Threat Model (K_SEC)

Door: Mike Schaatsbergen, MD2A

Wat is het product?

Een webapp om als gebruiker eten te bestellen van bedrijven die eten aanbieden op de app. Een webapp waarmee bedrijven hen eten kunnen aanbieden op de app om geld te verdienen.

Op welke momenten kunnen gebruikers/bedrijven informatie leveren aan de server?

1. Login formulieren
2. Registratie formulier
3. Ajax requests
4. Nieuw product formulier
5. Instellingen formulier

Welke zijn de meest relevante veiligheids bedreigingen voor deze punten?

1. Login formulieren

    XSS, SLQ Injection, DDoS, mogelijke code injection

2. Registratie formulier

    XSS, SLQ Injection, DDoS, mogelijke code injection

3. Ajax requests

    Code injection, DDoS, cross-site request forgery

4. Nieuw product formulier

    XSS, SLQ Injection, DDoS, mogelijke code injection

5. Instellingen formulier

Het hacken/veranderen van andermans account, XSS, SLQ Injection, DDoS, mogelijke code injection

Hoe beveiligen we ertegen?

Aangezien we gebruik maken van Laravel als framework kunnen voor een groot deel al zeker zijn dat de meeste aanvallen zoals XSS of SQL Injection al moeilijk tot bijna onmogelijk zijn om te proberen.

We zullen aandacht moeten besteden aan het beveiligen van acties die alleen bepaalde mensen mogen doen, zoals: heet aanpassen van ander mensen hun instellingen. Verder zullen we ook aandacht moeten besteden aan het beveiligen van AJAX requests naar de servers, we zullen moeten verifieren dat die requests van onze webservers komen en niet van externe severs die misschien proberen aan te vallen.

Tijdens development zo hierop moeten worden toegevoegt.