|  |  |  |
| --- | --- | --- |
| **OFFENCE/DEFENCE** | | |
| Hack-avond WAP5 | | 20/12/2021 |
| Groep | | **Offence**  Must Have Caffeine  Richard de Jong  Ruud Beerkens  Teun Cortooms  **Defence**  Who’s The Boss |
| <Tijd> | <Activiteit> | <Beschrijving> |
| 20:45 | Errors oproepen mbv velden      ‘ in de GET url wordt wel meegestuurd, maar geeft een lege lijst als resultaat. De input wordt goed escaped.      E-mail en phone worden ook escaped. Maar hebben het probleem dat de database vervuild wordt omdat er geen backend validatie plaatsvindt. | **Injection (A1)**  Injectiekwetsbaarheden zoals SQL-, OS-commando- of LDAP-injectie, ontstaan wanneer niet-geverifieerde data door een hacker wordt verzonden als onderdeel van een commando of query. Deze data kan onbedoelde commando’s uitvoeren of ongeautoriseerde toegang tot gegevens verschaffen.  **OTG-BUSLOGIC-001**  Test Business Logic Data Validation |
|  |  | **Broken Authentication (A2)**  Authenticatiecontrole- en sessiebeheermechanismes worden vaak niet correct geïmplementeerd, waardoor aanvallers de identiteit van andere gebruikers aan kunnen nemen. | |
|  | Geen autorisatie op endpoints. | **Sensitive Data Exposure (A3)**  Veel applicaties en API-endpoints beschermen gevoelige gegevens onvoldoende. Denk hierbij aan persoonsgegevens, documenten en autorisatiegegevens. Kwaadwillende kunnen deze dan stelen of wijzigen voor creditcardfraude, identiteitsdiefstal of andere misdrijven. Gevoelige gegevens moeten extra worden beschermd door middel van versleuteling of andere speciale voorzorgsmaatregelen. |
|  |  | **XML External Entities (A4)**  Verouderde of slecht geconfigureerde XML-verwerkers staan vaak het laden van externe entiteiten toe. Aanvallers kunnen dit misbruiken om bijvoorbeeld toegang tot lokale bestanden te krijgen, os-commando’s uit te voeren of DoS-situaties te creëren om het systeem (tijdelijk) onbruikbaar te maken. | |
| 20:30 | Script wordt wel escaped, maar business logic valideert de input niet. We kunnen rotzooi sturen naar de database, waardoor deze onbruikbaar wordt.  In de database worden ook negatieve aantallen geaccepteerd en opgeslagen. Dit leidt tot een negatieve prijs op de order als de web applicatie verder wordt uitgebouwd. | **Cross-Site Scripting (XSS) (A7)**  We spreken van XSS-injectie als een applicatie gegevens zonder filtering en/of encodering naar een web browser zendt. XSS-injectie stelt aanvallers in staat om scripts uit te voeren, gebruikerssessies te kapen, websites te beschadigen of de gebruiker naar andere sites te leiden.  **OTG-BUSLOGIC-001**  Test Business Logic Data Validation | |
| 21:00 | Alleen public users.  Admin logt in via framework authenticatie.    Restaurant succesvol verwijderd. Autorizatie niet geimplementeerd. | **Broken Access Control (A5)**  Beperkingen wat een gebruiker wel of niet mag uitvoeren binnen een applicatie worden in veel gevallen niet correct afgedwongen. Aanvallers kunnen deze fouten misbruiken om toegang te krijgen tot functionaliteit en/of informatie zonder dat ze hiertoe geautoriseerd zijn. | |
|  |  | **Using Components with Known Vulnerabilities (A9)**  Componenten zoals libraries, frameworks en andere software-modules draaien vaak met volledige autorisatie. Als een kwetsbaar onderdeel wordt geëxploiteerd kan dit tot dataverlies leiden of een overname van de server faciliteren. Componenten met reeds bekende kwetsbaarheden ondermijnen de beveiliging van de applicatie en faciliteren een scala aan mogelijke aanvallen. | |
|  |  | **Security Misconfiguration (A6)**  Goede beveiliging vereist een correcte configuratie die wordt afgestemd op de applicatie, frameworks, applicatieserver, webserver, databaseserver en platform. Beveiligingsinstellingen moeten worden gedefinieerd, geïmplementeerd en onderhouden omdat deze standaards vaak onveilig zijn. Daarnaast moet alle software up-to-date zijn. |
|  |  | **Insecure Deserialization (A8)**  Applicaties converteren objecten alvorens deze worden opgeslagen. Het terug converteren van deze objecten gebeurt vaak onveilig en kan worden misbruikt om os commando’s uit te voeren. In sommige gevallen stelt het de applicatie zelfs kwetsbaar op voor andere injectie aanvallen. |
|  |  | **Insufficient Logging & Monitoring (A10)**  Een tekort aan logging en monitoring kan aanvallers de tijd geven zich dieper in een systeem te nestelen en proberen zich permanent toegang te verschaffen. Gemiddeld wordt een lek pas na 200+ dagen gedetecteerd. Dit geeft aanvallers voldoende tijd om zelfs toegang te krijgen tot andere systemen en opgeslagen gegevens in te zien, wijzigen of zelfs te verwijderen. |