

Hoeveel aandacht besteed jij aan security testing?

Don't let this be you!

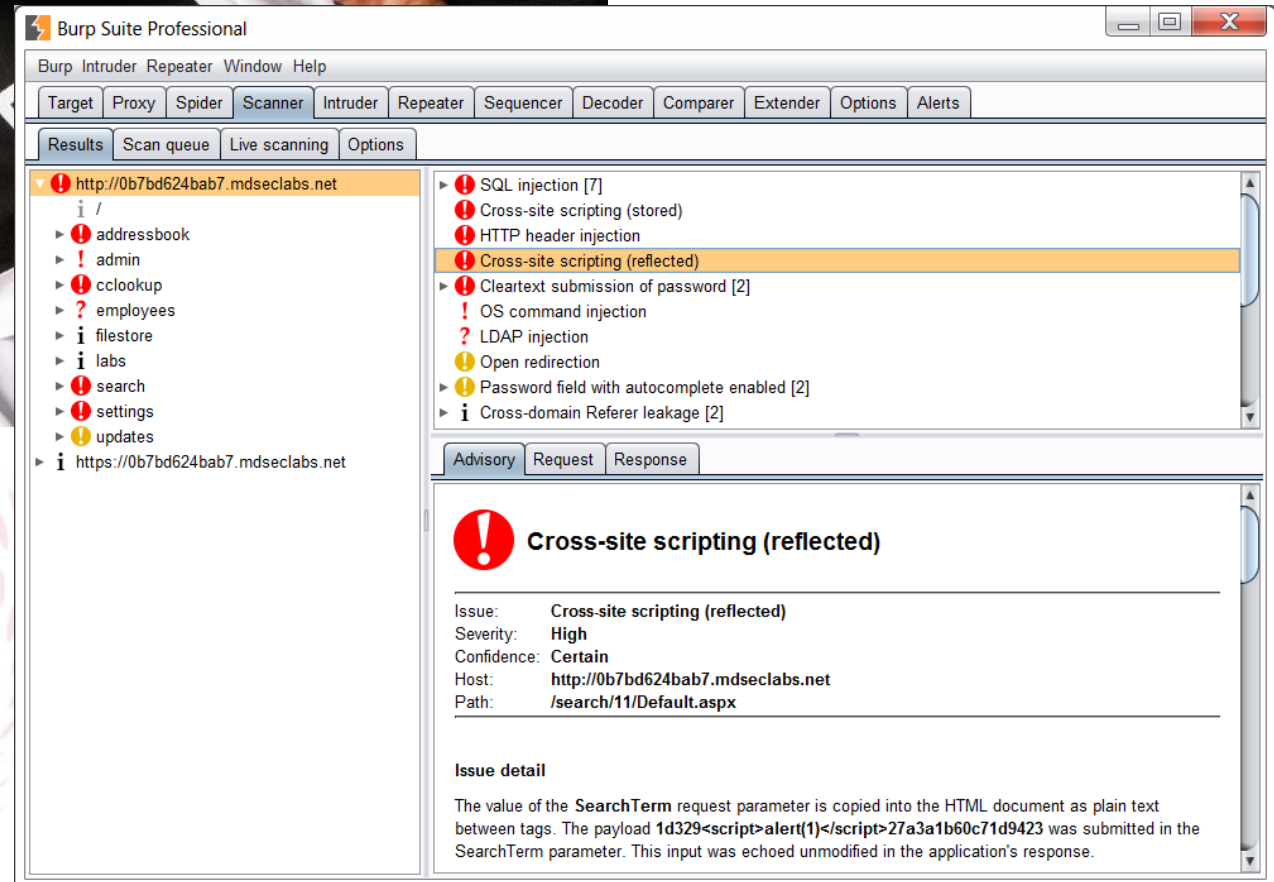
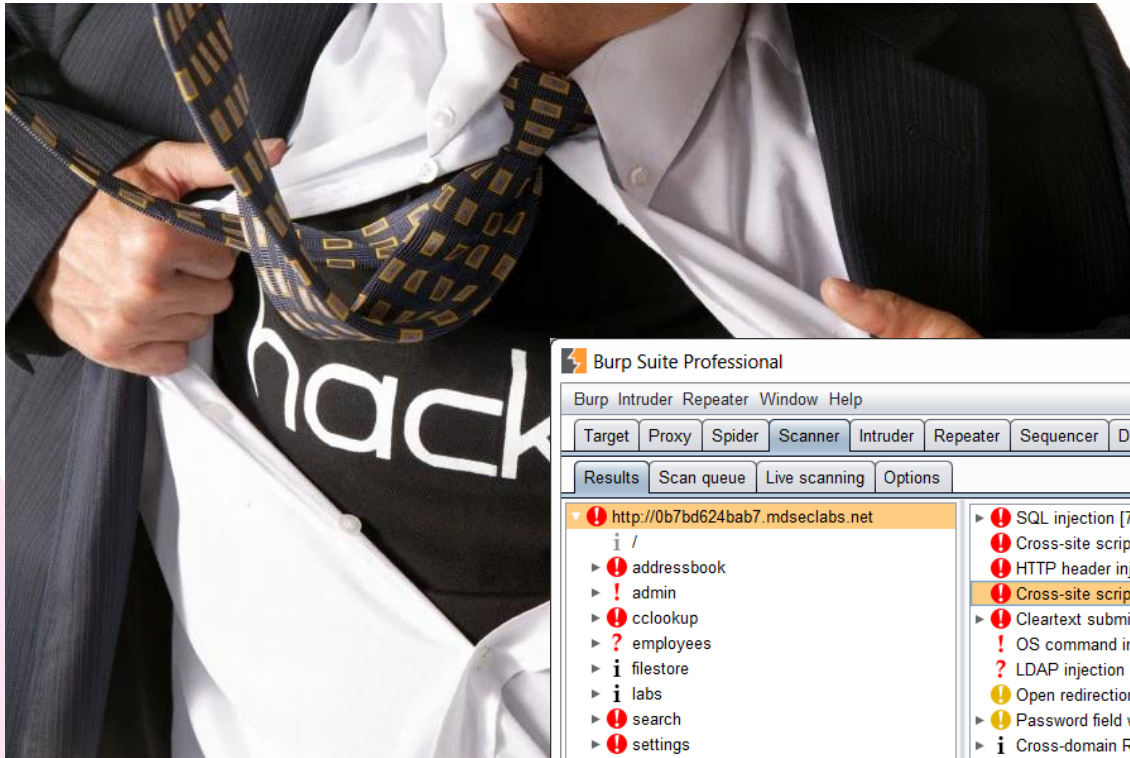


