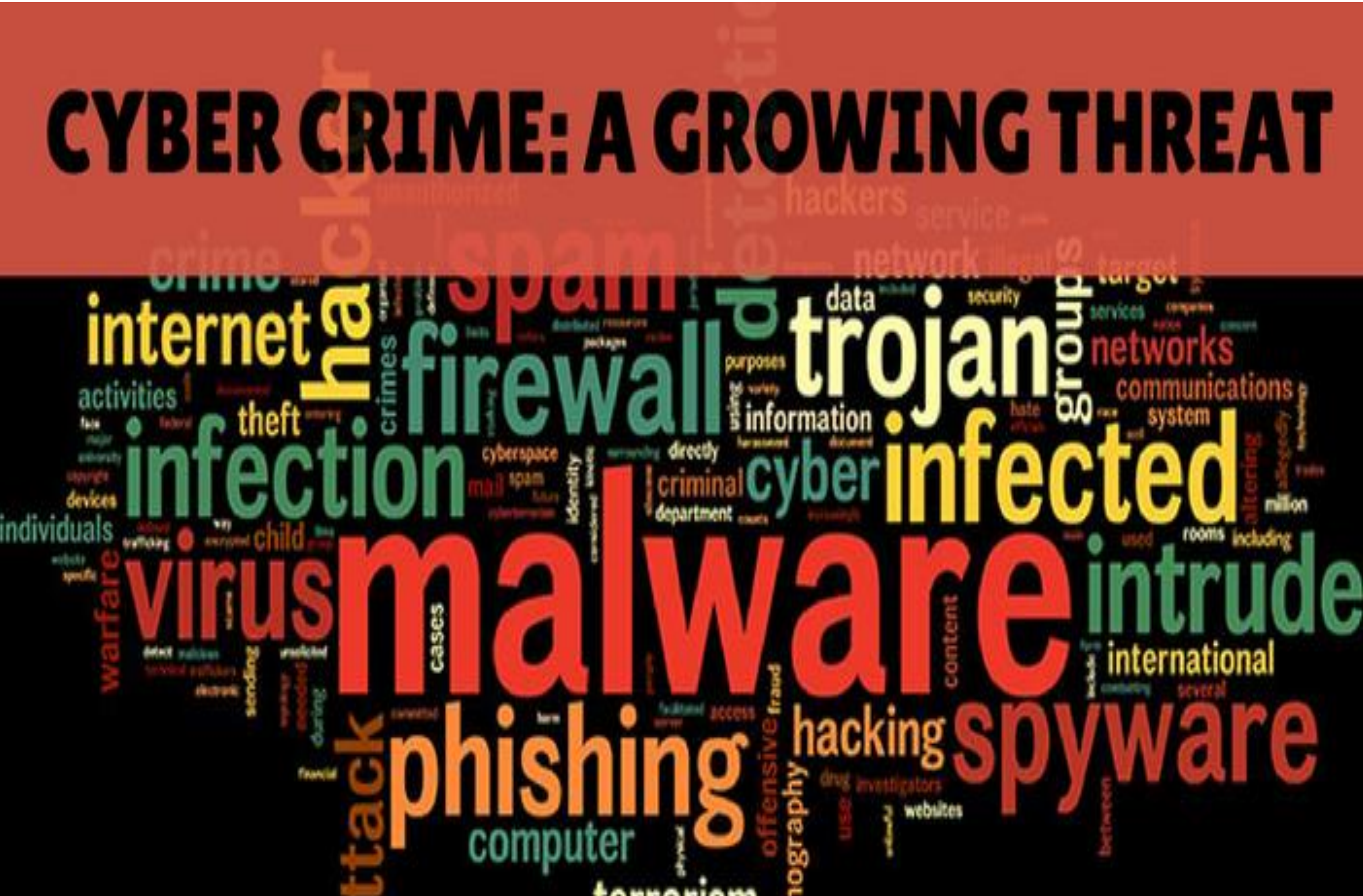
Hoeveel aandacht besteed jij aan security testing?

Security is always excessive until it's not enough

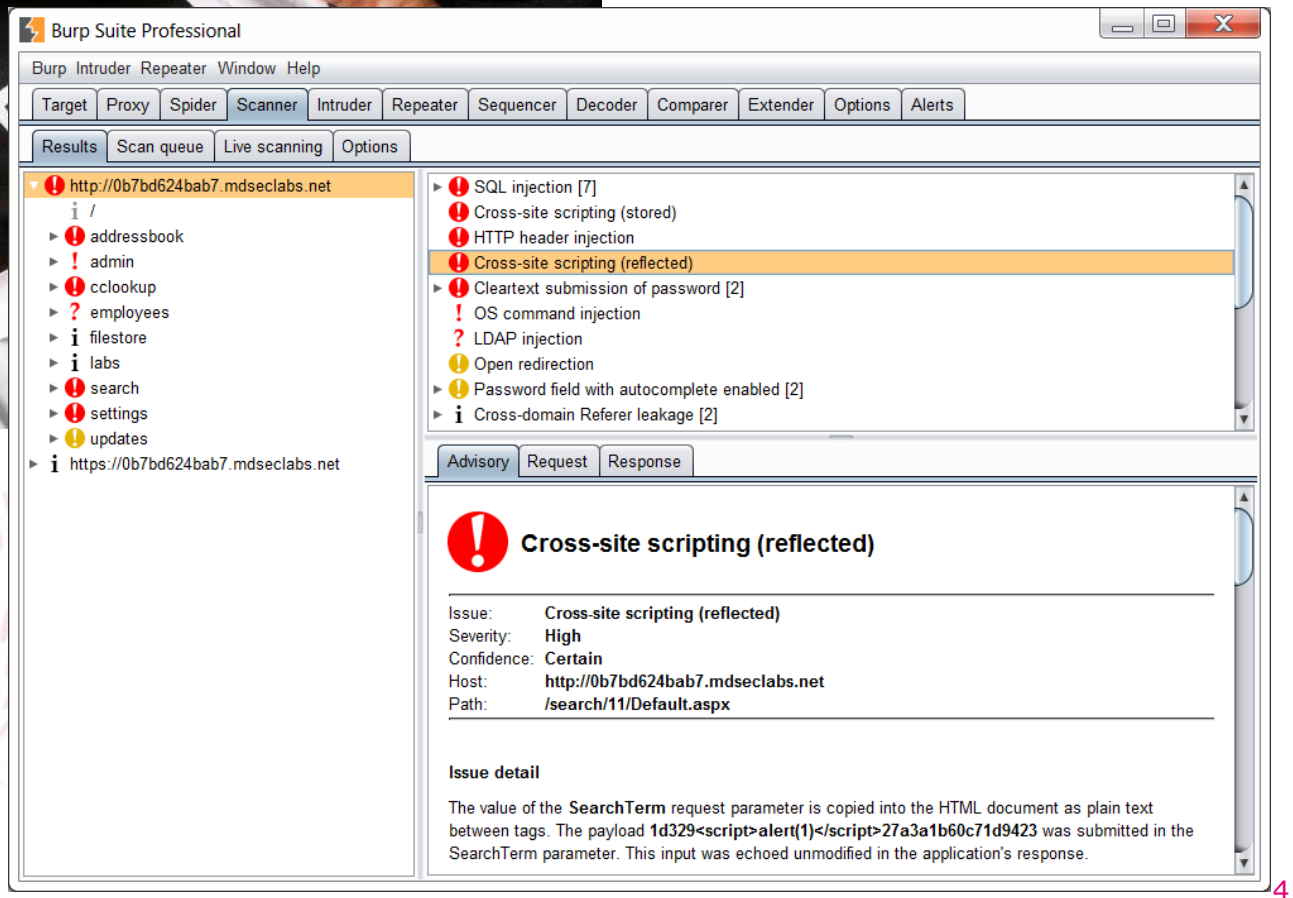

CYBER CRIME: A GROWING THREAT
hackers
network
internet
trojan
firewall
networks
communications
activities
theft
information
system
infection
cyber
infected
criminal
individuals
child
malware
virus
intrude
international
warfare
phishing
hacking
spyware
computer
attack
crimes
groups
data
security
target
spam
crime
offensive
investigators
websites
department
cyberspace
directly
identity
million
rooms
including
devices
altering
cases
content
fraud
access
sending

Wat is een pentest?

