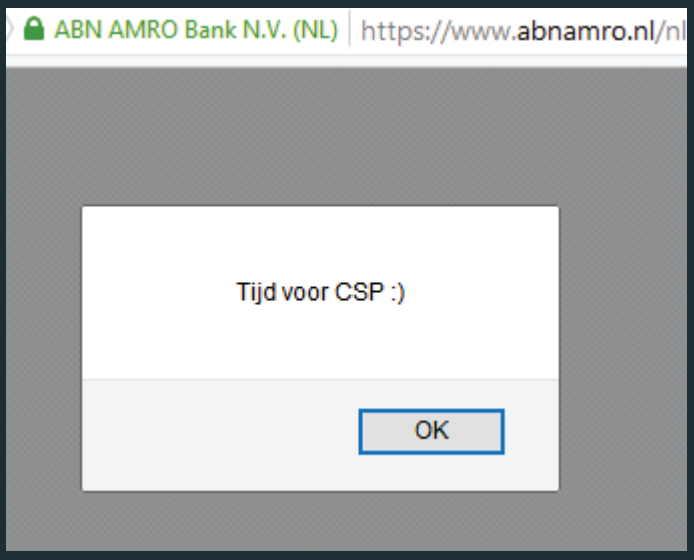
Bankenwebsites en XSS

Tijd voor CSP



Versie:
1.0

Datum:
24-8-2016

Naam:
Wouter S. van Dongen MSc CISSP CISA
wouter.vandongen@dongit.nl

DongIT

N Dong-IT BV
A Schipholweg 103
2316 XC Leiden

BTW NL851599011B01
KVK 55184391
IBAN NL71RABO0167805479

T 071 5249213
E info@dongit.nl
W www.dongit.nl
W www.websecurityscan.eu

Web Security Scan

Controle over de browser

Cross-site scripting, ook wel XSS genoemd, is al sinds de opkomst van dynamische websites één van de meest voorkomende kwetsbaarheden in webapplicaties. De OWASP-top 10 is een lijst met de meest kritische kwetsbaarheden in webapplicaties opgesteld door security experts over de hele wereld. Sinds de eerste publicatie van de OWASP-top 10 in 2007 (https://www.owasp.org/index.php/OWASP_Top_10) heeft XSS steevast een prominente top 3-positie gehad. Door misbruik te maken van een XSS-kwetsbaarheid kan een aanvaller controle krijgen over de browser van de bezoeker van de website. Zo kan bijvoorbeeld data die aan de bezoeker wordt getoond doorgestuurd worden naar de aanvaller, kunnen acties verricht worden alsof de gebruiker dit heeft gedaan, of kan de getoonde inhoud van de site aangepast worden. Met name bij financiële instellingen kan XSS grote gevolgen hebben. Voor meer informatie over XSS, zie: https://en.wikipedia.org/wiki/Cross-site_scripting.

Schuddende bankenwebsites - kamervragen

Ook afgelopen jaar is weer gebleken dat XSS een van de meest voorkomende kwetsbaarheden is. Acunetix, bouwer van securitysoftware, voerde in 2015 15.000 securityscans uit. Vrijwel de helft van alle gescande websites had te maken met een ernstige kwetsbaarheid (XSS- of SQL-injectie), zie http://www.acunetix.com/blog/articles/acunetix-web-application-vulnerability-report-2015/.

Zelfs de websites van banken hebben een rijk verleden aan XSS-kwetsbaarheden, ondanks dat deze behoren tot de best beveiligde websites van het land, die regelmatig onderworpen worden aan securitytesten.

