**Technical threats**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico | Beschrijving | Likelihood of occurence (kans) | Hazard severity (impact) | Te ondernemen actie |
| Injection (SQL, OS e.a.) | Commando’s in SQL kunnen onveilig gemixt worden met de gebruikersinvoer. | Unlikely | Serious | Minimale user input toestaan. |
| Authorisatiefouten | Aanvallers kunnen andermans account overnemen in een sessie. | Very Unlikely | Major | Authenticatie- en sessiebeheermechanismen correct implementeren. |
| Lekken van gevoelige data | Door bijv. een gebrek aan versleuteling kan een aanvallers aan gevoelige data komen. | Unlikely | Major | Zorgen dat SQL-server niet van buiten toegankelijk is. |
| Mogelijkheid tot uploaden virussen | Het kan dat door een gebrekkige controle op de geüploade bestanden een kwaadaardig bestand geüpload wordt. | Possible | Moderate | Type bestand controleren tijdens upload. |
| Falende toegangscontroles | Dankzij een gebrekkige authenticatie kan een aanvallers ongewild op het account van een gebruiker inloggen. | Probable | Moderate | Door gebruiker wachtwoord laten veranderen. |
| Falende toegangscontrole Admin | Dankzij een gebrekkige authenticatie kan een aanvallers ongewild op het account van de Admin inloggen. | Unlikely | Major | Admin zijn wachtwoord laten veranderen. |
| Configuratiefouten | De software kan standaard ingesteld staan uit gemak, waarbij niet gebruik gemaakt wordt van de security-functies. | Possible | Moderate | Huidige software instellingen controleren en veranderen indien nodig. |
| Cross-site-scripting (XSS) | Een aanvallers kan andermans browsersessie overnemen door scripts in een webpagina te injecteren. | Probable | Minor | Mogelijke input door gebruiker minimaliseren en rigoreus valideren. |
| Cross-site request forgery (CSRF) | Een aanvallers kan een gebruiker forceren tot het doen van een ongewilde aanvraag, bijv. Het sturen van een link die automatisch je wachtwoord veranderd. | Probable | Minor | Creeëren pre-sessies (sessie voor een user is geauthentiseerd) en token mitigatie. |
| Onveilige deserialisatie | Een aanvaller kan een getransporteerd object uit een programmeertaal aan passen, waardoor de server overgenomen kan worden. | Possible | Serious | Input valideren. |
| Gebruik van software met bekende kwetsbaarheden | De gebruikte software kan bekende kwetsbaarheden hebben, die een aanvaller kan exploiteren. | Very Unlikely | Serious | Updates installeren. |
| Onvoldoende logging en monitoring | Zonder mogelijke aanvalspogingen te kunnen detecteren, is het niet mogelijk hier op te reageren. | Unlikely | Moderate | Implementatie zinvolle logging tool. |

**Financial threats**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico | Beschrijving | Kans | Impact | Te ondernemen actie |
| Afkappen project door Don Diablo | Don Diablo kan het project stopzetten als opdrachtgever door omstandigheden. | Very Unlikely | Major | Opdoeken project |

**Human threats**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico | Beschrijving | Kans | Impact | Te ondernemen actie |
| Misbruik van rechten door Admin of Promoteam | De Admin of leden van het promoteam kunnen misbruik maken van de rechten die aan hun gegeven zijn. | Possible | Moderate | Inperken rechten Admin of Promoteam; |