Security is always excessive until it's not enough

CYBER CRIME: A GROWING THREAT



- 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



Burp Suite Professional

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Results Scan queue Live scanning Options

- ! http://0b7bd624bab7.mdseclabs.net
 - i /
 - ! addressbook
 - ! admin
 - ! cclookup
 - ? employees
 - i filestore
 - i labs
 - ! search
 - ! settings
 - ! updates
 - i https://0b7bd624bab7.mdseclabs.net

! SQL injection [7]
! Cross-site scripting (stored)
! HTTP header injection
! Cross-site scripting (reflected)
! Cleartext submission of password [2]
! OS command injection
? LDAP injection
! Open redirection
! Password field with autocomplete enabled [2]
i Cross-domain Referer leakage [2]

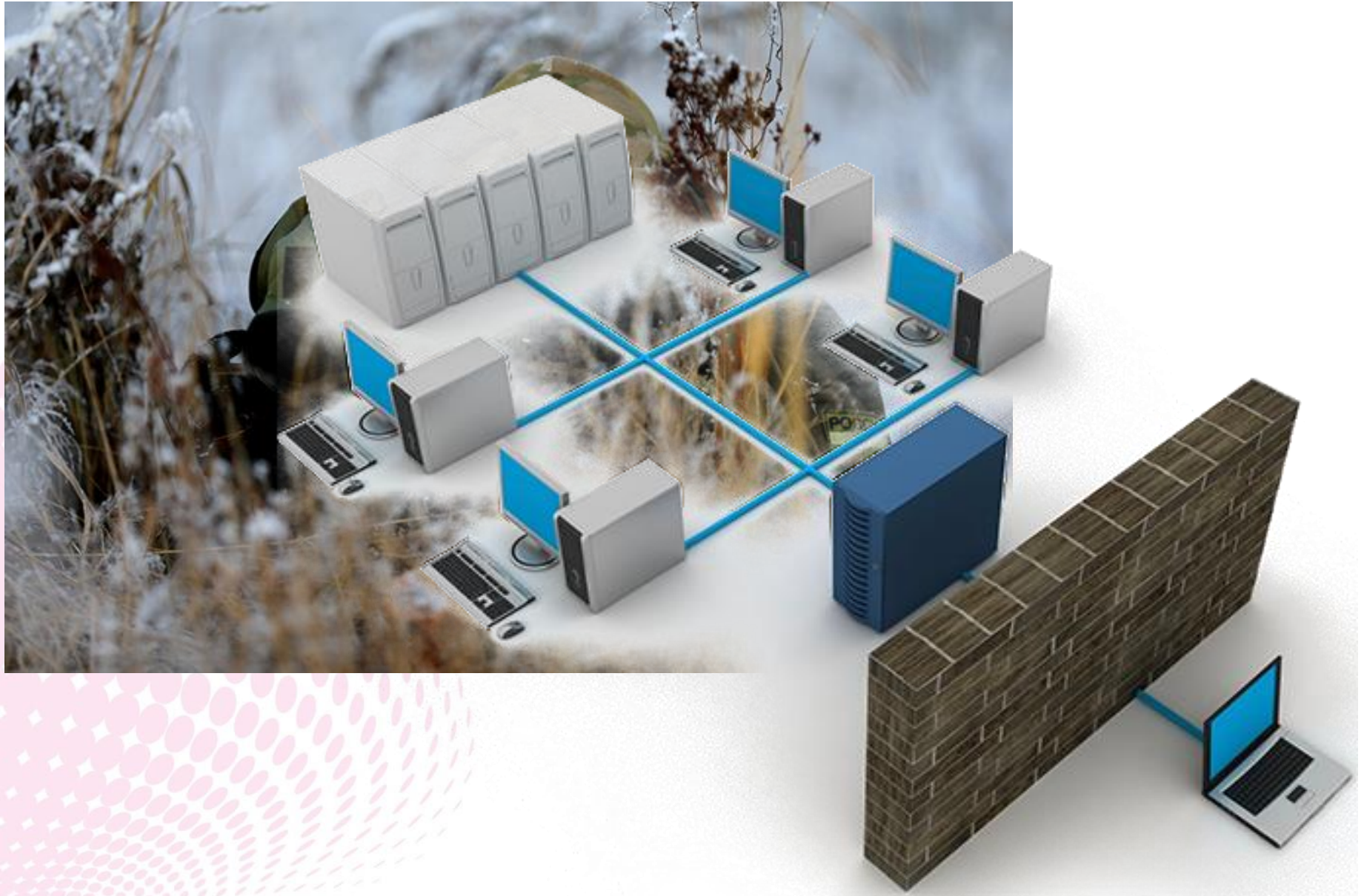
Advisory Request Response

! Cross-site scripting (reflected)

Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Certain
Host: http://0b7bd624bab7.mdseclabs.net
Path: /search/11/Default.aspx

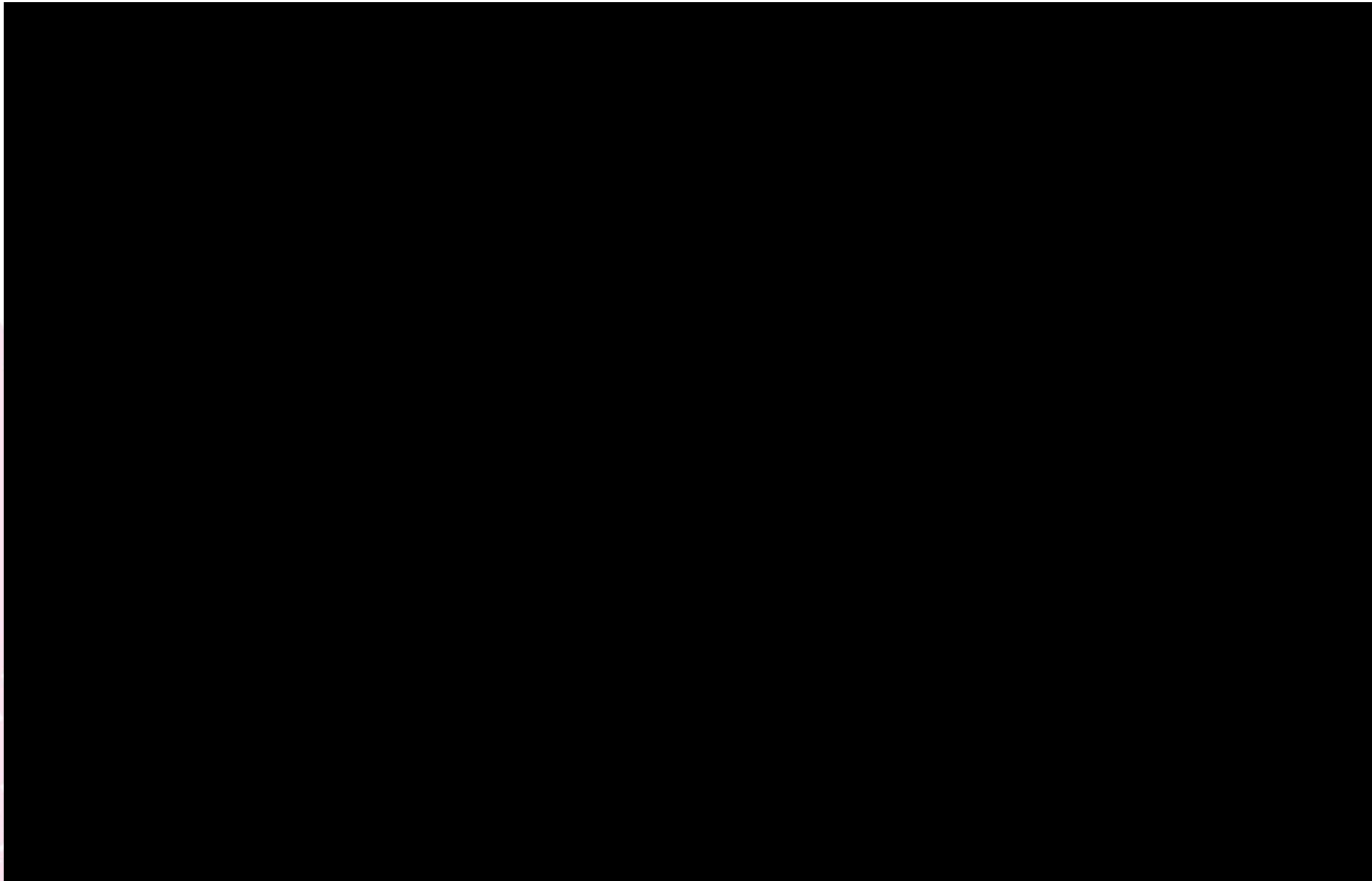
Issue detail

The value of the **SearchTerm** request parameter is copied into the HTML document as plain text between tags. The payload `1d329<script>alert(1)</script>27a3a1b60c71d9423` was submitted in the SearchTerm parameter. This input was echoed unmodified in the application's response.

