Lab 05.1: Web security – SOP (Same Origin Policy)

4. Tasks

4.1. SOP lab

4.1.1. Setup

a) Tải VNC Viewer trên máy.

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

Mô tả được tạo tự động

b) Tạo máy ảo



c) Kích hoạt VNC Viewer

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

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

Mô tả được tạo tự động

e) Fire up Firefox inside the web-client container, enter http://siteb.com or whichever of the above 3 sites. Home page of those sites will be displayed:

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

Mô tả được tạo tự động

4.1.2. Using JS to access DOM objects of the web site.

• Load sitea in browser.

• Open Web Developer >> Console Panel (Ctrl + Shift + K)

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

Mô tả được tạo tự động

Right-click on page > View page source to display source of web page. Take notes of ids in body part of page.

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

Mô tả được tạo tự động

IDs in body part: header, js

Goto Console Panel, with javascript:

a. Try to access DOM objects of page: document.body, document.body.innerText,

document.body.innerHTML or whichever that you can.

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

Mô tả được tạo tự động

b. Change the text “Hey,Site B is working” to “Header text is modified via document object”.



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

Mô tả được tạo tự động

c. Create a newwin variable for a new tab:

var newwin = window.open(http://sitea.com,”right”). Can you access document object of newwin? Explain why if you could not.

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

Mô tả được tạo tự động

Không thể truy cập vào document object của newwin vì SOP ngăn chúng ta truy cập object từ cross-site.

d. Enter JS code to set the new location for tab siteb which is the opener of current tab:

• Click sitea.com tab, Ctrl + Shift + K to open Console Panel.

window.opener.location=”http://parentsite.com”.

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

Mô tả được tạo tự động

e. Try JS code to access document.body object of window.opener. Explain why if you could not.



We cant access document.body object of window.opener because POS prevent us from accessing object from other site that not in the same domain.

4.1.3. Frame objects

Access http://parentsite.com then choose parentsite in list of sites on iframe

picker.

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

Mô tả được tạo tự động

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

Mô tả được tạo tự động

a) Can you access window.framea, window.frameb?.

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

Mô tả được tạo tự động

Yes, we can access window.framea, window.frameb

b) Can you access document.body of framea, frameb from parentsite?

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

Mô tả được tạo tự động

No, we cant with the same reason.

• Select sitea.com in list of sites on iframe picker.

Ảnh có chứa văn bản, Phông chữ, hàng, màu trắng

Mô tả được tạo tự động

c) Can you access window.parentsite?

Ảnh có chứa văn bản, Phông chữ, màu trắng, hàng

Mô tả được tạo tự động

Yes, we can

d) Can you access document.body object of parentsite.com? Which object of parentsite that sitea can access?



No, we cant access document.body object of parentsite.com

Object of parentsite that sitea can access:

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

Mô tả được tạo tự động

• Select parentsite.com in list of sites on iframe picker, define a variable named hello: var hello=”world”

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

Mô tả được tạo tự động

e) Can you access hello from sitea, siteb?

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

Mô tả được tạo tự động Ảnh có chứa văn bản, Phông chữ, số, ảnh chụp màn hình

Mô tả được tạo tự động

No, we cant access hello from sitea, siteb.

4.1.4. Sending POST request to a site:

a) Access <http://sitea.com/post.html>

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

Mô tả được tạo tự động

b) Type some text in textbox then click “Submit query”. What would show up?

Explain why you see that.

When I type some text then click “Submit query”, it will me the siteb.com

To explain why, we have to see the page source of http://sitea.com/post.html

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

Mô tả được tạo tự động

So we can see that it had used a form have action to siteb.com. And because of that, when we submit, the form will navigate us to siteb.com.

c) Repeat step (a), toggle Web console >> Network (Ctrl + Shift + E)

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Hệ điều hành

Mô tả được tạo tự động

d) Repeat step (b), examine the request and response header. What can you conclude about POST form request.

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Phần mềm đa phương tiện

Mô tả được tạo tự động

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

Mô tả được tạo tự động

Conclude about POST form request: When we send data using POST request, the data will be contained in request.body

4.1.5. Access image, stylesheet from other sites

a) In the Inspector panel of sitea.com, can you change sitea’s image to image from siteb.com?

By modify the img tag source from “a.png” to “<http://siteb.com/b.png>” we can change sitea’s image to image from siteb.com

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Trang web

Mô tả được tạo tự động

b) In the Inspector panel of sitea.com, can you change the stylesheet to that of siteb.com?

Yes, we can. By the same way of a), we just need to change the link tag href from “site.css” to “<http://siteb.com/site.css>”

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

Mô tả được tạo tự động

4.1.6. SOP applies to web storage

Load www.sitea.com in one tab, open Web developer panel > Storage, check that the

LocalStorage is empty (Storage >> Local Storage). Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

a) Define a new variable named first = 10. You can define either:with javascript in console: window.LocalStorage[“first”] = 100 or Add Item in Storage tab

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

Mô tả được tạo tự động

b) Open sitea.com in a new tab. Can you access first variable in this tab? Change first to a new value, go back to the previous sitea.com tab, what is the value of first then.



Yes we can access the first variable in a new tab

Then we will change it to “10”



Back to the previous tab, check the “first” variable

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

Mô tả được tạo tự động

We will see it change to 10 too like we have modified in another tab.

c) Can you access first from siteb.com?

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

Mô tả được tạo tự động

No, we cant access “first” from siteb.com

d) Close all sitea.com tabs. How about first variable when sitea.com is re-opened.

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

Mô tả được tạo tự động

It still there and doesnt disappear.

e) Close browser then re-open, does first variable still exist?

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

Mô tả được tạo tự động

It still exit even we close and re-open the browser

f) What can you conclude about Local Storage?

LocalStorage là cơ chế lưu trữ web không có thời hạn, cho phép dữ liệu tồn tại qua nhiều phiên duyệt web. Dữ liệu chỉ có thể truy cập từ cùng miền, và được chia sẻ qua các tab của cùng trang web. Nó phù hợp để lưu trữ thông tin lâu dài như tùy chỉnh người dùng, nhưng không nên lưu dữ liệu nhạy cảm như mật khẩu.

• Repeat the above steps from (a) to (e) but with Session Storage. What can you conclude about Session Storage?

For Session Storage

Load www.sitea.com in one tab, open Web developer panel > Storage, check that the

SessionStorage is empty (Storage >> Session Storage).

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

Mô tả được tạo tự động

a) Define a new variable named first = 10. You can define either: with javascript in console: window.sessionStorage[“first”] = 100 or Add Item in Storage tab

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

Mô tả được tạo tự động

b) Open sitea.com in a new tab. Can you access first variable in this tab? Change first to a new value, go back to the previous sitea.com tab, what is the value of first then.

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

Mô tả được tạo tự động

No, we cant access “first” in new tab

c) Can you access first from siteb.com?

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

Mô tả được tạo tự động

No, we cant access “first” from siteb.com

d) Close all sitea.com tabs. How about first variable when sitea.com is re-opened.

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

Mô tả được tạo tự động

We can not access “first” when sitea.com is re-opened

e) Close browser then re-open, does first variable still exist?

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

Mô tả được tạo tự động

The “first” variable isnt exist

f) What can you conclude about Session Storage?

Session Storage lưu dữ liệu tạm thời trong một tab. Dữ liệu chỉ tồn tại trong tab đó và bị xóa khi tab hoặc cửa sổ bị đóng. Mỗi tab có không gian riêng, dù cùng miền cũng không truy cập được từ tab khác.