#h1:Web beveiliging

#h2:Introductie

In de wondere wereld van het web waarin alles kan en mag zijn we natuurlijk blij dat we heel veel kunnen maken en dat alleen onze fantasie de beperkende factor is. Echter lopen we dan al snel aan tegen het feit dat er altijd mensen met meer kunde dan wel fantasie rondlopen. Deze mensen kunnen helpen onze kennis en wijsheden met betrekking tot de websites uit te breiden.

Helaas staan we er vaak niet bij stil dat er ook mensen zijn die hun superieure kennis gebruiken om andermans websites te misbruiken voor het “kwaad” (spam / dubieuze content / machtsvertoon / etc ). Voor deze personen moeten we proberen de toegang tot onze websites zo moeilijk mogelijk te maken, door de lat zo hoog mogelijk te leggen. Voordat we dit kunnen realiseren moeten we ons eerst in de gedachtewereld van degenen met de kwade bedoelingen storten.

#h2:Hackers en Crackers

Hackers zijn eigenlijk personen die software en in ons geval websites afzoeken naar lekken in de beveiliging en deze kenbaar maken aan de eigenaar / beheerder van de website. Daarentegen zijn crackers de personen die ditzelfde doen maar dan met slechte bedoelingen. Ze gebruiken gevonden beveiliging lekken voor hun eigen doeleinden en blijven op deze manier zelf buiten schot. Dit is meestal niet de doelstelling van de maker van de site.

Dit lezende zijn hackers eigenlijk “goed” en crackers juist “slecht”. Dit klopt ook maar door de jaren heen zijn de termen verweven en worden ook hackers nu als slecht ervaren. Vandaar dat in dit document hackers zowel als crackers onder de noemer slecht vallen tenzij dit expliciet wordt aangegeven.

#h2:Mijn eerste website.

Wie een website online wil hebben zal moeten beginnen van het vinden van een geschikte hosting partij. Hosting is te vinden in allerlei soorten en maten en niet te vergeten prijs classes. We gaan ons in dit artikel alleen richten op een paar basis wensen die de beveiliging ten goede zal komen. Dit betekent niet dat een hosting provider zonder deze punten goed is, wellicht hebben ze een alternatief voor de beveiliging die u probeert te evenaren.

<table><tr><td>Wat</td><td>Wat is het / Waarom</td></tr><tr><td>FTP</td><td>ftp staat voor “bestand verstuur protocol” (file transfer protocol). Dit is een goede manier om uw bestanden te kopiëren naar uw website. Bij gewoon gebruik (zoals bij de meeste gebruikers) is dit echter niet beveiligd. Als u verbinding maakt wordt uw gebruikersnaam en wachtwoord als platte tekst zichtbaar. Iedereen die op de lijn luistert, heeft nu uw aanmeldnaam en wachtwoord en kan hetzelfde dan u.

</td></tr><tr><td>SSH</td><td>Ssh staat voor “beveiligde inlog” (Secure Shell) dit is al voor de wat gevorderde gebruikers. U kunt via bepaalde tools een ssh verbinding maken met de hosting en zo beveiligd inloggen waarna u via ftp de bestanden toch beveiligd kunt overzenden.

</td></tr><tr><td>SFTP</td><td>Dit is eigenlijk een combinatie van SSH en FTP met SFTP maakt u gelijk al een beveiligde verbinding en kunt u met een gerust hart uw website online zetten. De overdracht is wel trager dan met gewoon FTP maar dit is zeker de moeite waard.

</td></tr><tr><td>Beveiligde directories</td><td>Dit ziet u vaak niet in de eerste overzichten staan maar is wel degelijk een belangrijk punt. De mogelijkheid van beveiligde directories houdt namelijk in dat u mappen, waarin u informatie plaatst die niet voor iedereen toegankelijk zou moeten zijn, beveiligt met een gebruikers naam / wachtwoord. Deze beveiliging wordt geregeld op het bestands systeem niveau van de server waarop uw website gehost word. Dit is zo ongeveer een beveiliging op het hoogste niveau. (veelal op unix/linux systemen beter bekend als .htaccess)

</td></tr><tr><td>SSL</td><td>Als u rondneust op het internet gebruikt u een niet beveiligde manier van surfen, oftewel HTTP (hyper text transfer protocol). Dit is ook prima omdat 80% van de informatie die u ziet op het internet voor iedereen vrij toegankelijk is en er dus geen reden voor betere veiligheid vereist is. Echter voor bijvoorbeeld beheer functies / bank transacties / gevoelige informatie overdracht is dit een ander verhaal. Hiervoor kunt u gebruik maken van HTTP over SSL (secure socket layer) beter bekend als HTTPS, wat u bij banktransacties via IDEAL vooraan in de adresbalk zult zien.

</td></tr></table>

*ftp / sfpt programma tip : FileZilla (gratis te vinden)

*ssh / telnet programma tip : Putty (gratis te vinden)

#h2:Website beheer

Tegenwoordig kunnen we bijna niet meer een website vinden waar doormiddel van een online module het beheer wordt uitgevoerd. Dus is het belangrijk dat we dit beveiligen.

