OWASP Report

My Koi Pond – Semester 4

***De OWASP Top 10 is een standaard bewustzijnsdocument voor ontwikkelaars en beveiliging van webapplicaties. Het vertegenwoordigt een brede consensus over de meest kritieke beveiligingsrisico's voor webapplicaties.***

Inhoud

[Top 10 Web Application Security Risks 1](#_Toc40955731)

[Injection. 1](#_Toc40955732)

[Maar aan welke senarios kun je dan denken? 1](#_Toc40955733)

[Hoe kun je deze hacks voorkomen? 1](#_Toc40955734)

[Ik gebruik JPA. Ik ben veilig, toch? 2](#_Toc40955735)

[Broken Authentication 3](#_Toc40955736)

[Maar aan welke senarios kun je dan denken? 3](#_Toc40955737)

[Hoe kun je deze hacks voorkomen? 3](#_Toc40955738)

[Sensitive Data Exposure 4](#_Toc40955739)

[Maar aan welke senarios kun je dan denken? 4](#_Toc40955740)

[Hoe kun je deze hacks voorkomen? 4](#_Toc40955741)

[XML External Entities (XXE) 5](#_Toc40955742)

[Maar aan welke scenario’s kun je dan denken? 5](#_Toc40955743)

[Hoe kun je deze hacks voorkomen? 5](#_Toc40955744)

[Broken Access Control 6](#_Toc40955745)

[Beperkingen op wat geauthenticeerde gebruikers mogen doen, worden vaak niet correct gehandhaafd. Aanvallers kunnen deze gebreken misbruiken om toegang te krijgen tot ongeoorloofde functionaliteit en/ of gegevens, zoals toegang krijgen tot de accounts van andere gebruikers, gevoelige bestanden bekijken, de gegevens van andere gebruikers wijzigen, toegangsrechten wijzigen, enz. 6](#_Toc40955746)

[Maar aan welke scenario’s kun je dan denken? 6](#_Toc40955747)

[Hoe kun je deze hacks voorkomen? 6](#_Toc40955748)

[Security Misconfiguration 7](#_Toc40955749)

[Maar aan welke scenario’s kun je dan denken? 7](#_Toc40955750)

[Hoe kun je deze hacks voorkomen? 7](#_Toc40955751)

[Cross-Site Scripting XSS 8](#_Toc40955752)

[Insecure Deserialization 8](#_Toc40955753)

[Using Components with Known Vulnerabilities 8](#_Toc40955754)

[Insufficient Logging & Monitoring 8](#_Toc40955755)

# Top 10 Web Application Security Risks

In dit document leg ik uit hoe OWASP wordt toegepast binnen mijn applicatie. Hierbij gebruik ik de top 10 meest voorkomende beveiligingsresico’s. In dit document ga ik niet laten zien hoe er misbruik van deze hacks kan worden gemaakt binnen mijn eigen applicatie wel geef ik algemene voorbeelden. in

Injection.

Injectiefouten, zoals SQL-, NoSQL-, OS- en LDAP-injectie, treden op wanneer niet-vertrouwde gegevens als onderdeel van een opdracht of query naar een interpreter in bijv. De backend worden gestuurd. De vijandige gegevens van de aanvaller kunnen de tolk ertoe verleiden onbedoelde opdrachten uit te voeren of toegang te krijgen tot gegevens zonder de juiste toestemming.

### Maar aan welke senarios kun je dan denken?

* Een applicatie gebruikt niet-vertrouwde gegevens bij de constructie van de volgende kwetsbare SQL-query:

String query = "SELECT \* FROM accounts WHERE custID = '" + request.getParameter ("id") + "'";

* Evenzo kan het blind vertrouwen van een applicatie in frameworks resulteren in queries die nog steeds kwetsbaar zijn (bijvoorbeeld Hibernate Query Language (HQL)):
* In beide gevallen wijzigt de aanvaller de parameterwaarde ‘id’ in zijn browser om te verzenden: ‘or‘ 1 ’=’ 1. Bijvoorbeeld:

http://example.com/app/accountView?id= 'of' 1 '=' 1

Query HQLQuery = session.createQuery ("FROM accounts WHERE custID = '" + request.getParameter ("id") + "'"));

### Hoe kun je deze hacks voorkomen?

* De voorkeursoptie is om een ​​veilige API te gebruiken, die het gebruik van de interpreter volledig vermijdt of een geparametriseerde interface biedt, of migreert om Object Relational Mapping Tools (ORM's) te gebruiken
* Gebruik positieve invoervalidatie aan serverzijde. Dit is geen volledige verdediging, aangezien voor veel toepassingen speciale tekens nodig zijn, zoals tekstgebieden of API's voor mobiele toepassingen.
* Voor eventuele resterende dynamische query's, ontsnapt u aan speciale tekens met de specifieke escape-syntaxis voor die interpreter.
* Gebruik LIMIT en andere SQL-besturingselementen binnen query's om massale openbaarmaking van records te voorkomen in het geval van SQL-injectie.

