YACHT

Testnet Voorjaarsevenement

05 April 2006

YACHT

Hack Me, Test Me

Websecurity test onmisbaar voor testanalist en testmanager

Edwin van Vliet
Yacht Test Expertise Center

Hack me, Test me
Websecurity test,
onmisbaar voor testspecialist en testmanager

YACHT

Doelstelling

- Impact van niet testen van Websecurity
- Welke invloed heeft het op eigen testproject?

Vragen

- Moet Websecurity testen altijd door specialist gebeuren ?
- Is het nodig om Websecurity test vlak voor productie te laten plaatsvinden?

YACHT

Voorbeeld uit het nieuws

Beveiliging geniet geen prioriteit

Zaterdag 23 maart 2006, Directies van ondernemingen maken zich niet zo bezorgd over beveiliging. Zo blijkt uit een onderzoek onder bijna zevenhonderd ceo's en cio's bij bedrijven in tweeëntwintig landen.

"Beveiliging is op orde, want er is genoeg in geïnvesteerd."
Gezond verstand of oogkleppen?

Hack levert ruimt een miljoen patiëntdossiers op

Zaterdag 3 september 2005, Beveiligingsexperts zijn er in geslaagd om 1,2 miljoen patiëntdossiers te achterhalen door 'in te breken' bij twee Nederlandse ziekenhuizen.

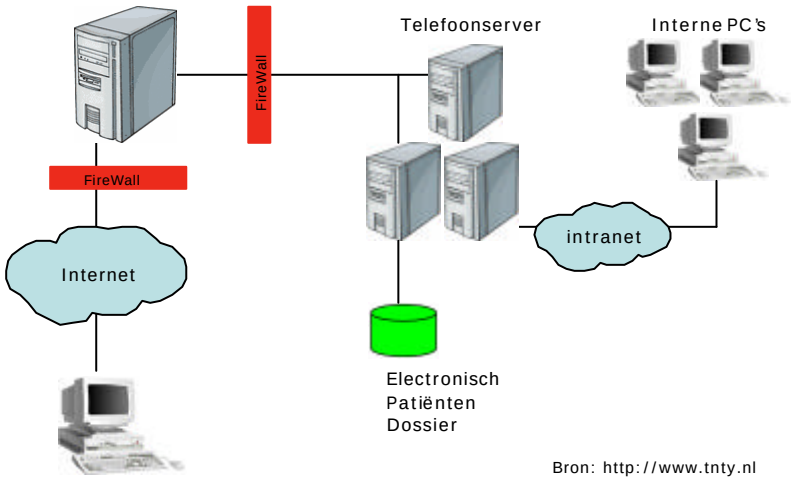
Beveiligingsexperts zijn er in geslaagd toegang te krijgen tot de patiëntgegevens van 1,2 miljoen personen. De beveiligingsbedrijven ITSX, Fox-IT en Madison Gurkha konden de databases van twee ziekenhuizen binnendringen nadat de ziekenhuizen daar toestemming voor hadden gegeven. ITSX omschrijft de beveiliging van de ziekenhuizen met de kwalificatie 'MKB-niveau'.

Bron: www.Computable.nl

Bron: www.Webwereld.nl

YACHT

Hack levert ruimt een miljoen patiënt gegevens op



Bron: http://www.tnty.nl

Hack me, Test me
Websecurity testen,
onmisbaar voor testspecialist en testmanager