- 7 Nederlandse onlinebankingsites kwetsbaar voor XSS: https://www.security.nl/posting/15099/7+Nederlandse+online+banking+sites+kwetsbaar+voor+XSS
- 5 Nederlandse banken hebben zelfde XSS-lek: http://webwereld.nl/security/40496-vijf-nederlandse-banken-hebben-zelfde-xss-lek, http://www.nu.nl/nuzakelijk-overig/2014968/gat-ontdekt-in-websites-banken.html
- 10 Nederlandse banken hadden XSS-kwetsbaarheid: http://tweakers.net/nieuws/100751/tien-banken-hadden-xss-kwetsbaarheid.html http://www.nu.nl/binnenland/3970812/beveiligingslek-banken-maakte-phishing-mogelijk.html

Naar aanleiding van het onderzoek van DongIT “10 Nederlandse banken hadden XSS-kwetsbaarheid” uit 2015, waarbij de bankenwebsites over het scherm schudden (https://www.youtube.com/watch?v=K0noqLisW_c), werden kamervragen gesteld, zie: https://zoek.officielebekendmakingen.nl/ah-455347.pdf. In het antwoord op vraag 3 geeft minister Dijsselbloem aan dat XSS-problemen vaker voorkomen:

“Het probleem van de in het artikel genoemde «cross site scripting» is vaker geconstateerd en eerder aangepakt door de banken.”

Tevens geeft de minister aan dat voldoende maatregelen worden genomen tegen XSS:

“De banken testen zelf op beveiligingslekken en zorgen dat hun systemen regelmatig worden geüpdate. Banken nemen bij het testen voor de invoering van software mitigerende maatregelen om kwetsbaarheden in productie te voorkomen”

*Een zeer voor de hand liggende mitigerende maatregel voor XSS wordt echter niet gebruikt, zie volgende paragraaf “*Content Security Policy nauwelijks in gebruik*”.*

Voorts wordt het volgende aangegeven door de minister:

"De Betaalvereniging Nederland heeft aangegeven niet bekend te zijn met aanvallen waarin gebruik werd gemaakt van het aangekaarte lek of vergelijkbare lekken."

Uit het volgende voorbeeld uit 2008 blijkt dat XSS-aanvallen in de praktijk voorkomen bij banken: https://news.netcraft.com/archives/2008/01/08/italian_banks_xss_opportunity_seized_by_fraudsters.html.

Content Security Policy nauwelijks in gebruik

Er bestaat een effectieve beveilingsmaatregel die XSS kan voorkomen: content security policy (CSP). Met CSP kan aangegeven worden welke type en vanaf welke locatie resources ingeladen mogen worden. CSP wordt breed ondersteund. 88.99% van de webbezoeken gebruikt een browser die CSP ondersteunt, zie: http://caniuse.com/#feat=contentsecuritypolicy. Gezien de hoeveelheid XSS-kwetsbaarheden in webapplicaties (ondanks reeds genomen maatregelen, zoals het uitvoeren van pentesten), is CSP met name voor de meest gevoelige websites van het land een absolute must als extra beveiligingslaag. Voor meer informatie over CSP, zie https://en.wikipedia.org/wiki/Content_Security_Policy.

De impact van XSS is het grootst op het hoofddomein (www) of het bankierendomein van een bank. Dit komt omdat het voor de bezoeker vertrouwde domeinen zijn. Het bekende webadres zal er in de browser ongewijzigd uitzien, inclusief het vertrouwde HTTPS-slotje - ondanks XSS-aanval.

DongIT onderzocht (op 21-3-2016) het gebruik van CSP op het hoofd- en bankierendomein van Nederlandse bankenwebsites. Hieruit blijkt dat van de 40 onderzochte domeinen slechts 4 domeinen gebruikt maken CSP.

Tabel 1: Overzicht hoofd- en bankierendomeinen

Domein	CSP	Opmerking
www.ing.nl	niet	
mijnzakelijk.ing.nl	niet	
mijn.ing.nl	niet	
www.abnamro.nl	niet	Geen los bankierendomein
www.rabobank.nl	niet	
bankieren.rabobank.nl	**wel**	
www.snsbank.nl	niet	Geen los bankierendomein
www.triodos.nl	niet	
bankieren.triodos.nl	niet	Content-Security-Policy-Report-Only
www.knab.nl	**wel**	
persoonlijk.knab.nl	**wel**	
www.asnbank.nl	niet	Geen los bankierendomein
www.vanlanschot.nl	niet	
login.vanlanschot.com	**wel**	
login.evivanlanschot.nl	niet	
www.evivanlanschot.nl	niet	
www.binck.nl	niet	
login.binck.nl	niet	
www.alex.nl	niet	
klant.alex.nl	niet	