### Ik gebruik JPA. Ik ben veilig, toch?

Dit is een veel voorkomende misvatting. JPA en andere ORM's ontheffen ons van het maken van handgecodeerde SQL-instructies, maar ze zullen ons er niet van weerhouden om kwetsbare code te schrijven.

Laten we eens kijken hoe de JPA-versie van het vorige voorbeeld eruitziet:

public List<AccountDTO> unsafeJpaFindAccountsByCustomerId(String customerId) {

String jql = "from Account where customerId = '" + customerId + "'";

TypedQuery<Account> q = em.createQuery(jql, Account.class);

return q.getResultList()

.stream()

.map(this::toAccountDTO)

.collect(Collectors.toList());

}

Hetzelfde probleem dat we eerder hebben genoemd, is hier ook aanwezig: we gebruiken niet-gevalideerde invoer om een ​​JPA-query te maken, dus we worden hier blootgesteld aan hetzelfde soort misbruik.

Daarom heb ik er in mijn project voor gekozen om de mijn interfaces te extende met de JpaRepository. De JpaRepository interface zorgt ervoor dat dit niet meer mogelijk is hoe dit werkt laat ik hieronder zien ook wel parameter escaping genoemd. Dit wordt helemaal verzorgt door het framework zelf. Ook is het niet mogelijk een injection via een url te plaatsen, wel is het mogelijk gegevens van een andere gebruiker op te vragen omdat hier ook niet voldoende tijd voor was. Hateoas is zeer complex en vond het dan ook belangrijker mij hier meer in te verdiepen.

String query1 = "select \* from MyBean where id = "+ id; //onveilig

String query2 = "select \* from MyBean where id = :id"; //veilig

## Broken Authentication

Toepassingsfuncties met betrekking tot authenticatie en sessiebeheer worden vaak onjuist geïmplementeerd, waardoor aanvallers wachtwoorden, sleutels of sessietokens kunnen compromitteren of andere implementatiefouten kunnen misbruiken om de identiteit van andere gebruikers tijdelijk of permanent over te nemen.

### Maar aan welke senarios kun je dan denken?

* Automatische laten invullen van inlog gegevens, het gebruik van lijsten met bekende wachtwoorden, is een veel voorkomende aanval. Het system stuurt elke oneindig inlog gegevens tot hij een correcte terug kijgt. Deze slaat hij dan op.
* Time-outs voor applicatiesessies zijn niet correct ingesteld. Een gebruiker gebruikt een openbare computer om toegang te krijgen tot een applicatie. In plaats van "logout" te selecteren, sluit de gebruiker eenvoudig het browsertabblad en loopt weg. Een aanvaller gebruikt een uur later dezelfde browser en de gebruiker is nog steeds geverifieerd.

### Hoe kun je deze hacks voorkomen?

* Implementeer waar mogelijk multi-factor authenticatie om geautomatiseerde invulling van legitimatiegegevens, brute force en gestolen hergebruikaanvallen te voorkomen.
* Implementeer zwakke wachtwoordcontroles, zoals het testen van nieuwe of gewijzigde wachtwoorden op basis van een lijst met de 10000 slechtste wachtwoorden.
* Stem het beleid voor wachtwoordlengte, complexiteit en rotatie af op elkaar
* Beperk of vertraag mislukte inlogpogingen. Registreer alle fouten en waarschuw beheerders wanneer het vullen van referenties, brute force of andere aanvallen worden gedetecteerd.
* Gebruik een server-side, veilige, ingebouwde sessiebeheerder die na inloggen een nieuwe willekeurige sessie-ID met hoge entropie genereert. Sessie-ID's mogen niet in de URL staan, veilig worden opgeslagen en ongeldig worden gemaakt na uitloggen, inactiviteit en absolute time-outs.

In mijn applicatie maak ik gebruik van jws tokens deze token zijn encrypted maar niet volledig veilig binnen mijn applicatie. Hier is helaas niet genoeg tijd voor binnen het semester en is ook niet een Prioriteit tijdens dit semster. Wanneer ik hier wel voldoende tijd voor had zou ik graag me meer verdiepen in oauth2 authenticatie. Zowel extern als intern met behulp van bijvoorbeeld google.

