

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**: | Střední |
| **Datum**: | 11. března 2017 |  |  |

**XSS zranitelnost při vkládání poznámky do TODO listu**

|  |  |
| --- | --- |
| **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. Vpravo v bočním panelu otevřu To-Do list a kliknu na „Přidat To-Do“ 3. Do políčka vložím hodnotu: <script>alert(1)</script> 4. Zvolím „Přidat“  **Očekávaný výstup**: Uživatelský vstup je zobrazen přesně tak, jak je zadán jako položka todolistu.  **Skutečný výstup**: Uživatelský vstup obsahující HTML značky je referován na výstup bez jakékoliv sanitizace. (Vyskočí javascriptový alert dialog se zobrazenou jedničkou, 2× při přidání položky, 1× při každém otevření To-Do listu).  Na úvodní přednášce k EasyProjectu mi bylo řečeno, že jde o záměr a v souvislosti s tím bych rád podotknul, že toto může být, pravda, neškodné, ale jen tak dlouho, dokud útočník nenajde způsob, jak přidávat ostatním uživatelům úkoly do To-Do listu. Proto si myslím, že by tato funkcionalita měla být minimálně nějakým způsobem ošetřena.  Druhý případ, kdy by toto chování mohlo být nežádoucí je rozšíření systému, kdy by uživateli byly To-Do položky generovány uživatelem s vyšším oprávněním, případně automaticky na základě přiřazovaných rolí a úkolů v rámci projektu.  Poznámka: XSS zranitelnost je zneužitelná k závažnějším útokům než je zobrazení okénka se zprávou. |