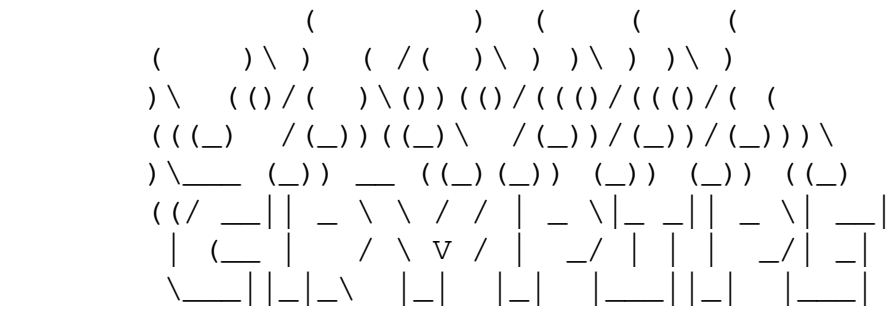

Report for subdomains of it.tuwien.ac.at

Nmap report

This is the result of the Nmap activity. **Here you can find only the relevant information**

Nmap scan for 128.131.12.70 : ['chat-q.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 85.06 seconds
```

Nmap scan for 128.130.34.222 : ['o365backup-test.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.73 seconds
```

Nmap scan for 217.175.195.167 : ['git.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp  open  http     Golang net/http server (Go-IPFS json-rpc or Infl
443/tcp open  ssl/http Golang net/http server (Go-IPFS json-rpc or Infl
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 17.51 seconds
```

Nmap scan for 128.131.13.26 : ['jira.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 44.14 seconds
```

Nmap scan for 128.130.35.218 : ['invenio-prod.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx 1.25.4
443/tcp open  ssl/http nginx 1.25.4

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds
```

Nmap scan for 128.130.36.26 : ['raws.it.tuwien.ac.at']

```
PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
1022/tcp open   ssh     OpenSSH 7.4 (protocol 2.0)

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```

Nmap scan for 128.131.12.125 : ['passt-test.it.tuwien.ac.at']

```
PORT    STATE  SERVICE VERSION
80/tcp  open   http    nginx 1.20.1
443/tcp closed https

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 24.35 seconds
```

Nmap scan for 128.131.12.126 : ['shiny-analytics.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx 1.26.0
443/tcp open  ssl/http nginx 1.26.0

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.72 seconds
```

Nmap scan for 128.131.20.173 : ['damap.it.tuwien.ac.at', 'test-damap.it.tuwien.ac.at']

```
PORT     STATE SERVICE            VERSION
80/tcp   open  http               nginx 1.25.4
443/tcp  open  ssl/http           nginx 1.25.4
8087/tcp open  ssl/simplifymedia?

1 service unrecognized despite returning data. If you know the service/
SF-Port8087-TCP:V=7.80%T=SSL%I=7%D=5/11%Time=663F801C%P=x86_64-pc-linux
SF:u%r(GenericLines,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-L
SF:th:\x200\r\nConnection:\x20close\r\n\r\n")%r(GetRequest,4FD,"HTTP/1\
SF:x20200\x20OK\r\nConnection:\x20close\r\nLast-Modified:\x20Tue,\x2025
SF:0Jan\x202022\x2009:09:53\x20GMT\r\nContent-Length:\x201087\r\nConten
SF:ype:\x20text/html\r\nAccept-Ranges:\x20bytes\r\nDate:\x20Sat,\x2011\
SF:May\x202024\x2014:26:36\x20GMT\r\n\r\n<!--\n\x20\x20~\x20Copyright\x
SF:016\x20Red\x20Hat,\x20Inc\.\x20and/or\x20its\x20affiliates\n\x20\x20
SF:20and\x20other\x20contributors\x20as\x20indicated\x20by\x20the\x20@a
SF:or\x20tags\.\n\x20\x20~\n\x20\x20~\x20Licensed\x20under\x20the\x20Ap
SF:e\x20License,\x20Version\x202\.0\x20\(the\x20\"License\"\);\n\x20\x2
SF:x20you\x20may\x20not\x20use\x20this\x20file\x20except\x20in\x20compl
SF:ce\x20with\x20the\x20License\.\n\x20\x20~\x20You\x20may\x20obtain\x2
SF:x20copy\x20of\x20the\x20License\x20at\n\x20\x20~\n\x20\x20~\x20http:
SF:ww\.apache\.org/licenses/LICENSE-2\.0\n\x20\x20~\n\x20\x20~\x20Unles
SF:20required\x20by\x20applicable\x20law\x20or\x20agreed\x20to\x20in\x2
```

```
SF:iting,\x20software\n\x20\x20~\x20distributed\x20under\x20the\x20Lice
SF:\x20is\x20distributed\x20on\x20an\x20\"AS\x20IS\"\x20BASIS,\n\x20\x2
SF:x20WITHOUT\x20WARRANTIES\x20OR\x20CONDITIONS\x20OF\x20ANY\x20KIND,\x
SF:ither\x20express\x20or\x20implied\.\n\x20\x20~\x20See\x20the\x20Lice
SF:\x20for\x20the\x20specific\x20language\x20governing\x20permissions\x
SF:nd\n\x20\x20~\x20limitations\x20under\x20the\x20License\.\n\x20\x20-
SF:n<!DOCTYPE\x20html\x20PU")%r(HTTPOptions,F3,"HTTP/1\.1\x20405\x20Met
SF:\x20Not\x20Allowed\r\nAllow:\x20GET,\x20HEAD,\x20POST\r\nConnection:
SF:0close\r\nContent-Length:\x2083\r\nContent-Type:\x20text/html\r\nDat
SF:x20Sat,\x2011\x20May\x202024\x2014:26:36\x20GMT\r\n\r\n<html><head><
SF:le>Error</title></head><body>405\x20-\x20Method\x20Not\x20Allowed</b
SF:></html>")%r(RTSPRequest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nC
SF:ent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1
SF:\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20
SF:se\r\n\r\n");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 91.87 seconds
```

Nmap scan for 128.130.33.25 : ['infoscreen.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.38
443/tcp open  ssl/http Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.22 seconds
```

Nmap scan for 128.131.14.18 : ['edm-portal.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx 1.20.1
443/tcp open  ssl/http nginx 1.20.1

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds
```

Nmap scan for 128.130.33.103 : ['svn.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.38
443/tcp open  ssl/http Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.81 seconds
```

Nmap scan for 109.70.102.196 : ['gitlab.it.tuwien.ac.at', 'minio.it.tuwien.ac.at', 'registry.it.tuwien.ac.at']

```
PORT    STATE  SERVICE  VERSION
80/tcp  closed http
443/tcp open   ssl/http Apache httpd
```

```
Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 17.21 seconds
```

Nmap scan for 128.131.34.109 : ['wallbuilder.it.tuwien.ac.at']

```
PORT     STATE SERVICE   VERSION
1720/tcp open  h323q931?

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 149.30 seconds
```

Nmap scan for 128.130.33.28 : ['plesk-test.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 122.39 seconds
```

Nmap scan for 128.130.33.70 : ['support-q.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 44.13 seconds
```

Nmap scan for 128.130.34.195 : ['selma.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.59
443/tcp open  ssl/http Apache httpd 2.4.59 ((Debian))

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.76 seconds
```

Nmap scan for 128.130.35.222 : ['survey.it.tuwien.ac.at']

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.37 ((Red Hat Enterprise Linux)
443/tcp open  ssl/http Apache httpd 2.4.37 ((Red Hat Enterprise Linux)

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.79 seconds
```

Nmap scan for 128.130.34.142 : ['oase.it.tuwien.ac.at']

```
PORT    STATE SERVICE        VERSION
443/tcp open  ssl/http-proxy Pound http reverse proxy
```

```
Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
```

Nmap scan for 128.131.8.16 : ['idp.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy HAProxy http proxy 1.3.1 or later
443/tcp open  ssl/http   Apache httpd
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 20.85 seconds
```

Nmap scan for 128.130.33.111 : ['service.it.tuwien.ac.at']

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 85.04 seconds
```

Nmap scan for 128.131.12.69 : ['chat-dev.it.tuwien.ac.at']

```
PORT    STATE SERVICE        VERSION
80/tcp  open  http-proxy     HAProxy http proxy 1.3.1 or later
443/tcp open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.00 seconds
```

Nmap scan for 128.130.35.207 : ['ocisdev.it.tuwien.ac.at', 'owncloud.it.tuwien.ac.at', 'tudocs.it.tuwien.ac.at', 'tudocsdev.it.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https