#h3:Tip 1 (minimaal aantal mappen):

Zorg dat uw beheer module zo weinig mogelijk hoofd mappen heeft. De voorkeur heeft te allen tijde een enkele hoofd map voor uw beheer. Veel genoemde namen zijn:

*Admin

*Manager

*Beheer

Op zich zijn deze namen niet een beveiliging risico op het moment van dit schrijven maar ze geven wel prijs wat het doel is en het zal niet onverstandig zijn (wanneer u zelf deze namen kunt bedenken) hier wat anders voor in de plaats te gebruiken. Dit om de robots (automatische scripts) die websites bezoeken, om zwakke plekken te ontdekken, het zo lastig mogelijk te maken. Door het gebruik van standaard namen wordt het hun gemakkelijk gemaakt uw site helemaal te doorzoeken.

#h3:Tip 2 (beveilig uw hoofd beheer map):

*Uw hosting provider heeft "beveiligde directories".

Maakt u gebruik van een hosting beheer module (bv Plesk, Cpanel, Helm, etc.), zoek dan na het aanmelden de module om uw mappen te beveiligen. De naam van dit onderdeel kan afhankelijk van taalinstellingen en of hosting beheer (module) verschillen maar de uitleg zal altijd wijzen op het feit dat u uw mappen kunt voorzien van een login-naam en wachtwoord.

*Uw voorziet in uw eigen beveiliging.

Kun u niet via uw hosting pakket een map voorzien van een login-naam en wachtwoord probeer dan via een script taal (PHP, PERL, Python, JavaScript, etc), die door uw hosting provider ondersteund wordt, dit zelf af te dwingen. (Zie hoofdstuk pagina beveiliging)

*Vraag uw hosting provider.

Vergeet nooit dat uw hosting provider er is om u te helpen. Email ze eens met de vraag wat u wilt bereiken qua beveiliging en wat ze in dezen voor u kunnen betekenen.

#h3:Tip 3 (kruip in de huid van uw belager):

Blijf altijd nadenken over de beveiliging van uw website en hoe u deze beheert. Als u een beveiliging lek kunt bedenken zullen anderen daar ook toe in staat zijn. Voorziet u in de bestrijding van dit lek dan zal de drempel voor het hacken van uw website weer een beetje hoger liggen.

#h2:Invoer van gegevens

Om een dynamische website betekenis te geven is het van belang dat u bezoekers aan het woord laat. Dit kan bijvoorbeeld doormiddel van een:

*(we)Blog met reacties.

*Gastenboek.

*Inlog gedeelte voor extra informatie.

*Opiniepeiling

*Inschrijven nieuwsbrief

Er zijn nog een aantal onderdelen te bedenken waarvoor u de invoer van gegevens door bezoekers laat doen.

#h3:Tip 1 (weet wat u doet met informatie):

Controleer of de gegevens overeenkomen met wat u verwacht. Dit voorkomt al de eerste frustratie als u de informatie wilde gebruiken om bijvoorbeeld een nieuwsbrief uit te sturen of als nieuwe bezoekers door de pagina’s SPAM heen moeten worstelen om uw interessante webpagina te kunnen bekijken.

Controleer waar mogelijk op een of meerdere van de volgende punten:

*Lengte van invoer (Een telefoon nummer bevat minimaal 10 cijfers)

*Speciale karakters (bevat het email adres minimaal een "@" en een "." )

*Betekenis (Een ISBN heeft bijvoorbeeld een controle getal)

*Structuur (een postcode heeft vier karakters + twee cijfers XXXX99)

#h3:Tip 2 (controleer de identiteit):

Voordat je weet wie er op je website rondloopt, kun je toch al een onderscheid maken tussen twee groepen bezoekers.

Gewenst zijn zoekmachines die je website breder bekend kunnen maken en iedereen die je website wil bewonderen en hier al dan niet interactie mee pleegt. Dat zijn de bezoekers die je wenst en die mogelijk vaker op je website komen.

Ongewenst zijn o.a. de bezoekers die de taal van je website niet begrijpen en deze kunnen dus onmogelijk nuttige informatie achter laten. Mensen die kwaad in de zin hebben zijn het gevaarlijkst voor je website en kunnen als de inhoud meteen online komt (zoals gastenboek) het meeste kwaad doen, gelukkig komt dit het minste voor.

En als laatste de grootste groep, de robots (scripts die beveiliging lekken zoeken).

Vraag dus waar mogelijk (niet te vaak maar wel vaak genoeg) naar een controle getal / woord. Voor bezoekers met een andere taalachtergrond is dit vaak niet te begrijpelijk genoeg om goed in te kunnen vullen. Voor robots ligt dit vaak wat anders omdat deze dit soort technieken kunnen herkennen en invullen. Laat je het controle getal / woord in een plaatje zien krijgen ook deze het al een stuk moeilijker.