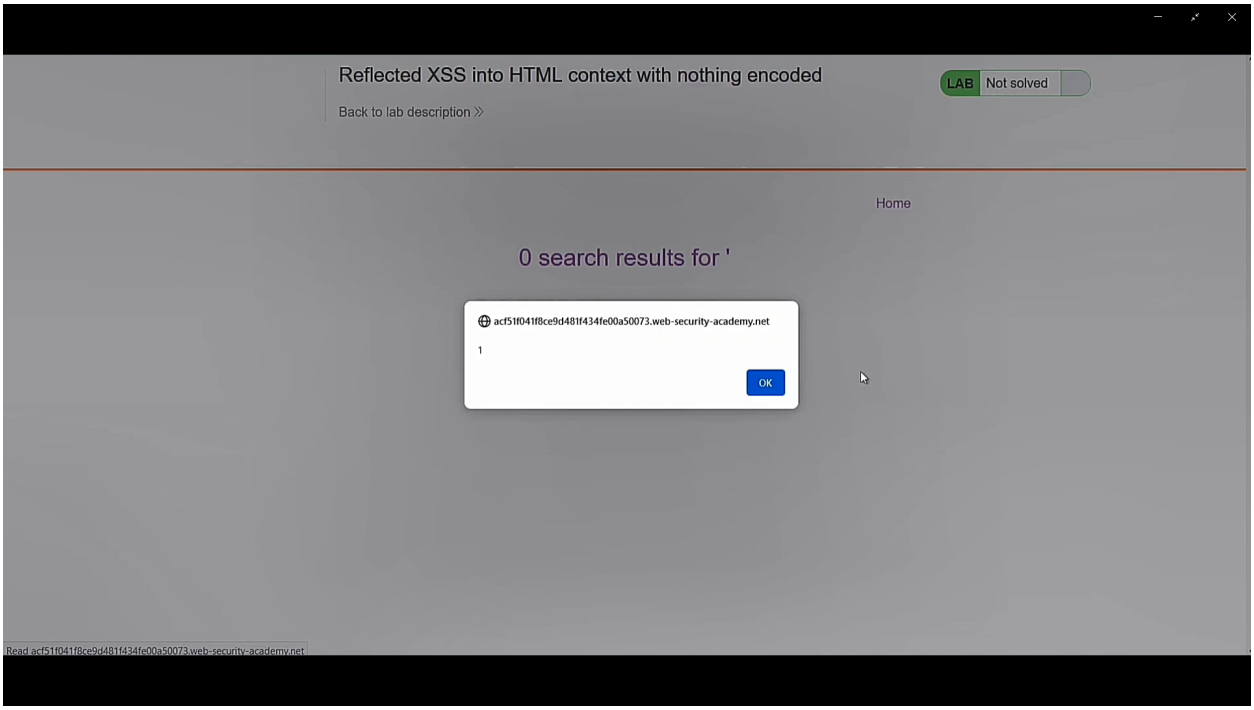
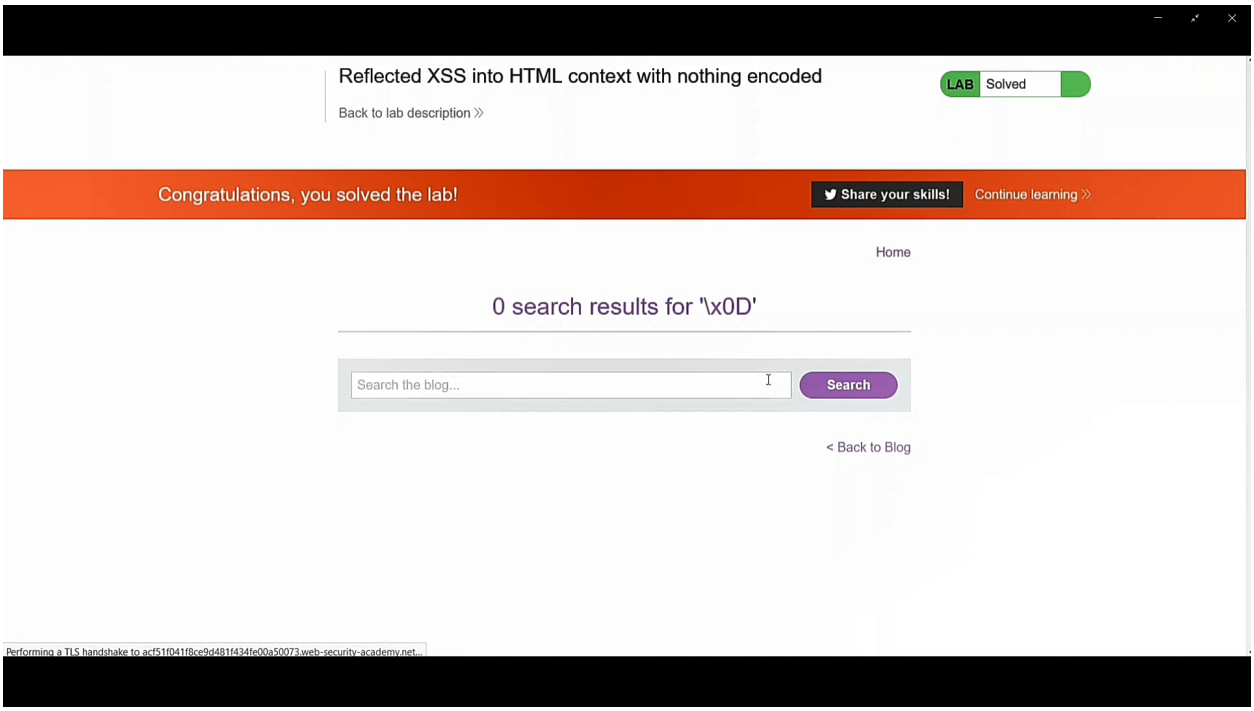
Testing of vulnerablity on portswigger labs





