



## Vervolg: De browser een machtig wapen?

In de twee voorgaande nieuwsbrieven zijn voorbeelden gegeven hoe een kwaadwillend persoon een Code injectie aanval kan inzetten om via een webserver toegang tot een bedrijfsnetwerk te krijgen. Om het onderwerp 'Code injectie' af te sluiten, laat onderstaand voorbeeld zien hoe een dergelijke aanval ook ingezet kan worden om persoonlijke informatie van een nietsvermoedende Internetgebruiker te verkrijgen (bv. wachtwoorden, creditcard- of bankrekening gegevens).

### Cross-site scripting

Cross-site scripting (XSS) is een beveiligingslek dat een aanvaller kan misbruiken om code te 'injecteren' tijdens een gebruikerssessie op een website. In tegenstelling tot de meeste lekken, is XSS niet van toepassing op een specifiek product, maar kan het problemen veroorzaken in alle software die HTML genereert en die niet speciaal is beveiligd tegen dergelijke programmeerpraktijken. Bij cross-site scripting is het de aanvaller te doen om via de browser persoonsgebonden informatie te verkrijgen van de nietsvermoedende gebruiker. Om interactie te krijgen met een gebruiker kan een aanvaller gebruikmaken van XSS door een e-mailbericht te verzenden met een ingesloten script of koppeling. Na activering wordt een query met een script in een van de argumenten naar een webserver verzonden. Het resultaat is dat er interactie is tussen de browser van de gebruiker en een website die door de aanvaller wordt beheert. De gebruiker heeft dit niet in de gaten aangezien de website er ogenschijnlijk onschuldig uitziet (bv. een kopie van de website van zijn of haar bank). Via deze website kan informatie worden verkregen van de gebruiker. Deze logt bijvoorbeeld in en/of vult een formulier in waarin persoonlijke informatie wordt gevraagd (bv. credit card gegevens). In feite wordt dus de identiteit van een ander gestolen waarmee vervolgens bijvoorbeeld aankopen gedaan kunnen worden (producten, vliegtickets, reizen, etc).

### Voorbeeld A (XSS aanval):

Een gebruiker logt in op een website om zijn aandelen te bekijken. Voor een persoonlijk contact wordt je doorgelinkt naar [www.organisatieX.nl/default.asp?naam=Marcel](http://www.organisatieX.nl/default.asp?naam=Marcel) en een server-side script genereert een welkomspagina welke zegt "Welkom terug Marcel!". De aandelen in uw portfolio worden opgeslagen in een database en de website plaatst een cookie op uw computer welke de sleutel bevat naar die database. De cookie wordt iedere keer opgevraagd wanneer de website van OrganisatieX wordt bezocht.

Een aanvaller herkent dat de website een cross-site scripting bug heeft. De aanvaller stuurt een e-mail waarin staat dat er een financieel voordeel te behalen is (1). Via de link in het bericht kan meer informatie verkregen worden. De ontvanger klikt op de link [www.organisatieX.nl/default.asp?naam=<script>codeXYZ\(\)</script>](http://www.organisatieX.nl/default.asp?naam=<script>codeXYZ()</script>) en krijgt het welkomspagina te zien met de tekst "Welkom terug !" (3). De naam is niet zichtbaar: dit komt doordat de browser heeft aangegeven dat je naam `<script>codeXYZ()</script>` is. Indien het script (4) de browser de opdracht geeft om het cookie met het aandelenportfolio te versturen naar de computer van de aanvaller (5), zal deze de opdracht uitvoeren. Immers kwam de opdracht van de website van organisatie X welke eigenaar is van het cookie.

De essentie van de aanval is dat de browser de malafide scripts zal uitvoeren in de security context van de site waar de browser dacht dat het vandaan kwam, en niet van de website van de aanvaller. Door dit te doen, heeft de aanvaller toegang binnen de veronderstelde beveiligde omgeving van de betrokken client en server. Om deze reden wordt de aanval "cross-site" genoemd.

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

### Secure Connection lanceert nieuwe versie van System Analysis Tool (SA2L)

Secure Connection heeft in januari 2006 een nieuwe versie van SA2L op de markt gebracht. Het programma, draait onder de vernieuwde StandardGUI. SA2L kan op basis van een analyse een maatwerk advies leveren, afgestemd op de specifieke kenmerken van het te onderzoeken informatiesysteem. Dit wordt bereikt door een uitgebreide decompositie van het systeem en een uitgebreide kennis van SA2L van vele soorten systemen. Voorbeelden hiervan zijn KA-systemen, ERP systemen, Workflow Management Systemen en E-business systemen op functioneel niveau en Client-Server, WEB based en Terminal Server based systemen op architectuurniveau. In onze nieuwe brochure leest u meer over SA2L.

### Actueel

#### Rootkits: de nieuwe virusplaag?

Onlangs kwam SonyBMG in het nieuws, omdat dit bedrijf de techniek van rootkits gebruikte om het kopiëren van CD's tegen te gaan. Nu worden ook andere bedrijven zoals Kaspersky en Symantec ervan beschuldigd rootkits te installeren op PC's.

De rootkit is een stukje software wat heel diep in de kernel van het operating systeem is genesteld. Een windows rootkit kan ondermeer de verkenners misleiden, zodat bepaalde programma's niet zichtbaar zijn. Zo zijn er rootkits die de FindFirstFile en FindNextFile API's kunnen onderscheppen. Een kernel mode rootkit kan er zelfs voor zorgen dat het proces niet voorkomt op de lijst van processen die op dat moment actief zijn. Een programma als rootkitrevealer vergelijkt daarom de output van de windows API's met een directe scan op de harde schijf en kan op deze manier discrepanties ontdekken. en daarmee een rootkit ontmaskeren. Rootkitrevealer is gratis te downloaden op [www.sysinternals.com](http://www.sysinternals.com)

Het is zeer waarschijnlijk dat virussen en andere malware meer van deze techniek gebruik zullen gaan maken.

