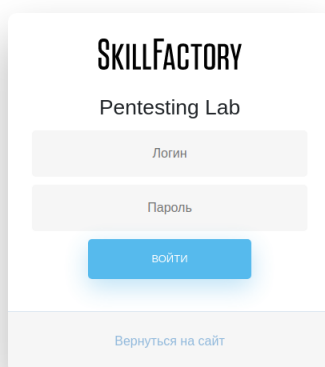


Assignment Report HW-04 - 11.7.1 - 11

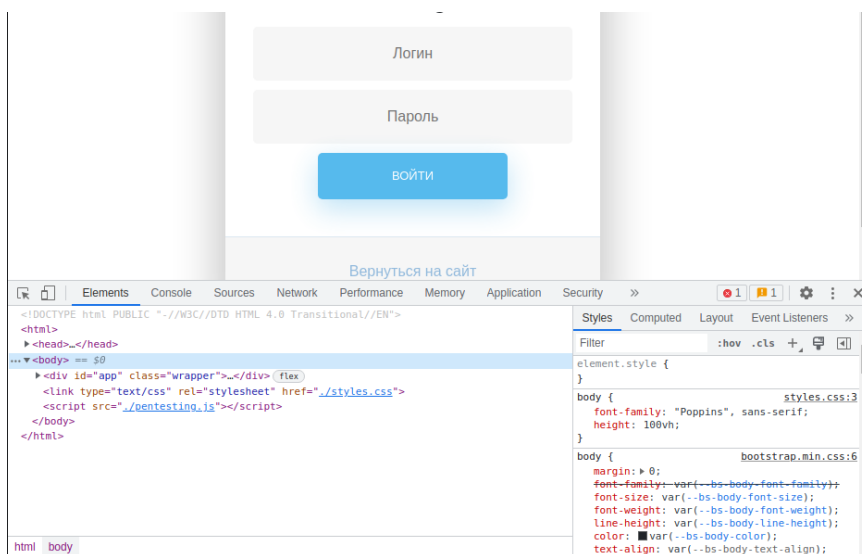
Tester's name: Stanley Ford

Lab "2" :

- General information:
 - Testing period: 01.01.2022
 - Test object: <http://51.250.73.193:5010/>
- Description of actions:
 1. Navigated to the address of the test object. I saw the authorization window in front of me (<http://51.250.73.193:5010/>)



2. First of all, of course, I wanted to check the page element and try to find something interesting.



This is where I noticed the connected `./pentesting.js` script and without thinking twice, I ran to look at its contents.

3. I saw a code in front of me that contains two accounts. Literally naked, in plain sight. At first, I didn't even believe that everything was so simple and easy, I was even upset that I didn't need to use Burp

Скриншот taken

View image

Pentesting Lab - Skillfactory x +

← → ↺ ⚠ Not secure | 51.250.73.193:5010

SKILLFACTORY

Pentesting Lab

Логин

Пароль

Войти

Page Elements Console Sources Network Performance Memory Application Security >>

Filesystem >> : [x] pentesting.js x

```

1 var app = new Vue({
2   el: '#app',
3   data: {
4     loggedIn: false,
5     loginFound: false,
6     errors: [],
7     form: {
8       login: '',
9       pass: '',
10    },
11    login: null,
12    pass: null,
13    user: null,
14    creds: {
15      url: '/',
16      login: "admin",
17      pass: "LastJob",
18      value: "WfEg3N0YXZpbCBkHhIhRlYnlnIGZsYmVgdjBk
19    },
20    {
21      url: '/secret',
22      login: "Admin",
23      pass: "Admin",
24      value: "flag*(I_AM*SUP3R_PRO_C00L_H4XK3R)"
25    }
26  },
27  mounted() {
28  },
29  },
30  computed: {
31    // form() {
32    //   return
33  }
34  }

```

Watch

Breakpoints

No breakpoints

Scope

Not paused

Call Stack

Not paused

XHR/fetch Breakpoints

DOM Breakpoints

Global Listeners

Event Listener Breakpoints

CSP Violation Breakpoints

Line 28, Column 16 Coverage: n/a

PenTesting Lab - Skillfacto x +

Not secure | 215.270.193.5010

View image

ПОЗДРАВЛЯЕМ, ВЫ ВОШЛИ КАК ADMIN!

