



## Kent u Cross-site Request Forgery?

Er duiken steeds meer kwaadaardige technieken op om via het internet (identiteits-)gegevens te bemachtigen en op deze manier geld te verdienen of andere voordelen te behalen.

Secure Connection wil u graag een overzicht geven van gebruikte technieken, met een stuk analyse, risico's en maatregelen tegen deze kwaadaardige technieken.

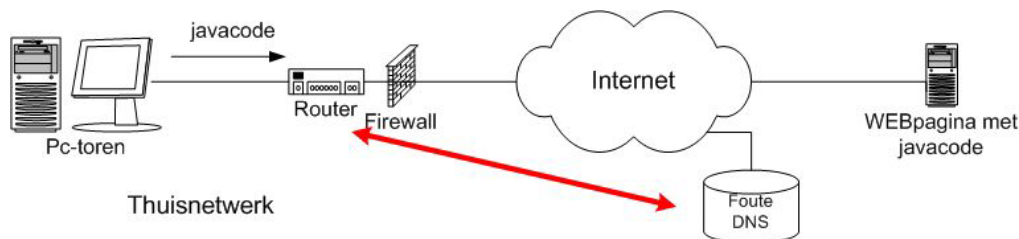
U kunt een overzicht vinden van deze technieken op [www.assutools.com/news/strategies/](http://www.assutools.com/news/strategies/).

Voorlopig hebben worden de volgende technieken uitgelegd:

- Code-injection
- Cross-site scripting
- Cross-site request forgery
- Phishing en pharming technieken

Het is de bedoeling u op de hoogte te houden van nieuwe ontwikkelingen op dit gebied.

In deze nieuwsbrief wordt het begrip cross-site request forgery behandeld aan de hand van een voorbeeld met een thuisnetwerk.



In dit geval probeert een kwaadwillend iemand de thuisrouter/firewall van iemand te kraken. Het is bekend dat velen het wachtwoord van hun thuisrouter gewoon op default laten staan. Het blijkt dat in de praktijk dat van 50 % van alle thuisrouters het wachtwoord op default staat.

Deze routers staan vaak wel dicht voor remote access en kunnen dus niet van buitenaf worden benaderd.

Het is echter heel goed mogelijk om met een javascript de router vanuit het thuisnetwerk te benaderen. Javascript wordt namelijk door de browser (client-side) uitgevoerd en niet vanuit de server, zoals php. Het is heel goed mogelijk om een javascript te schrijven die via webaccess toegang verschaft tot de router (met default wachtwoord) en dan bijvoorbeeld de verwijzing naar de DNS server verandert naar een adres van een "foute" DNS server.

Deze DNS server zal bijvoorbeeld een bank-url ([www.mybank.nl](http://www.mybank.nl)) vertalen naar ip-adres van een nepsite die er hetzelfde uitziet als de normale banksite.

Op deze manier is het heel eenvoudig geworden om de bankgegevens van het slachtoffer op te vangen, waarna de rekening kan worden geplunderd (onder de voorwaarde dat de betreffende bank een zwak authenticatiemechanisme gebruikt, wat helaas nog steeds voorkomt).

Het is mogelijk om het uitvoeren van javascript in de browser te blokkeren (zie uw browser instellingen). Dit houdt echter in dat vele sites dan niet meer goed worden weergegeven. Bijna iedereen heeft daarom het uitvoeren van javascript aanstaan.

Een ander probleem is dat er niet op een link hoeft te worden geklikt. Het simpel browsen naar een dergelijke foute site is al voldoende.

De beste remedie tegen deze aanval is het default wachtwoord te wijzigen! Natuurlijk is het ook verstandig om niet zomaar op iedere link in een emailtje te klikken. Maar als het default wachtwoord is gewijzigd werkt de beschreven truc niet meer.

Jeremiah Grossman and T.C. Niedzialkowski hebben een presentatie op Blackhat, waarbij gebruik werd gemaakt van JavaScript om een intern netwerk te kunnen aanvallen vanuit het internet.

Zie <http://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html>.

## Nieuws op assutools.com

Secure Connection brengt regelmatig het laatste relevante security nieuws op haar website. U kunt dit lezen op <http://www.assutools.com/news/recent.htm>.

## Actueel

### Gestolen laptop terug dankzij tracing software

De laptop van de vrouw van James Melin, een comptuer-programmeur in California is teruggevonden, dankzij tracing software op de laptop.

James Melin staat een deel van zijn computerpower vrijwillig af voor onderzoek naar leven in de ruimte.

De programmeur, SETI(at)home, zoekt regelmatig contact met de universiteit van California. De computers van de vrijwilligers worden in de idle time gebruikt voor dataverwerking van gegevens uit de ruimte.

Alle gebruikers van SETI(at)home kunnen zien wie er op een bepaald moment is ingelogd op het systeem met het bijbehorende IP adres.

De laptop was op nieuwjaarsdag 2007 gestolen uit het huis van de familie Melin.

De dieven hadden de software op de laptop ongemoeid gelaten, waardoor SETI(at)home nog steeds contact zocht met de universiteit van California

Het IP adres werd aan de politie doorgegeven. Deze kon via de internet provider het juiste adres achterhalen.

### Bron:

<http://mcpmag.com/news/article.asp?EditorialsID=1218>