## Sensitive Data Exposure

Veel webapplicaties en API's beschermen gevoelige gegevens, zoals financiën, gezondheidszorg en PII, niet goed. Aanvallers kunnen dergelijke zwak beschermde gegevens stelen of wijzigen om creditcardfraude, identiteitsdiefstal of andere misdaden uit te voeren. Gevoelige gegevens kunnen worden gecompromitteerd zonder extra bescherming, zoals versleuteling in rust of onderweg, en vereisen speciale voorzorgsmaatregelen bij uitwisseling met de browser.

### Maar aan welke senarios kun je dan denken?

* Een applicatie versleutelt creditcardnummers in een database met automatische databasecodering. Deze gegevens worden echter automatisch gedecodeerd wanneer ze worden opgehaald, waardoor een SQL-injectiefout creditcardnummers in duidelijke tekst kan ophalen.
* Een site gebruikt of handhaaft geen TLS voor alle pagina's of ondersteunt zwakke codering. Een aanvaller bewaakt het netwerkverkeer (bijvoorbeeld op een onveilig draadloos netwerk), downgradet verbindingen van HTTPS naar HTTP, onderschept verzoeken en steelt de sessiecookie van de gebruiker. De aanvaller herhaalt deze cookie en kaapt de (geverifieerde) sessie van de gebruiker, waarbij hij toegang krijgt tot de privégegevens van de gebruiker of deze wijzigt. In plaats van het bovenstaande zouden ze alle getransporteerde gegevens kunnen veranderen, b.v. de ontvanger van een geldoverdracht.
* De wachtwoorddatabase gebruikt unsalted of eenvoudige hashes om ieders wachtwoorden op te slaan. Door een fout in het uploaden van bestanden kan een aanvaller de wachtwoorddatabase ophalen. Alle unsalted hashes kunnen worden geanaliseerd met een regenboogtabel met vooraf berekende hashes. Hashes gegenereerd door eenvoudige of snelle hash-functies kunnen door GPU's worden gekraakt, zelfs als ze zijn gesalt.

### Hoe kun je deze hacks voorkomen?

* Classificeer gegevens die zijn verwerkt, opgeslagen of verzonden door een applicatie. Identificeer welke gegevens gevoelig zijn volgens privacywetgeving, wettelijke vereisten of zakelijke behoeften.
* Pascontroles toe volgens de classificatie.
* Sla gevoelige gegevens niet onnodig op. Gooi het zo snel mogelijk weg of gebruik PCI DSS-compatibele tokenisatie of zelfs truncatie. Gegevens die niet worden bewaard, kunnen niet worden gestolen.
* Zorg ervoor dat up-to-date en sterke standaardalgoritmen, protocollen en sleutels aanwezig zijn; gebruik goed sleutelbeheer.
* Versleutel alle gegevens die onderweg zijn met veilige protocollen zoals TLS met perfecte forward secrecy (PFS) -codes, coderingsprioritering door de server en veilige parameters. Dwing versleuteling af met richtlijnen zoals HTTP Strict Transport Security (HSTS).
* Schakel caching uit voor reacties die gevoelige gegevens bevatten.
* Sla wachtwoorden op met behulp van sterke adaptieve en gezouten hashingfuncties met een werkfactor (vertragingsfactor), zoals Argon2, scrypt, bcrypt of PBKDF2.
* Controleer onafhankelijk de effectiviteit van configuratie en instellingen.

Zoals eerder al aangegevens is in mijn project de security niet de hoogste Prioriteit. Alle wachtwoorden daarintegen worden wel gehast met het bcrypt protocol en veilig opgeslagen in de database. Overige gevens op de applicatie hebben geen encrypty nodig omdat deze opgeslagen gevens niet schadelijk zijn en ongevoelig. Waneer ik wel voldoende tijd had gehad had ik me graag verdiept in het verder salten van de gevoelige data met een personal key ook had ik dan kunnen kijken naar een validator voor wachtwoorden die bijvoorbeeld een rainbowtable checkt.

## XML External Entities (XXE)

Veel oudere of slecht geconfigureerde XML-processors evalueren externe entiteitsreferenties binnen XML-documenten. Externe entiteiten kunnen worden gebruikt om interne bestanden vrij te geven met behulp van de bestands-URI-handler, interne bestandsshares, interne poortscanning, externe code-uitvoering en denial of service-aanvallen.

