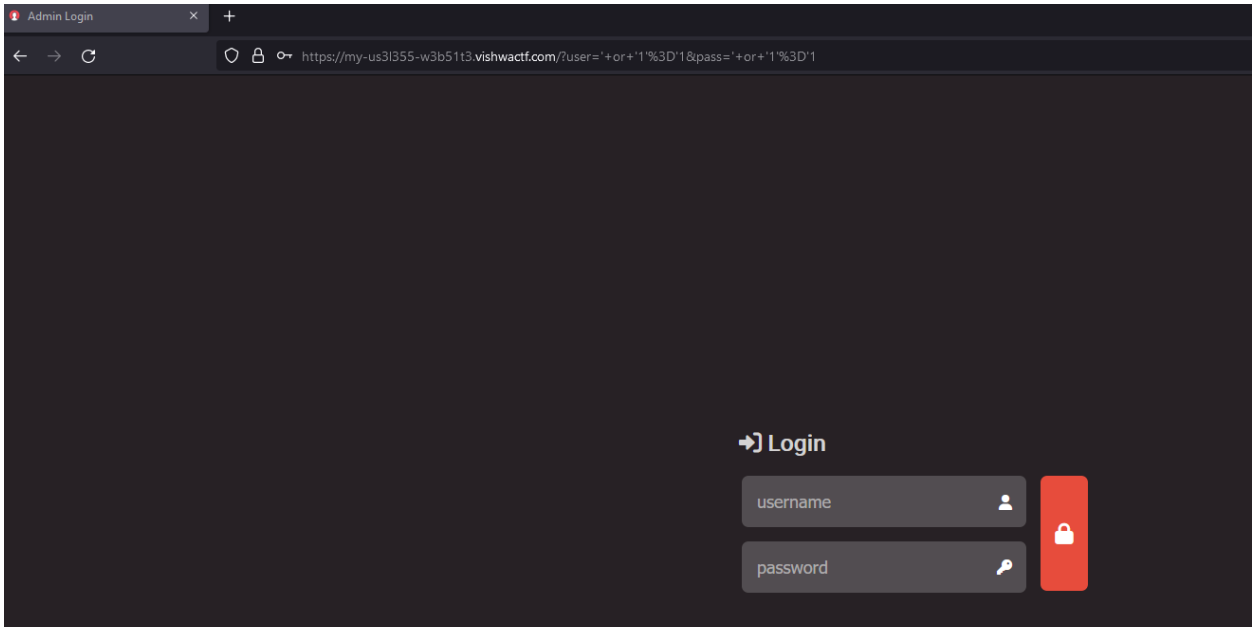
Vishawa CTF Write Up

Category: Web

Challenge 1: "My Useless Webiste" For 250 Points

- Challenge gives a link to a simple login page that asks for a username and password. The page has javascript that prevents one from typing in spaces — presumably to prevent SQL injection attacks. This means that the attack is probably along those lines.
    - The javascript to prevent this is "*function AvoidSpace(event) { var k = event ? event.which : window.event.keyCode; if (k == 32) return false; }*"
    - Both username and password inputs call this function with onkeypress to send each keypress to the function. The function will prevent the ASCII character 32, which is a space, from being entered.
- **Solution: Two solutions…**
    - (1) Change return false to return true in the AvoidSpace function OR copy and paste SQL injection parameter into the input field: **' or '1'='1**
    - (2) Enter the following URL get parameters for SQL injection: https://my-us3l355-w3b51t3.vishwactf.com/?user=%27+or+%271%27%3D%271&pass=%27+or+%271%27%3D%271



Challenge 2: “Stock Bot” for 250

- **Challenge:**
- **Observations:** Looking at the source code, there is a script tag with the following code. It seems like “/Products/check.php?product=**argument**” is going to be very useful because the javascript checks don’t apply here.

```
<script>
    // Hint: Along with other products the Flag is also available in the Products directory
    function sendMsg() {
        var msg = document.querySelector('#input-msg').value;
        document.querySelector('#input-msg').value = "";
        div = document.querySelector('.chat-body');
        div.innerHTML += "<div id='user-chat' class='user-div'><p class='user-msg msg'>" + msg + "</p></div>";
        div.scrollTop = div.scrollHeight;
        if(!msg.includes('Flag')){
            async function fetchDataAsync(url) {
            try {
                const response = await fetch(url);
                obj = (await response.json());
                div.innerHTML += "<div class='bot-div'><img src='bot.png' class='bot-avatar' /><p class='bot-msg msg'>"+obj['Quantity']+"</p></div>"
            } catch (error) {
                div.innerHTML += "<div class='bot-div'><img src='bot.png' class='bot-avatar' /><p class='bot-msg msg'>No such product</p></div>"
            }
                div.scrollTop = div.scrollHeight;
            }
            fetchDataAsync('/Products/check.php?product='+msg);
        }
        else{
            div.innerHTML += "<div class='bot-div'><img src='bot.png' class='bot-avatar' /><p class='bot-msg msg'>No such product</p></div>"
            div.scrollTop = div.scrollHeight;
        }
    }
</script>
```

- **Solution:** Going to the URL “https://stock-bot.vishwactf.com/Products/check.php?product=Flag” provides the JSON output of "*VishwaCTF{b0T_kn0w5_7h3_s3cr3t}*"