Risicoanalyse  
  
Use Case

Risicoanalyse

Risico-kaart

|  |  |  |
| --- | --- | --- |
| Use Cases | | |
| Use Case | Als (Role) | Wil ik **<functionaliteit>** |
| 1 | **Als anonieme gebruiker** | **wil ik een zoekfunctie kunnen gebruiken om e-cars te huren.** |
| 2 | **Als anonieme gebruiker** | **wil ik een overzicht van de vijf e-cars met de laagste huurtarieven kunnen zien.** |
| 3 | **Als huurder** | **wil ik mijn persoonlijke gegevens kunnen invoeren om een e-car te huren.** |
| 4 | **Als verhuurder** | **wil ik een account kunnen aanmaken en inloggen om mijn auto's te beheren.** |

**Risicoanalyse**

**Use Case 1: Als anonieme gebruiker wil ik een zoekfunctie kunnen gebruiken om e-cars te huren.**

**Risico's:**

* **DoS-aanvallen:** Overbelasting van de zoekfunctie door veelvuldige aanvragen.
* **Injection-aanvallen:** Kwetsbaarheid voor SQL-injectie bij zoekopdrachten.
* **Onjuiste inputvalidatie:** Ontbreken van validatie kan leiden tot incorrecte zoekresultaten of fouten.

**Maatregelen:**

* **Rate limiting:** Beperking van het aantal zoekopdrachten per IP-adres.
* **Input sanitization:** Gebruik van voorbereid statements en input sanitization om SQL-injecties te voorkomen.
* **Input validatie:** Implementeren van strikte validatieregels voor zoektermen.

**Use Case 2: Als anonieme gebruiker wil ik een overzicht van de vijf e-cars met de laagste huurtarieven kunnen zien.**

**Risico's:**

* **Data exposure:** Onbevoegde toegang tot gevoelige informatie.
* **DoS-aanvallen:** Overbelasting van de overzichtspagina door veelvuldige aanvragen.
* **Onjuiste sortering:** Mogelijke fouten bij het sorteren van huurtarieven.

**Maatregelen:**

* **Access control:** Beveiliging van gevoelige gegevens en minimale gegevens blootstellen.
* **Rate limiting:** Beperking van het aantal verzoeken per IP-adres.
* **Validatie en verificatie:** Zorgvuldige controle en sortering van huurtarieven voordat ze worden weergegeven.

**Use Case 3: Als huurder wil ik mijn persoonlijke gegevens kunnen invoeren om een e-car te huren.**

**Risico's:**

* **Data leakage:** Blootstelling van persoonlijke gegevens.
* **Injection-aanvallen:** Kwetsbaarheid voor SQL-injectie bij invoer van gegevens.
* **Onjuiste inputvalidatie:** Mogelijke foutieve invoer van gegevens.

**Maatregelen:**

* **Data encryption:** Versleuteling van persoonlijke gegevens in de database.
* **Input sanitization:** Gebruik van voorbereid statements en input sanitization om SQL-injecties te voorkomen.
* **Input validatie:** Implementeren van strikte validatieregels voor alle ingevoerde gegevens.

**Use Case 4: Als verhuurder wil ik een account kunnen aanmaken en inloggen om mijn auto's te beheren.**

**Risico's:**

* **Brute force aanvallen:** Pogingen om wachtwoorden te raden en toegang te krijgen tot accounts.
* **Account hijacking:** Onbevoegde toegang tot verhuurdersaccounts.
* **Data leakage:** Blootstelling van gevoelige accountgegevens.

**Maatregelen:**

* **Rate limiting:** Beperking van het aantal inlogpogingen per IP-adres.
* **Multi-factor authentication:** Extra beveiligingslaag bij het inloggen.
* **Input validatie:** Implementeren van strikte validatieregels voor alle accountgerelateerde gegevens.

Risico-kaart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Use Case** | **Risico** | **Impact** | **Waarschijnlijkheid** | **Prioriteit** | **Maatregel** |
| 1 | DoS-aanvallen | Hoog | Middel | Hoog | Rate limiting, audit logs |
| 1 | Injection-aanvallen | Hoog | Hoog | Hoog | Input sanitization, gebruik voorbereid statements |
| 1 | |  |  | | --- | --- | |  | Onjuiste inputvalidatie | | Middel | Middel | Middel | |  |  | | --- | --- | |  | Strikte validatieregels | |
| 2 | Data exposure | Hoog | Middel | Hoog | Access control, minimale gegevens blootstellen |
| 2 | DoS-aanvallen | Hoog | Middel | Hoog | Rate limiting, audit logs |
| 2 | Onjuiste sortering | Middel | laag | laag | |  |  | | --- | --- | |  | Validatie en verificatie | |
| 3 | Data leakage | Hoog | Middel | Hoog | |  |  | | --- | --- | |  | Data encryption | |
| 3 | |  |  | | --- | --- | |  | Injection-aanvallen | | Hoog | Hoog | Hoog | |  |  | | --- | --- | |  | Input sanitization, gebruik voorbereid statements | |
| 3 | |  |  | | --- | --- | |  | Onjuiste inputvalidatie | | Middel | Middel | Middel | |  |  | | --- | --- | |  | Strikte validatieregels | |
| 4 | |  |  | | --- | --- | |  | Brute force aanvallen | | Hoog | Middel | Hoog | Rate limiting, multi-factor authentication |
| 4 | Account hijacking | Hoog | Middel | Hoog | |  |  | | --- | --- | |  | Multi-factor authentication, audit logs | |
| 4 | Data leakage | Hoog | Middel | Hoog | Data encryption |
| 4 | Onjuiste inputvalidatie | Middel | Middel | Middel | Strikte validatieregels |