# Abuse Cases

## #1 Ander ID meegeven

|  |  |
| --- | --- |
| Naam | Ander ID meegeven |
| Versie | 1.0 |
| Actor | Werknemer/manager |
| Use Cases | * Ziekmelden * Betermelden * Verlof aanvragen * Verlof aanvragen goed of afkeuren * Inzien resterende saldo |
| Bechrijving | Een werknemer of manager geeft een valse of ongepaste identificatie op om ongeoorloofde voordelen te verkrijgen, zoals onterecht ziekteverlof of extra verlofdagen. |
| Scenario’s | * Een werknemer meldt zich ziek met een vervalst ID om zijn afwezigheid te rechtvaardigen. * Een manager keurt een verlofaanvraag goed op basis van een vals ID. |
| Impact | * Financieel: Onterecht uitbetaalde vergoedingen of verlofuren kunnen leiden tot financiële verliezen voor het bedrijf. * Reputatie: Herhaaldelijk misbruik kan het vertrouwen in het bedrijf en zijn werknemers aantasten. * Operationele verstoring: Ongeoorloofde afwezigheid kan leiden tot personeelstekorten en verminderde productiviteit. |
| Maatregelen | * Verificatieprocessen: Implementeer een systematisch verificatieproces voor de identificatie van werknemers bij ziekmeldingen en verlofaanvragen. * Training: Bied training aan medewerkers over de gevolgen van identiteitsmisbruik en het belang van eerlijkheid. * Monitoring: Voer regelmatig audits uit op ziekmeldingen en verlofaanvragen om verdachte patronen te identificeren. * Klokkenluidersysteem: Implementeer een vertrouwelijk systeem waar medewerkers misbruik kunnen melden zonder angst voor repercussies. |

## #2 Saldo aanpassen

|  |  |
| --- | --- |
| Naam | Ander ID meegeven |
| Versie | 1.0 |
| Actor | Werknemer |
| Use Cases | * Inzien resterende saldo |
| Bechrijving | Een werknemer of manager past onterecht het saldo van verlofuren of andere voordelen aan, bijvoorbeeld door gebruik te maken van een valse identificatie of door te profiteren van systeemfouten. |
| Scenario’s | * Een werknemer past zijn eigen verlofsaldo aan zonder toestemming of buiten de vastgestelde procedures om. * Een manager wijzigt het saldo van een werknemer om extra verlofdagen toe te kennen zonder de juiste goedkeuring. * Een werknemer gebruikt toegang van een collega om hun saldo te manipuleren. |
| Impact | * Financieel: Onterecht uitbetaalde verlofdagen kunnen leiden tot aanzienlijke financiële verliezen voor de organisatie. * Verlies van vertrouwen: Medewerkers kunnen het vertrouwen in het management en het systeem verliezen, wat leidt tot een negatieve werkcultuur. * Operationele verstoring: Onjuiste saldi kunnen leiden tot problemen met personeelsplanning en beschikbare resources. |
| Maatregelen | * Toegangscontrole: Implementeer strikte toegangscontroles en machtigingen voor het aanpassen van saldo’s, zodat alleen bevoegde personen deze wijzigingen kunnen doorvoeren. * Auditlogs: Zorg voor gedetailleerde auditlogs van alle wijzigingen aan saldi, zodat verdachte activiteiten gemakkelijk kunnen worden geïdentificeerd en onderzocht. * Regelmatige controles: Voer periodieke controles uit op saldo-aanpassingen om onregelmatigheden tijdig op te sporen. * Training en bewustwording: Train medewerkers in de procedures rondom saldo-aanpassingen en de gevolgen van misbruik. |

## #3 Scripts toevoegen

|  |  |
| --- | --- |
| Naam | Ander ID meegeven |
| Versie | 1.0 |
| Actor | Werknemer/admin |
| Use Cases | * Verlof aanvragen * Accounts beheren * Groepen beheren * Categorieën beheren |
| Bechrijving | Een werknemer of manager voegt ongeautoriseerde scripts toe aan het systeem, met als doel de functionaliteit te manipuleren of onterecht toegang te verkrijgen tot gegevens en functionaliteiten. |
| Scenario’s | * Een werknemer voegt een script toe dat automatisch verlofaanvragen indient zonder de juiste goedkeuring. * Een manager plaatst een script dat gegevens van andere medewerkers kan inzien of manipuleren. * Een werknemer gebruikt een script om systeeminstellingen te wijzigen, wat de integriteit van de gegevens aantast. |
| Impact | * Gegevensintegriteit: Ongeautoriseerde scripts kunnen leiden tot onjuiste of vervalste gegevens in het systeem, wat invloed heeft op rapportages en besluitvorming. * Beveiligingsrisico: Het toevoegen van scripts kan kwetsbaarheden creëren in de beveiliging van het systeem, waardoor het risico op datalekken toeneemt. * Operationele verstoring: De werking van het systeem kan verstoord worden, wat leidt tot downtime of andere technische problemen. |
| Maatregelen | * Toegangsbeperkingen: Implementeer strikte toegangsbeperkingen zodat alleen bevoegde medewerkers scripts kunnen toevoegen of wijzigen. * Code-review proces: Introduceer een proces voor het controleren van scripts voordat ze aan het systeem worden toegevoegd, om mogelijke risico's te identificeren. * Monitoring en logging: Houd logs bij van alle toevoegingen van scripts, en monitor deze logs regelmatig om verdachte activiteiten te detecteren. * Training: Bied training aan over de risico's van ongeautoriseerd gebruik van scripts en de gevolgen voor de organisatie. |