2 services unrecognized despite returning data. If you know the service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==========
SF-Port80-TCP:V=7.80%I=7%D=5/11%Time=663F7A1E%P=x86_64-pc-linux-gnu%r(G
SF:equest,5D,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\ncontent-lengt
SF:x200\r\nlocation:\x20https:///\r\nconnection:\x20close\r\n\r\n")%r(H
SF:Options,5D,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\ncontent-leng
SF:\x200\r\nlocation:\x20https:///\r\nconnection:\x20close\r\n\r\n")%r(
SF:PRequest,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x
SF:0\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-T
SF::\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYo
SF:x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")
```

```
SF:X11Probe,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x
SF:0\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-T
SF::\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYo
SF:x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")
SF:RPCCheck,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x
SF:0\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-T
SF::\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYo
SF:x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")
SF:DNSVersionBindReqTCP,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nConte
SF:length:\x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\
SF:Content-Type:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20requ
SF:</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20request\.\n</body
SF:html>\n")%r(DNSStatusRequestTCP,CF,"HTTP/1\.1\x20400\x20Bad\x20reque
SF:r\nContent-length:\x2090\r\nCache-Control:\x20no-cache\r\nConnection
SF:20close\r\nContent-Type:\x20text/html\r\n\r\n<html><body><h1>400\x20
SF:\x20request</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20reques
SF:\n</body></html>\n")%r(Help,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r
SF:ontent-length:\x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x2
SF:ose\r\nContent-Type:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\
SF:request</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20request\.\
SF:body></html>\n")%r(SSLSessionReq,CF,"HTTP/1\.1\x20400\x20Bad\x20requ
SF:\r\nContent-length:\x2090\r\nCache-Control:\x20no-cache\r\nConnectio
SF:x20close\r\nContent-Type:\x20text/html\r\n\r\n<html><body><h1>400\x2
SF:d\x20request</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20reque
SF:.\n</body></html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)============
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/11%Time=663F7A24%P=x86_64-pc-linux-
SF:%r(GetRequest,49C,"HTTP/1\.1\x20302\x20Found\r\ndate:\x20Sat,\x2011\
SF:May\x202024\x2014:01:08\x20GMT\r\nexpires:\x20Thu,\x2019\x20Nov\x201
SF:\x2008:52:00\x20GMT\r\ncache-control:\x20no-store,\x20no-cache,\x20m
SF:-revalidate\r\npragma:\x20no-cache\r\ncontent-security-policy:\x20de
SF:lt-src\x20'self';\x20script-src\x20'self'\x20'unsafe-eval';\x20style
SF:c\x20'self'\x20'unsafe-inline';\x20frame-src\x20\*;\x20img-src\x20\*
SF:0data:\x20blob:;\x20font-src\x20'self'\x20data:;\x20media-src\x20\*;
SF:0connect-src\x20\*\r\nset-cookie:\x20tu_oc=vp9v0ro35fb5bfojpag2gnus7
SF:x20path=/;\x20secure;\x20HttpOnly;\x20Secure\r\nset-cookie:\x20oc_se
SF:onPassphrase=IIYmj71MGKPeFpuuINS3TV5JejY63R3%2Bo0zamfK%2FE5elp1%2BrL
SF:5q6tEPKDEmlPiDk7idP2fkFrtV8cFev6o3IefzutdSS%2FkurkM7q40h7p8H27g6RyOo
SF:NRdFF9U;\x20expires=Sat,\x2011-May-2024\x2014:21:08\x20GMT;\x20Max-A
SF:1200;\x20path=/;\x20secure;\x20HttpOnly;\x20SameSite=Strict;\x20Secu
SF:r\nx-content-type-options:\x20nosniff\r\nx-xss-protection:\x200\r\nx
SF:bots-tag:\x20none\r\nx-frame-options:\x20SAMEORIGIN\r\nx-download-op
SF:ns:\x20noopen\r\nx-permitted-cross-domain-policies:\x20none\r\nlocat
SF:)%r(HTTPOptions,49C,"HTTP/1\.1\x20302\x20Found\r\ndate:\x20Sat,\x201
SF:20May\x202024\x2014:01:08\x20GMT\r\nexpires:\x20Thu,\x2019\x20Nov\x2
SF:81\x2008:52:00\x20GMT\r\ncache-control:\x20no-store,\x20no-cache,\x2
SF:st-revalidate\r\npragma:\x20no-cache\r\ncontent-security-policy:\x20
SF:ault-src\x20'self';\x20script-src\x20'self'\x20'unsafe-eval';\x20sty
SF:src\x20'self'\x20'unsafe-inline';\x20frame-src\x20\*;\x20img-src\x20
SF:x20data:\x20blob:;\x20font-src\x20'self'\x20data:;\x20media-src\x20\
SF:x20connect-src\x20\*\r\nset-cookie:\x20tu_oc=i19s3u1rdrak0oi6ne4lkc2
SF:;\x20path=/;\x20secure;\x20HttpOnly;\x20Secure\r\nset-cookie:\x20oc_
SF:sionPassphrase=mrWvvE%2FVOdLcNrPFcWzyvcbFB3vIAMihzcMRRLP9tA5ywIdJ%2B
```