Here is the attached link of the video:-

https://drive.google.com/file/d/1PhAxXrOGM3509q_SyO6e_tWOrS4qB3HL/view?usp=sharing

Detailed Scanned Report of website:-

http:// zero.webappsecurity.com/

Summary of the Report:

Severeity	Medium	Low
1	1	6

1) Issues in the security of communication: The communications done by the user's device or browser by the server protocol is not secured as its port is open and is not encrypted. It is using the "HTTP" which is open and unencrypted, it should be "HTTPS" in order to be encrypted. As a result of this vulnerability, the attackers may perform "SQL injections" and "cross-site scripting" in order and motive to steal the data such as card details of the bank, cookies and sometimes even passwords.

Solutions suggested: In order to protect your website, it's very necessary to encrypt the webserver with HTTPS as the initial action.

2) Absence of content security policy: Content security policy is very essential for the blocking of the process of cross-site scripting in order to protect the site. It protects the site from the vulnerability to XSS, without which hackers can easily exploit.

Solutions suggested: Set the response of every HTTP as a content security header.

3) Absence of Security header X-frame-options: It prevents the user from getting a victim to the click-hijacking, it blocks the third party. It avoids the site getting vulnerable to the "man in the middle attack" where the path towards the server can get diverted to the third party website which gives a response similar to the original website.

4) Absence of Security header X-XSS protection: It stops the website from loading when the reflected cross-site scripting attack is detected and thus protect the

website from vulnerability.

Solutions suggested: Set the X-XSS header protection as X-XSS-protection 1; mode=block.

5) Absence of the security header X-Content-Type-Options:

In order to resolve this vulnerability it's highly recommended to X-Content-Type-Options: nonsiff.

6) Missing Security Header Referer Policy: It controls the limit of information about referrer the browser will send for each request originated from current web applications.