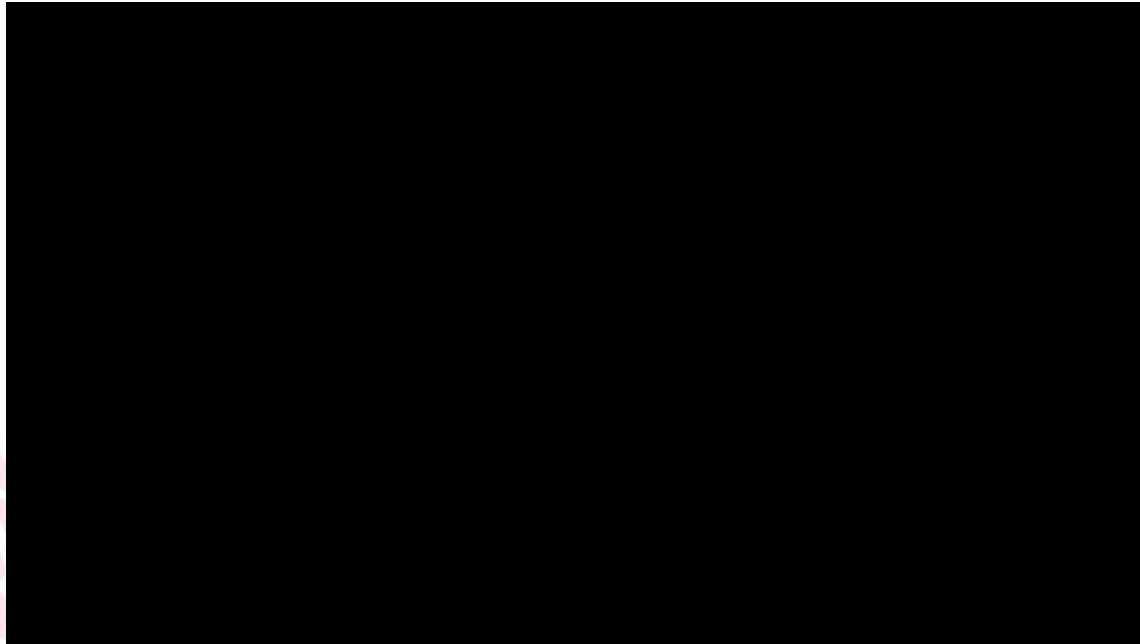


- Non tech hacking
 - Tail bagging
 - (Spear)Fishing
 - Whaling
 - Dumpster diving
 - Etc.

"Amateurs hack systems, professionals hack people"



How not to scan!



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



OWASP ZAP





Visit 'www.kza.nl' in browser
Check history in ZAP

admin | Logout English

Security Shepherd

Admin Submit

History Search Alerts Output +

Filter: OFF

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
95	27/11/15 08:24:48	GET	http://www.kza.nl/onze-diensten/testuitvoering/	200	OK	188 ms	12.61 KiB	Medium		Form, Script, Comment
58	27/11/15 08:23:00	GET	http://www.kza.nl/media/99618/kza_waardecreatie...	200	OK	134 ms	3.18 KiB	Medium		Form
56	27/11/15 08:23:00	GET	http://www.kza.nl/360/html5/d360.js	200	OK	314 ms	9.11 KiB	Medium		
25	27/11/15 08:22:59	GET	http://www.kza.nl/360/html5/d360.css	200	OK	40 ms	11.85 KiB	Medium		
16	27/11/15 08:22:59	GET	http://www.kza.nl/scripts/jquery.cycle.js	200	OK	106 ms	63.14 KiB	Medium		Comment
10	27/11/15 08:22:59	GET	http://www.kza.nl/scripts/media.js	200	OK	33 ms	1.98 KiB	Medium		
9	27/11/15 08:22:59	GET	http://www.kza.nl/scripts/global.js	200	OK	30 ms	5.28 KiB	Medium		Comment
7	27/11/15 08:22:59	GET	http://www.kza.nl/scripts/jquery.colorbox-min.js	200	OK	44 ms	9.29 KiB	Medium		
6	27/11/15 08:22:59	GET	http://www.kza.nl/scripts/jquery-1.7.1.min.js	200	OK	54 ms	91.67 KiB	Medium		Script, Comment
5	27/11/15 08:22:58	GET	http://www.kza.nl/css/style.css	200	OK	82 ms	47.5 KiB	Medium		Comment
3	27/11/15 08:22:58	GET	http://www.kza.nl/css/print.css	200	OK	19 ms	0 bytes			
1	27/11/15 08:22:58	GET	http://www.kza.nl/	200	OK	139 ms	17.84 KiB	Medium		Form, Script, Comment

Alerts 0 0 1 5 0 Current Scans 0 0 0 0 0 0 0 0 0 0



Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
95	27/11/15 08:24:48	GET	http://www.kza.nl/onze-diensten/testuitvoer/	200	OK	188 ms	12.61 KiB	Medium		Form, Script, Comment
58	27/11/15 08:23:00	GET	http://www.kza.nl/media/99618/kza_waardecreeatie...	200	OK	134 ms	3.18 KiB	Medium		Form
56	27/11/15 08:23:00	GET	http://www.kza.nl/360/html5/d360.is	200	OK	314 ms	9.11 KiB	Medium		

Quick Start **Request** Response

Header: Text Body: Text

```
GET http://www.kza.nl/onze-diensten/testuitvoer/
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Referer: http://www.kza.nl/
Cookie: __utma=1.1175270550.1448608980.1448608980.1448608980.1448608980
|utmccn=(direct)|utmcmd=(none); __utmt=1
Connection: keep-alive
Host: www.kza.nl
```