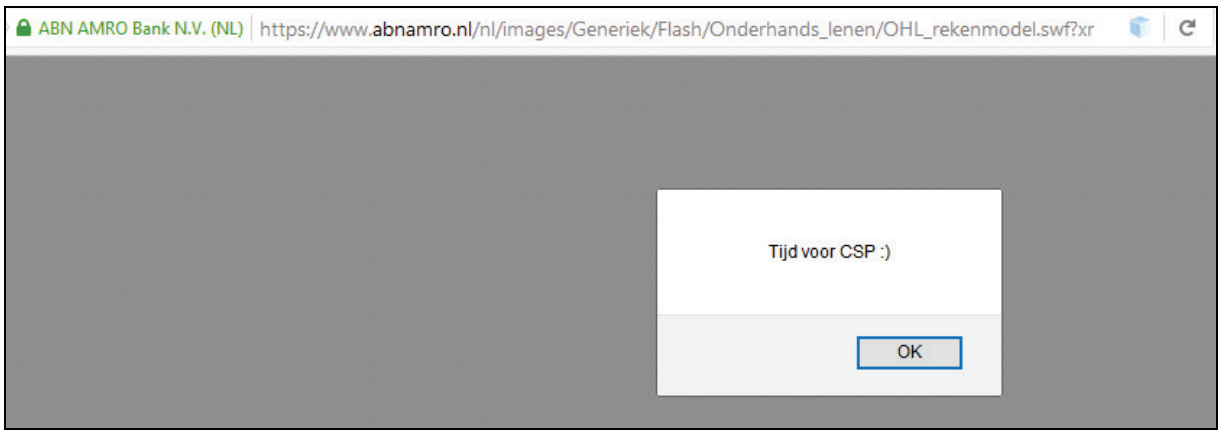
www.leaseplanbank.nl	niet	
sparen.leaseplanbank.nl	niet	
www.regiobank.nl	niet	
www.moneyou.nl	niet	
secure.moneyou.nl	niet	
www.nibcdirect.nl	niet	
sparen.nibcdirect.nl	niet	
www.robeco.nl	niet	
mijn.asrbank.nl	niet	
www.asrbank.nl	niet	
www.argenta.nl	niet	
internetbanking.argenta.nl	niet	
www.dhbbank.com	niet	
netbanking.dhbbank.com	niet	
nl.saxobank.com	niet	
www.saxotrader.com	niet	
www.icscards.nl	niet	
www.mijn-icsbusiness.nl	niet	
www.degiro.nl	niet	
trader.degiro.nl	niet	