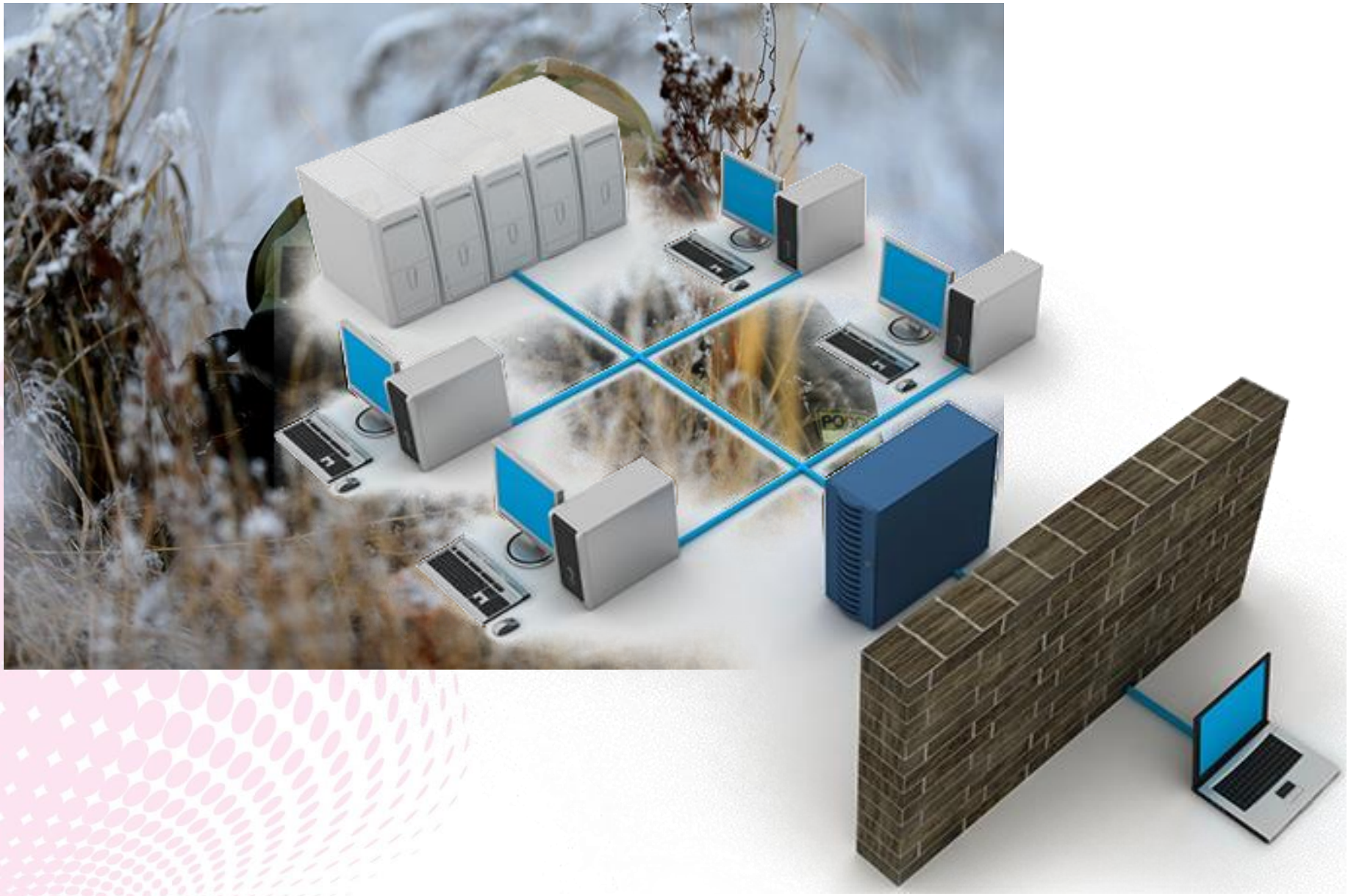
- Informatieveiligheid assessment.

- Black box vs White box
- Bestaat uit verschillende onderdelen
  - Informatie winnen
  - Scannen
  - Controle configuraties
  - Authenticatie
  - Authorisatie
  - Controle session management
  - Data validatie en sanitatie
  - Foutafhandeling

Penetratietesten



Reconniassance



Social Engineering

- Non tech hacking
  - Tail bagging
  - (Spear)Fishing
  - Whaling
  - Dumpster diving
  - Etc.

"Amateurs hack systems, professionals hack people"

Social Engineering

How not to scan!

- Eerste stap voor de laptops :
- Scan op :
- http://www.123cybersecurity.nl/poort-scan/

