dinsdag 28 januari 2020

Test Plan Boomershop

Sohil, Joshua, Wiebe, Taurese en Osman

LOGIN, ACCOUNT AANMAKEN

- Gevaar: SQL Injection
- Hoe te voorkomen

Gebruik LIMIT en andere SQL-besturingselementen in query's om massale openbaarmaking van records te voorkomen in geval van SQL-injectie.

CONTROLEREN/REGELEN SERVER BESCHIKBAARHEID

- Gevaar: Lekken van geheime data
- Hoe te voorkomen

Classificeer gegevens die door een applicatie zijn verwerkt, opgeslagen of verzonden. Bepaal welke gegevens gevoelig zijn volgens privacywetgeving, wettelijke vereisten of zakelijke behoeften.

VERWIJDEREN MAALTIJDEN, BESTELLING PLAATSEN

- Gevaar: POST modificatie (andere producten verwijderen)
- Hoe te voorkomen

Implementeer eenmaal toegangscontrolemechanismen en hergebruik deze in de hele applicatie, inclusief het minimaliseren van CORS-gebruik.

ADRESGEGEVENS AANLEVEREN, ONLINE BETALEN, EEN BESTELLING KAN ALLEEN GEDAAN WORDEN DOOR ONLINE BETALINGEN, CASH GELD WORDT NIET GEACCEPTEERD

- Gevaar: Data lekken

- Hoe te voorkomen

Zorg ervoor dat actuele en krachtige standaardalgoritmen, protocollen en sleutels aanwezig zijn; gebruik goed sleutelbeheer.

BEKIJKEN MAALTIJDDETAILS, ZOEKEN NAAR AANBIEDERS IN DE DIRECTE OMGEVING ZOEKEN NAAR SOORTEN MAALTIJDEN, BEZORGSTATUS BEKIJKEN

- Gevaar: XSS
- Hoe te voorkomen

Ontsnappen aan niet-vertrouwde HTTP-verzoekgegevens op basis van de context in de HTML-uitvoer (hoofdtekst, kenmerk, JavaScript, CSS of URL) lost gereflecteerde en opgeslagen XSS-kwetsbaarheden op. Het cheatsheet ‘XSS-preventie’ van OWASP bevat details over de vereiste technieken voor gegevensontsnapping.

BEHEREN VAN DE AANBIEDERS, PRODUCTBEHEER VAN DE AANBIEDERS
BEHEREN VAN BEZORGERS, BESTEL ORDER DETAILS BEHEREN, ACCEPTATIE ACCOUNT, MAALTIJDEN EN DETAILS TOEVOEGEN, WIJZIGEN DETAILS EN MAALTIJD GEGEVENS, MAALTIJDEN TOEVOEGEN AAN WINKELWAGEN

- Gevaar: SQL Injection, XSS
- Hoe te voorkomen

De voorkeursoptie is om een veilige API te gebruiken, die het gebruik van de tolk volledig vermijdt of een geparametriseerde interface biedt, of migreren om Object Relational Mapping Tools (ORM's) te gebruiken. Opmerking: Zelfs wanneer deze zijn geparametreerd, kunnen opgeslagen procedures nog steeds SQL-injectie introduceren.