Quick Start Request **Response**

Header: Text Body: Text

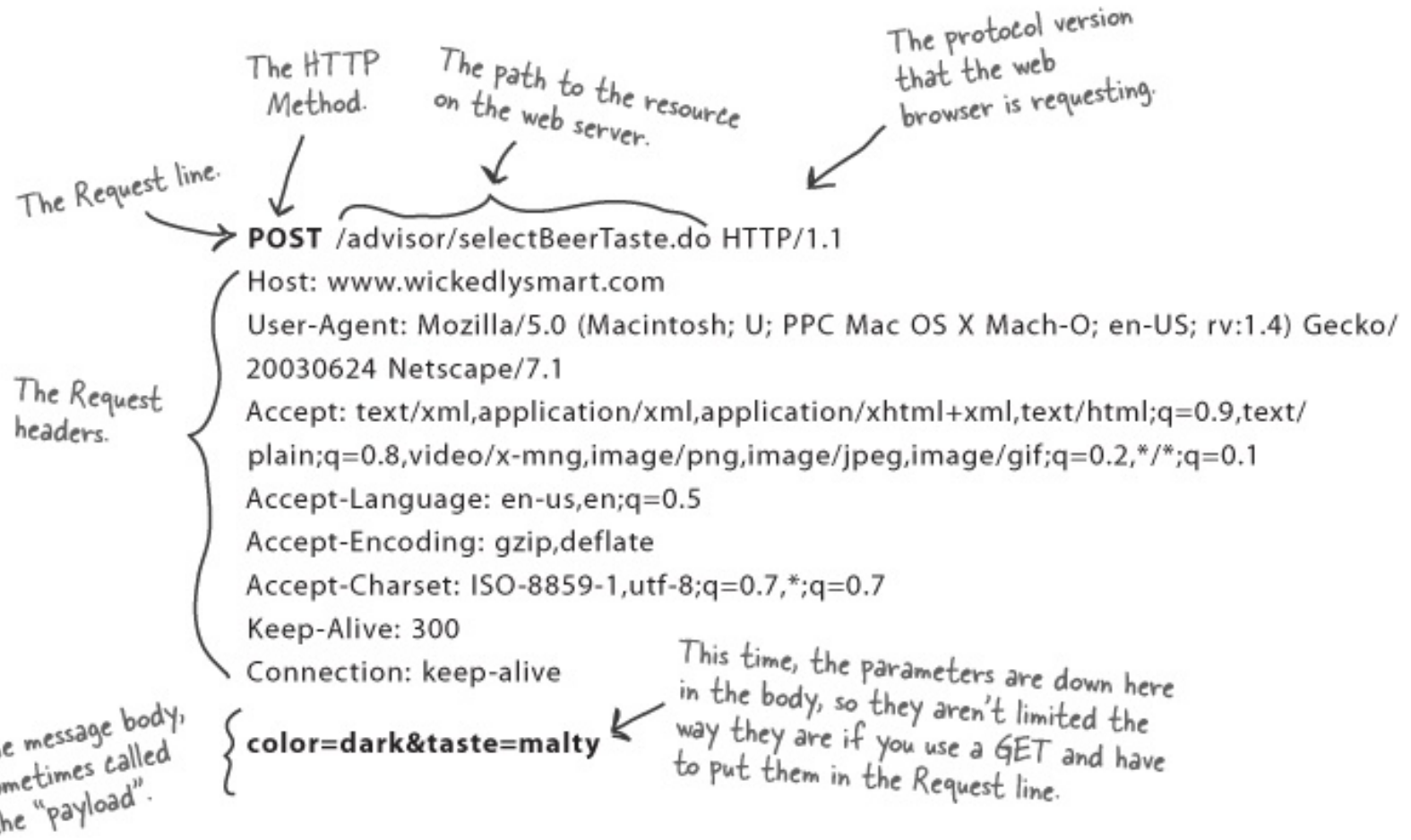
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Fri, 27 Nov 2015 07:24:43 GMT
Content-Length: 12909
```