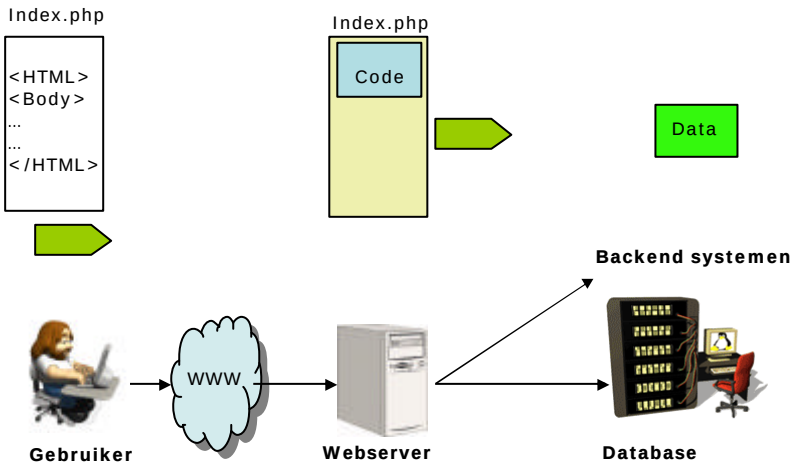
YACHT

Agenda

- Wat is websecurity testen ?
- Wat is het verschil met security testen ?
- Hoe past websecurity in uw testproject ?
- Hoe leer je websecurity testen?

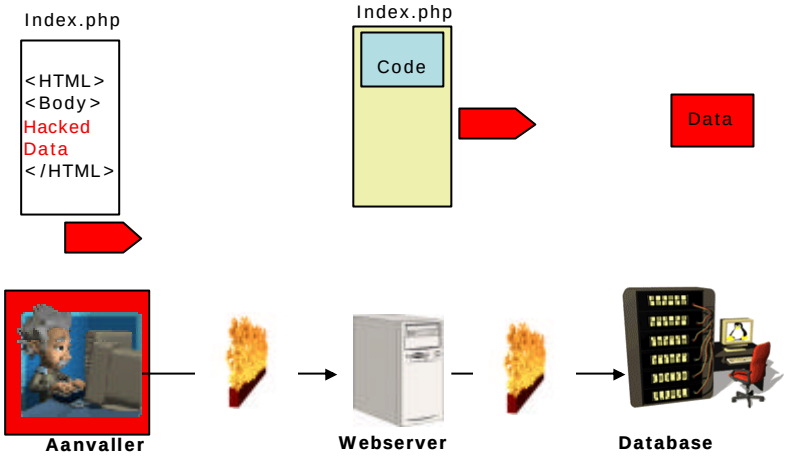
Internet Infrastructuur

YACHT



YACHT

Internet Infrastructuur
WebSecurity vs Security



YACHT

Wat is Websecurity test ?

Functioneel testen is een onderzoek of iets correct werkt.

Websecurity testen is het onderzoeken of het mogelijk is om iets incorrect te laten werken

1. Herkennen van symptomen (aanvalmogelijkheden) via HTTP
   - URL Adresbalk;
   - invoervelden;
   - cookies en
   - autorisaties.
2. Bepalen van potentiële gevolgschade

Relatie Websecurity testen en OWASP

YACHT

OWASP
The Open Web Application Security Project
http://www.owasp.org

Open groep die gericht is op het begrijpen en verbeteren van beveiliging van webapplicaties en webdiensten

Honderden vrijwilligers experts wereldwijd

Inclusief in Nederland

http://www.owasp.org/local/netherlands.html

De OWASP Top 10

YACHT

- Broken Access Control
- Unvalidated Parameters
- Broken Account and Session Management
- Cross-Site scripting (XSS) Flaws
- Buffer Overflows
- Command Injection Flaws
- Error Handling Problems
- Insecure Use of Cryptography
- Remote Administration Flaws
- Web and Application Server Misconfiguration