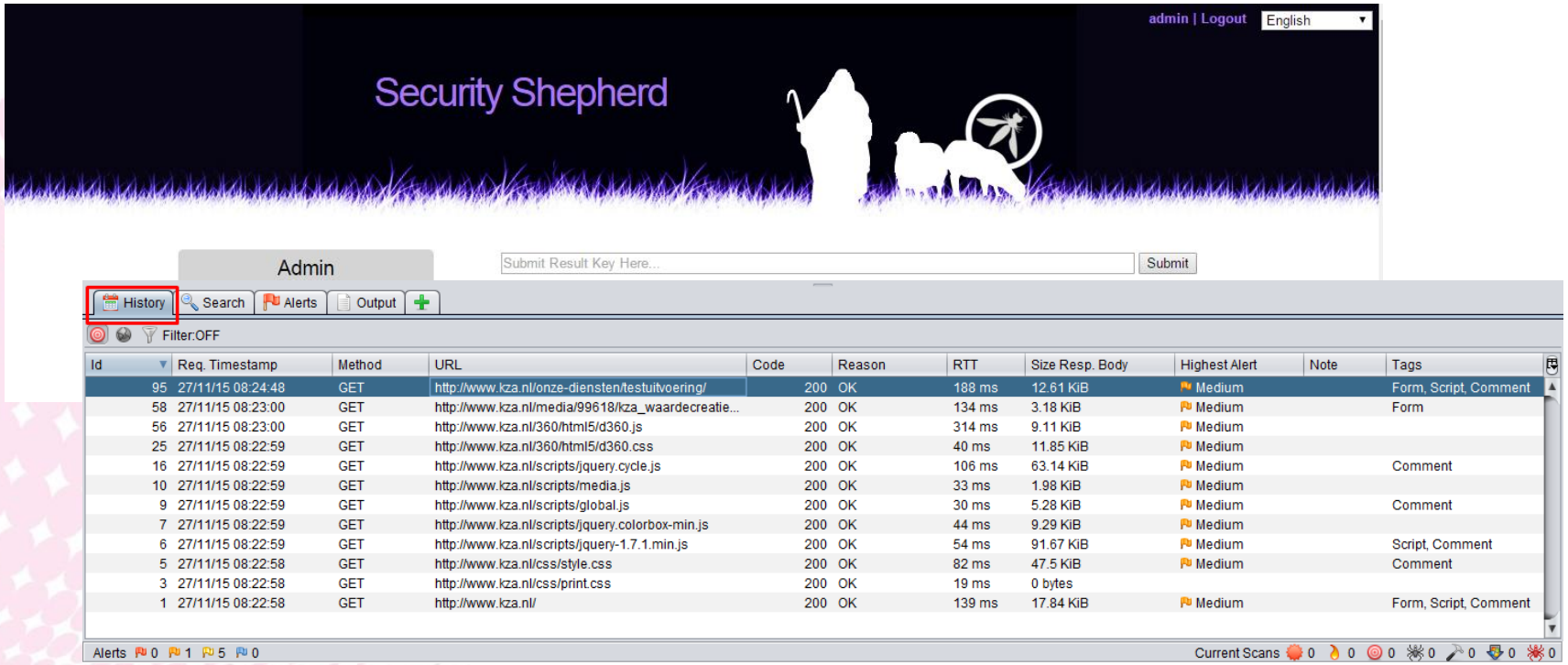
TLS/SSL configuratie

kza
TSS QA AND TESTING

OWASP ZAP

Visit 'www.kza.nl' in browser

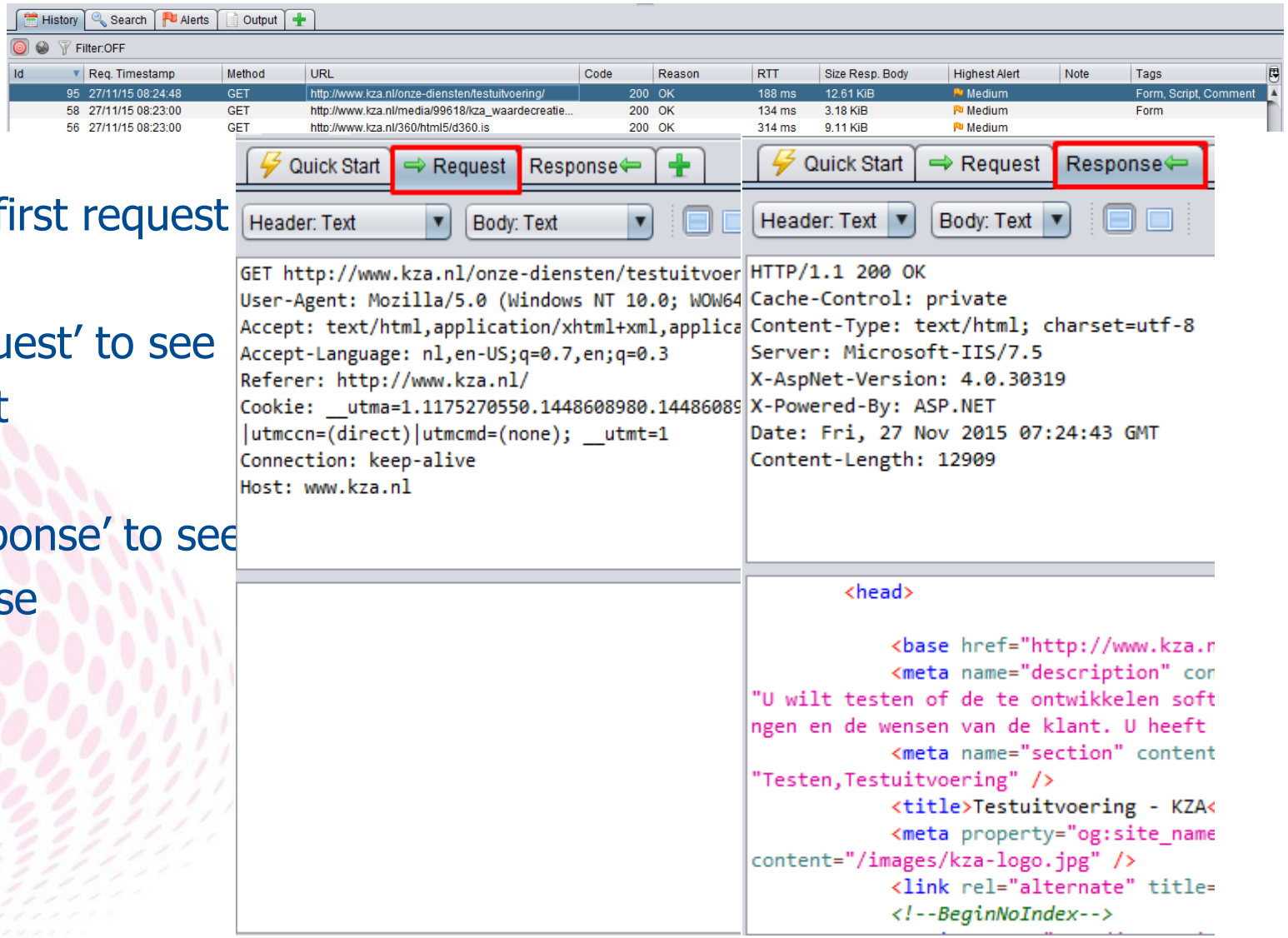
Check history in ZAP



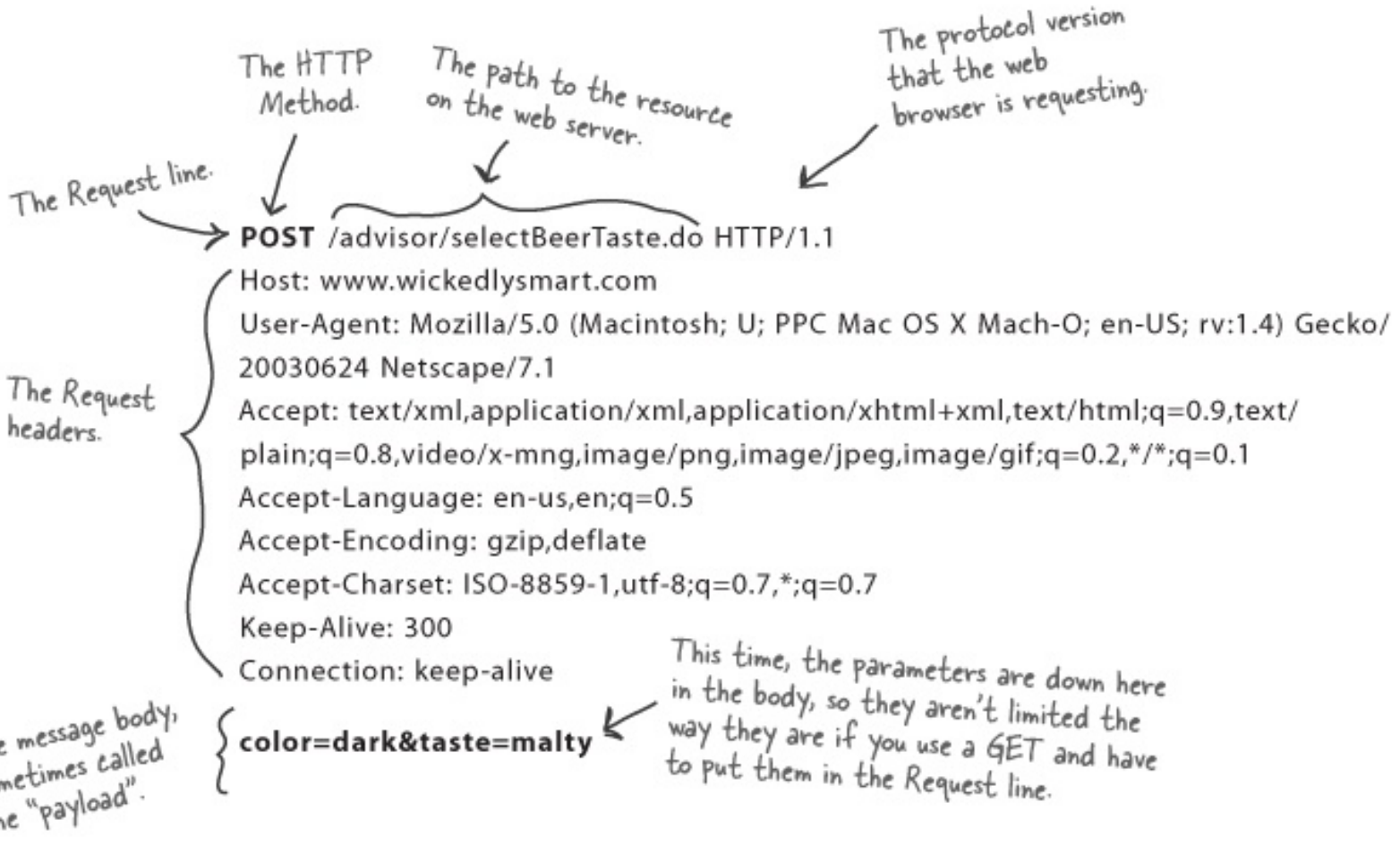
Select the first request

Select 'request' to see the request

Select 'response' to see the response



HTTP Request



