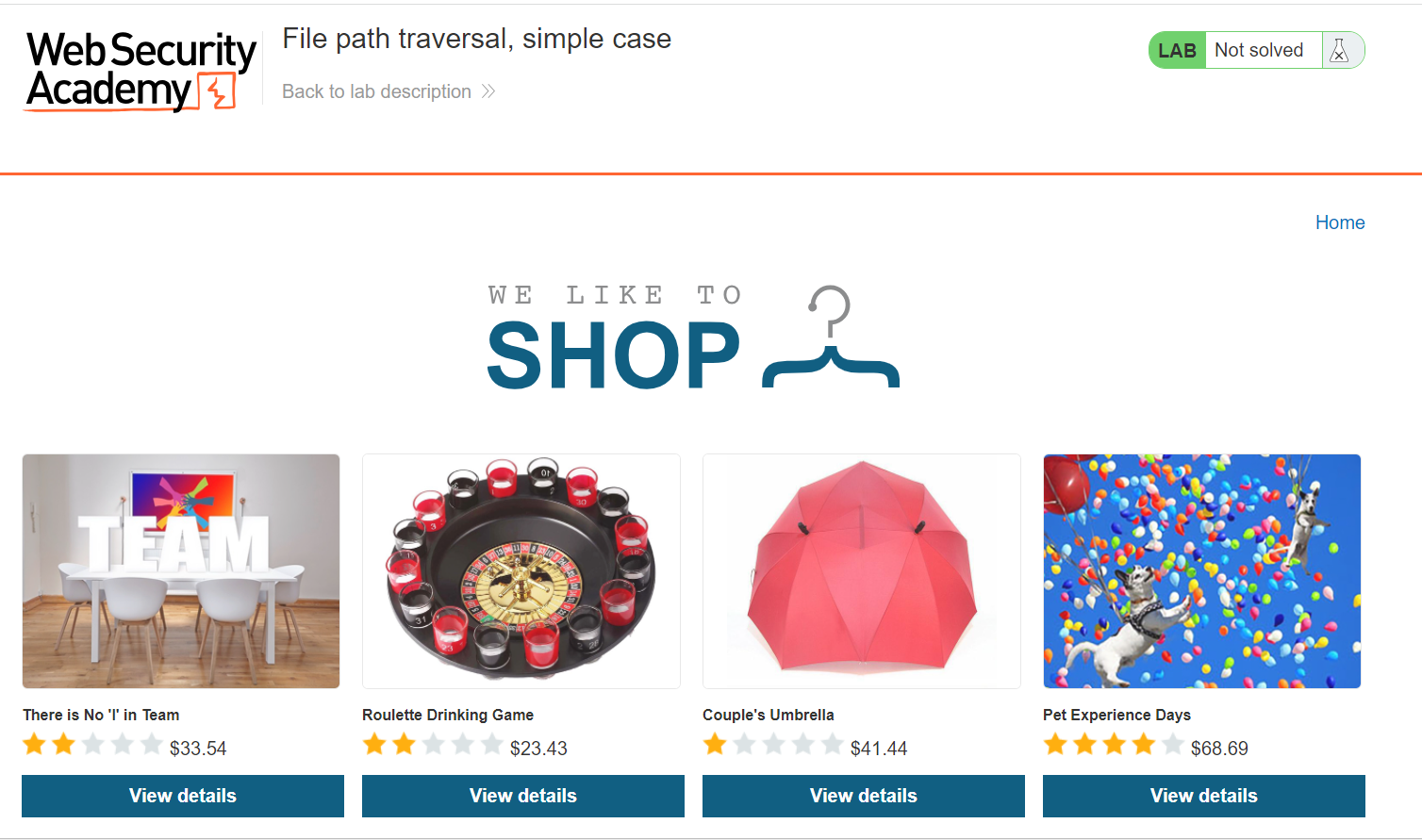
Description automatically generated

I have performed the scripting attack by using the input field of posting the comment

A screenshot of a computer

Description automatically generated

1. [File path traversal, simple case](https://portswigger.net/web-security/file-path-traversal/lab-simple)



