Lab 05: Web security – CSRF (Cross-Site-Request-Forgery)

4. Tasks

4.1 Setup

a) Install VNC viewer on the host computer.

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

>> docker-compose up --build -d

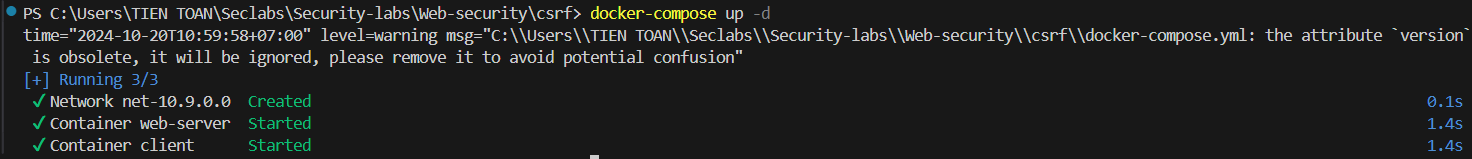
This command will bring up 2 containers connecting to the same LAN: The web client (10.9.0.6), a web server (10.9.0.5), a sniffer-host

[web-client] ---- 10.9.0.0/24 -----[web-server]

The web server is configured with 2 virtual servers running on it:

mysite.com stands for a clean website.

darksite.com malicious website setup by the attacker



c) Fire up VNC viewer on the host computer to connect to the web client on docker network by entering localhost:5900 on the address bar of VNC viewer. After the first connection is successfully established, a thumbnail of web-client computer in VNC will show up ready for connection.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

d) Attach to the console of web-client docker container by entering:

>> docker exec -it client sh -l

Execute the following command to append hostname configuration lines from /tmp/hosts to the end of /etc/hosts file.

# cat /tmp/hosts >> /etc/hosts

Execute tail command to make sure those 3 lines exist in the /etc/hosts file.

5c92cca8817f:/# tail -n5 /etc/hosts

. . .

10.9.0.5 mysite.com

10.9.0.5 darksite.com

Ảnh có chứa văn bản, phần mềm, Phông chữ, Phần mềm đa phương tiện

Mô tả được tạo tự động

4.2. Conducting the Transaction

a) Fire up Firefox inside the web-client container, enter http://mysite.com/login.php

to login with credentials (admin, password)

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

Mô tả được tạo tự động

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

Mô tả được tạo tự động

After successfully login, enter amount and the receiver’s name, click Transfer to proceed doing the transaction.

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

Mô tả được tạo tự động

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

Mô tả được tạo tự động

b) Open Developer Tool (Ctrl + Shift + K), click Network tab then click reload page to view request/response headers, take note the cookie value.

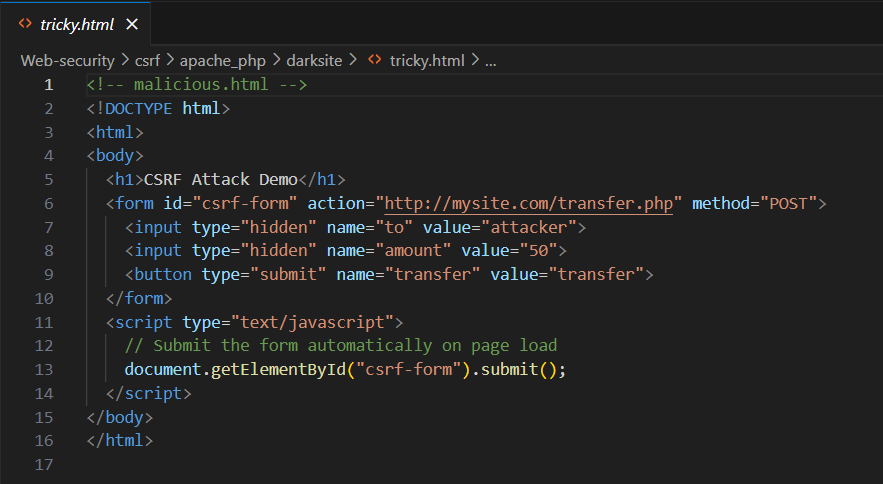
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Cookie: PHPSESSID=5nr4pis0b1meaen3s665qebmr2

4.3. Cross-Site-Request-Forgery

By observing page with Inspector in Developer Tool, the attacker forge the request by creating a hidden form that will be submitted automatically when loaded. This form is stored as tricky.html hosted on http://darksite.com that setup by the attacker.



Attacker can send an email with a link that whenever user clicks the link, an amount of money from admin’s account will be transferred to the attacker

Enter http://darksite.com/tricky.html to simulate the mentioned scenario.

Ảnh có chứa văn bản, Phông chữ, hàng, số

Mô tả được tạo tự động

Explain the reason why attacker can succeed with this forgery request.

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

Mô tả được tạo tự động

Cookie: PHPSESSID=5nr4pis0b1meaen3s665qebmr2

As you can see here, the browser has auto sent our cookie with the cross-site request when we access to the <http://darksite.com/tricky.html>. Because the request was sent with our cookie, the server will think that request was sent by us and execute that in the same way as the same-site request.

4.4. Trying to attack directly without forgery request.

a) Start an independent docker container by executing:

docker run -p 6080:80 --net=net-10.9.0.0 -v ${HOME}/shm:/dev/shm dorowu/ubuntu-desktop-lxde-vnc

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

Mô tả được tạo tự động

b) Open browser then enter http://localhost:6080 in the address bar to access GUI desktop of the newly created docker container.

Ảnh có chứa máy tính, cầu vồng, đa phương tiện, ảnh chụp màn hình

Mô tả được tạo tự động

I will install nano for editing file more easier

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

Mô tả được tạo tự động

Edit file /etc/hosts by nano



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

Mô tả được tạo tự động

c) Open firefox inside the docker container GUI, enter http://darksite.com/tricky.html. How does the transaction finish? Explain your observation.

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

Mô tả được tạo tự động

The transaction finish at mysite.com/login.php .

Explain: Because we havent login yet, the browser doesn’t have cookie to attach with the cross-site request. So when the server receive the request, it doesn’t know who send this request => cant execute the request and require us to login so that the server will know who send the request by cookie attach with the request.

And because of that, this code in transfer.php will prevent us from doing action without authentication

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

Mô tả được tạo tự động

d) Is there any way that make this attack succeed? Do it! (Modify cookie?)

4.5. Secure server code

Modify server code to protect the web server from CSRF attack.

We can modify server code to protect the web server by creating a token, if the request token matches with the token we create in the side => then we allow

So we will give token to user when they login successfully: ( in login.php)

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

Mô tả được tạo tự động

Then in transfer.php, we have to modify the code to check the token:

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 ảnh chụp màn hình, văn bản, Phông chữ, số

Mô tả được tạo tự động

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

Mô tả được tạo tự động

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

Mô tả được tạo tự động

Successfully apply the countermeasure.