Source: safaribooksonline.com

The HTTP Response

Status, header and data

HTTP Response headers:

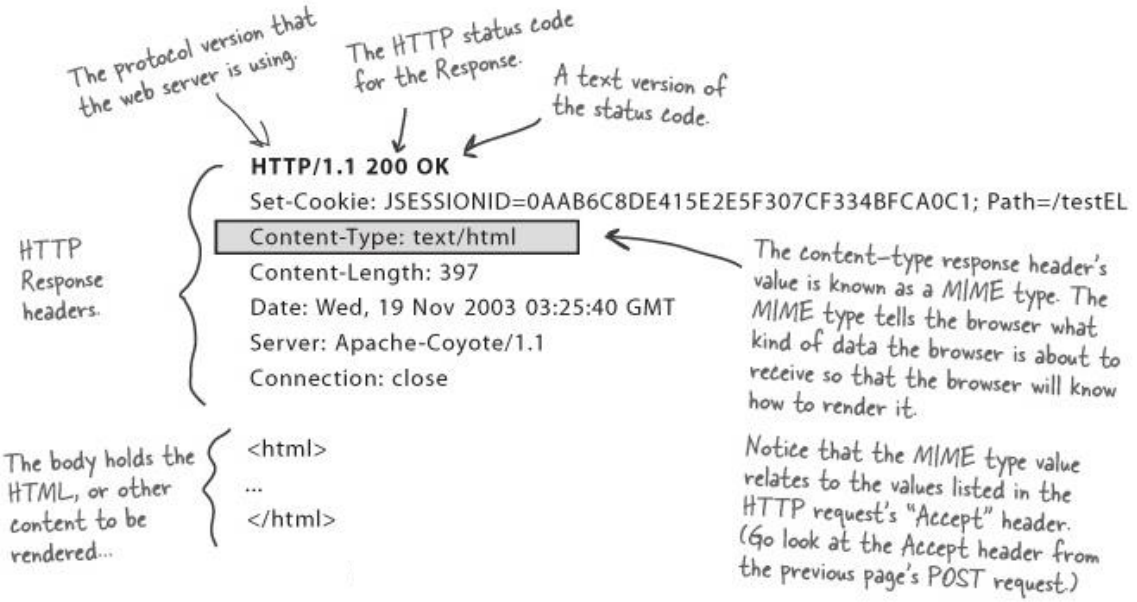
- Content-type
- Expires
- Last-Modified
- WWW-Authenticate
- Set-Cookie
- Etc.

Content types:

- text/html
- Image/gif
- application/word
- etc.

Encoding

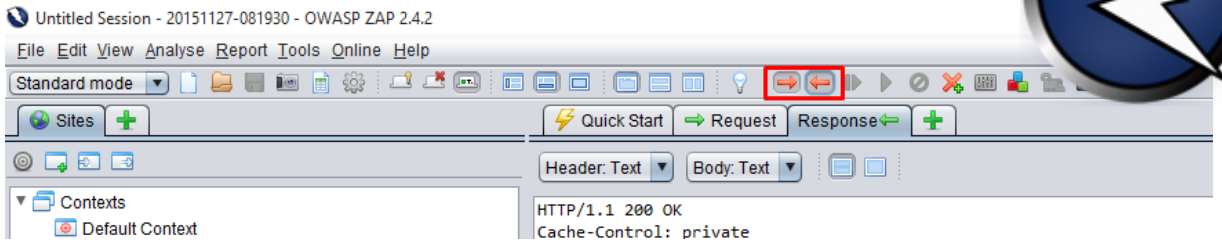
- MIME, readable text, byte stream
  - etc.