Tijd voor CSP

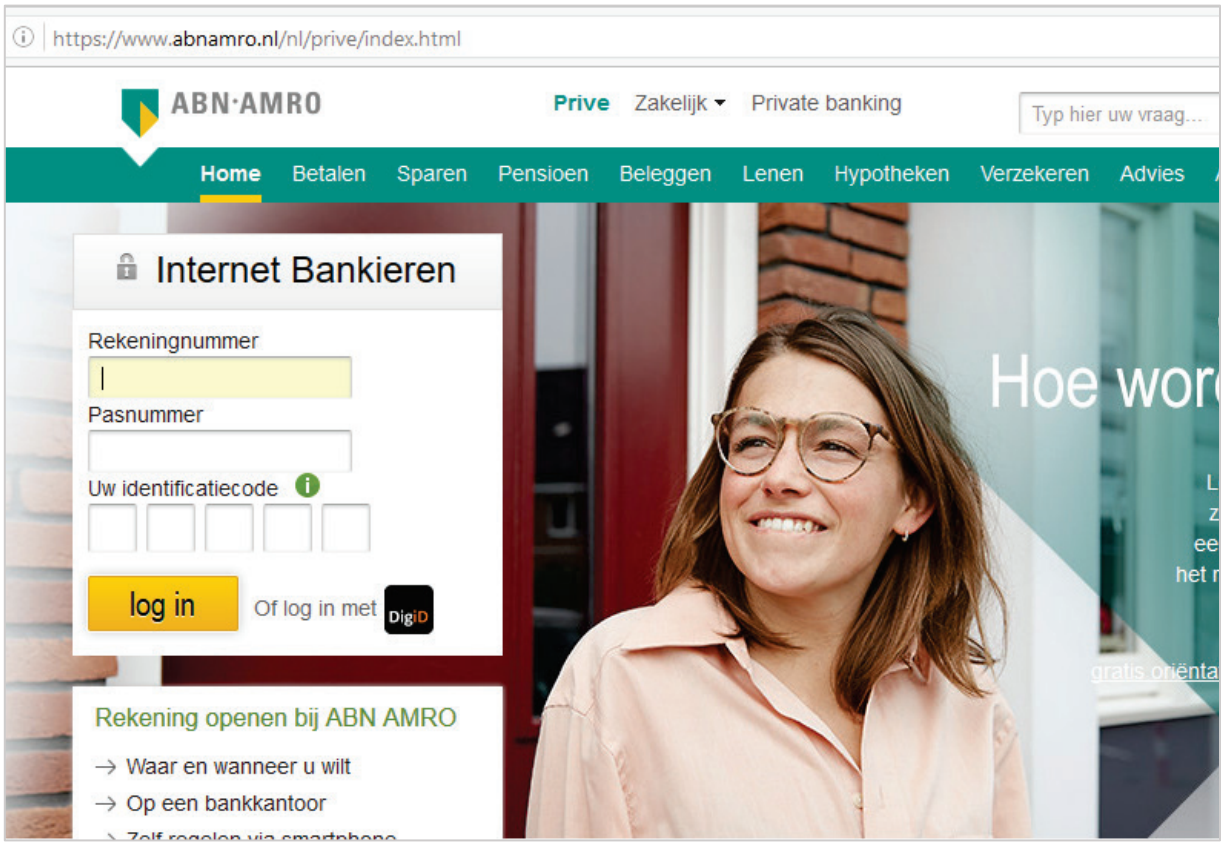
Uit jaaroverzichten van diverse beveiligingsbedrijven, alsook de OWASP-top 10-lijsten tot nu toe, blijkt dat XSS al ruim 10 jaar ongewijzigd zeer frequent wordt aangetroffen in webapplicaties. Dit beeld zal zeer waarschijnlijk komende jaren niet veranderen. Het gaat hierbij om ernstige kwetsbaarheden.

Ondanks dat volledig voorkomen van deze kwetsbaarheden waarschijnlijk niet haalbaar is, is verregaande mitigatie van de effecten ervan relatief eenvoudig haalbaar: 90% van webbezoeken gebruikt een browser die CSP ondersteunt. Het is dan ook opmerkelijk dat op het moment slechts 4 domeinen van banken gebruik maken van CSP. Ondanks dat pentesten regelmatig uitgevoerd worden en er een responsiblediscloserebeleid van toepassing is, wordt XSS met regelmaat aangetroffen bij banken.

Om aan te geven dat XSS ook in 2016 nog altijd aanwezig is en dat daarom urgentie vereist is met de invoer van CSP bij bankenwebsites, sluit ik als volgt af:



Figuur 1: Uitvoer XSS op hoofddomein van de ABN-AMRO-bank in 2016



Figuur 2: Formulier geïnjecteerd doormiddel van kwetsbaarheid. Tevens is een DigiD-inlogmogelijk toegevoegd aan de website.

Versiebeheer

Tabel 2: versiebeheer

Versie	Opmerking	Datum
0.4	Initiële rapportage.	21-3-2016
0.5	- Toevoeging Italiaanse XSS phising aanval - Screenshot ABN Amro fomulier toegevoegd	24-8-2016