Probleemstelling

Het probleem is dat tegenwoordig websites kwetsbaar zijn voor cyber aanvallen die verricht worden door hackers. Hackers proberen deze kwetsbaarheden te exploiteren met als doel om schade toe te richten aan een website. Er zijn nog veel websites die makkelijk exploiteerbare kwetsbaarheden vertonen. In de meeste gevallen weet de eigenaar niets af van deze kwetsbaarheden. Websites hebben tegenwoordig toegang tot kostbare data, ik zeg toegang omdat de data opgeslagen staat in een database. Via de website kan een gebruiker toegang krijgen tot deze database. De website is ook waar de meeste kwetsbaarheden zich bevinden, hackers zijn dus ook erop uit om van deze kwetsbaarheden gebruikt te maken om aan de kostbare data te komen. Websites hebben verschillende doeleinden. Dit bepaald over wat voor data een website beschikt en dus ook de kostbaarheid van de data. Neem een webshop als voorbeeld, deze heeft als gevoelige data klantengegevens, productgegevens, financiële gegevens. Wanneer er een kwetsbaarheid voordoet op een webshop dan kan je je voorstellen dat het flink kan mis lopen wanneer de gegevens naar buiten worden gelekt.

Doelstelling

Zoals eerder gezegd weten de eigenaren meestal niet dat zich kwetsbaarheden voor doen op hun websites. Hierdoor zullen zij weinig tot geen tijd besteden aan het verbeteren van hun website beveiliging dit kan tot grote gevolgen leiden. De doel is om deze website eigenaren bewust te maken van de kwetsbaarheden die zich op hun websites bevinden zodat zij actie kunnen ondernemen om de beveiliging van hun website aan te scherpen.

Opdracht

De wijze waarop dit gebeurd is al vastgesteld door mijn opdrachtgever. Met behulp van een web security scanner zal er een rapport geproduceerd worden die aantoont waar de kwetsbaarheden zich bevinden. De web security scanner moet echter nog wel gebouwd worden, dit is waar ik tot mijn recht kom. Ik ben in dienst genomen om de security software te schrijven. Er is nog helemaal niks, dus is zal van scratch moeten beginnen wat ook de uitdaging is.

Hoofdvraag

Hoe kan ik met behulp van een web security scanner de website eigenaren bewust maken van de kwetsbaarheden die zich bevinden op hun website(s)?

Deelvragen

* Wat is een website?
* Wat is web security
* Wat maakt OWASP 10-top lijst zo belangrijk?
* Wat zijn bestaande scan applicaties?
* Wat zijn de belangrijkste features van acunetix?
* Wat voor data verzameld acunetix?
* Test bestaande scan applicaties?
* Hoe groot is het probleem?

Wat zijn websites?

Een website is een verzameling van webpagina’s waar een gebruiker doormiddel van hyperlinks door heen kan navigeren. Websites worden geschreven in de markup taal HTML en kunnen bekeken worden op een webbrowser. Websites worden gehost op een server, servers over de hele wereld zijn met elkaar verbonden om een netwerk te vormen. Deze netwerk noem je de Wereld Wijde Web (WWW).

Wat is web security?

Web security is een vertakking van Informatie beveiliging dat zich specifiek bezig houdt met de beveiliging van websites. Web beveiliging werd echter pas een probleem met de komst van web 2.0. Bij de voorganger, web 1.0 konden gebruikers voornamelijk alleen informatie te bekijken. De web beveiliging problemen begonnen echt pas een rol te spelen op de punt dat gebruikers meer rechten verkregen op de websites. Gebruikers konden naast het bekijken van informatie ook informatie creëren en bewerken. Voorbeeld hiervan is het aanmaken van accounts voor een internet dienst. Deze veranderingen brachten niet alleen innovatie manieren van informatiebeheer met zich mee maar ook veel beveiliging issues. Een grote beveiligingsprobleem dat optrad met de komst van web 2.0 is het verzenden van informatie naar de server in de vorm van een verzoek. Dit simpele concept wat in wezen een vorm is van communicatie tussen gebruiker en server hebben hackers jaren lang gebruikt om websites te comprimeren, en nog steeds. Over de jaren zijn er nog veel meer beveiliging bedreigingen ontdekt. Er is veel onderzoek gedaan naar beveiliging bedreigingen zo heeft Bedrijven hebben zich gespecialiseerd in het beveiligen van websites, zo brengt OWASP ieder jaar een top 10 lijst van de meest voorkomende kwetsbaarheden [OWASP].

OWASP top 10 lijst

A1 Injection

A2 Broken Authentication end Session Management (XSS)

A3 Cross Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Missing Function Level Access Control

A8 Cross Site Request Forgery Attacks

A9 Using Components with Known Vulnerabilities Components

A10 Unvalidated Redirects and Forwards

[checkmarx, 2017]

Welke kwetsbaarheden kunnen voorkomen op een website?