Source: safaribooksonline.com

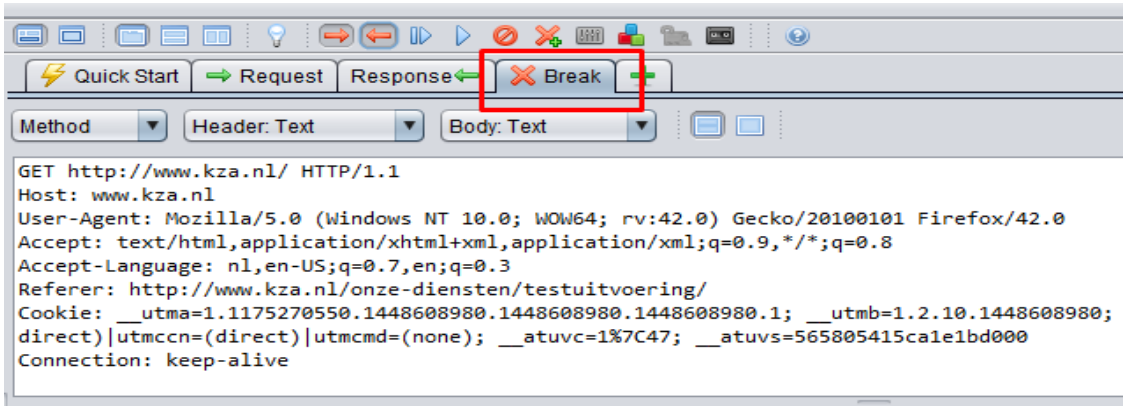
Intercept a request

Enable intercept in ZAP



Click on 'home' in browser

Check 'Break' tab in ZAP



Click ' ' to send request

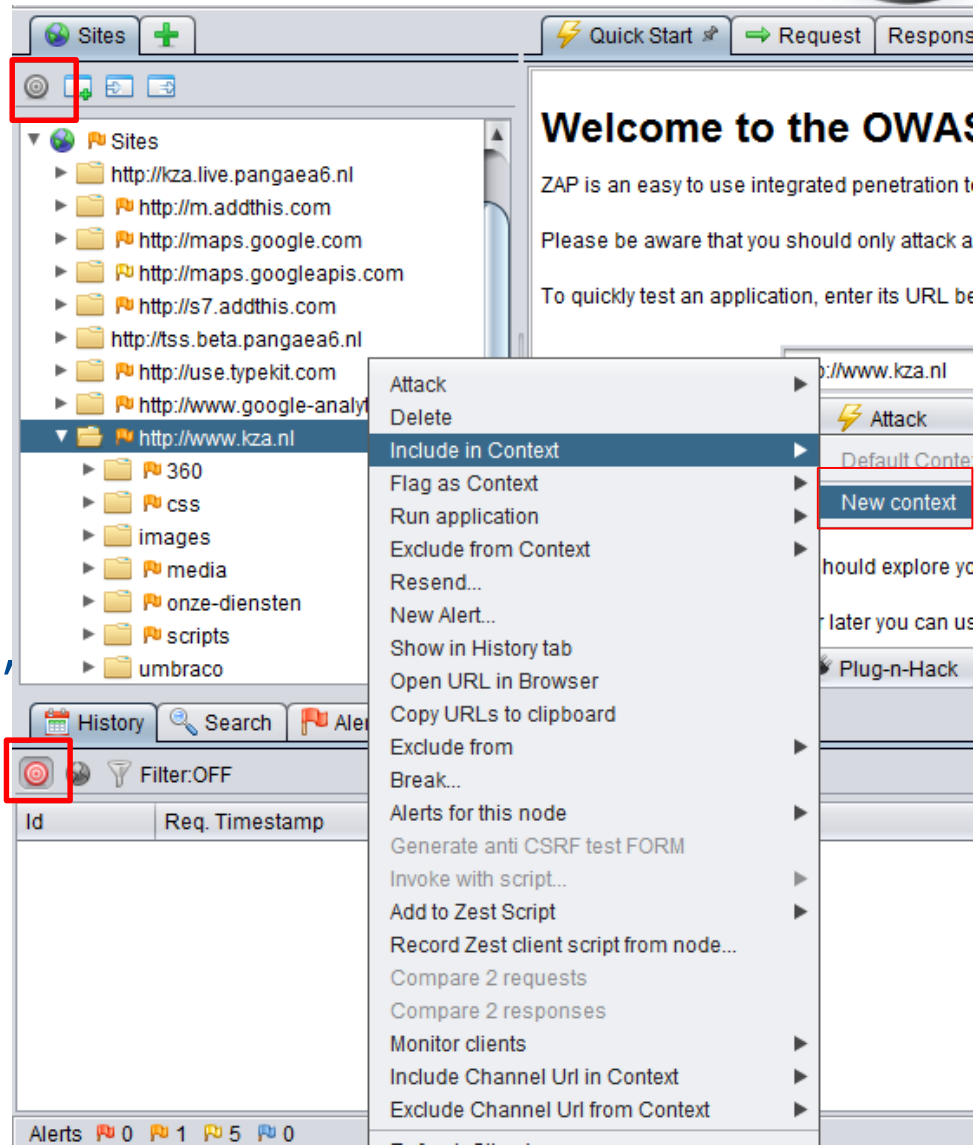
Scope

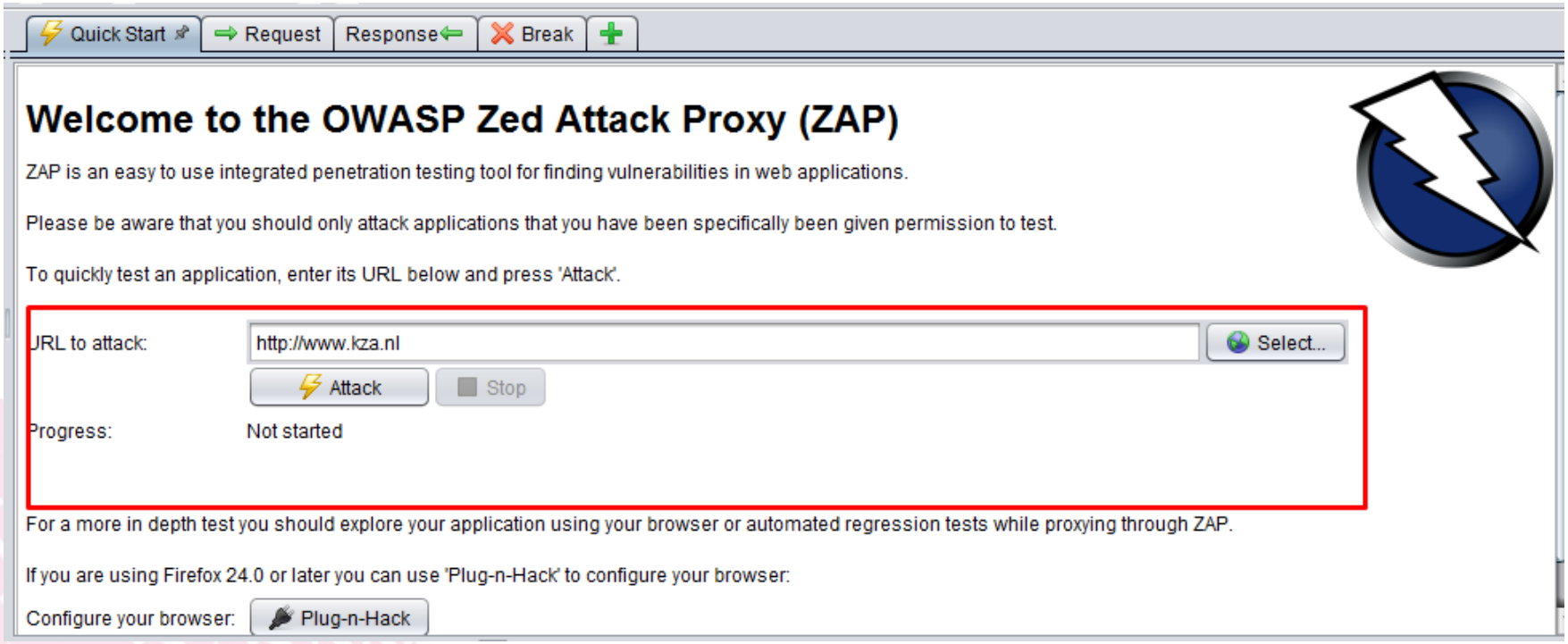
Useful to
1) only show sites of interest
2) scope additional tools in ZAP

Go to ‘Sites’

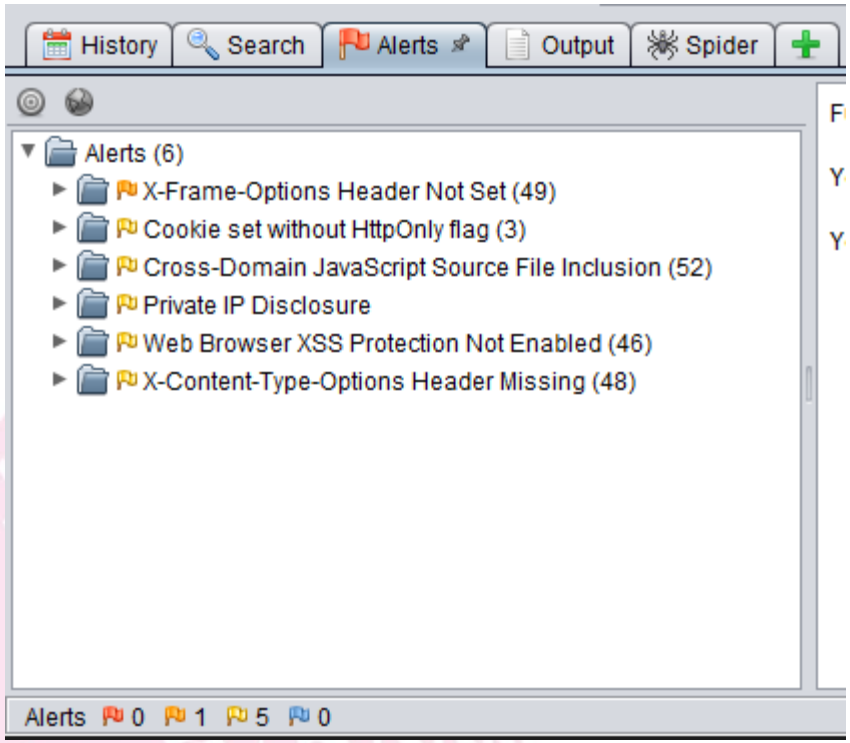
Right-click on ‘http://www.kza.nl’

