

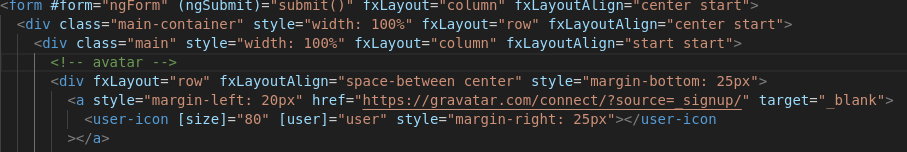
**Finding Name: Untrusted Page allowed to open new window**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Pushkar Goel | SCR | SCR Team Member | Ontrack | Natalia Khbotova | Yes |
| Jaspriya Kaur | SCR | SCR Team Lead | Ontrack | Natalia Khbotova | Yes |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

An untrusted page has been allowed to open a new window in the file **doubtfire-web/src/app/common/edit-profile-form/edit-profile-form.component.html** as a newly opened window have been given access back to the originating window



**Path : doubtfire-web/src/app/common/edit-profile-form/edit-profile-form.component.html**

This could allow basic phishing attacks (the window.opener object is not null and thus window.opener.location can be set to a malicious website by the opened page).

For instance, an attacker can put a link (say: "http://example.com/mylink") on the website that changes, when opened, the original page to "http://example.com/fake\_login". On "http://example.com/fake\_login" there is a fake login page which could trick real users to enter their credentials. This would create a vulnereability in the app allowing for exploitation of user trust

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

The modified script which arises due to the insecure code can have severe business implications. It allows attackers to inject malicious scripts into web applications, compromising the security and integrity of the system. The impact includes theft of sensitive data such as student data such as grades, personal details, and academic records as well as login credentials. Moreover, This can disrupt the OnTrack operations by defacing websites, redirecting users to malicious sites, or spreading malware. Also, the stolen information can be used by attackers to conduct spear phising campaign using the leaked information

**Affected Assets**

* Data assets
* Web Application
* Server Infrastructure
* Regulatory Compliance

**Remediation Advice**

* To prevent pages from abusing window.opener, use rel=noopener on <a href=> to force its value to be null on the opened pages.  
    
  <a style="margin-left: 20px" href="https://gravatar.com/connect/?source=\_signup/" target="\_blank" rel="noopener">

**Contact Details**

Pushkar Goel – s222162584@deakin.edu.au

**Secure Code Review Leader Feedback.**