Lab 05: Web security – XSS – File Upload Vulnerabilities

4. Tasks

4.1. Setup

In windows Terminal, change working directory to Xss-Fileupload. Fire up docker-compose to create the docker-container set for this lab.

>> docker-compose up --build



This command will bring up 2 containers connecting to the same LAN: A SQL server running mysql named mysql-10.9.0.6, and a web server named www-10.9.0.5

4.2. Reflected-xss attack

Access page at <http://localhost:3128/xss-reflect.php>.

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, ảnh chụp màn hình

Mô tả được tạo tự động

a) Try various plain text input then click Submit to see the result.

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

Result when I input hello.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Source code for xss-reflect.php is an input form written in PHP as shown above.

b) Try various text with html tag input then click Submit to see the result.

Try this input text:

<h1>Heading 1</h1><h2>Heading 2</h2><p style="color:red;">This is a red paragraph.</p>

This will be shown:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

As reflected text became part of page, you can input JavaScript code, it will then be executed when button Submit is hit.

4.2.1. Attack

c) Try to input this to see the result: <script>alert("How are hacked")</script>

Ảnh có chứa Phần mềm đa phương tiện, phần mềm, ảnh chụp màn hình

Mô tả được tạo tự động

d) Enter JavaScript code to print out cookies from the web page.

I can use <script>console.log(document.cookie)</script> to print out cookies from the web page

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, ảnh chụp màn hình

Mô tả được tạo tự động

e) Suppose you want to steal cookies from this page and send it to a remote computer. Find the way to implement this.

So, if I want to steal cookies from this pages and send it to a remote computer. I can construct a form and then send the data to that remote computer.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Mô tả được tạo tự động

4.2.2. Countermeasure

Refer to the web for security measures, modify code to implement a countermeasure to protect the web page from this kind of attack. Demonstrate your success.

So at here, i use the medthod in php, that is htmlspecialchars => will convert html special characters into HTML entities prevents website from being attacked.

>> docker-compose up –build again to apply the modify

Let’s check

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

Successfully apply the countermeasure.

4.3 Stored-XSS Attack

Access page at <http://localhost:3128/xss-stored.php>.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Mô tả được tạo tự động

4.3.1. Attack

a) Try various plain text or text inside html tag comments then click Submit to see the result.

The result when I input abc

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Mô tả được tạo tự động

The result when I input <h1>Heading 1</h1><h2>Heading 2</h2><p style="color:red;">This is a red paragraph.</p>

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

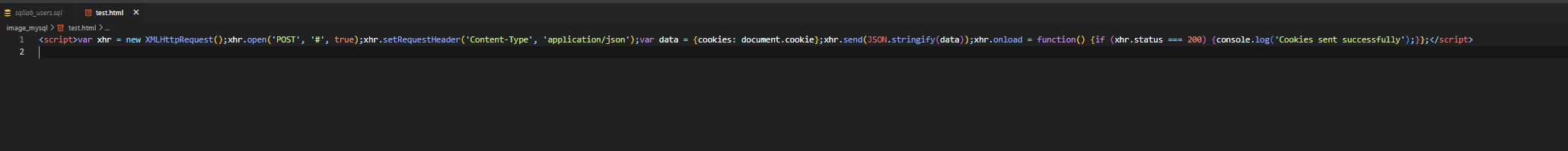
b) Try to input a JavaScript code in the comment box, the code will be stored and executed each time submit button is hit.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

c) Implement the way you steal cookie in 4.2.1 (e) for this task

Because the comment display section has a br element every line so that it will reduce it to 1 line

Then as you can see, we have sent coookie succesfully

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

4.3.2. Countermeasure

Refer to the web for security measures, modify code to implement a countermeasure to protect the web page from this kind of attack. Demonstrate your success.

We also use the htmlspecialchar to prevent this kind of attack.

This is the code after modify

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động

Let’s check the result

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

Successfully apply the countermeasure.

4.4 Fileupload Attack

Access the file upload page at <http://localhost:3128/fileupload.php>

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

4.4.1. Attack

After finish uploading PHP shellcode on the web server, attach to the console attacker machine:

docker exec -it attacker /bin/sh



Start listing on attacker by entering at the attacker terminal:

/ # nc -lv 9090

Listening on [0.0.0.0] (family 0, port 9090)

On Browser Address Bar, enter: <http://localhost:3128/uploads/rs.php>

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

4.4.2. Countermeasures

To prevent file upload attacks, web developers must implement security measures such as:

• Validating file types and extensions to ensure that only allowed file types are uploaded.

• Restricting file size to prevent uploading of large files that can cause denial of service attacks.

• Scanning uploaded files for malware and viruses

• Storing uploaded files in a secure location with restricted access.

Modify code to restrict uploaded file type to jpg, png, jpeg and gif only. Demonstrate your success

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Hệ điều hành

Mô tả được tạo tự động

Let rebuild and check result

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

Successfully apply the countermeasure.