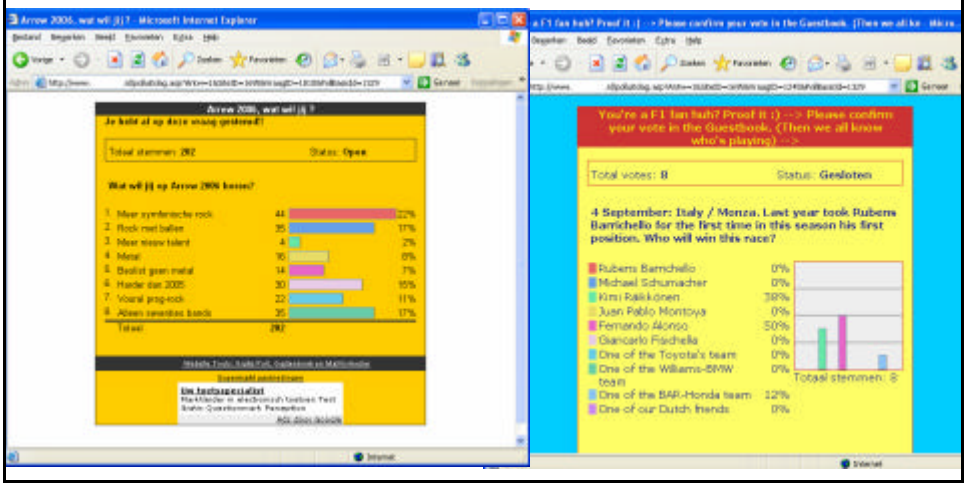
Demonstratie OWASP Top 10
Broken access Control

YACHT

Hoe hou je een gebruiker weg van andermans informatie ?

www. ... /polluitslag.asp?**Vraagid = 1810**

www. ... /polluitslag.asp?**Vraagid = 1245**

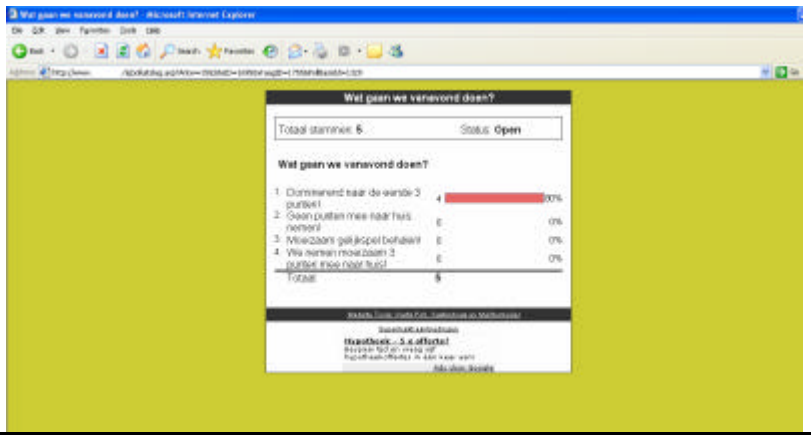


Demonstratie OWASP Top 10
Unvalidated parameter

YACHT

Parameters die naar de webserver worden gestuurd, word niet gecontroleerd op correctheid

http:// .... /polluitslag.asp ? **Antw = 1** **Antw = 15 .....**



Demonstratie OWASP Top 10
Command Injection (1)
SQL injection

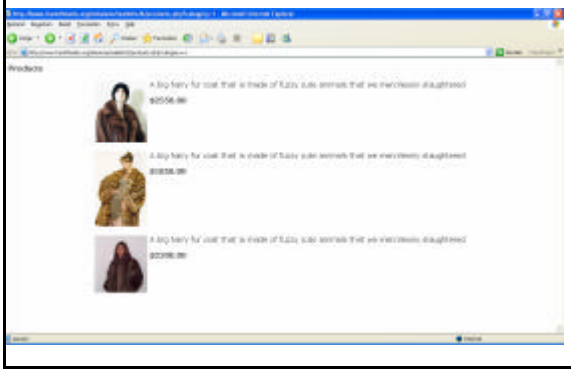
YACHT

Is het mogelijk om commando's te geven naar achterliggende systemen?