```
<head>
<base href="http://www.kza.nl/" />
<meta name="description" content="U wilt testen of de te ontwikkelen software aan de wensen van de klant. U heeft de mogelijkheid om te testen op de volgende punten:
<meta name="section" content="Testen, Testuitvoering" />
<title>Testuitvoering - KZA</title>
<meta property="og:site_name" content="Testuitvoering" />
<link rel="alternate" title="Testuitvoering" href="http://www.kza.nl/images/kza-logo.jpg" />
<!--BeginNoIndex-->
```

Select the first request

Select 'request' to see the request

Select 'response' to see the response



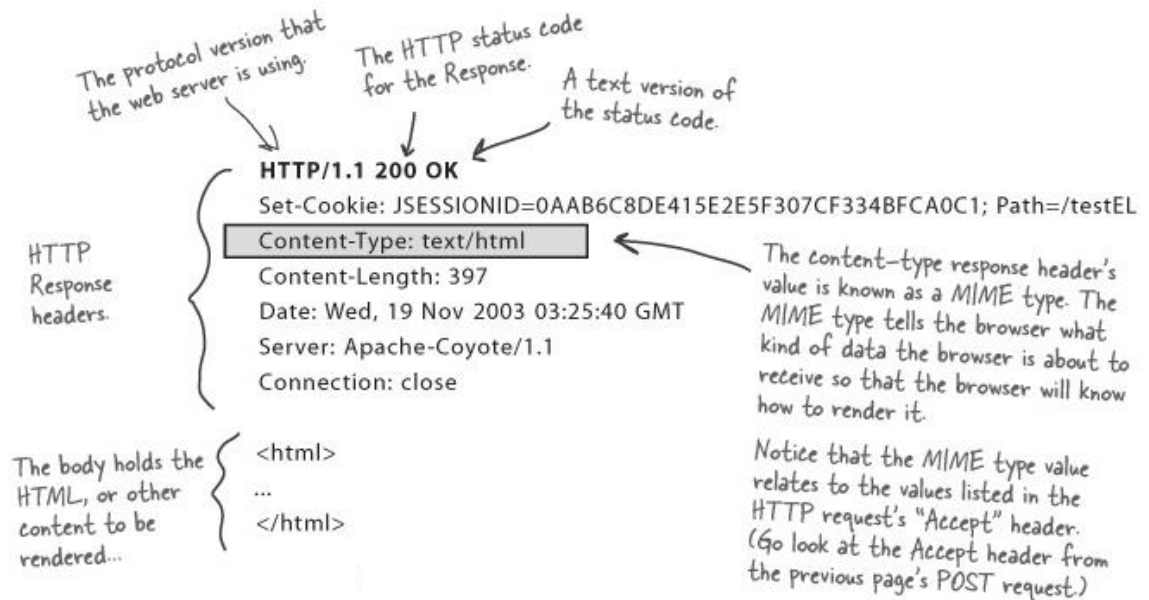


Status, header and data
HTTP Response headers:

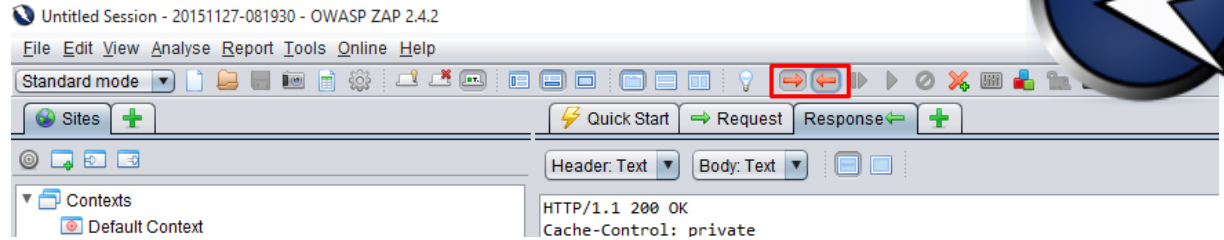
Content-type
Expires
Last-Modified
WWW-Authenticate
Set-Cookie
Etc.

Content types:
text/html
Image/gif
application/word
etc.

