


# Forgot Password

 Tags	web exploit
--	-------------

## SKR CTF – Forget Password (Web Exploitation Writeup)

**Platform:** SKR CTF

**Category:** Web Exploitation

**Difficulty:** Beginner

**Flag:** `SKR{N3ver_Us3_J@v4Scr1pT_F0r_Au7h3nt1c4ti0n_7c1744}`

### Challenge Summary

This challenge is a classic example of why hardcoding credentials in client-side JavaScript is a bad idea. The goal was simple: inspect the web app, find the login credentials, and retrieve the flag.



### Tools Used

- Chrome or Firefox
- Developer Tools (Inspect Element)
- Basic JavaScript reading skills

### Step-by-Step Guide

#### 1. Open Developer Tools

Right-click anywhere on the page and select **Inspect**, or press `Ctrl+Shift+I`.

#### Navigate to the JavaScript Source

In the **Sources** tab, go to:

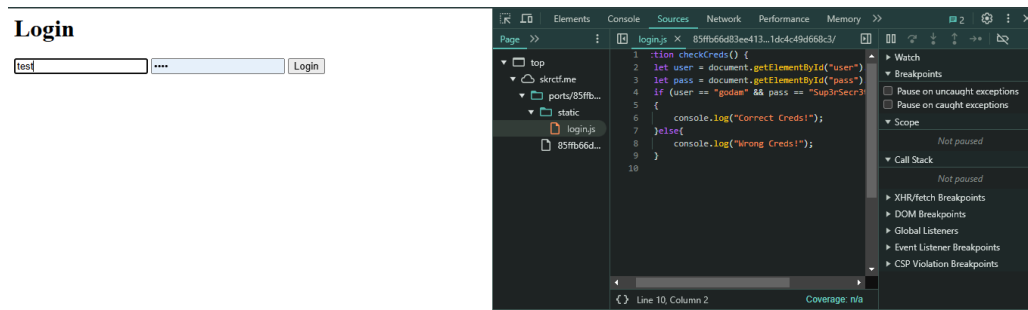
Page → static → login.js

Here's what you'll find:

javascript

```
const username = "godam";  
const password = "Sup3rSecr3t4ndS3cur3P";
```

Boom — credentials exposed.

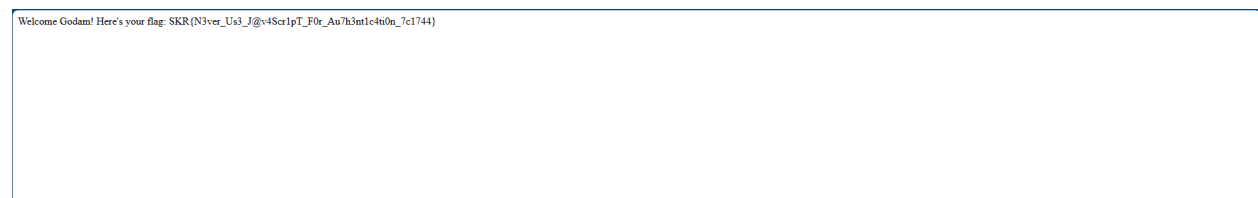


### 3. Log In

Go back to the login page and enter:




- **Username:** godam
- **Password:** Sup3rSecr3t4ndS3cur3P

Once logged in, the flag is revealed immediately:



SKR{N3ver\_Us3\_J@v4Scr1pT\_F0r\_Au7h3nt1c4ti0n\_7c1744}

## Lessons Learned

-  Never store sensitive data in client-side code.
-  Always inspect JavaScript files during web exploitation.
-  Even simple challenges teach powerful lessons.