```
SF:fE7yxGJ4%2BIxoFgoorJoZkZtfY9uE3MAnFSqJ%2BzF6Jl2PqdrwisVoi2fdQf6z9dM4
SF:QlHIbNNaG;\x20expires=Sat,\x2011-May-2024\x2014:21:08\x20GMT;\x20Max
SF:e=1200;\x20path=/;\x20secure;\x20HttpOnly;\x20SameSite=Strict;\x20Se
SF:e\r\nx-content-type-options:\x20nosniff\r\nx-xss-protection:\x200\r\
SF:robots-tag:\x20none\r\nx-frame-options:\x20SAMEORIGIN\r\nx-download-
SF:ions:\x20noopen\r\nx-permitted-cross-domain-policies:\x20none\r\nloc
SF:o");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.04 seconds
```

Joomscan report

This is the result of the Joomscan activity. **Here you can find only the relevant information Remeber: when the text is red, something interesting is found**

Joomscan for webstats-dev.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Full Path Disclosure (FPD)

[++] Full Path Disclosure (FPD) in 'https://webstats-dev.it.tuwien.ac.at/index.php?option=com_jotloader&section[]=' :

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://webstats-dev.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for infoscreen.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://infoscreen.it.tuwien.ac.at/manage/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for ocisdev.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://ocisdev.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://ocisdev.it.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for o365backup-test.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://o365backup-test.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for damap.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+ +] Admin page : https://damap.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for oase.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+ +] Admin page : https://oase.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for www.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[+ +] robots.txt is found

- path : https://www.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://www.it.tuwien.ac.at/fileadmin/*temp*/
- https://www.it.tuwien.ac.at/typo3/
- https://www.it.tuwien.ac.at/typo3conf/
- https://www.it.tuwien.ac.at/typo3/sysext/frontend/Resources/Public/*
- https://www.it.tuwien.ac.at/404/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for tube1.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+ +] Admin page : https://tube1.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for chat-dev.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Full Path Disclosure (FPD)

[++] Full Path Disclosure (FPD) in 'https://chat-dev.it.tuwien.ac.at/mambo/mambots/editors/mostlyce/jscripts/tiny_mce/plugins/spellchecker/classes/PSpellShell.php' :

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://chat-dev.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for webstats.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Full Path Disclosure (FPD)

[++] Full Path Disclosure (FPD) in 'https://webstats.it.tuwien.ac.at/index.php?option=com_jotloader&section[]=' :

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://webstats.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for git.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://git.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://git.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://git.tuwien.ac.at/
- https://git.tuwien.ac.at/autocomplete/users
- https://git.tuwien.ac.at/autocomplete/projects
- https://git.tuwien.ac.at/search
- https://git.tuwien.ac.at/admin
- https://git.tuwien.ac.at/profile
- https://git.tuwien.ac.at/dashboard
- https://git.tuwien.ac.at/users
- https://git.tuwien.ac.at/api/v*
- https://git.tuwien.ac.at/help
- https://git.tuwien.ac.at/s/
- https://git.tuwien.ac.at/-/profile
- https://git.tuwien.ac.at/-/ide/
- https://git.tuwien.ac.at/-/experiment

- https://git.tuwien.ac.at/users/sign_in
- https://git.tuwien.ac.at/users/sign_up
- https://git.tuwien.ac.at/users/*/snippets
- https://git.tuwien.ac.at/*/new
- https://git.tuwien.ac.at/*/edit
- https://git.tuwien.ac.at/*/raw
- https://git.tuwien.ac.at/*/realtime_changes
- https://git.tuwien.ac.at/groups/*/analytics
- https://git.tuwien.ac.at/groups/*/contribution_analytics
- https://git.tuwien.ac.at/groups/*/group_members
- https://git.tuwien.ac.at/groups/*/-/saml/sso
- https://git.tuwien.ac.at//.git$
- https://git.tuwien.ac.at/*/archive/
- https://git.tuwien.ac.at//*repository/archive*
- https://git.tuwien.ac.at/*/activity
- https://git.tuwien.ac.at/*/blame
- https://git.tuwien.ac.at/*/commits
- https://git.tuwien.ac.at/*/commit
- https://git.tuwien.ac.at//*commit*/.patch
- https://git.tuwien.ac.at//*commit*/.diff
- https://git.tuwien.ac.at/*/compare
- https://git.tuwien.ac.at/*/network
- https://git.tuwien.ac.at/*/graphs
- https://git.tuwien.ac.at//*merge requests*/.patch
- https://git.tuwien.ac.at//*merge requests*/.diff
- https://git.tuwien.ac.at//*merge requests*//diffs
- https://git.tuwien.ac.at/*/deploy_keys
- https://git.tuwien.ac.at/*/hooks
- https://git.tuwien.ac.at/*/services

- https://git.tuwien.ac.at/*/protected branches
- https://git.tuwien.ac.at/*/uploads/
- https://git.tuwien.ac.at/*/project members
- https://git.tuwien.ac.at/*/settings
- https://git.tuwien.ac.at/*/-/import
- https://git.tuwien.ac.at/*/-/environments
- https://git.tuwien.ac.at/*/-/jobs
- https://git.tuwien.ac.at/*/-/requirements management
- https://git.tuwien.ac.at/*/-/pipelines
- https://git.tuwien.ac.at/*/-/pipeline schedules
- https://git.tuwien.ac.at/*/-/dependencies
- https://git.tuwien.ac.at/*/-/licenses
- https://git.tuwien.ac.at/*/-/metrics
- https://git.tuwien.ac.at/*/-/incidents
- https://git.tuwien.ac.at/*/-/value stream analytics
- https://git.tuwien.ac.at/*/-/analytics
- https://git.tuwien.ac.at/*/insights

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for survey.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://survey.it.tuwien.ac.at/admin/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for owncloud.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[+ +] robots.txt is found

- path : https://owncloud.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://owncloud.it.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for selma.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[+ +] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[+ +] robots.txt is found

- path : https://selma.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt

- https://selma.it.tuwien.ac.at/cgi-bin

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for chat-q.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Full Path Disclosure (FPD)

[++] Full Path Disclosure (FPD) in 'https://chat-q.it.tuwien.ac.at/mambo/mambots/editors/mostlyce/jscripts/tiny_mce/plugins/spellchecker/classes/PSpellShell.php' :

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://chat-q.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for idp.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://idp.it.tuwien.ac.at/robots.txt

- Interesting path found from robots.txt
- https://idp.it.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for jira.it.tuwien.ac.at_jscan

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://jira.it.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://jira.it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://jira.it.tuwien.ac.at/sr/
- https://jira.it.tuwien.ac.at/si/
- https://jira.it.tuwien.ac.at/charts
- https://jira.it.tuwien.ac.at/secure/ConfigureReport.jspa
- https://jira.it.tuwien.ac.at/secure/ConfigureReport!default.jspa
- https://jira.it.tuwien.ac.at/secure/attachmentzip/
- https://jira.it.tuwien.ac.at/secure/AboutPage.jspa
- https://jira.it.tuwien.ac.at/secure/JiraCreditsPage!default.jspa
- https://jira.it.tuwien.ac.at/secure/credits/AroundTheWorld!default.jspa
- https://jira.it.tuwien.ac.at/secure/ViewKeyboardShortcuts!default.jspa
- https://jira.it.tuwien.ac.at/secure/ViewProfile.jspa
- https://jira.it.tuwien.ac.at/login.jsp

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Nikto report

This is the result of the Nikto activity. **Here you can find only the relevant information**
Remeber: some discoveries could be false positive, since nikto checks the response code for some vulnerabilities -> example XSS

Nikto scan for git.tuwien.ac.at_nikto

- Target Host: git.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff

Nikto scan for autodiscover.it.tuwien.ac.at_nikto

- Target Host: autodiscover.it.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0x35 0x57a9e0870fc0c
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Hostname 'autodiscover.it.tuwien.ac.at' does not match certificate's CN 'autoconfig.zid.tuwien.ac.at'
- OPTIONS /: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
- -3233: GET /icons/README: /icons/README: Apache default file found.

Nikto scan for chat-q.it.tuwien.ac.at_nikto

- Target Host: chat-q.it.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000
- GET /: Uncommon header 'x-instance-id' found, with contents: g4ohbvGJgLdhezGXE
- GET /: Uncommon header 'x-xss-protection' found, with contents: 1
- GET /: Uncommon header 'content-security-policy' found, with contents: default-src 'self' ; connect-src *; font-src 'self' data:; frame-src *; img-src * data:; media-src * data:; script-src 'self' 'unsafe-eval' ; style-src 'self' 'unsafe-inline'
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
- GET /favicon.ico: Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x5e6bfbbaa9d886afe43fe8b15b3e123c8239d544
- GET /kboard/: /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
- GET /sshome/: /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
- GET /tiki/tiki-install.php: /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
- -396: GET /_vti_bin/shtml.exe: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not

attempted.
- GET /forums//admin/config.php: /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
- GET /forums//administrator/config.php: /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.
- -2411: GET /hola/admin/cms/htmltags.php?datei=./sec/data.php: /hola/admin/cms/htmltags.php?datei=./sec/data.php: hola-cms-1.2.9-10 may reveal the administrator ID and password.
- -59619: GET /inc/config.php: /inc/config.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