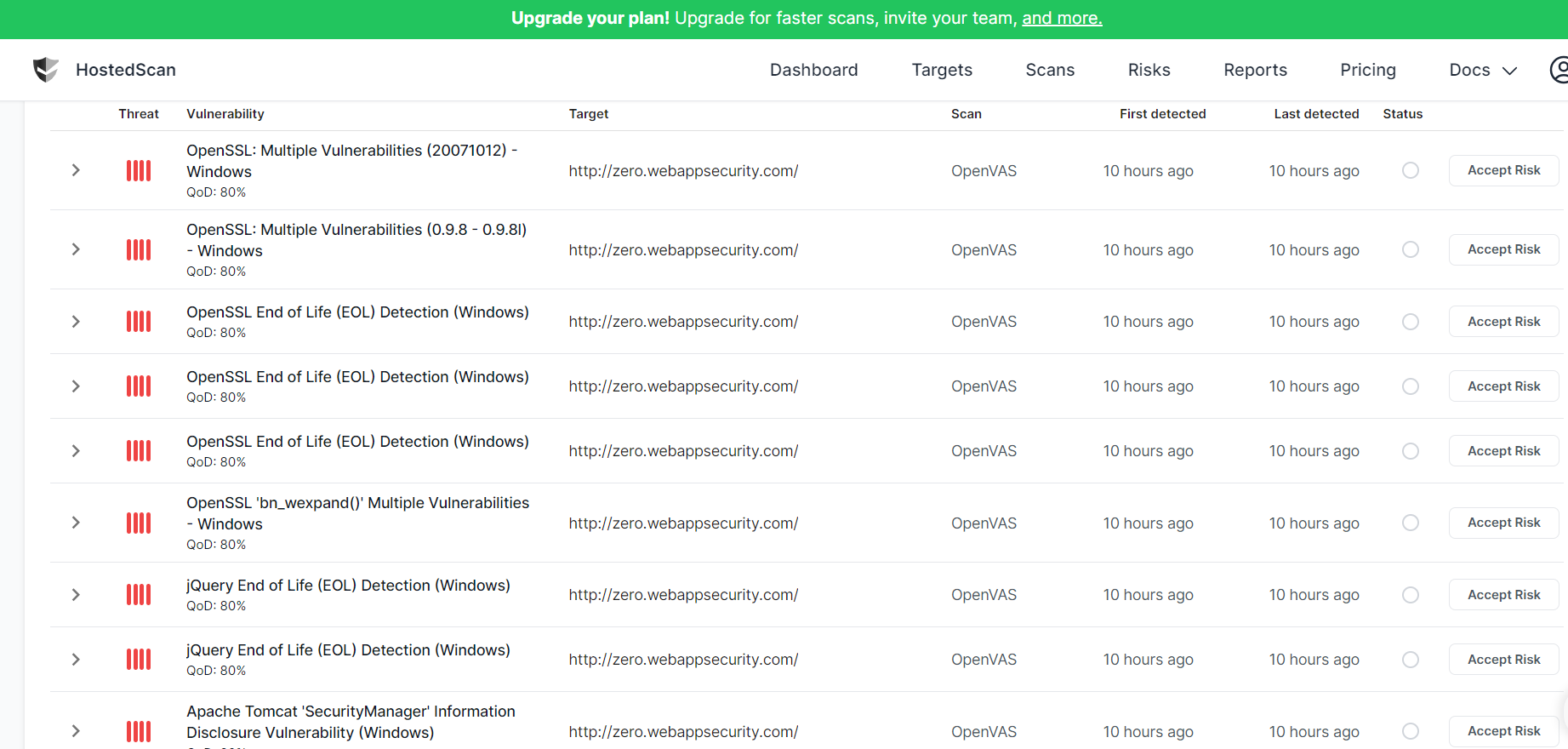
Instead of using burp suite I have changed the file path in the console

A screenshot of a computer

Description automatically generated

**Task 2:**

For this task I have used the “Hostedscan” an online vulnerability scanner as the netsparker is not available as an open source after trying the automated vulnerability scan this is the output of the critical vulnerabilities.



So, I chose the first vulnerability to write the report. The vulnerability is "OpenSSL: Multiple Vulnerabilities (20071012) - Windows."

OpenSSL: Multiple Vulnerabilities (20071012) - Windows

Critical

cvss score: 9.3

Description:

OpenSSL is prone to multiple vulnerabilities.

The following vulnerabilities exist:

- A flaw in OpenSSL's DTLS implementation which could lead to the compromise of clients and servers with DTLS enabled. (CVE-2007-4995)

- An off-by-one error in SSL\_get\_shared\_ciphers(), a function that should normally only be used for logging or debugging. (CVE-2007-5135)

Solution:

Update to version 0.9.8f or later.

**Task 3:**

**Website URL:** <http://testasp.vulnweb.com/>

**Description:** The website "testasp.vulnweb.com" is a vulnerable test site designed for educational and testing purposes. It is intentionally insecure to help security professionals understand and practice identifying vulnerabilities.

**Vulnerability Description:**

The website "testasp.vulnweb.com" is intentionally designed with known vulnerabilities:

SQL Injection Vulnerability: The site is susceptible to SQL injection attacks, which allow an attacker to manipulate the database by injecting malicious SQL code into input fields.

Cross-Site Scripting (XSS) Vulnerability: The site contains a cross-site scripting vulnerability, which allows an attacker to inject malicious scripts into web pages viewed by other users, potentially leading to data theft or session hijacking.

**Screenshots:**

**A screenshot of a computer

Description automatically generated**

By seeing the post we can understand the that the username is admin then we can perform the very basic sql attack to gain the admin access.

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

There we go, we got the admin access and we can even post the message which is vulnerable to the XSS(cross side scripting).

**Potential Impact:**

The impact of these vulnerabilities can be significant, including:

Unauthorized access to the website's database.

Theft of sensitive data, including user credentials.

The execution of malicious scripts on users' browsers.