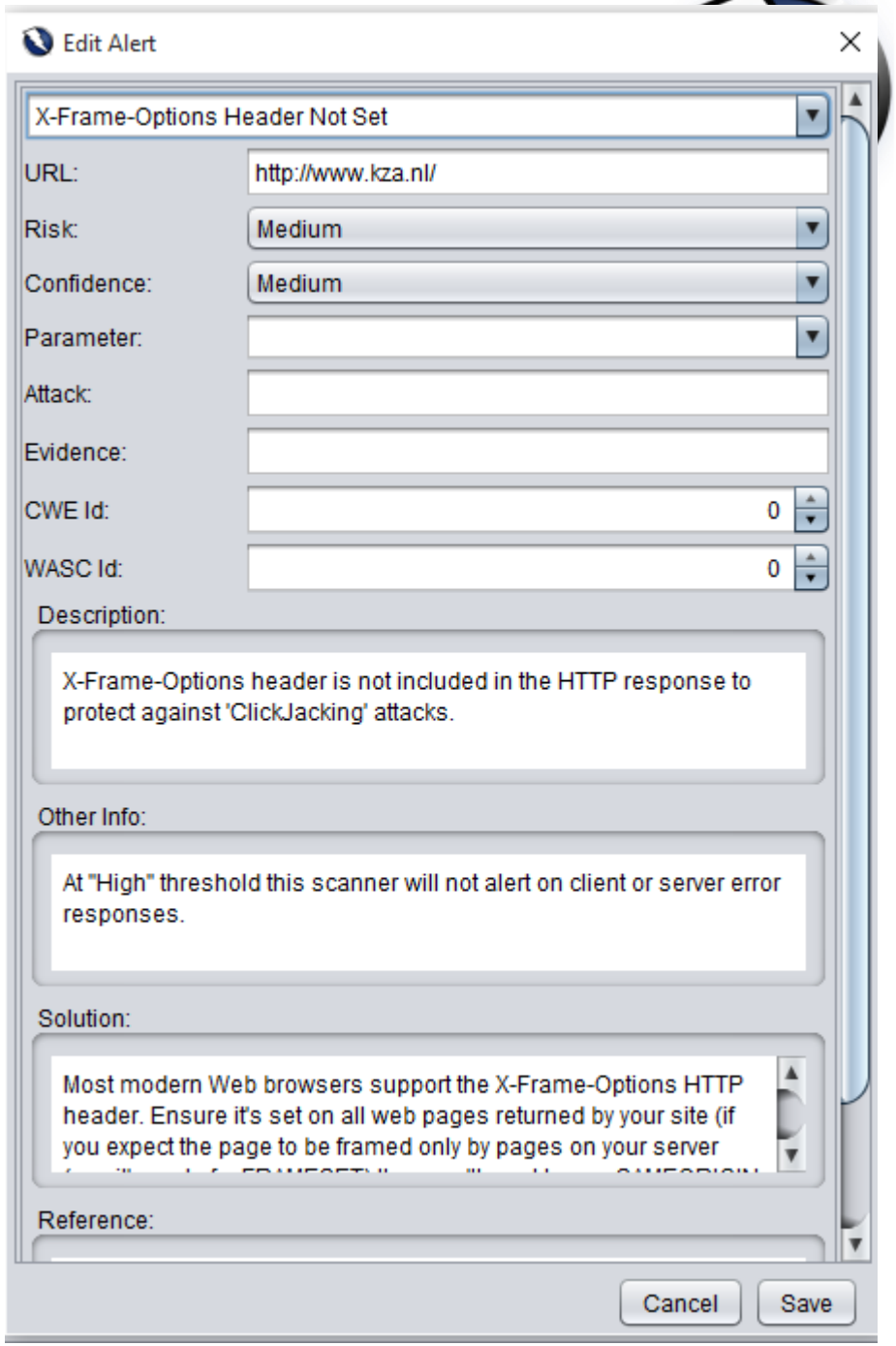
Select ‘Add to scope’



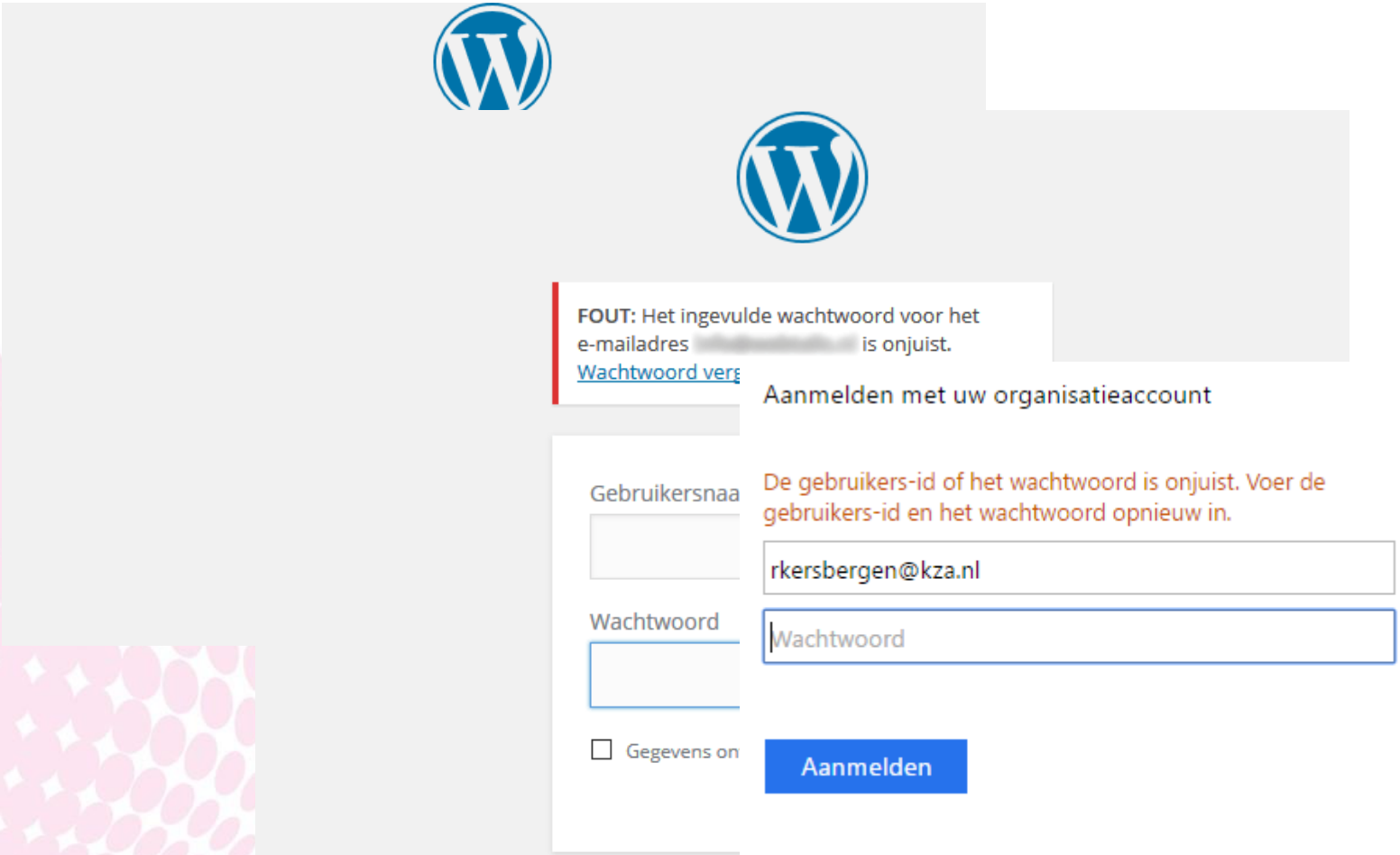

Quick Start
Request
Response
Break
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://www.kza.nl
Select...
Attack
Stop
Progress:
Not started
For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.
If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:
Configure your browser:
Plug-n-Hack