Http:// ..... ?**category = 1**

Code:

SQL = SELECT a,b,c,d FROM products Where cat = <category> ;



Demonstratie OWASP Top 10
Command Injection (1)
SQL injection

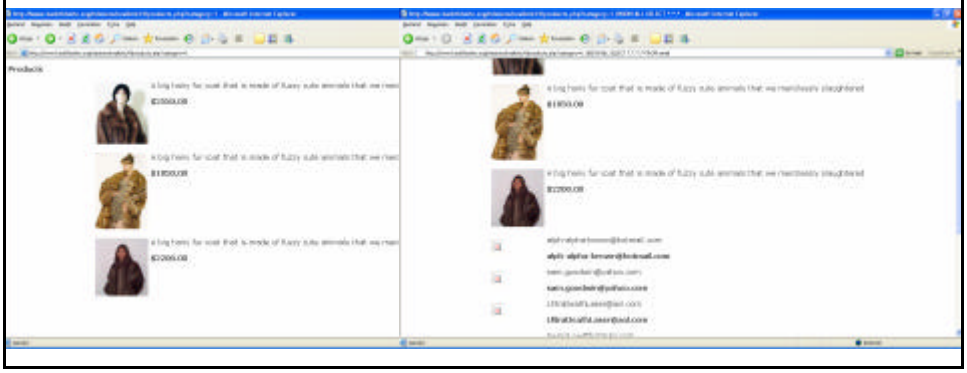
YACHT

Is het mogelijk om commando's te geven naar achterliggende systemen?

Http:// ..... ?category = **1 UNION ALL SELECT *,*,* FROM email**

Code:

SQL = SELECT a,b,c,d FROM products Where cat = **1 UNION ALL SELECT *,*,* FROM email** ;



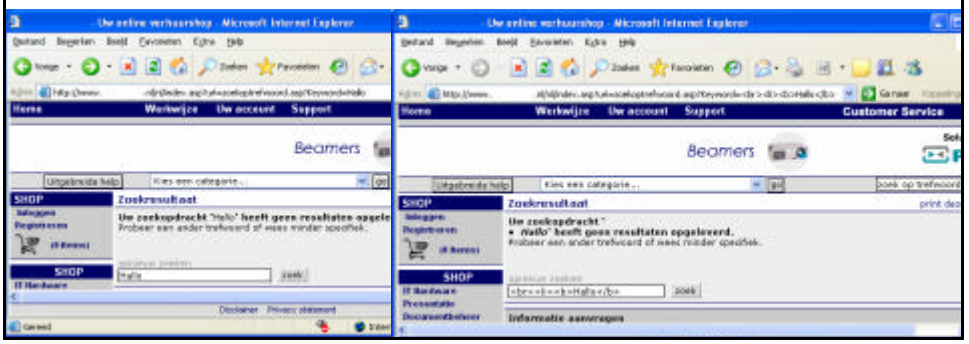
Demonstratie OWASP Top 10
Cross-Site scripting (XSS) flaws

YACHT

Is het mogelijk om programmeertaal (script) toe te voegen in een webpagina ?