- -8204: GET /gb/index.php?login=true: /gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'.
- GET /getaccess: /getaccess: This may be an indication that the server is running getAccess for SSO
- GET /vgn/performance/TMT/Report/XML: /vgn/performance/TMT/Report/XML: Vignette CMS admin/maintenance script available.
- GET /vgn/ppstats: /vgn/ppstats: Vignette CMS admin/maintenance script available.
- GET /vgn/record/previewer: /vgn/record/previewer: Vignette CMS admin/maintenance script available.
- GET /vgn/vr/Saving: /vgn/vr/Saving: Vignette CMS admin/maintenance script available.
- GET /scripts/iisadmin/bdir.htr: /scripts/iisadmin/bdir.htr: This default script shows host info, may allow file browsing and buffer a overrun in the Chunked Encoding data transfer mechanism, request /scripts/iisadmin/bdir.htr??c:<dirs> . MS02-028. CA-2002-09.
- GET /scripts/iisadmin/ism.dll: /scripts/iisadmin/ism.dll: Allows you to mount a brute force attack on passwords
- GET /scripts/tools/ctss.idc: /scripts/tools/ctss.idc: This CGI allows remote users to view and modify SQL DB contents, server paths, docroot and more.
- -17654: GET /SiteServer/Admin/commerce/foundation/driver.asp: /SiteServer/Admin/commerce/foundation/driver.asp: Displays a list of installed ODBC drivers.
- GET /basilix/mbox-list.php3: /basilix/mbox-list.php3: BasiliX webmail application prior to 1.1.1 contains a XSS issue in 'message list' function/page
- GET /clusterframe.jsp: /clusterframe.jsp: Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS attacks.
- GET /bb-dnbd/faxsurvey: /bb-dnbd/faxsurvey: This may allow arbitrary command execution.
- -6591: GET /scripts/Carello/Carello.dll: /scripts/Carello/Carello.dll: Carello 1.3 may allow commands to be executed on the server by replacing hidden form elements. This could not be tested by Nikto.
- GET /scripts/tools/dsnform: /scripts/tools/dsnform: Allows creation of ODBC Data Source
- -17657: GET /SiteServer/Admin/knowledge/dsmgr/users/UserManager.asp: /SiteServer/Admin/knowledge/dsmgr/users/UserManager.asp: Used to create, modify, and potentially delete LDAP users and groups.
- GET /readme.eml: /readme.eml: Remote server may be infected with the Nimda virus.
- GET /scripts/httpodbc.dll: /scripts/httpodbc.dll: Possible IIS backdoor found.
- GET /scripts/proxy/w3proxy.dll: /scripts/proxy/w3proxy.dll: MSProxy v1.0 installed
- GET /SiteServer/admin/: /SiteServer/admin/: Site Server components admin. Default account may be 'LDAP_Anonymous', pass is 'LdapPassword_1'. see http://www.wiretrip.net/rfp/p/doc.asp/i1/d69.htm
- GET /pccsmysqladm/incs/dbconnect.inc: /pccsmysqladm/incs/dbconnect.inc: This file should not be accessible, as it contains database connectivity information. Upgrade to

version 1.2.5 or higher.
- GET /iisadmin/: /iisadmin/: Access to /iisadmin should be restricted to localhost or allowed hosts only.
- GET /PDG_Cart/oder.log: /PDG_Cart/oder.log: Shopping cart software log
- GET /ows/restricted%2eshow: /ows/restricted%2eshow: OWS may allow restricted files to be viewed by replacing a character with its encoded equivalent.
- GET /WEB-INF./web.xml: /WEB-INF./web.xml: Multiple implementations of j2ee servlet containers allow files to be retrieved from WEB-INF by appending a '.' to the directory name. Products include Sybase EA Service, Oracle Containers, Orion, JRun, HPAS, Pramati and others. See http://www.westpoint.l
- GET /view_source.jsp: /view_source.jsp: Resin 2.1.2 view_source.jsp allows any file on the system to be viewed by using ..\ directory traversal. This script may be vulnerable.
- -6181: GET /officescan/cgi/cgiChkMasterPwd.exe: /officescan/cgi/cgiChkMasterPwd.exe: Trend Micro Officescan allows you to skip the login page and access some CGI programs directly.
- GET /pbserver/pbserver.dll: /pbserver/pbserver.dll: This may contain a buffer overflow. http://www.microsoft.com/technet/security/bulletin/ms00-094.asp
- GET /administrator/gallery/uploadimage.php: /administrator/gallery/uploadimage.php: Mambo PHP Portal/Server 4.0.12 BETA and below may allow upload of any file type simply putting '.jpg' before the real file extension.
- GET /upload.asp: /upload.asp: An ASP page that allows attackers to upload files to server
- GET /uploadx.asp: /uploadx.asp: An ASP page that allows attackers to upload files to server
- GET /vgn/ac/delete: /vgn/ac/delete: Vignette CMS admin/maintenance script available.
- GET /vgn/ac/esave: /vgn/ac/esave: Vignette CMS admin/maintenance script available.
- GET /vgn/asp/previewer: /vgn/asp/previewer: Vignette CMS admin/maintenance script available.
- GET /vgn/asp/style: /vgn/asp/style: Vignette CMS admin/maintenance script available.
- GET /vgn/jsp/controller: /vgn/jsp/controller: Vignette CMS admin/maintenance script available.
- GET /vgn/jsp/jspstatus56: /vgn/jsp/jspstatus56: Vignette CMS admin/maintenance script available.
- GET /vgn/jsp/previewer: /vgn/jsp/previewer: Vignette CMS admin/maintenance script available.
- GET /vgn/legacy/edit: /vgn/legacy/edit: Vignette CMS admin/maintenance script available.
- GET /WEB-INF/web.xml: /WEB-INF/web.xml: JRUN default file found.
- -35707: GET /forum/admin/wwforum.mdb: /forum/admin/wwforum.mdb: Web Wiz Forums password database found.
- -52975: GET /guestbook/admin/o12guest.mdb: /guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password.
- -15971: GET /MIDICART/midicart.mdb: /MIDICART/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
- -53413: GET /shopping400.mdb: /shopping400.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available.
- GET /adm/config.php: /adm/config.php: PHP Config file may contain database IDs and passwords.
- GET /contents.php?new_language=elvish&mode=select: /contents.php?

new_language=elvish&mode=select: Requesting a file with an invalid language selection from DC Portal may reveal the system path.
- -53303: GET /simplebbs/users/users.php: /simplebbs/users/users.php: Simple BBS 1.0.6 allows user information and passwords to be viewed remotely.
- GET /typo3conf/database.sql: /typo3conf/database.sql: Typo3 SQL file found.
- -53386: GET /vchat/msg.txt: /vchat/msg.txt: VChat allows user information to be retrieved.
- GET /webcart-lite/orders/import.txt: /webcart-lite/orders/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web.
- GET /webcart/carts/: /webcart/carts/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
- GET /webcart/config/clients.txt: /webcart/config/clients.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web.
- GET /WS_FTP.ini: /WS_FTP.ini: Can contain saved passwords for FTP sites
- -17661: GET /SiteServer/Admin/knowledge/persmbr/VsLsLpRd.asp: /SiteServer/Admin/knowledge/persmbr/VsLsLpRd.asp: Expose various LDAP service and backend configuration parameters
- -17660: GET /SiteServer/Admin/knowledge/persmbr/VsTmPr.asp: /SiteServer/Admin/knowledge/persmbr/VsTmPr.asp: Expose various LDAP service and backend configuration parameters
- GET /nsn/fdir.bas:ShowVolume: /nsn/fdir.bas:ShowVolume: You can use ShowVolume and ShowDirectory directly on the Novell server (NW5.1) to view the filesystem without having to log in
- GET /forum/admin/database/wwForum.mdb: /forum/admin/database/wwForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein
- -6196: GET /servlet/SchedulerTransfer: /servlet/SchedulerTransfer: PeopleSoft SchedulerTransfer servlet found, which may allow remote command execution. See http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21999
- -6196: GET /servlets/SchedulerTransfer: /servlets/SchedulerTransfer: PeopleSoft SchedulerTransfer servlet found, which may allow remote command execution. See http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21999
- GET /vgn/legacy/save: /vgn/legacy/save: Vignette Legacy Tool may be unprotected. To access this resource, set a cookie called 'vgn_creds' with any value.
- GET /IDSWebApp/IDSjsp/Login.jsp: /IDSWebApp/IDSjsp/Login.jsp: Tivoli Directory Server Web Administration.
- GET /quikstore.cgi: /quikstore.cgi: A shopping cart.
- GET /smg_Smxcfg30.exe?vcc=3560121183d3: /smg_Smxcfg30.exe?vcc=3560121183d3: This may be a Trend Micro Officescan 'backdoor'.
- GET /nsn/..%5Cutil/chkvol.bas: /nsn/..%5Cutil/chkvol.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/copy.bas: /nsn/..%5Cutil/copy.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/del.bas: /nsn/..%5Cutil/del.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/dsbrowse.bas: /nsn/..%5Cutil/dsbrowse.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/lancard.bas: /nsn/..%5Cutil/lancard.bas: Netbase util access is

possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/rd.bas: /nsn/..%5Cutil/rd.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/ren.bas: /nsn/..%5Cutil/ren.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/send.bas: /nsn/..%5Cutil/send.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/slist.bas: /nsn/..%5Cutil/slist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cutil/userlist.bas: /nsn/..%5Cutil/userlist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cweb/fdir.bas: /nsn/..%5Cweb/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cwebdemo/env.bas: /nsn/..%5Cwebdemo/env.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /nsn/..%5Cwebdemo/fdir.bas: /nsn/..%5Cwebdemo/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
- GET /CVS/Entries: /CVS/Entries: CVS Entries file may contain directory listing information.
- -8450: GET /3rdparty/phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: /3rdparty/phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. BID-7963.
- -8450: GET /pma/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: /pma/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. BID-7963.
- GET /catalog.nsf: /catalog.nsf: A list of server databases can be retrieved, as well as a list of ACLs.
- GET /names.nsf: /names.nsf: User names and groups can be accessed remotely (possibly password hashes as well)
- -31150: GET /USER/CONFIG.AP: /USER/CONFIG.AP: MIPCD configuration information. MIPCD should not have the web interface enabled.
- GET /cgi-bin/cgi_process: /cgi-bin/cgi_process: WASD reveals a lot of system information in this script. It should be removed.