Encoding
MIME, readable text, byte stream
etc.



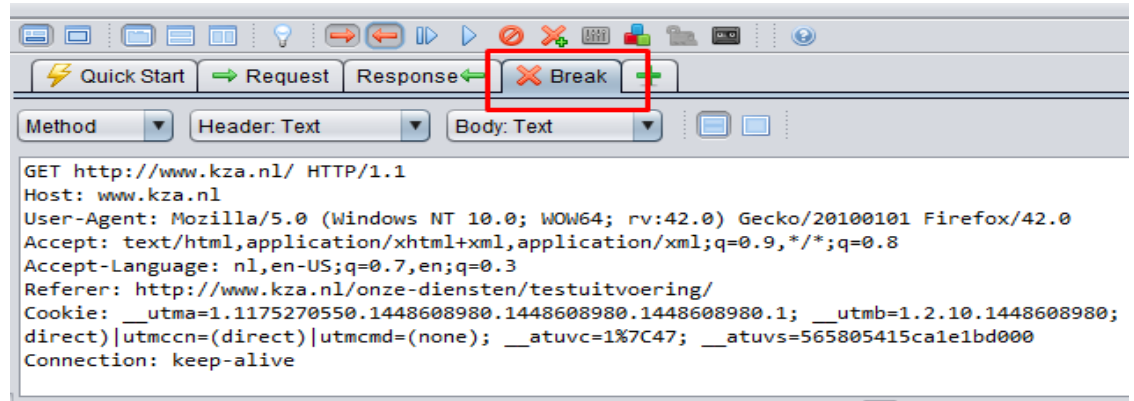
Intercept a request



Enable intercept in ZAP

Click on 'home' in browser

Check 'Break' tab in ZAP



Click ' ' to send request



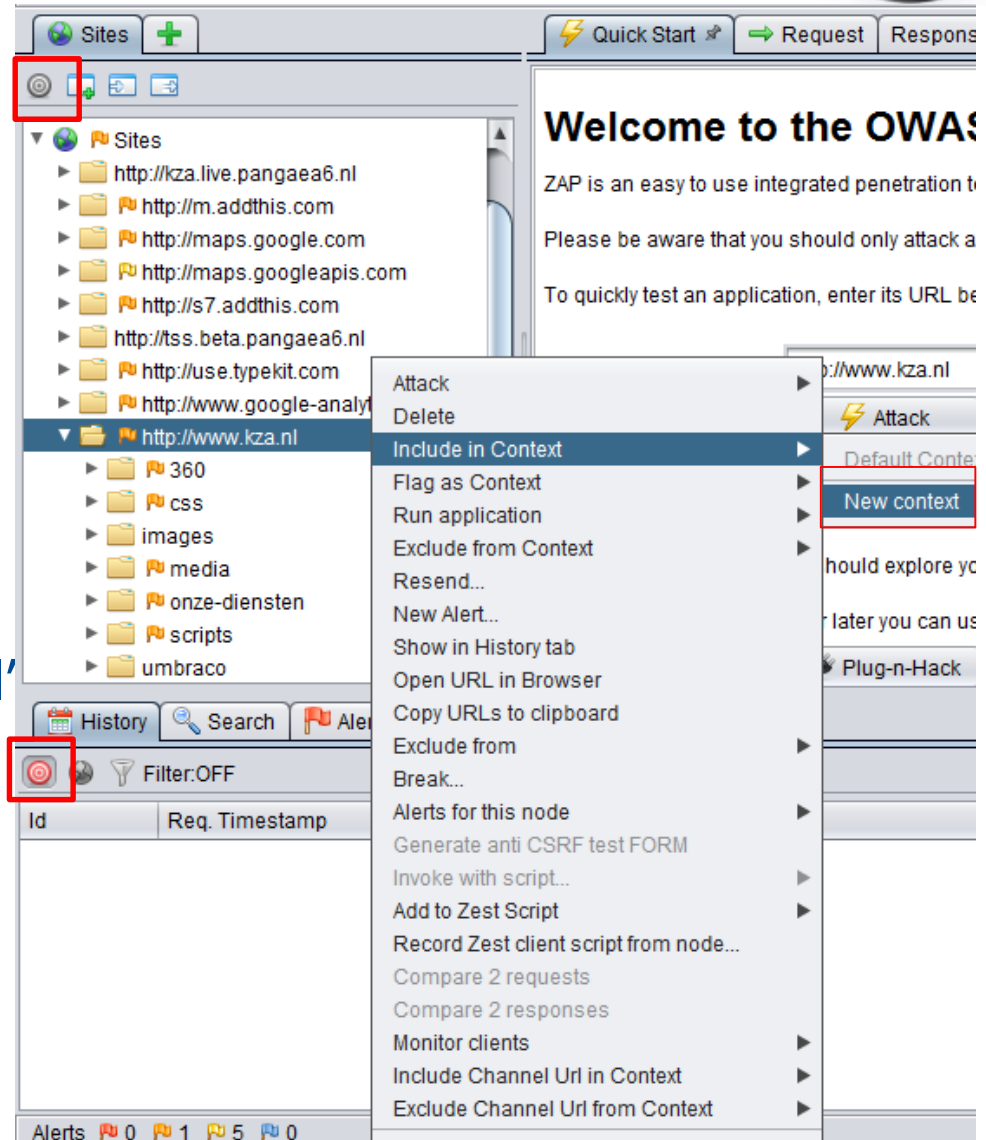
Useful to

- 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 given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

JURL to attack:

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:

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



FOUT: Het ingevulde wachtwoord voor het e-mailadres is onjuist.

[Wachtwoord vergeet](#)

Aanmelden met uw organisatieaccount

Gebruikersnaam

De gebruikers-id of het wachtwoord is onjuist. Voer de gebruikers-id en het wachtwoord opnieuw in.

Wachtwoord

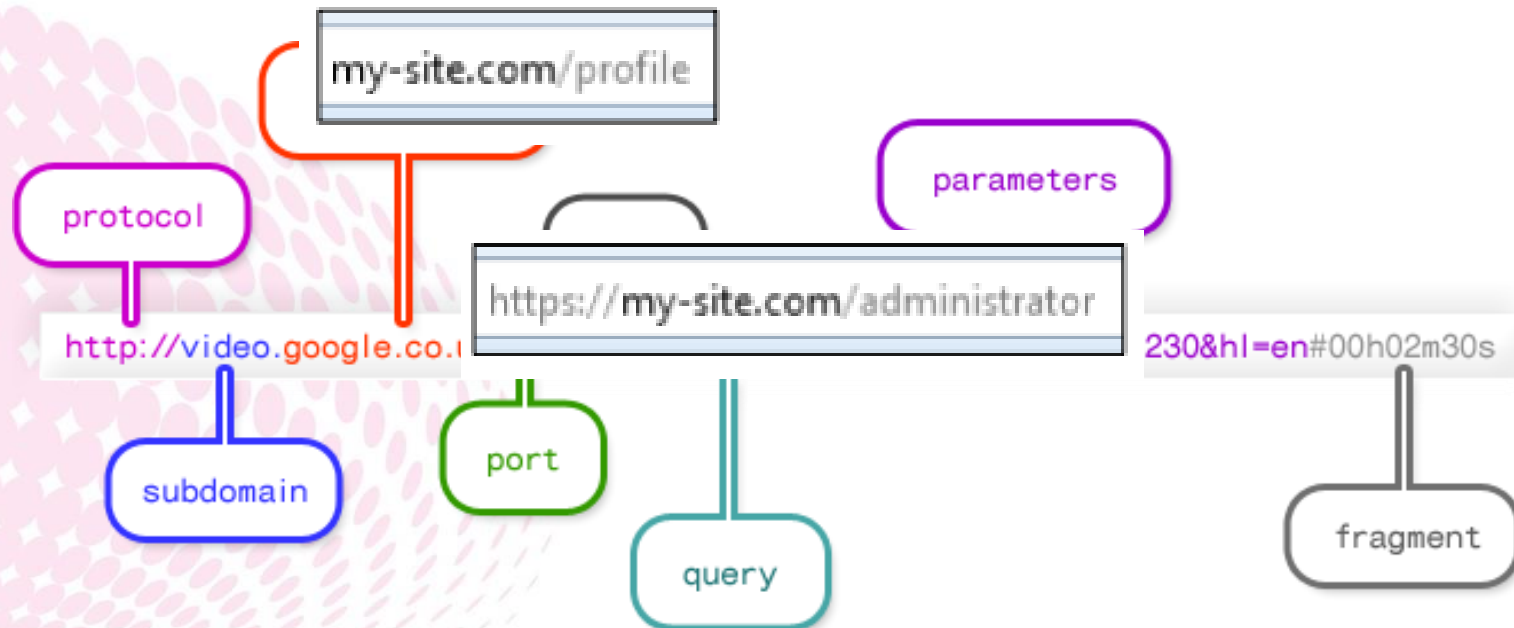
Gegevens onthouden

Aanmelden