7) Server technology used information technology is found:

Software/Version	Category
Apache Tomcat 4.1+	Web Servers
Twitter Bootstrap	Web Frameworks
Font Awesome	Font Scripts
jquery 1.8.2	Javascript Frameworks

An attacker can misuse this information to perform the task against the software type and versions.

Below are the attached evidence of the scanned results of the websites:-

I➤ Our Vulnerability & Exploits Database Here

SUMMARY SCAN REPORT

This site was checked for a lot of vulnerabilities, with up to hundreds of tests for each vulnerability and this site contain ***4 VULNERABILITIE(S)*** in Sep 07, 2021. Because you scan this site in *LIGHT Version* we excluded the **landing page(s) scan** and some tests like **SQL INJECTION, XSS, LFI & RFI Attacks, Cookie Injection ,etc...** For FULL SCAN report, please create an account, BUY CREDIT(S) and add your website.

More than 80% from websites contain 1 or more than 1 issue on landingpage!

APPLICATION LEGEND	ISSUES(S) Detected
High - VERY CRITICAL ISSUE(S). An attacker can get FULL access of your server and can destry everything.	1 Issue(s)
Medium - CRITICAL ISSUE(S). An attacker can steal confidential informations from your DB, informations like (Users, Passwords, Payment informations, etc..)	2 Issues
Low - LOW TYPE ISSUE(S). If browsers are not updated, an attacker can steal confidential informations like (Users, Full names, Phone numbers, etc..) and then use that for SPAM, PHISHING, SELL	1 Issue
Information - INFORMATIONS (GOOD PRACTICE). We recommend this. In this way you can eliminate spams and reports to be notified to blacklist with your IP(s) and mails.	0 Issue(s)

Open Port(s) Detected

Port Number	Services	Daemon Info

CyberSecurityWebTest

Services Pricing Register Login

APPLICATION LEGEND	ISSUES(S) Detected
High - VERY CRITICAL ISSUE(S). An attacker can get FULL access of your server and can destry everything.	1 Issue(s)
Medium - CRITICAL ISSUE(S). An attacker can steal confidential informations from your DB, informations like (Users, Passwords, Payment informations, etc..)	2 Issues
Low - LOW TYPE ISSUE(S). If browsers are not updated, an attacker can steal confidential informations like (Users, Full names, Phone numbers, etc..) and then use that for SPAM, PHISHING, SELL	1 Issue
Information - INFORMATIONS (GOOD PRACTICE). We recommend this. In this way you can eliminate spams and reports to be notified to blacklist with your IP(s) and mails.	0 Issue(s)

Open Port(s) Detected

Port Number	Services	Daemon Info

All Scanned Ports are Closed or Filtered ✓

Information about this type of Vulnerability –

CyberSecurityWebTest

Services Pricing Register Login

risk

Information about this type of Vulnerability –

➤ Open ports are used by applications and services for internet communication. If a port is open (like 3306 or 80, etc...), we know as there are running a "MySQL Server" or "Web server" and they may have vulnerabilities or bugs and you have higher risk to having a vulnerability that can be exploited.

Server Information

CyberSecurityWebTest

Services Pricing Register Login

Server Information

WebServer Name	Apache-Coyote/1.1
Cpanel Detected cPanel	**NO - Safe** ✓
Web Mail Detected	**NO - Safe** ✓
Vulnerabilities Detected	**YES**
Severity	High
Find Server Name	➤ FIND VULNERABILITY
Vulnerability in Google	
HOW TO FIX	Need FULL SCAN

Clickjacking Vulnerability

Vulnerability	Clickjacking
Vulnerabilities Detected	**YES**
Severity	*Medium*
HOW TO FIX	Need FULL SCAN

Information about this type of Vulnerability

Clickjacking is an attack that force a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, steal credentials or sensitive information, transfer money, or purchase products online.

Because we discovered as your website is not configured corectly, We strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

HOW TO FIX	Need FULL SCAN

Information about this type of Vulnerability

Clickjacking is an attack that force a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, steal credentials or sensitive information, transfer money, or purchase products online.