- GET /ht_root/wwwroot/-/local/httpd$map.conf: /ht_root/wwwroot/-/local/httpd$map.conf: WASD reveals the http configuration file. Upgrade to a later version and secure according to the documents on the WASD web site.
- GET /local/httpd$map.conf: /local/httpd$map.conf: WASD reveals the http configuration file. Upgrade to a later version and secure according to the documents on the WASD web site.
- GET /852566C90012664F: /852566C90012664F: This database can be read using the replica ID without authentication.

- GET /mail.box: /mail.box: The mail database can be read without authentication.
- GET /statrep.nsf: /statrep.nsf: Any reports generated by the admins can be retrieved.
- GET /Config1.htm: /Config1.htm: This may be a D-Link. Some devices have a DoS condition if an oversized POST request is sent. This DoS was not tested. See http://www.phenoelit.de/stuff/dp-300.txt for info.
- GET /...../config.sys: /...../config.sys: PWS allows files to be read by prepending multiple '.' characters. At worst, IIS, not PWS, should be used.
- GET /.....\temp\temp.class: /.....\temp\temp.class: Cisco ACS 2.6.x and 3.0.1 (build 40) allows authenticated remote users to retrieve any file from the system. Upgrade to the latest version.
- -4015: GET /jigsaw/: /jigsaw/: Jigsaw server may be installed. Versions lower than 2.2.1 are vulnerable to Cross Site Scripting (XSS) in the error page.
- GET /cfdocs/expeval/sendmail.cfm: /cfdocs/expeval/sendmail.cfm: Can be used to send email; go to the page and fill in the form
- GET /ammerum/: /ammerum/: Ammerum pre 0.6-1 had several security issues.
- GET /cbms/editclient.php: /cbms/editclient.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/
- GET /cbms/realinv.php: /cbms/realinv.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/
- GET /ext.dll?MfcIsapiCommand=LoadPage&page=admin.hts%20&a0=add&a1=root&a2=%5C: /ext.dll?MfcIsapiCommand=LoadPage&page=admin.hts%20&a0=add&a1=root&a2=%5C: This check (A) sets up the next bad blue test (B) for possible exploit. See http://www.badblue.com/down.htm
- GET /admin/system_footer.php: /admin/system_footer.php: myphpnuke version 1.8.8_final_7 reveals detailed system information.
- -59646: GET /chat/!nicks.txt: /chat/!nicks.txt: WF-Chat 1.0 Beta allows retrieval of user information.
- GET /config.php: /config.php: PHP Config file may contain database IDs and passwords.
- GET /examples/jsp/snp/anything.snp: /examples/jsp/snp/anything.snp: Tomcat servlet gives lots of host information.
- GET /cgi-bin/handler: /cgi-bin/handler: Comes with IRIX 5.3 - 6.4; allows to run arbitrary commands
- -29786: GET /admin.php?en_log_id=0&action=users: /admin.php?en_log_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
- -3233: GET /admin/admin_phpinfo.php4: /admin/admin_phpinfo.php4: Mon Album from http://www.3dsrc.com version 0.6.2d allows remote admin access. This should be protected.
- -5178: GET /dostuff.php?action=modify_user: /dostuff.php?action=modify_user: Blahz-DNS allows unauthorized users to edit user information. Upgrade to version 0.25 or higher. http://blahzdns.sourceforge.net/
- -35876: GET /agentadmin.php: /agentadmin.php: Immobilier agentadmin.php contains multiple SQL injection vulnerabilities.
- GET /sqldump.sql: /sqldump.sql: Database SQL?
- GET /servlet/SessionManager: /servlet/SessionManager: IBM WebSphere reconfigure servlet (user=servlet, password=manager). All default code should be removed from servers.
- GET /ip.txt: /ip.txt: This may be User Online from http://www.elpar.net version 2.0, which has a remotely accessible log file.

- GET /livehelp/: /livehelp/: LiveHelp may reveal system information.
- -59536: GET /logicworks.ini: /logicworks.ini: web-erp 0.1.4 and earlier allow .ini files to be read remotely.
- -3204: GET /megabook/files/20/setup.db: /megabook/files/20/setup.db: Megabook guestbook configuration available remotely.
- GET /order/order_log_v12.dat: /order/order_log_v12.dat: Web shopping system from http://www.io.com/~rga/scripts/cgiorder.html exposes order information, see http://www.mindsec.com/advisories/post2.txt
- GET /orders/order_log.dat: /orders/order_log.dat: Web shopping system from http://www.io.com/~rga/scripts/cgiorder.html exposes order information, see http://www.mindsec.com/advisories/post2.txt
- GET /pmlite.php: /pmlite.php: A Xoops CMS script was found. Version RC3 and below allows all users to view all messages (untested). See http://www.phpsecure.org/?zone=pComment&d=101 for details.
- GET /isapi/count.pl?: /isapi/count.pl?: AN HTTPd default script may allow writing over arbitrary files with a new content of '1', which could allow a trivial DoS. Append /../../../../../ctr.dll to replace this file's contents, for example.
- GET /logjam/showhits.php: /logjam/showhits.php: Logjam may possibly allow remote command execution via showhits.php page.
- GET /photo/manage.cgi: /photo/manage.cgi: My Photo Gallery management interface. May allow full access to photo galleries and more.
- -5374: GET /pub/english.cgi?op=rmail: /pub/english.cgi?op=rmail: BSCW self-registration may be enabled. This could allow untrusted users semi-trusted access to the software. 3.x version (and probably some 4.x) allow arbitrary commands to be executed remotely.
- -240: GET /scripts/wsisa.dll/WService=anything?WSMadmin: /scripts/wsisa.dll/WService=anything?WSMadmin: Allows Webspeed to be remotely administered. Edit unbroker.properties and set AllowMsngrCmds to 0.
- -3092: GET /SetSecurity.shm: /SetSecurity.shm: Cisco System's My Access for Wireless. This resource should be password protected.
- -3092: GET /_vti_pvt/deptodoc.btr: /_vti_pvt/deptodoc.btr: FrontPage file found. This may contain useful information.
- -3092: GET /_vti_pvt/services.org: /_vti_pvt/services.org: FrontPage file found. This may contain useful information.
- -28260: POST /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings.
- -3092: POST /_vti_bin/_vti_aut/author.dll?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=tr /_vti_bin/_vti_aut/author.dll?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=tr We seem to have authoring access to the FrontPage web.
- -3092: GET /_vti_bin/_vti_aut/dvwssr.dll: /_vti_bin/_vti_aut/dvwssr.dll: This dll allows anyone with authoring privs to change other users file, and may contain a buffer overflow for unauthenticated users. See also : http://www.wiretrip.net/rfp/p/doc.asp?id=45&iface=1. MS00-025.
- -3092: GET /_vti_bin/_vti_aut/fp30reg.dll: /_vti_bin/_vti_aut/fp30reg.dll: Some versions of the FrontPage fp30reg.dll are vulnerable to a buffer overflow. See http://www.microsoft.com/technet/security/bulletin/ms03-051.asp for details.
- -473: GET /_vti_pvt/access.cnf: /_vti_pvt/access.cnf: Contains HTTP server-specific access control information. Remove or ACL if FrontPage is not being used.

- -473: GET /_vti_pvt/writeto.cnf: /_vti_pvt/writeto.cnf: Contains information about form handler result files. Remove or ACL if FrontPage is not being used.
- -48: GET /doc: /doc: The /doc directory is browsable. This may be /usr/doc.
- -568: GET /blahb.ida: /blahb.ida: Reveals physical path. To fix: Preferences -> Home directory -> Application & check 'Check if file exists' for the ISAPI mappings. MS01-033.
- -568: GET /blahb.idq: /blahb.idq: Reveals physical path. To fix: Preferences -> Home directory -> Application & check 'Check if file exists' for the ISAPI mappings. MS01-033.
- -578: GET /level/16: /level/16: CISCO HTTP service allows remote execution of commands
- -578: GET /level/16/exec//show/access-lists: /level/16/exec//show/access-lists: CISCO HTTP service allows remote execution of commands
- -578: GET /level/16/level/16/exec//show/interfaces: /level/16/level/16/exec//show/interfaces: CISCO HTTP service allows remote execution of commands
- -578: GET /level/16/exec//show: /level/16/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/18/exec//show: /level/18/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/20/exec//show: /level/20/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/24/exec//show: /level/24/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/26/exec//show: /level/26/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/28/exec//show: /level/28/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/32/exec//show: /level/32/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/34/exec//show: /level/34/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/36/exec//show: /level/36/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/40/exec//show: /level/40/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/42/exec//show: /level/42/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/44/exec//show: /level/44/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/48/exec//show: /level/48/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/50/exec//show: /level/50/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/52/exec//show: /level/52/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/56/exec//show: /level/56/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/58/exec//show: /level/58/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/60/exec//show: /level/60/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/64/exec//show: /level/64/exec//show: CISCO HTTP service allows remote execution of commands

- -578: GET /level/66/exec//show: /level/66/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/68/exec//show: /level/68/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/72/exec//show: /level/72/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/74/exec//show: /level/74/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/76/exec//show: /level/76/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/80/exec//show: /level/80/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/82/exec//show: /level/82/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/84/exec//show: /level/84/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/88/exec//show: /level/88/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/90/exec//show: /level/90/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/92/exec//show: /level/92/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/96/exec//show: /level/96/exec//show: CISCO HTTP service allows remote execution of commands