Zoeken op **Hallo**

Zoeken op **<li>Hallo**



Demonstratie OWASP Top 10
Cross-Site scripting (XSS) flaws

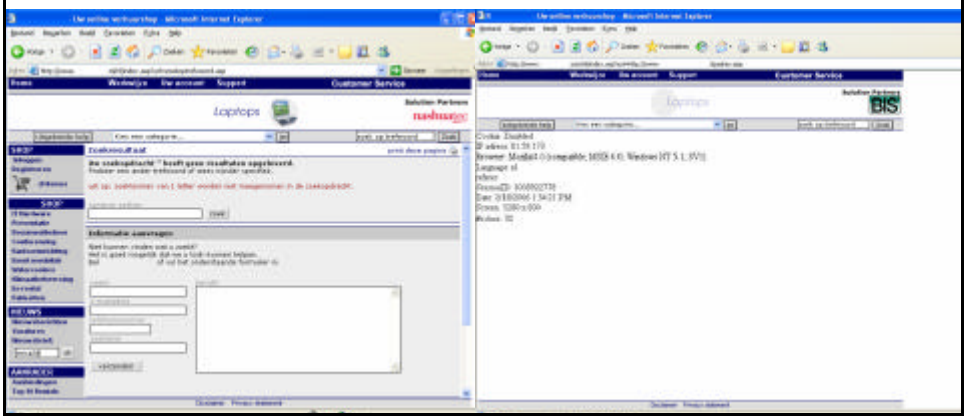
YACHT

Is het mogelijk om broncode (script) toe te voegen in een webpagina ?

Code van een andere webserver kan worden uitgevoerd.

www. ... / index.asp?**url= zoekwoord.asp**

www. ... / index.asp?**url= http://www....**



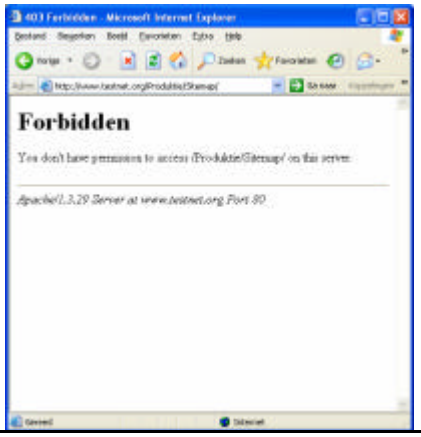
Demonstratie OWASP Top 10
Error handling (1)

YACHT

Geven foutmeldingen meer informatie over de opzet van de site?

HTTP 404

HTTP 403 ✍ Directory aanwezig



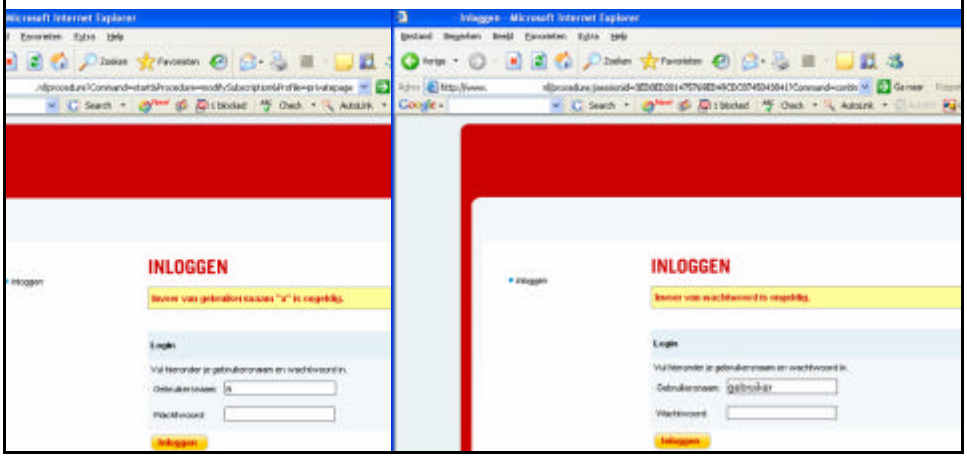
Demonstratie OWASP Top 10
Error handling (2)

YACHT

Geven foutmeldingen meer informatie over de opzet van de site?

Incorrecte gebruiker

Incorrect wachtwoord



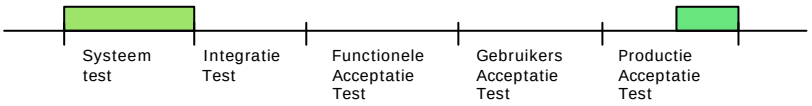
Soorten fouten

YACHT

BUG	Security fouten, ontstaan tijdens programmeren
FLAW	Security fouten, ontstaan door design of architectuur
THREAT	Security gevolgen als gevolg van een BUG of een FLAW

Aandachtspunten voor Testmanager (1)

YACHT



	Code inspectie	Systeem test	Productie test
1. Code review	**Security Specialist**		
2. Controle Site gerelateerde security		**Test Engineer**	
3. Penetratie test			**Security Specialist**

Aandachtspunten voor Test engineer

YACHT

Iedere Test Engineer kan symptomen testen !!