WWEgb3N0YXZpbCBkbHliHRIYnlhIGZsYWcgdiBkaXJla3RvcmlpLCBhIHVga2Frb3ktIG5lIHNRyXpodS4gTG9naWdGdG90IHpoZSwgcGFzc3dvcuQ6IEFkbWlu

Разлогиниться

Elements Console Sources Network Performance Memory Application Security >>

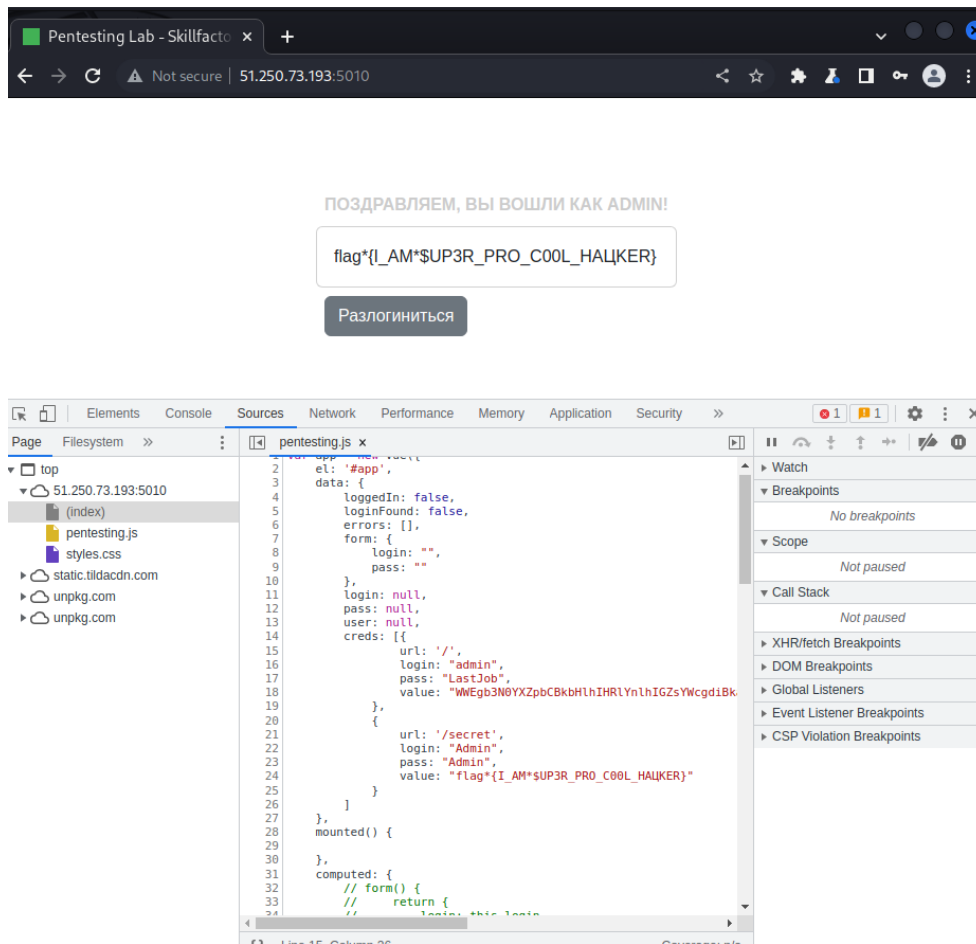
Page Filesystem >> : [x] pentesting.js x

- top
 - (index)
 - pentesting.js
 - styles.css
 - static.tildacdn.com
 - unpkg.com
 - unpkg.com

```
1 var app = new Vue({
2   el: '#app',
3   data: {
4     loggedIn: false,
5     loginFound: false,
6     errors: [],
7     form: {
8       login: '',
9       pass: '',
10    },
11    login: null,
12    pass: null,
13    user: null,
14    creds: {
15      url: '/',
16      login: 'admin',
17      pass: 'LastJob',
18      value: 'WWEgb3N0YXZpbCBkbHliHRIYnlhIGZsYWcgdiBkaXJla3RvcmlpLCBhIHVga2Frb3ktIG5lIHNRyXpodS4gTG9naWdGdG90IHpoZSwgcGFzc3dvcuQ6IEFkbWlu'
19    },
20  },
21  {
22    login: 'Admin',
23    pass: 'Admin',
24    value: 'flag{I_AM_SUP3R_PRO_C00L_H4UKER!}'
25  }
26 },
27 mounted() {
28
29
30 },
31 computed: {
32   // form() {
33     return /
```

Line 28, Column 16 Coverage: n/a

6. However, to be fair, I went to this account of yours and saw the cherished flag in front of me:



Итого, ответ, что я искал: **flag*{I AM*\$UP3R PRO C00L H4CKER}**