Because we discovered as your website is not configured corectly, We strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

XSS Vulnerability

XSS Header	XSS Header
Vulnerabilities Detected	**YES**
Severity	*Medium*
HOW TO FIX	Need FULL SCAN

Information about this type of Vulnerability

If XSS Heaader missing, which means that this website could be at risk of a Cross-site Scripting (XSS) attacks. This is the most basic type of cross-site scripting vulnerability. This type of cyber security issue is clasified on ISO27001-A.14.2.5.

Because we discovered as your website is not configured corectly, We strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

Information about this type of Vulnerability –

- If XSS Heaader missing, which means that this website could be at risk of a Cross-site Scripting (XSS) attacks. This is the most basic type of cross-site scripting vulnerability. This type of cyber security issue is clasified on ISO27001-A.14.2.5.
- Because we discovered as your website is not configured corectly, We strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

Certificate (HTTPS) Issues

Availability	Need FULL SCAN
Vulnerabilities Detected	Need FULL SCAN
Severity	*High*
HOW TO FIX	Need FULL SCAN

Information about this type of Vulnerability –

- TLS/SSL technology is commonly used in websites and web applications together with the HTTP protocol. It is also used by several other services and protocols. Weak SSL encryption or ciphers SSL ecnription may drive your web application to some vulnerability like POODLE, BEAST, and CRIME.
- If you want to verify the TLS/SSL encription we strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

Information about this type of Vulnerability –

- TLS/SSL technology is commonly used in websites and web applications together with the HTTP protocol. It is also used by several other services and protocols. Weak SSL encryption or ciphers SSL ecnription may drive your web application to some vulnerability like POODLE, BEAST, and CRIME.
- If you want to verify the TLS/SSL encription we strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

E-mail Disclosed

Disclosed	NO
E-mail	-
Severity	*Information*
HOW TO FIX	Don't Need - OK ✓

Information about this type of Vulnerability –

- Any email address that are unnecessary mult be deleted. This step is necesary to reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

HOW TO FIX Don't Need - OK

Information about this type of Vulnerability –

- Any email address that are unnecessary mult be deleted. This step is necesary to reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

Form Vulnerability

Forms Count	1
Vulnerabilities Detected	YES
Severity	Low
HOW TO FIX	Need FULL SCAN

Information about this type of Vulnerability –

- If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

- Because we discovered more than 1 Open Port, We Strongly recommend you to have a **FULL SCAN NOW** to be informed how you solve this type of issue.

Vulnerability Issues: Cross-Site Scripting

Domain*: vulweb.com*

- There is one loophole detected in your website, which can harm your website as it is subjectable to the risk of being attacked by attackers who can log in and steal data without any authorization.

Steps needed in order to cross verify the vulnerability of the website:

- Visit the website *vulweb.com*
- Click on the search bar on the top
- Now, to find the different payloads vulnerable to your website, you can intercept the request via burp-suite software
- You will find one of the payloads "<image/src/onerror=prompt(8)>" which is vulnerable to your website.

Description: This payload can cause harm to your website as it is vulnerable to your website i.e there is some loophole in your website which needs to be fixed immediately. Usually, with the help of this payload, the attacker can log in to your website without authorization and can inject malicious code. They can even steal data which may be sensitive. The most important thing to note here is that most of WAFs blocks 'script' and 'iframe' at the time of blocking XSS, but they are incapable of blocking 'img'. Therefore it is highly advisable to take an action immediately.

Mitigations: Now, you need to focus on the "img scr" that the browser knows what will come i.e image, therefore the browser will not invoke the parser like XML & HTML parser. The browser will send the request and read the MIMEs i.e image or jpg or gif. If the answer does not have content-type then many of the

browsers will guess based on extension i.e they will only guess image MIMEs, magic numbers but they will not guess esoteric format.

Below is the attached video as evidence:

https://drive.google.com/file/d/1k8jzy424UOOCrXHxA1sIsIojqUdSTamL/view?usp=sharing