### Maar aan welke scenario’s kun je dan denken?

* De aanvaller probeert gegevens van de server te extraheren:

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>

<foo>&xxe;</foo>

* Een aanvaller onderzoekt het privé-netwerk van de server door de bovenstaande ENTITY-regel te wijzigen in:

<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>

* Een aanvaller probeert een denial-of-service-aanval uit door een potentieel eindeloos bestand op te nemen:

<!ENTITY xxe SYSTEM "file:///dev/random" >]>

### Hoe kun je deze hacks voorkomen?

* Gebruik waar mogelijk minder complexe gegevensindelingen zoals JSON en vermijd serialisering van gevoelige gegevens.
* Patch of upgrade alle XML-processors en bibliotheken die in gebruik zijn door de applicatie of op het onderliggende besturingssysteem. Gebruik afhankelijkheidscheckers. Werk SOAP bij naar SOAP 1.2 of hoger.
* Schakel XML externe entiteit en DTD-verwerking uit in alle XML-parsers in de applicatie, volgens de OWASP Cheat Sheet ‘XXE Prevention’.
* Implementeer positieve ("whitelisting") invoervalidatie, filtering of opschoning aan serverzijde om vijandige gegevens in XML-documenten, headers of nodes te voorkomen.
* Controleer of de functionaliteit voor het uploaden van XML- of XSL-bestanden inkomende XML valideert met XSD-validatie of vergelijkbaar.

Voor mijn applicatie gebruik ik de sjon gegevensindelingen voor het terug koppelen naar de frontend ook het receiven in het sjon formaat. Dit is niet van toepassing op mijn applicatie omdat xml niet wordt gebruikt.

## Broken Access Control

## Beperkingen op wat geauthenticeerde gebruikers mogen doen, worden vaak niet correct gehandhaafd. Aanvallers kunnen deze gebreken misbruiken om toegang te krijgen tot ongeoorloofde functionaliteit en/ of gegevens, zoals toegang krijgen tot de accounts van andere gebruikers, gevoelige bestanden bekijken, de gegevens van andere gebruikers wijzigen, toegangsrechten wijzigen, enz.

### Maar aan welke scenario’s kun je dan denken?

* De applicatie gebruikt niet-geverifieerde gegevens in een SQL-aanroep die toegang heeft tot accountgegevens:

pstmt.setString(1, request.getParameter("acct"));

ResultSet results = pstmt.executeQuery( );

Een aanvaller wijzigt eenvoudig de ‘acct’ -parameter in de browser om het gewenste accountnummer te verzenden. Als de aanvaller niet correct is geverifieerd, heeft hij toegang tot het account van elke gebruiker.

<http://example.com/app/accountInfo?acct=notmyacct>

* Een aanvaller forceert eenvoudig browses om URL's te targeten. Beheerdersrechten zijn vereist voor toegang tot de beheerderspagina.

http://example.com/app/getappInfo

<http://example.com/app/admin_getappInfo>

If an unauthenticated user can access either page, it’s a flaw. If a non-admin can access the admin page, this is a flaw.

### Hoe kun je deze hacks voorkomen?

* JWT-tokens moeten na uitloggen ongeldig worden gemaakt op de server.

Ontwikkelaars en QA-medewerkers moeten functionele toegangscontrole-eenheid en integratietests opnemen.

* Snelheidslimiet aantal requests per minuut of dag API- en controllertoegang om de schade door geautomatiseerde aanvalstooling te minimaliseren.
* Registreer mislukte toegangscontroles en waarschuw beheerders indien nodig (bijv. Herhaalde storingen).
* Modeltoegangscontroles moeten het eigendom van records afdwingen, in plaats van te accepteren dat de gebruiker elk record kan maken, lezen, bijwerken of verwijderen.

Mijn applicatie maakt door de tijdsdruk niet volledig gebruik van het authorization management system van spingboot security. Mijn applicatie maakt vooralsnog alleen gebruik van authorization checks op de frontend. Ik heb natuurlijk wel uitgezocht hoe het werkt en toegepast kan worden mocht het ooit toegepast worden in de backend. Wanneer er voldoende tijd was had ik hier een extra validatie kunnen bouwen die het checken van het aantal inlog pogingen checked en een request limiet insteld.

## Security Misconfiguration

Verkeerde configuratie van de beveiliging is het meest voorkomende probleem. Dit is meestal het gevolg van onveilige standaardconfiguraties, onvolledige of ad-hocconfiguraties, open cloudopslag, verkeerd geconfigureerde HTTP-headers en uitgebreide foutmeldingen die gevoelige informatie bevatten. Niet alleen moeten alle besturingssystemen, frameworks, bibliotheken en applicaties veilig zijn geconfigureerd, maar ze moeten ook tijdig worden gepatcht / geüpgraded.