In dit deel zal ik het onderdeel beveiligingskwetsbaarheden uitgebreider behandelen. Zoals al eerder geschreven kunnen websites meer kwetsbaarheden hebben dan er op in hand te tellen is. Echter zal ik mij richten op de top 10 lijst die OWASP heeft opgesteld omdat deze de meest voorkomen in een website en dus ook vaak worden exploiteert door hackers.

A1 Injection

Injecties zijn cyberaanvallen die ervoor zorgen dat er code met kwaadaardige bedoelingen van een applicatie door wordt verzonden naar een ander systeem. Deze aanvallen verrichten aanroepen (Calls) naar besturing systemen via systeem aanroepen, externe programma’s via shell commando’s, en ook aanroepen naar de backend systemen zoals databases, hier wordt vooral SQL voor gebruikt (SQL injectie), [OWASP injection flaws, 2017]. Webapplicaties maken veel gebruik van externe programma’s voor het uitvoeren van specifieke taken. Bij het gebruik van een externe applicatie worden HTTP request uitgevoerd, indien deze niet goed opgevangen worden kunnen aanvallers kwaadaardige injecties sturen naar de externe applicaties, die op hun beurt het blind zullen uitvoeren. Er zijn verschillende types van injecties, maar SQL injectie zijn de meest gevaarlijke vorm van injecties. //Kwetsbaarheden toelichten

A2 Broken Authentication and Session Management (XSS)

Authenticatie en session management hebben beide te maken met het managen van gebruikers en het behouden van de identity van de gebruiker. Authenticatie is het proces van bepalen of de gebruiker echt is wie hij beweert dat hij is. Session management zoals de naam al suggereert gaat over het managen van actieve sessions. Deze kwetsbaarheid kan er naar toe leiden dat aanvallers onbevoegd toegang krijgen. //Kwetsbaarheid toelichten

A3 Cross Site Scripting (XSS)

Cross site scripting is een aanval waarbij kwaadaardige scripts worden geïnjecteerd in een website. Dit gebeurt wanneer een hacker kwaadaardige code(frontside script) verstuurd naar een eindgebruiker. De script taal die voornamelijk wordt gebruikt om XSS aanvallen te verrichten is Javascript. Javascript wordt gebruikt om componenten op een HTML websites functioneel te maken. Deze kwetsbaarheid kan overal gebruikt worden waar de website input van de gebruiker gebruikt om functionaliteiten te verrichten. Er zijn honderden variatie van deze aanvallen en dat maakt het moeilijk om de XSS aanvallen op te vangen en uit te filteren. Om dit tegen te gaan zullen website eigenaren input moeten valideren tegen verwachte XSS patronen.

A4 Insecure Direct Object References

Object referenties die niet goed beveiligd zijn tegen deze type aanvallen kunnen grootte beveiligingsrisico’s hebben voor de kostbare data die een website waarborgt. Insecure Direct Object Reference laat hackers de autorisatie passeren en zorgt ervoor dat resources direct bereikbaar zijn. Door het aanpassen van parameter waarden die direct verwijzen naar objecten in de broncode kunnen hackers de twee opgenoemde actie uitvoeren. Hackers kunnen gebruikersgegevens, bestanden en meer onderscheppen.

Hoe groot is het web security probleem?

Ik heb met mijn collega’s, vrienden en familie leden gesproken over het betreffende probleem en we zijn het er allemaal mee eens dat het ook echt een probleem is. Maar wat is de omvang van het probleem? Gelukkig zijn er security bedrijven die hier onderzoek naar hebben gedaan. Twee daarvan zal ik behandelen om antwoord te krijgen op mijn vraag.

De drie bedrijven zijn:

* IBM Security
* Symantec

IBM Security 2016

De security afdeling van IBM heeft in 2016 de rapport X-Force Threat Intelligence Report gepubliceerd waarin verschillende onderwerpen worden besproken op gebied van Cyber Security. Het rapport van 2017 is nog niet publiekelijk gepubliceerd. Er wordt terug gekeken naar het jaar 2015, een zeer actieve jaar voor cybercriminelen. Er wordt vermeld dat cybercriminelen het gemunt hebben op grotere doelwitten en dat zij niet meer zo zeer bezig zijn met het stelen van emails en wachtwoorden, hoewel dit nog zeker in grote schaal gebeurt, maar door de vraag naar waardevollere data doelwitten hebben als patiënt gegevens van gezondheidsinstituten en andere overheidsinstanties. Een voorbeeld hier van is een incident in de zorg sector waarbij hackers gevoelige data hebben gestolen van 55 zorgverzekeraars. Het gaat om de persoonlijke gegevens van 110 miljoen klanten [Motherboard, 2015]. In een artikel die gepubliceerd is door helpnetsecurity wordt de bug behandeld die de e-commerce CMS Magento plaagt. Waarbij 100,000 Magento websites het gevaar liepen om op afstand overgenomen worden(remote control) of het kan leiden tot een data breach. In een andere rapport van IBM genaamd *Cost of Data Breach Study* wordt vermeld dat de totale kosten van de data breaches over 2015 geschat wordt op $3.70 miljoen dollar. In 2014 stond de teller op $3,52 miljoen dit betekent dat er een stijging was van 7%,. Er wordt verwacht dat er in de jaren die erop volgen de kosten alleen maar zullen toenemen.

