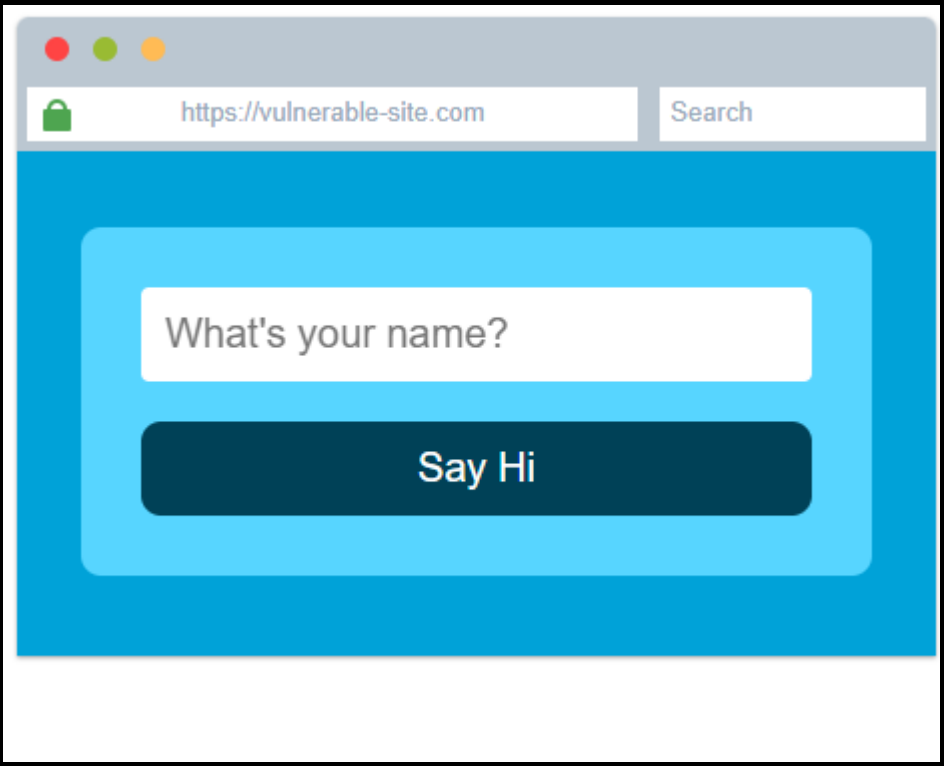
inject HTML task tryhackme

Page • Tag

есть таск:

> View the website on this task and inject HTML so that a malicious link to http://hacker.com is shown.

Решение: открываем этот сайт и видим данную картину:



введя в поле *whats your name?* условно loh мы получим welcome loh уяснили

т.к это таск внутри tryhackme а не внешний сайт , я могу посмотреть код элемента фрейма т.е один из двух окнов при нажатии просмотреть код фрейма мы увидим это:

```html
<!DOCTYPE html>
<html>

<head>
    <title>How websites work</title>
    <link rel="stylesheet" href="css/style.css"></link>
</head>

<body>
    <div id='html-code-box'>
        <div id='html-bar'>
            <span id='html-url'>https://vulnerable-site.com</span>
        </div>
        <div class='theme' id='html-code'>
            <p id='welcome-msg'></p>
            <form id='form' autocomplete="off">
                <div class='form-field'>
                    <input class="input-text" type="text" id="name" placeholder="What's your name?">
                </div>
                <button onclick="sayHi()" type='button' class='login'>Say Hi</button>
            </form>
        </div>
    </div>
    <script src='js/script.js'></script>
    <script>
        function sayHi() {
            const name = document.getElementById('name').value
            document.getElementById("welcome-msg").innerHTML = "Welcome " + name
            setTimeout(checkAnswer, 100)
        }
    </script>
</body>

</html>
```

мы знаем что нам нужно обмануть поле ввода, тут скорее всего должна стоять защита на xss запрос, а защита стоит в JS скрипте и тут есть ссылка на него при переходе мы увидим это:

```js
function checkAnswer() {
    const name = (document.getElementById("welcome-msg").innerHTML).toLowerCase()
    let userInput = name.split('welcome ')
    if(userInput.length > 0) {
        userInput = userInput[1]
        console.log(userInput)
        if(userInput.includes('http://hacker.com') && userInput.includes('<a href')
            && userInput.includes('</a>')) {
                alert('Congratulations! The answer is ' + decodeBase64("SFRNTF9JTkozQ1RJME4="))
            }
    }
}

function decodeBase64(s) {
    var e={},i,b=0,c,x,l=0,a,r='',w=String.fromCharCode,L=s.length;
    var A="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
    for(i=0;i<64;i++){e[A.charAt(i)]=i;}
    for(x=0;x<L;x++){
        c=e[s.charAt(x)];b=(b<<6)+c;l+=6;
        while(l>=8){((a=(b>>>(l-=8))&0xff)||(x<(L-2)))&&(r+=w(a));}
    }
    return r;
};
```

и тут у нас открывается дорога на 2 варианта решения задачи:

1 самый простой:
мы видим строчку с условием ввода анти xss система скажем так:

```
if(userInput.includes('http://hacker.com') && userInput.includes('<a href')
    && userInput.includes('</a>')) {
        alert('Congratulations! The answer is ' + decodeBase64("SFRNTF9JTkozQ1RJME4="))
    }
```

в конце написано:
`alert('Congratulations! The answer is ' + decodeBase64("SFRNTF9JTkozQ1RJME4="))`

мы можем декодировать то что находится в скобках у decodeBase64 в cyberchef и получить флаг

2 способ как просит задача:
видя условие этого кода мы можем сделать вывод что мы можем встроить ссылку в имя где пишется welcome (....) через html инъекцию, благодаря данному нам условию итог выглядит так:

`<a href="http://hacker.com">loh</a>`

ввожу это в строку ввода и нам выведет флаг
Ч.Т.Д