

De browser een machtig wapen?

Slechts een browser en een goede editor behoren tot het wapenarsenaal welke nodig is om een aanval uit te voeren op webgebaseerde applicaties. Een aanval die uitgevoerd kan worden door onvolkomenheden in de programmatuur (code).

In onze vorige nieuwsbrief hebben we met een Cisco HTTP-lek het onderwerp 'code injectie' aangehaald. Zoals de naam al aangeeft wordt bij dit type aanval een bepaalde letter-teken combinatie (code) geïnjecteerd die door de website als een instructie geïnterpreteerd kan worden. Vormen van code injectie aanvallen zijn bijvoorbeeld cross-site-scripting, SQL/XML injectie, buffer overflow, file includes en HTML invoeging. In deze en in de volgende nieuwsbrief worden deze typen aanvallen via drie voorbeelden verduidelijkt.

Voorbeeld A (1ste orde code injectie aanval):

Door een browser wordt via een dynamische pagina, genaamd getnews.asp, het nieuws van 24 januari 2006 opgevraagd. Bij het uitvoeren van onderstaande instructie door de webserver, ontvangt getnews.asp het bestand 24Jan2006.html van het file systeem en stuurt deze naar de browser.

<http://www.nieuwsorganisatie.nl/online/getnews.asp?item=24Jan2006.html>

Een persoon met kwaadwillende bedoelingen herkent het potentiële probleem en zal de waarde van het item vervangen door:

<http://www.nieuwsorganisatie.nl/online/getnews.asp?item=../../../../Windows/win.....>

De term "../../../../" staat voor "één directory omhoog". Dus betekent de waarde van het item "ga vier directories omhoog en geef win.ini weer in de browser". Dit voorbeeld wordt ook wel 'directory traversal' genoemd. Een Internetgebruiker kan dan als het ware uit de beschermde root-directory stappen en toegang verkrijgen tot andere directories en bestanden. Het uitvoeren van commando's van het systeem behoort dan tot de mogelijkheden.

Bovenstaand voorbeeld behoort tot de categorie '1ste orde code injectie' aanvallen. Bij de verschillende vormen van code-injectie gericht op web-based applicaties, berust het principe op de directe uitvoering van de 'ingevoegde' code om een aanval uit te voeren.

Naast de '1ste orde code injectie' aanvallen zijn er ook aanvallen die niet op een directe uitvoering zijn berust. Bij 2e orde code injectie aanvallen maakt een aanvalleur gebruik van de mogelijkheid om malafide code in een dataopslagsysteem te injecteren zodat deze in een later stadium uitgevoerd kan worden.

Voorbeeld B (2e orde code injectie aanval):

Verschiedende websites bieden de mogelijkheid om persoonlijke informatie in te vullen bij het aanmaken van een gebruikersnaam. Als een kwaadwillende gebruiker de mogelijkheid heeft om malafide code in een dataveld te injecteren, wordt deze opgeslagen in het back-end systeem. Normaliter is deze informatie persoonlijk en zal de informatie niet snel geraadpleegd worden. Maar op het moment dat deze persoon naar de ondersteuningsdienst belt om informatie over zijn account op te vragen of te laten wijzigen, wordt de code uitgevoerd en dus de aanval van binnenuit geïnitieerd.

Secure Connection B.V. kan u van dienst zijn om uw webserver(s) en webapplicatie(s) te beveiligen tegen, onder andere, deze typen aanvallen.

Mogelijke beveiligingsmaatregelen:

- De beste manier om te controleren of uw website en applicaties kwetsbaar zijn voor Directory Traversal, SQL Injectie, Cross site scripting en andere web kwetsbaarheden aanvallen is om een Web Vulnerability Scanner te gebruiken;
- Webmasters dienen ervoor te zorgen dat geen van hun pagina's gebruikersinvoer terugstuurt welke niet gevalideerd is: het ontleden van een string en nagaan of er geen vreemde karakters en woorden in voorkomen.
- Organisaties dienen er voor te zorgen dat alle primaire dataverwerkingscomponenten en secundaire applicaties in staat zijn om de data die daadwerkelijk wordt gebruikt te 'zuiveren' van malafide code en data van andere verwerkingsbronnen niet zonder meer te vertrouwen;

Vernieuwde versie van PDA2L

Het geautomatiseerde programma voor het uitvoeren van Proces- en Systeemanalyses binnen een organisatie (PDA2L) is op verschillende punten vernieuwd. Zo is er nu o.a. de keuzemogelijkheid om in het programma een selectie te maken van de kennisdatabase en om alleen ten opzichte van een baseline aanvullende maatregelen te kiezen.

In de bijgesloten brochure kunt u meer informatie vinden over dit vernieuwde product.

Actueel

Computercriminaliteit rukt op

Zo heette de uitzending van Nova vorige week waarin nogmaals duidelijk werd gemaakt dat criminele organisaties bezig zijn hun werkerrein te verleggen naar het Internet.

Afpersing, fraude en diefstal praktijken op het Internet worden voor criminele bendes interessanter en lucratiever door o.a. de groei van e-commerce en de opkomst van breedbandverbindingen.

De kans om een succesvolle aanval uit te voeren neemt toe doordat de beveiliging van computernetwerken van bedrijven, overheden en particuliere pc-gebruikers te wensen overlaat. Er zijn tal van kwetsbaarheden waar een crimineel misbruik van kan maken.

Dit blijkt ook wel uit een nieuwe trend: data ontvoeren voor losgeld. Voorbeelden A en B in deze nieuwsbrief geven aan hoe een code-injectie aanval onderdeel kan uitmaken van zo'n dergelijke gijzelingsactie. Door uitvoering van malafide code kan bijvoorbeeld belangrijke data worden gecijferd. Alleen tegen betaling van losgeld krijgt het bedrijf of de persoon de (enige) sleutel waarmee de data weer ontcijfert kan worden.

Kijk op novatv.nl om de uitzending te bekijken.