- -578: GET /level/98/exec//show: /level/98/exec//show: CISCO HTTP service allows remote execution of commands
- -18810: GET /users.lst: /users.lst: LocalWEB2000 users.lst passwords found
- -3722: GET /lcgi/lcgitest.nlm: /lcgi/lcgitest.nlm: Novell web server shows the server environment
- -13403: GET /com/novell/webaccess: /com/novell/webaccess: Novell web server allows directory listing
- -4808: GET /axis-cgi/buffer/command.cgi: /axis-cgi/buffer/command.cgi: Axis WebCam 2400 may allow overwriting or creating files on the system. See http://www.websec.org/adv/axis2400.txt.html for details.
- -561: GET /server-status: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.
- -1264: GET /publisher/: /publisher/: Netscape Enterprise Server with Web Publishing can allow attackers to edit web pages and/or list arbitrary directories via Java applet. CVE-2000-0237.
- -2117: GET /cpanel/: /cpanel/: Web-based control panel
- -2119: GET /shopping/diag_dbtest.asp: /shopping/diag_dbtest.asp: VP-ASP Shopping Cart 5.0 contains multiple SQL injection vulnerabilities. CVE-2003-0560, BID-8159
- -250: GET /wwwboard/passwd.txt: /wwwboard/passwd.txt: The wwwboard password file is browsable. Change wwwboard to store this file elsewhere, or upgrade to the latest version.
- -272: GET /msadc/msadcs.dll: /msadc/msadcs.dll: See RDS advisory RFP9902, CVE-1999-1011, MS98-004, MS99-025 RFP-9902 BID-29 (http://www.wiretrip.net/rfp/p/doc.asp/i2/d1.htm), CIAC J-054 http://www.ciac.org/ciac/bulletins/j-054.shtml www.securityfocus.com/bid/529
- -2735: GET /musicqueue.cgi: /musicqueue.cgi: Musicqueue 1.20 is vulnerable to a buffer overflow. Ensure the latest version is installed (exploit not attempted). http://musicqueue.sourceforge.net/
- -284: GET /iisadmpwd/aexp2b.htr: /iisadmpwd/aexp2b.htr: Gives domain and system

name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy. CVE-1999-0407. BID-4236. BID-2110.
- -2842: GET //admin/aindex.htm: //admin/aindex.htm: FlexWATCH firmware 2.2 is vulnerable to authentication bypass by prepending an extra '/'. http://packetstorm.linuxsecurity.com/0310-exploits/FlexWATCH.txt
- -2948: GET /rademail.pl: /rademail.pl: @Mail WebMail 3.52 contains an SQL injection that allows attacker to read any email message for any address registered in the system. Example to append to rademail.pl: ?id=666&folder=qwer'%20or%20EmailDatabase_v.Account='victim@atmail.com&print=1
- -3: GET /iissamples/exair/search/query.asp: /iissamples/exair/search/query.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. CVE-1999-0449. BID-193.
- -3092: GET /access-log: /access-log: This might be interesting...
- -3092: GET /acciones/: /acciones/: This might be interesting...
- -3092: GET /accounting/: /accounting/: This might be interesting...
- -3092: GET /adm/: /adm/: This might be interesting...
- -3092: GET /admin.php3: /admin.php3: This might be interesting...
- -3092: GET /admin/: /admin/: This might be interesting...
- -3092: GET /administration/: /administration/: This might be interesting...
- -3092: GET /Agent/: /Agent/: This might be interesting...
- -3092: GET /agentes/: /agentes/: This might be interesting...
- -3092: GET /analog/: /analog/: This might be interesting...
- -3092: GET /applicattions/: /applicattions/: This might be interesting...
- -3092: GET /archivar/: /archivar/: This might be interesting...
- -3092: GET /archives/: /archives/: This might be interesting...
- -3092: GET /atc/: /atc/: This might be interesting...
- -3092: GET /backdoor/: /backdoor/: This might be interesting...
- -3092: GET /banco/: /banco/: This might be interesting...
- -3092: GET /bbv/: /bbv/: This might be interesting...
- -3092: GET /bdatos/: /bdatos/: This might be interesting...
- -3092: GET /buy/: /buy/: This might be interesting...
- -3092: GET /c/: /c/: This might be interesting...
- -3092: GET /caja/: /caja/: This might be interesting...
- -3092: GET /cash/: /cash/: This might be interesting...
- -3092: GET /ccbill/secure/ccbill.log: /ccbill/secure/ccbill.log: This might be interesting... CC Bill log file?
- -3092: GET /cert/: /cert/: This might be interesting...
- -3092: GET /cfdocs/exampleapp/email/application.cfm: /cfdocs/exampleapp/email/application.cfm: This might be interesting...
- -3092: GET /cfdocs/exampleapp/publish/admin/application.cfm: /cfdocs/exampleapp/publish/admin/application.cfm: This might be interesting...
- -3092: GET /client/: /client/: This might be interesting...
- -3092: GET /compra/: /compra/: This might be interesting...
- -3092: GET /compressed/: /compressed/: This might be interesting...
- -3092: GET /config/checks.txt: /config/checks.txt: This might be interesting...
- -3092: GET /connect/: /connect/: This might be interesting...
- -3092: GET /correo/: /correo/: This might be interesting...
- -3092: GET /css: /css: This might be interesting...
- -3092: GET /cuentas/: /cuentas/: This might be interesting...
- -3092: GET /dan_o.dat: /dan_o.dat: This might be interesting...
- -3092: GET /data/: /data/: This might be interesting...
- -3092: GET /dbase/: /dbase/: This might be interesting...

- -3092: GET /demos/: /demos/: This might be interesting...
- -3092: GET /devel/: /devel/: This might be interesting...
- -3092: GET /DMR/: /DMR/: This might be interesting...
- -3092: GET /down/: /down/: This might be interesting...
- -3092: GET /downloads/: /downloads/: This might be interesting...
- -3092: GET /employees/: /employees/: This might be interesting...
- -3092: GET /enviamail/: /enviamail/: This might be interesting...
- -3092: GET /excel/: /excel/: This might be interesting...
- -3092: GET /fbsd/: /fbsd/: This might be interesting...
- -3092: GET /fileadmin/: /fileadmin/: This might be interesting...
- -3092: GET /forum/: /forum/: This might be interesting...
- -3092: GET /fpadmin/: /fpadmin/: This might be interesting...
- -3092: GET /gfx/: /gfx/: This might be interesting...
- -3092: GET /graphics/: /graphics/: This might be interesting...
- -3092: GET /hidden/: /hidden/: This might be interesting...
- -3092: GET /hitmatic/analyse.cgi: /hitmatic/analyse.cgi: This might be interesting...
- -3092: GET /hits.txt: /hits.txt: This might be interesting...
- -3092: GET /hit_tracker/: /hit_tracker/: This might be interesting...
- -3092: GET /html/: /html/: This might be interesting...
- -3092: GET /HyperStat/stat_what.log: /HyperStat/stat_what.log: This might be interesting...
- -3092: GET /ibill/: /ibill/: This might be interesting...
- -3092: GET /img/: /img/: This might be interesting...
- -3092: GET /import/: /import/: This might be interesting...
- -3092: GET /includes/: /includes/: This might be interesting...
- -3092: GET /information/: /information/: This might be interesting...
- -3092: GET /ingreso/: /ingreso/: This might be interesting...
- -3092: GET /internal/: /internal/: This might be interesting...
- -3092: GET /jdbc/: /jdbc/: This might be interesting...
- -3092: GET /jrun/: /jrun/: This might be interesting...
- -3092: GET /libro/: /libro/: This might be interesting...
- -3092: GET /log.htm: /log.htm: This might be interesting...
- -3092: GET /logfiles/: /logfiles/: This might be interesting...
- -3092: GET /logger/: /logger/: This might be interesting...
- -3092: GET /logs.txt: /logs.txt: This might be interesting...
- -3092: GET /logs/: /logs/: This might be interesting...
- -3092: GET /logs/error_log: /logs/error_log: This might be interesting...
- -3092: GET /mail/: /mail/: This might be interesting...
- -3092: GET /master.password: /master.password: This might be interesting...
- -3092: GET /mbox: /mbox: This might be interesting...
- -3092: GET /message/: /message/: This might be interesting...
- -3092: GET /ministats/admin.cgi: /ministats/admin.cgi: This might be interesting...
- -3092: GET /mp3/: /mp3/: This might be interesting...
- -3092: GET /msql/: /msql/: This might be interesting...
- -3092: GET /Msword/: /Msword/: This might be interesting...
- -3092: GET /netscape/: /netscape/: This might be interesting...
- -3092: GET /new/: /new/: This might be interesting...
- -3092: GET /noticias/: /noticias/: This might be interesting...
- -3092: GET /oracle: /oracle: This might be interesting...
- -3092: GET /order/: /order/: This might be interesting...
- -3092: GET /orders/orders.txt: /orders/orders.txt: This might be interesting...
- -3092: GET /outgoing/: /outgoing/: This might be interesting...
- -3092: GET /pages/: /pages/: This might be interesting...

- -3092: GET /passwd: /passwd: This could be interesting...
- -3092: GET /passwd.adjunct: /passwd.adjunct: This could be interesting...
- -3092: GET /passwd.txt: /passwd.txt: This could be interesting...
- -3092: GET /password: /password: This could be interesting...
- -3092: GET /PDG_Cart/: /PDG_Cart/: This might be interesting...
- -3092: GET /pix/: /pix/: This might be interesting...
- -3092: GET /polls: /polls: This might be interesting...
- -3092: GET /pr0n/: /pr0n/: This might be interesting...
- -3092: GET /pron/: /pron/: This might be interesting...
- -3092: GET /pruebas/: /pruebas/: This might be interesting...
- -3092: GET /public/: /public/: This might be interesting...
- -3092: GET /purchase/: /purchase/: This might be interesting...
- -3092: GET /pwd.db: /pwd.db: This might be interesting...
- -3092: GET /readme: /readme: This might be interesting...
- -3092: GET /README.TXT: /README.TXT: This might be interesting...
- -3092: GET /readme.txt: /readme.txt: This might be interesting...
- -3092: GET /registered/: /registered/: This might be interesting...
- -3092: GET /reseller/: /reseller/: This might be interesting...
- -3092: GET /retail/: /retail/: This might be interesting...
- -3092: GET /sample/: /sample/: This might be interesting...
- -3092: GET /save/: /save/: This might be interesting...
- -3092: GET /scratch: /scratch: This might be interesting...
- -3092: GET /search.vts: /search.vts: This might be interesting...
- -3092: GET /search97.vts: /search97.vts: This might be interesting...
- -3092: GET /secret/: /secret/: This might be interesting...
- -3092: GET /servicios/: /servicios/: This might be interesting...
- -3092: GET /shop/: /shop/: This might be interesting...