Websecurity testen is het onderzoeken of het mogelijk is om iets incorrect te laten werken

Specialiseer:

- Een functionele tester kent heel goede de werking van een applicatie, de gebruikte systemen en de onderlinge verbanden.
- Specialiseer je op het security testen van Flaws.

Juridische bescherming

YACHT

Tester: Wees geen hacker
Werk met nadrukkelijk goedkeuring

Sitebeheerder: Nieuwe wet Computercriminaliteit II (25 April 2006)
beschermt sitebeheerders tegen hackers.

Hoe herkent men een hacker aanval ?

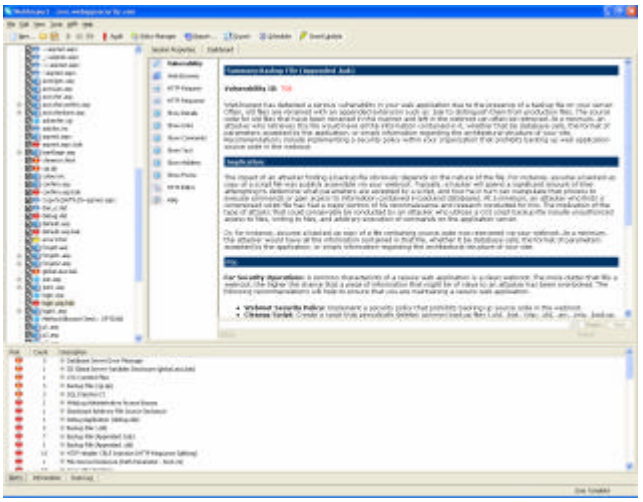
Hoe registreert u de aanval?

Geldt de bescherming ook in het land van de hacker?

YACHT

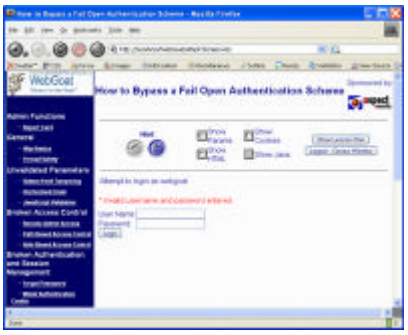
Tooling
Webinspect

SPI DYNAMICS



YACHT

Trainingsfaciliteiten
OWASP Webgoat



YACHT

Trainingsfaciliteiten
Hack Me´s

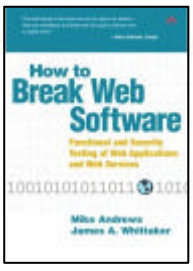
1001 Hack me's

www.HackThisSite.org
www.HackerGames.net

YACHT

En Verder ..

Boek:



James A. Whittaker
ISBN 0-321-36944-0

Links:

Public Vuln list	http://www.evuln.com
Security.NL	http://www.security.nl/
OWASP	http://www.owasp.org
OWASP testing doc	OWASPTesting_PhaseOne.pdf
Standaard Wachtwoorden	http://www.cirt.net/cgi-bin/passwd.pl
SQL injectie	http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf


YACHT
Interim Professionals
Bedankt voor uw aandacht
Gelderlandplein 75a
1082 LV Amsterdam
(020) 301 3100
Edwin.van.Vliet@yacht.nl
www.Yacht.nl
Amsterdam, Arnhem, Breda, Diemen, Eindhoven, Groningen, Hengelo, 's Hertogenbosch,
Leeuwarden, Maastricht, Rotterdam, Utrecht, Voorburg, Zwolle