## #4 Brute force aanvallen

|  |  |
| --- | --- |
| Naam | Ander ID meegeven |
| Versie | 1.0 |
| Actor | Werknemer/manager/admin |
| Use Cases | * Inloggen |
| Bechrijving | Een kwaadwillende actor probeert herhaaldelijk in te loggen op het systeem door meerdere combinaties van gebruikersnamen en wachtwoorden te gebruiken om toegang te krijgen tot gevoelige informatie. |
| Scenario’s | * Een aanvaller probeert via geautomatiseerde tools meerdere wachtwoordcombinaties voor een werknemersaccount totdat hij toegang krijgt. * Een werknemer of manager die zijn wachtwoord vergeten is, voert herhaaldelijk verkeerde wachtwoorden in om weer toegang te krijgen, waardoor het account tijdelijk wordt geblokkeerd. * Een insider threat probeert via brute force toegang te krijgen tot gevoelige data door te profiteren van een zwak wachtwoordbeleid. |
| Impact | * Gegevenslekken: Toegang tot vertrouwelijke informatie kan leiden tot datalekken, wat de organisatie schade toebrengt. * Reputatieschade: Klanten en medewerkers kunnen het vertrouwen in de organisatie verliezen als gevoelige informatie wordt gelekt. |
| Maatregelen | * Accountvergrendeling: Implementeer een beleid voor accountvergrendeling na een bepaald aantal mislukte inlogpogingen, zodat automatische aanvallen worden vertraagd. * Twee-factor-authenticatie (2FA): Voer 2FA in om een extra beveiligingslaag toe te voegen, waardoor het moeilijker wordt voor aanvallers om toegang te krijgen, zelfs als ze het wachtwoord kennen. * Wachtwoordcomplexiteit: Vereis sterke wachtwoorden met een combinatie van letters, cijfers en symbolen, en wijzig deze regelmatig. |

## #5 Man in the middle

|  |  |
| --- | --- |
| Naam | Ander ID meegeven |
| Versie | 1.0 |
| Actor | Werknemer/manager/admin |
| Use Cases | * (Actor’s, alles) |
| Bechrijving | Een kwaadwillende actor onderschept en manipuleert communicatie tussen een werknemer/manager en het systeem, waardoor gegevens worden gestolen of gewijzigd zonder dat de betrokken partijen zich hiervan bewust zijn. |
| Scenario’s | * Een werknemer logt in op het systeem via een onveilige verbinding, waardoor een aanvaller in staat is om inloggegevens te onderscheppen. * Een manager die verlofaanvragen goedkeurt, heeft zijn communicatie via een onbeveiligd netwerk lopen, waardoor een aanvaller toegang krijgt tot vertrouwelijke informatie. * Een werknemer ontvangt een vervalste e-mail die lijkt te komen van het IT-team, waarin gevraagd wordt om inloggegevens te verstrekken via een kwaadaardige website. |
| Impact | * Gegevensdiefstal: Gevoelige informatie, zoals inloggegevens en persoonlijke gegevens, kan worden gestolen en misbruikt. * Reputatieschade: Het verlies van vertrouwen van medewerkers en klanten kan schadelijk zijn voor de reputatie van de organisatie. * Financiële verliezen: Kosten die voortvloeien uit herstelmaatregelen en mogelijke juridische gevolgen kunnen financieel belastend zijn. * Operationele verstoring: Wijzigingen in gegevens kunnen leiden tot fouten in processen en beslissingen. |
| Maatregelen | * Versleuteling: Implementeer versleuteling (zoals HTTPS) voor alle gegevensoverdracht tussen gebruikers en het systeem om onderschepping te voorkomen. * VPN gebruik: Moedig medewerkers aan om een Virtual Private Network (VPN) te gebruiken wanneer ze verbinding maken met bedrijfsnetwerken, vooral vanaf externe locaties. * Bewustwordingstraining: Train medewerkers over de risico's van man-in-the-middle aanvallen en hoe ze verdachte communicatie kunnen herkennen. |