### Maar aan welke scenario’s kun je dan denken?

* De application server wordt geleverd met voorbeeldtoepassingen die niet van de productieserver zijn verwijderd. Deze voorbeeldtoepassingen hebben bekende beveiligingsfouten die aanvallers gebruiken om de server te beschadigen. Als een van deze applicaties de beheerdersconsole is en de standaardaccounts niet zijn gewijzigd, logt de aanvaller in met standaardwachtwoorden en neemt het over.
* Directory listing is niet uitgeschakeld op de server. Een aanvaller ontdekt dat ze eenvoudig mappen kunnen weergeven. De aanvaller vindt en downloadt de gecompileerde Java-klassen, die ze decompileren en reverse-engineeren om de code te bekijken. De aanvaller vindt dan een ernstig gebrek aan toegangscontrole in de applicatie.
* De configuratie van de applicatieserver staat gedetailleerde foutmeldingen toe, b.v. stacktraces, terug te sturen naar gebruikers. Dit stelt mogelijk gevoelige informatie of onderliggende gebreken bloot, zoals componentenversies waarvan bekend is dat ze kwetsbaar zijn.

### Hoe kun je deze hacks voorkomen?

* Een herhaalbaar verhardingsproces dat het snel en gemakkelijk maakt om een ​​andere omgeving te implementeren die goed is vergrendeld. Ontwikkelings-, QA- en productieomgevingen moeten allemaal identiek worden geconfigureerd, met verschillende referenties die in elke omgeving worden gebruikt. Dit proces moet worden geautomatiseerd om de inspanning die nodig is om een ​​nieuwe veilige omgeving in te richten tot een minimum te beperken.
* Een minimaal platform zonder onnodige functies, componenten, documentatie en voorbeelden. Verwijder of installeer niet-gebruikte functies en frameworks.
* Een gesegmenteerde applicatiearchitectuur die een effectieve, veilige scheiding tussen componenten of tenants biedt, met segmentatie-, containerisatie- of cloudbeveiligingsgroepen (ACL's).
* Een geautomatiseerd proces om de effectiviteit van de configuraties en instellingen in alle omgevingen te verifiëren.

Error handeling binnen mijn applicatie word afgehandeld met spring rest data. Deze is geconfigureerd naar mijn wensen. Verdere restricties zijn nog niet toepast zoals rollen binnen de applicatie wel is het inloggen vereist om data te kunnen uitlezen. Ook is er een implementatie van hateoas hal die restricties legt op het gebruik van id binnen de applicatie.

## Cross-Site Scripting XSS

XSS-fouten treden op wanneer een applicatie niet-vertrouwde gegevens op een nieuwe webpagina opneemt zonder de juiste validatie of ontsnapping, of een bestaande webpagina bijwerkt met door de gebruiker verstrekte gegevens met behulp van een browser-API die HTML of JavaScript kan maken. Met XSS kunnen aanvallers scripts uitvoeren in de browser van het slachtoffer, die gebruikerssessies kunnen kapen, websites kunnen beschadigen of de gebruiker kunnen omleiden naar kwaadaardige sites.

## Insecure Deserialization

Onveilige deserialisatie leidt vaak tot uitvoering van externe code. Zelfs als gebreken in de deserialisatie niet leiden tot uitvoering van externe code, kunnen ze worden gebruikt om aanvallen uit te voeren, waaronder herhalingsaanvallen, injectie-aanvallen en escalatie-aanvallen met bevoegdheden.

## Using Components with Known Vulnerabilities

Componenten, zoals bibliotheken, frameworks en andere softwaremodules, werken met dezelfde rechten als de applicatie. Als een kwetsbaar onderdeel wordt misbruikt, kan een dergelijke aanval ernstig gegevensverlies of overname van servers vergemakkelijken. Applicaties en API's die componenten gebruiken met bekende kwetsbaarheden kunnen de verdediging van applicaties ondermijnen en verschillende aanvallen en impacts mogelijk maken.

## Insufficient Logging & Monitoring

Onvoldoende logging en monitoring, in combinatie met ontbrekende of ineffectieve integratie met incidentrespons, stelt aanvallers in staat systemen verder aan te vallen, doorzettingsvermogen te behouden, naar meer systemen te draaien en gegevens te manipuleren, te extraheren of te vernietigen. De meeste inbreukonderzoeken laten zien dat de tijd om een ​​inbreuk te detecteren meer dan 200 dagen bedraagt, meestal gedetecteerd door externe partijen in plaats van interne processen of monitoring.