Forms

Category: General Skills, Web
Created: Nov 8, 2020 5:05 PM
Points: 125
Solved: Yes
Subjective Difficulty: 🔥

WriteUp:

Author: @Tibotix

🔎 Research:

We are given am internet address which contains 1000 login Forms, but only one is working correctly.

📝 Vulnerability Description:

No exact Vulnerability

🧠 Exploit Development:

At the bottom there is a script calles verify which checks username and password:

```
<script type="text/javascript">
function verify() {
user = document.getElementById("username").value;
pass = document.getElementById("password").value;
if (user === "admin" && pass === "password123") {
document.getElementById("submit").value = "correct_login";
} else {
document.getElementById("submit").value = "false";
}
document.form.submit();
}
</script>
```

So we had to search where the `verify` funtion is called:

```
<div class="section container" style="background-color:#B15B79">
        <h3 style = "color:#FFFFFF">Form 673</h3>
        <form method="post" name = "form" id="form">
            <div>
                <input placeholder="Username" name="username" type="text"
id="username" style = "color:#FFFFFF">
            </div>
            <div>
                <input placeholder="Password" name="password" type="text"
id="password" style="color:#FFFFFF">
            </div>
            <button name="submit" id="submit" onclick="verify(); return false;"
class="btn-flat" style = "background-color:#FFFFFF;
color:#FFFFFF">Submit</button>
        </form>
    </div>
```

So we need to go to Form 673 and submit username=**admin** and password=**password123**

Exploit Programm:

```
```

Run Exploit:

FLAG: nactf{cl13n75_ar3_3v11}

Summary / Difficulties:

This was a really simple basic challenge. No real Hacking required.

Further References:

-

Used Tools:

-

Notes:

-