In [] wordt er geïllustreerd welke industrieën het meest gedupeerd worden door aanvallen en wat de meeste voorkomende aanval types waren in 2015.

Voor mij zijn de cijfers over SQL injecties en misconfiguraties het meest interessant want deze twee komen voor in het OWASP top 10 lijst die ik in dit document uitgebreid behandel en die veel invloed heeft op het ontwerpen van mijn security web scanner. Ook interessant is dat verre weg de meest aangevallen industrie de computer service is, met 30.2%. Onder deze industrie valt natuurlijk website en webservers en dit onderstreept weer eens dat web security scanners zeker een belangrijke rol hebben in het veilig maken van de wereld wijde web.

Symantec rapport 2017

In april 2017 bracht Symantic de Internet Security Threat Report uit. Symantic behandelt een variatie van onderwerpen in de kader Internet Security. Onderwerpen als Ransomware, phishing, IoT en nog veel meer. Voor mijn onderzoek zijn de onderwerpen Big numbers en Web attacks interessant. Ik zal deze twee onderwerpen toelichten met als doel een indruk te geven over hoe de cybercriminaliteit zich heeft ontwikkelt in de afgelopen jaren.

Big Numbers

Het hoofdstuk Big numbers laat ons in getallen en illustraties zien wat er in de afgelopen jaren is gebeurt op gebied van cybercriminaliteit. Symantic heeft in het rapport gepubliceerd dat er in totaal 3943 breaches (schendingen) waren gepleegd door cybercriminelen. Een breach is een vorm van een cyberaanval op een website die in de bezit is van privacy gevoelige data. Het doel is om die data te stelen. DataBreachToday een nieuws website die artikelen over cyber security publiceert heeft op 24 mei een artikel gepubliceerd over de data breach op Target in 2013. De breach zorgde ervoor dat de pinpas informatie van 41 miljoen klanten werden uitgelekt. Target heeft ingestemd om 18.5 miljoen aan schadevergoeding te betalen [databreachtoday, Target, 24 mei 2017]. Dit was een zijsprong naar nieuws artikel, maar het lijnt wel uit hoeveel schade een cyberaanval kan toe richten.

Een breach is een serieuze zaak omdat het gaat om privacy gevoelige data waar criminelen misbruikt van kunnen maken. Neem als voorbeeld identiteitsfraude, een veelvoorkomende criminele activiteit op de wereld wijde web. In 2014 zijn er circa 1.2 miljard identiteiten uitgelekt aan de buitenwereld van verscheidenen websites [Symantic/Breaches, 2017, p10].

Web in cijfers

Symantec heeft in de kader van web gepubliceerd dat in de afgelopen drie jaren meer dan 70% van alle scande websites kwetsbaarheden bevat waarvan 9 á 20 procent zorgwekkend is. Symantec heeft een aantal belangrijke bevindingen gemaakt die een aantal zaken boven water halen.

Voor ik begin aan de bevindingen is het van belang dat de lezer met de term Exploit Kit bekent wordt. Exploit Kits (EK)..

1) Web aanvallen, dit is een vorm van cyberaanvallen, zijn met 32% gedaald over de afgelopen jaar maar wat dit niet betekent is dat het geen groot probleem meer is. Gemiddeld werden er in 2016 iedere dag ongeveer 229,000 web aanvallen ontdekt.

2) Exploit kits waren tot 2015 het meeste populairste manier om aanvallen te verrichten op website. Maar in 2016 is het aantal aanvallen via EK gedaald met 60% en krijgt aanvallen via de email de voorkeur. Dit betekent echter niet dat aanvallen op websites gedaald zijn, cybercriminelen gebruiken simpel weg een ander methode om de aanvallen te verrichten.

3) Van alle Exploit Kits is RIG de meest populaire en was verantwoordelijk voor 35% van alle web aanvallen in 2016. Ransom.Cerber, een ransomware malware, werd voornamelijk door RIG gedistribueerd.

4) Gemiddeld werden er 2.4 browser kwetsbaarheden per dag ontdekt in 2016. In 2015 waren dat er 3 per dag. Threatpost heeft in december 2016 een artikel gepubliceerd over browser kwetsbaarheden. Het artikel ging over Google’s Chrome browser en de kwetsbaarheden waar het mee kampt. Google gaf bounties uit voor het oplossen van deze problemen, de bounties konden een bedrag van 7,500 dollar bereiken. In het artikel worden 21 security bugs genoemd, deze zijn alle opgelost [threatpost, 2016].