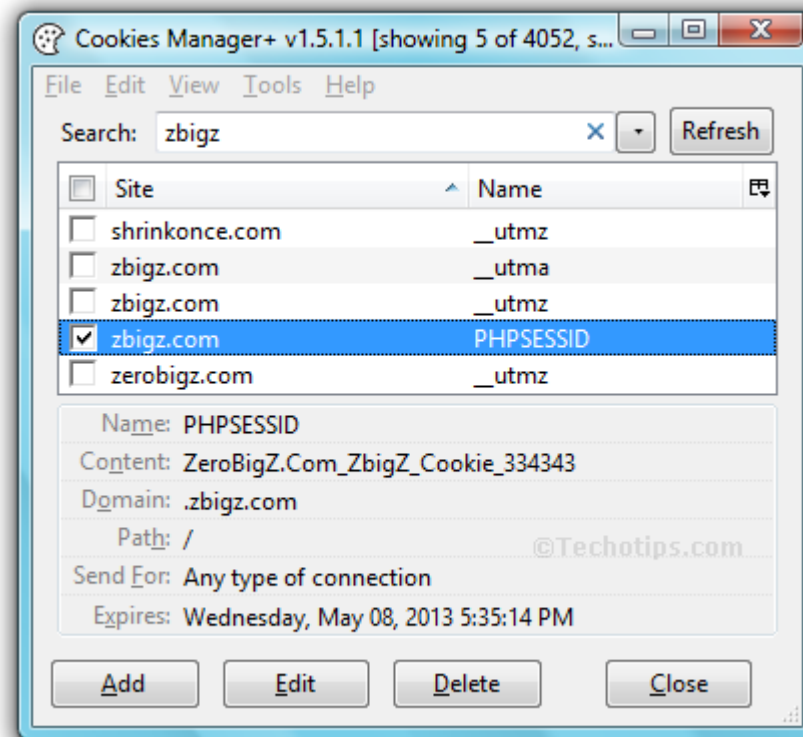
Authenticatie : Ben je wie je zegt dat je bent?

Authorisatie : Heb je toegang/rechten om te zien wat je ziet?

URL Tampering



- Cookiemanager+

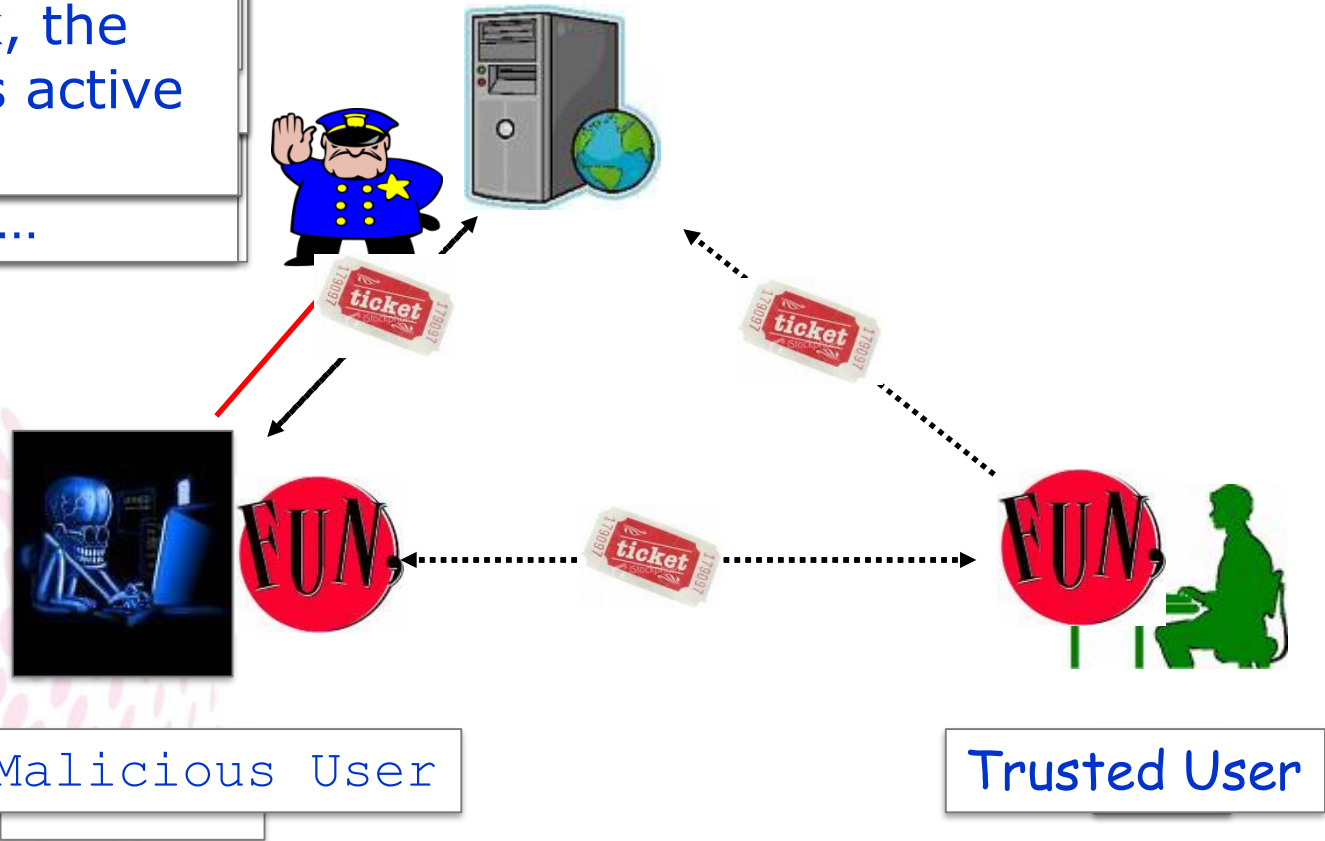


Session management basics



When Ted opens the interesting link, the script becomes active ...
authenticated ...

Vulnerable application



Malicious User

Trusted User

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

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 or 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

- 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

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

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)

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

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