ZAP - SCANNER


History
Search
Alerts
Output
Spider
Alerts (6)
X-Frame-Options Header Not Set (49)
Cookie set without HttpOnly flag (3)
Cross-Domain JavaScript Source File Inclusion (52)
Private IP Disclosure
Web Browser XSS Protection Not Enabled (46)
X-Content-Type-Options Header Missing (48)
Alerts 0 1 5 0


Edit Alert
X-Frame-Options Header Not Set
URL:
http://www.kza.nl/
Risk:
Medium
Confidence:
Medium
Parameter:
Attack:
Evidence:
CWE Id:
0
WASC Id:
0
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Other Info:
At "High" threshold this scanner will not alert on client or server error responses.
Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server
Reference:
Cancel
Save

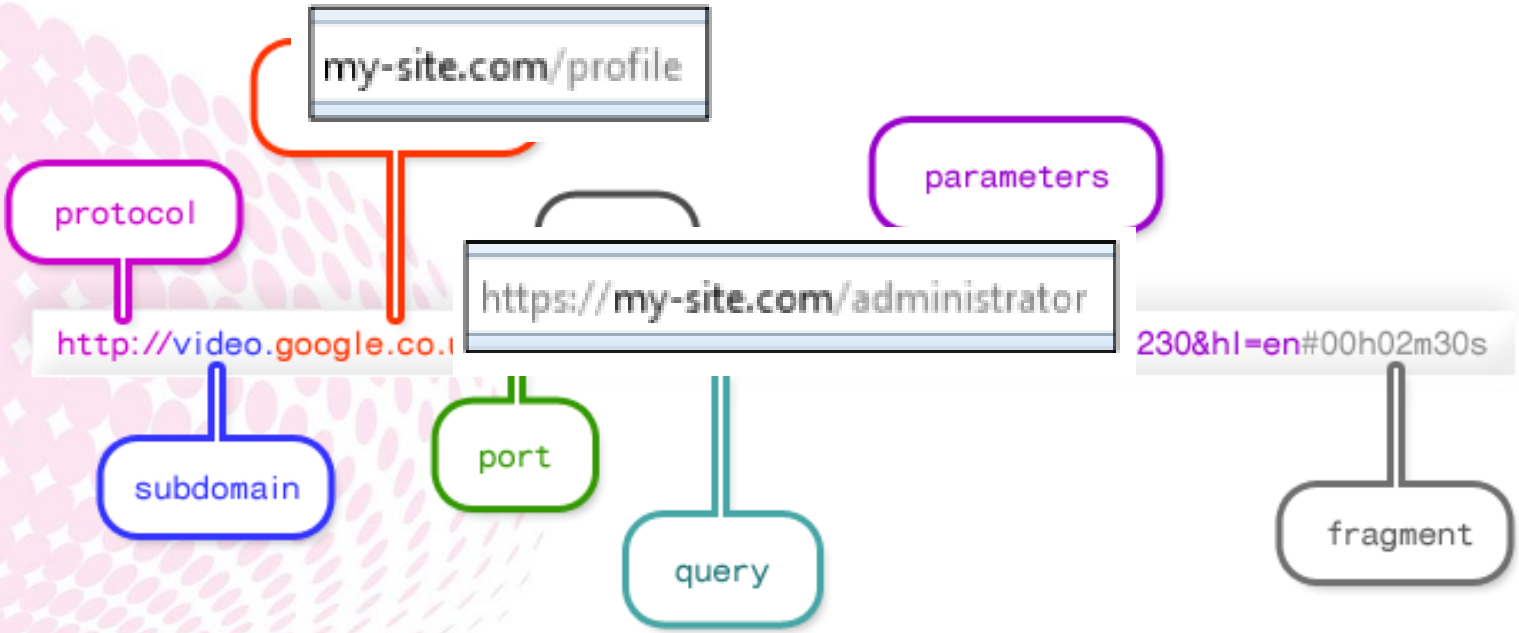
Authenticatie



Authorisatie

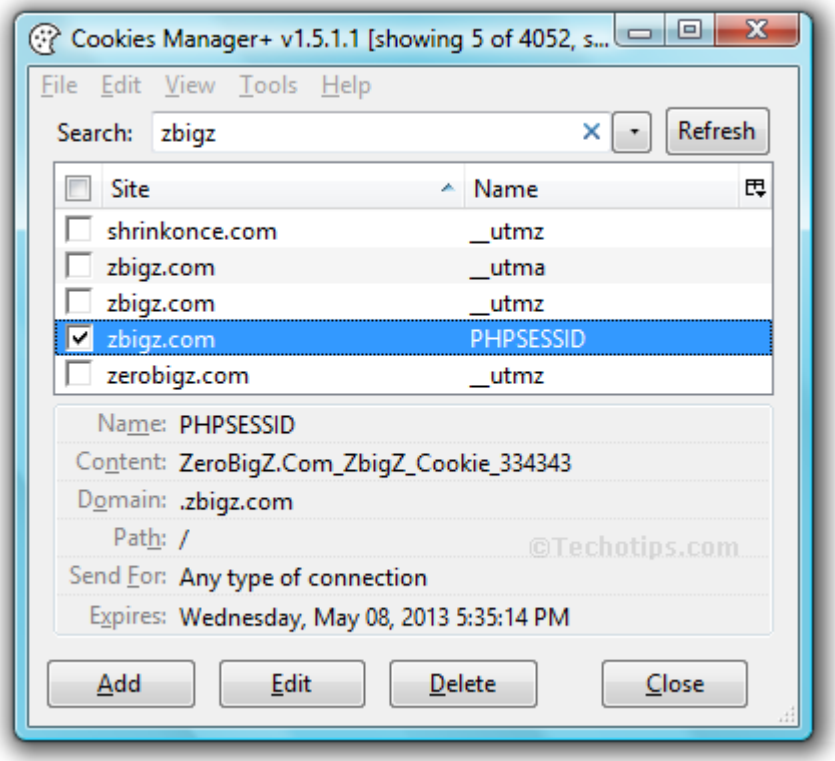
Authenticatie :Ben je wie je zegt dat je bent?
Authorisatie :Heb je toegang/rechten om te zien wat je ziet?

