

Management projektů

Programová podpora řízení rizik v projektech

Tým Octopus

Hlášení o chybě software

**Hlášení o chybě software**

|  |  |  |  |
| --- | --- | --- | --- |
| **Software**: | Easy Project | **Verze**: | - |
| **Autor**: | Daniel Dušek (xdusek21@stud.fit.vutbr.cz) | **Závažnost**: | Vysoká |
| **Datum**: | 11. března 2017 |  |  |

**XSS zranitelnost při vkládání Nového projektu**

|  |  |
| --- | --- |
| **Přesný popis**: | V rámci výuky používáme demo na adrese: https://mpr-fit.easyproject.cz/  **Kroky pro reprodukci**:  1. Přihlásím se na adrese: https://mpr-fit.easyproject.cz/ 2. Nahoře v liště vyberu **Projekty > Nový projekt** 3. Do položky **Jméno** zadám hodnotu <script>alert(22)</script> 4. Popřidávám uživatele, na které chci „zaútočit“ jako pracovníky na projektu a projekt uložím. 5. Nyní nahoře vpravo kliknu na hamburgerové menu **Další > Můj účet > Vybrat kartu Projekty**  **Očekávaný výstup**: Načte se mi seznam projektů, na nichž se podílím, s ošetřeným názvem projektu (tak jako to je v jiných částech systémů).  **Skutečný výstup**: Javascript zobrazí v alert okénku hodnotu ‚22‘.  Poznámka: XSS zranitelnost je zneužitelná k závažnějším útokům než je zobrazení okénka se zprávou. |