URL Tampering

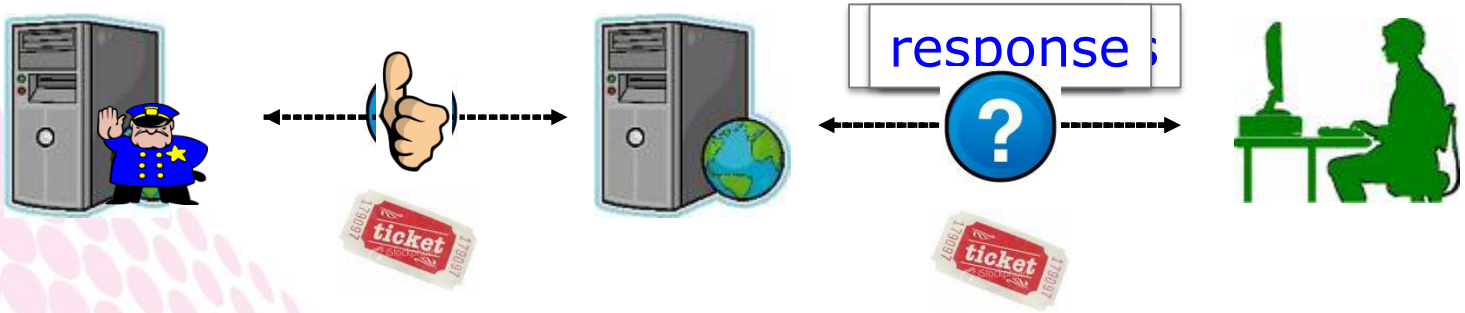


Sessiebeheer

- Cookiemanager+



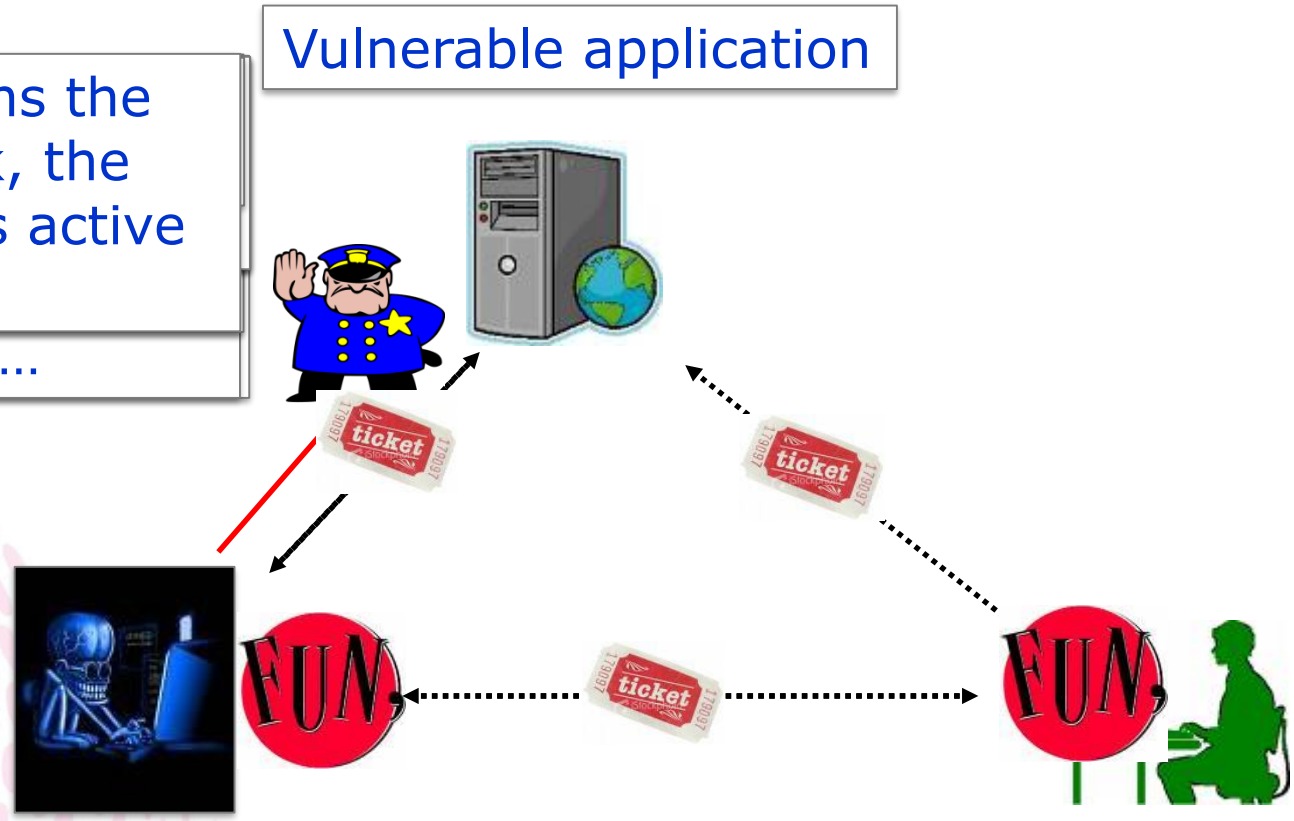
Session management basics



Session hijacking

When Ted opens the interesting link, the script becomes active …

authenticated …



Foutafhandeling

- Hoe forceer je een foutmelding?
  - Doe wat geks!

Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (tbxUserName="<script> alert 'HOI'...").

Description: Request Validation has detected a potentially dangerous client input value, and processing of the request has been aborted. This value may indicate an attempt to compromise the security of your application, such as a cross-site scripting a setting validateRequest=false in the Page directive or in the configuration section. However, it is strongly recommended that your application explicitly check all inputs in this case.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (tbxUserName="<script> alert 'HOI'...").

Source Error:

```
[No relevant source lines]
```

Source File: c:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\root\5feee454\49c3cc81\App_Web_76pufk9q.1.cs **Line:** 0

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (tbxUserName="<script> alert 'HOI'...").]
   System.Web.HttpRequest.ValidateString(String s, String valueName, String collectionName) +8817730
   System.Web.HttpRequest.ValidateNameValueCollection(NameValueCollection nvc, String collectionName) +111
   System.Web.HttpRequest.get_Form() +129
   System.Web.HttpRequest.get_HasForm() +8817831
   System.Web.UI.Page.GetCollectionBasedOnMethod(Boolean dontReturnNull) +97
   System.Web.UI.Page.DeterminePostBackMode() +63
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +6785
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +242
   System.Web.UI.Page.ProcessRequest() +80
   System.Web.UI.Page.ProcessRequestWithNoAssert(HttpContext context) +21
   System.Web.UI.Page.ProcessRequest(HttpContext context) +49
   ASP.login_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\root\5feee454\49c3cc81\App_Web_76pufk9q.1.cs:0
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +181
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +75
```

Version Information: Microsoft .NET Framework Version:2.0.50727.8009; ASP.NET Version:2.0.50727.8015

Data validatie en sanitatie

Data validatie

- SQL injectie
- XSS

- Bestandsupload
  - Upload een virus!
  - Download het EICAR test-virus van de volgende website: http://www.eicar.org/download/eicar.com.txt
  - Wijzig het bestand in eicar.exe en upload het

SQL Injectie: Hoe te testen

Test cases

- Voeg stuurkarakters toe aan input en let op foutmeldingen
  - SQL: ` ` | ; “ / \
  - OS Injection: | + / ? \
- Probeer bekende aanvalspatronen
  - SQL: ‘ AND ‘1’=‘1’ -- vergelijken met ‘ AND ‘1’=‘2’ --
  - OS Injection: |dir of |ls
- Email injection: voeg ; toe aan einde email adres

Waar op te letten

- Foutmeldingen
- Afwijkende resultaten
- Langere responstijden

XSS: Hoe te testen

Test cases

- Probeer HTML injectie eerst
  - Verschil tussen test en test
- Controleer source in browser waar veld terecht komt
  - Let op afsluittekens zoals " of ">
  - Let op afsluitblokken zoals </TEXTAREA>
- Pas testgevallen aan

Waar op te letten

- Veranderingen in de layout
  - Afwijkende opmaak (bold tekst)
  - Afwijkende of extra blokken)
- Popups (bij testgevallen met alert() input)

Recap

- Penetratie testen voor applicaties
- Awareness workshops (Testers, Ontwikkelaar, Gebruikers)
- Securitybeleid implementaties
- Voor al uw security vraagstukken

Recap

- Recap
  - Informatie winnen
  - Scannen
  - Controle configuraties
  - Authenticatie
  - Authorisatie
  - Controle session management
  - Data validatie en sanitatie
  - Foutafhandeling