- -3092: GET /spwd: /spwd: This might be interesting...
- -3092: GET /ss.cfg: /ss.cfg: This might be interesting...
- -3092: GET /stat/: /stat/: This might be interesting...
- -3092: GET /Statistics/: /Statistics/: This might be interesting...
- -3092: GET /stats.htm: /stats.htm: This might be interesting...
- -3092: GET /stats.txt: /stats.txt: This might be interesting...
- -3092: GET /Stats/: /Stats/: This might be interesting...
- -3092: GET /store/: /store/: This might be interesting...
- -3092: GET /stylesheet/: /stylesheet/: This might be interesting...
- -3092: GET /super_stats/access_logs: /super_stats/access_logs: This might be interesting...
- -3092: GET /support/: /support/: This might be interesting...
- -3092: GET /sys/: /sys/: This might be interesting...
- -3092: GET /temp/: /temp/: This might be interesting...
- -3092: GET /temporal/: /temporal/: This might be interesting...
- -3092: GET /test.html: /test.html: This might be interesting...
- -3092: GET /test.txt: /test.txt: This might be interesting...
- -3092: GET /tests/: /tests/: This might be interesting...
- -3092: GET /tools/: /tools/: This might be interesting...
- -3092: GET /trabajo/: /trabajo/: This might be interesting...
- -3092: GET /trees/: /trees/: This might be interesting...
- -3092: GET /user/: /user/: This might be interesting...
- -3092: GET /users/scripts/submit.cgi: /users/scripts/submit.cgi: This might be interesting...
- -3092: GET /vfs/: /vfs/: This might be interesting...
- -3092: GET /warez/: /warez/: This might be interesting...

- -3092: GET /web800fo/: /web800fo/: This might be interesting...
- -3092: GET /webaccess/access-options.txt: /webaccess/access-options.txt: This might be interesting...
- -3092: GET /webboard/: /webboard/: This might be interesting...
- -3092: GET /webcart/: /webcart/: This might be interesting...
- -3092: GET /weblog/: /weblog/: This might be interesting...
- -3092: GET /WebShop/templates/cc.txt: /WebShop/templates/cc.txt: This might be interesting...
- -3092: GET /website/: /website/: This might be interesting...
- -3092: GET /WebTrend/: /WebTrend/: This might be interesting...
- -3092: GET /work/: /work/: This might be interesting...
- -3092: GET /wusage/: /wusage/: This might be interesting...
- -3092: GET /www/: /www/: This might be interesting...
- -3092: GET /wwwlog/: /wwwlog/: This might be interesting...
- -3092: GET /wwwstats/: /wwwstats/: This might be interesting...
- -3092: GET /wwwthreads/3tvars.pm: /wwwthreads/3tvars.pm: This might be interesting...
- -3092: GET /advworks/equipment/catalog_type.asp: /advworks/equipment/catalog_type.asp: This might be interesting...
- -3092: GET /carbo.dll: /carbo.dll: This might be interesting...
- -17670: GET /clocktower/: /clocktower/: Site Server sample files. This might be interesting...
- -17670: GET /market/: /market/: Site Server sample files. This might be interesting.
- -3092: GET /scripts/counter.exe: /scripts/counter.exe: This might be interesting...
- -17669: GET /scripts/cphost.dll: /scripts/cphost.dll: cphost.dll may have a DoS and a traversal issue.
- -3092: GET /scripts/fpadmcgi.exe: /scripts/fpadmcgi.exe: This might be interesting...
- -3092: GET /site/iissamples/: /site/iissamples/: This might be interesting...
- -3092: GET /_mem_bin/: /_mem_bin/: This might be interesting - User Login
- -3092: GET /perl/files.pl: /perl/files.pl: This might be interesting...
- -3092: GET /scripts/convert.bas: /scripts/convert.bas: This might be interesting...
- -3233: GET /cgi-dos/args.bat: /cgi-dos/args.bat: Default FrontPage CGI found.
- -3092: GET /hostingcontroller/: /hostingcontroller/: This might be interesting...probably HostingController, www.hostingcontroller.com
- -3092: GET /databases/: /databases/: Databases? Really??
- -3092: GET /img-sys/: /img-sys/: Default image directory should not allow directory listing.
- -3092: GET /javadoc/: /javadoc/: Documentation...?
- -3092: GET /manager/: /manager/: May be a web server or site manager.
- -3092: GET /account.nsf: /account.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /admin.nsf: /admin.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /admin5.nsf: /admin5.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /archive/l_domlog.nsf: /archive/l_domlog.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /billing.nsf: /billing.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /books.nsf: /books.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /certlog.nsf: /certlog.nsf: This database can be read without authentication, which may reveal sensitive information.

- -3092: GET /chatlog.nsf: /chatlog.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /cldbdir.nsf: /cldbdir.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /customerdata.nsf: /customerdata.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /database.nsf: /database.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /dclf.nsf: /dclf.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /DEASLog02.nsf: /DEASLog02.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /DEASLog04.nsf: /DEASLog04.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /decsadm.nsf: /decsadm.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /default.nsf: /default.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /doladmin.nsf: /doladmin.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /domadmin.nsf: /domadmin.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /events5.nsf: /events5.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /groups.nsf: /groups.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /help5_client.nsf: /help5_client.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /iNotes/Forms5.nsf/$DefaultNav: /iNotes/Forms5.nsf/$DefaultNav: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /kbccv11.nsf: /kbccv11.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /kbssvv11.nsf: /kbssvv11.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /leilog.nsf: /leilog.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /log4a.nsf: /log4a.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /l_domlog.nsf: /l_domlog.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /mail10.box: /mail10.box: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /mail3.box: /mail3.box: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /mail5.box: /mail5.box: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /mail9.box: /mail9.box: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /msdwda.nsf: /msdwda.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /mtdata/mtstore.nsf: /mtdata/mtstore.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /nntp/nd000002.nsf: /nntp/nd000002.nsf: This database can be read

without authentication, which may reveal sensitive information.
- -3092: GET /nntp/nd000004.nsf: /nntp/nd000004.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /notes.nsf: /notes.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /private.nsf: /private.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /qpadmin.nsf: /qpadmin.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /quickstart/qstart50.nsf: /quickstart/qstart50.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /sample/faqw46: /sample/faqw46: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /sample/pagesw46: /sample/pagesw46: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /sample/site1w4646: /sample/site1w4646: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /secret.nsf: /secret.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /smbcfg.nsf: /smbcfg.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /smency.nsf: /smency.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /smtime.nsf: /smtime.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /smtp.nsf: /smtp.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /smtpobwq.nsf: /smtpobwq.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /srvnam.htm: /srvnam.htm: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /stauths.nsf: /stauths.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /stconf.nsf: /stconf.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /stlog.nsf: /stlog.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /stsrc.nsf: /stsrc.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /today.nsf: /today.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /web.nsf: /web.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3092: GET /welcome.nsf: /welcome.nsf: This database can be read without authentication, which may reveal sensitive information.
- -3093: GET /finances.xls: /finances.xls: Finance spreadsheet?
- -3093: GET /add_acl: /add_acl: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/auth.php: /admin/auth.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/cfg/configsite.inc.php+: /admin/cfg/configsite.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/credit_card_info.php: /admin/credit_card_info.php: This might be

interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/index.php: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/objects.inc.php4: /admin/objects.inc.php4: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /admin/upload.php: /admin/upload.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /adv/gm001-mc/: /adv/gm001-mc/: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /approval/ts_app.htm: /approval/ts_app.htm: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /auth.inc.php: /auth.inc.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /bandwidth/index.cgi: /bandwidth/index.cgi: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /bigsam_guestbook.php?displayBegin=9999...9999: /bigsam_guestbook.php?displayBegin=9999...9999: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /board/index.php: /board/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /caupo/admin/admin_workspace.php: /caupo/admin/admin_workspace.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /communique.asp: /communique.asp: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /community/index.php?analized=anything: /community/index.php?analized=anything: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /compte.php: /compte.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /cutenews/comments.php: /cutenews/comments.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /cutenews/shownews.php: /cutenews/shownews.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /Data/settings.xml+: /Data/settings.xml+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /database/metacart.mdb+: /database/metacart.mdb+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /dbabble: /dbabble: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /defines.php: /defines.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /doc/admin/index.php: /doc/admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /dotproject/modules/projects/view.php: /dotproject/modules/projects/view.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /dotproject/modules/tasks/addedit.php: /dotproject/modules/tasks/addedit.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /do_map: /do_map: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /emumail.cgi?type=.%00: /emumail.cgi?type=.%00: This might be

interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /enteteacceuil.php: /enteteacceuil.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /eventcal2.php.php: /eventcal2.php.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /faqman/index.php: /faqman/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /filemgmt/brokenfile.php: /filemgmt/brokenfile.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /filemgmt/viewcat.php: /filemgmt/viewcat.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /forum/newthread.php: /forum/newthread.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -10447: GET /get_od_toc.pl?Profile=: /get_od_toc.pl?Profile=: WebTrends get_od_toc.pl may be vulnerable to a path disclosure error if this file is reloaded multiple times.
- -3093: GET /globals.pl: /globals.pl: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /homebet/homebet.dll?form=menu&option=menu-signin: /homebet/homebet.dll?form=menu&option=menu-signin: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /includes/footer.php3: /includes/footer.php3: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /infos/faq/index.asp: /infos/faq/index.asp: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /intranet/browse.php: /intranet/browse.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /ipchat.php: /ipchat.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /livredor/index.php: /livredor/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /mail/include.html: /mail/include.html: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /mail/src/read_body.php: /mail/src/read_body.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /mantis/summary_graph_functions.php?g_jpgraph_path=http%3A%2F%2Fattackershost%2Flistings.txt%3F: /mantis/summary_graph_functions.php?g_jpgraph_path=http%3A%2F%2Fattackershost%2Flistings.txt%3F: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /members/ID.pm: /members/ID.pm: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /modif/delete.php: /modif/delete.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /modules/Forums/attachment.php: /modules/Forums/attachment.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /modules/WebChat/in.php+: /modules/WebChat/in.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /modules/Your_Account/navbar.php+: /modules/Your_Account/navbar.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /msadc/Samples/SELECTOR/showcode.asp?|-|0|404_Object_Not_Found: /msadc/Samples/SELECTOR/showcode.asp?|-|0|404_Object_Not_Found: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /myguestBk/admin/delEnt.asp?id=NEWSNUMBER|-|0|

404_Object_Not_Found: /myguestBk/admin/delEnt.asp?id=NEWSNUMBER|-|0|404_Object_Not_Found: This might be interesting... has been seen in web logs from an unknown scanner.

- -3093: GET /nphp/nphpd.php: /nphp/nphpd.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /options.inc.php+: /options.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /parse_xml.cgi: /parse_xml.cgi: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /php/php4ts.dll: /php/php4ts.dll: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /pm/lib.inc.php: /pm/lib.inc.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /poppassd.php3+: /poppassd.php3+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /produccart/pdacmin/login.asp?|-|0|404_Object_Not_Found: /produccart/pdacmin/login.asp?|-|0|404_Object_Not_Found: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /productcart/pc/Custva.asp?|-|0|404_Object_Not_Found: /productcart/pc/Custva.asp?|-|0|404_Object_Not_Found: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /protected/: /protected/: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /protectedpage.php?uid='%20OR%20''='&pwd='%20OR%20''=': /protectedpage.php?uid='%20OR%20''='&pwd='%20OR%20''=': This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /room/save_item.php: /room/save_item.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /scripts/tradecli.dll: /scripts/tradecli.dll: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /security/web_access.html: /security/web_access.html: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /servers/link.cgi: /servers/link.cgi: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /shop/php_files/site.config.php+: /shop/php_files/site.config.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /staticpages/index.php: /staticpages/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /sw000.asp?|-|0|404_Object_Not_Found: /sw000.asp?|-|0|404_Object_Not_Found: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /technote/print.cgi: /technote/print.cgi: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /tinymsg.php: /tinymsg.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /ttforum/index.php: /ttforum/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /tutos/file/file_select.php: /tutos/file/file_select.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /uifc/MultFileUploadHandler.php+: /uifc/MultFileUploadHandler.php+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /utils/sprc.asp+: /utils/sprc.asp+: This might be interesting... has been seen in web logs from an unknown scanner.

- -3093: GET /vars.inc+: /vars.inc+: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /VBZooM/add-subject.php: /VBZooM/add-subject.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /wbboard/reply.php: /wbboard/reply.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /webmail/src/read_body.php: /webmail/src/read_body.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /XMBforum/buddy.php: /XMBforum/buddy.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /x_stat_admin.php: /x_stat_admin.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /_head.php: /_head.php: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /ows-bin/oasnetconf.exe?-l%20-s%20BlahBlah: /ows-bin/oasnetconf.exe?-l%20-s%20BlahBlah: This might be interesting... has been seen in web logs from an unknown scanner.
- -3093: GET /database/: /database/: Databases? Really??
- -3093: GET /.wwwacl: /.wwwacl: Contains authorization information
- -3093: GET /.www_acl: /.www_acl: Contains authorization information
- -3093: GET /.access: /.access: Contains authorization information
- -3093: GET /.bashrc: /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.
- -3093: GET /.forward: /.forward: User home dir was found with a mail forward file. May reveal where the user's mail is being forwarded to.
- -3093: GET /.history: /.history: A user's home directory may be set to the web root, the shell history was retrieved. This should not be accessible via the web.
- -3093: GET /.htaccess: /.htaccess: Contains authorization information
- -3093: GET /.mysql_history: /.mysql_history: Database SQL?
- -3093: GET /.pinerc: /.pinerc: User home dir found with a PINE rc file. May reveal system information, directories and more.
- -3093: GET /.proclog: /.proclog: User home dir with a Procmail log file. May reveal user mail traffic, directories and more.
- -3093: GET /.procmailrc: /.procmailrc: User home dir with a Procmail rc file. May reveal subdirectories, mail contacts and more.
- -3093: GET /.profile: /.profile: User home dir with a shell profile was found. May reveal directory information and system configuration.
- -3093: GET /.sh_history: /.sh_history: A user's home directory may be set to the web root, the shell history was retrieved. This should not be accessible via the web.
- -3093: GET /.ssh/known_hosts: /.ssh/known_hosts: A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
- -3233: GET /jservdocs/: /jservdocs/: Default Apache JServ docs should be removed.
- -3233: GET /ojspdemos/basic/simple/usebean.jsp: /ojspdemos/basic/simple/usebean.jsp: Oracle 9i default JSP page found, may be vulnerable to XSS in any field.
- -3233: GET /servlet/HelloWorldServlet: /servlet/HelloWorldServlet: JRun default servlet found. All default code should be removed from servers.
- -3233: GET /servlet/SessionServlet: /servlet/SessionServlet: JRun or Netware WebSphere default servlet found. All default code should be removed from servers.
- -3233: GET /servlet/SnoopServlet: /servlet/SnoopServlet: JRun, Netware Java Servlet Gateway, or WebSphere default servlet found. All default code should be removed from servers.
- -3233: GET /admcgi/scripts/Fpadmcgi.exe: /admcgi/scripts/Fpadmcgi.exe: Default FrontPage CGI found.

- -3233: GET /bin/admin.pl: /bin/admin.pl: Default FrontPage CGI found.
- -3233: GET /bin/CGImail.exe: /bin/CGImail.exe: Default FrontPage CGI found.
- -3233: GET /bin/fpsrvadm.exe: /bin/fpsrvadm.exe: Default FrontPage CGI found.
- -3233: GET /cgi-bin/cfgwiz.exe: /cgi-bin/cfgwiz.exe: Default FrontPage CGI found.
- -3233: GET /cgi-bin/contents.htm: /cgi-bin/contents.htm: Default FrontPage CGI found.
- -3233: GET /scripts/admin.pl: /scripts/admin.pl: Default FrontPage CGI found.
- -3233: GET /scripts/CGImail.exe: /scripts/CGImail.exe: Default FrontPage CGI found.
- -3233: GET /scripts/fpadmin.htm: /scripts/fpadmin.htm: Default FrontPage CGI found.
- -3233: GET /_private/: /_private/: FrontPage directory found.
- -3233: GET /_private/registrations.txt: /_private/registrations.txt: Default FrontPage file found.
- -3233: GET /_vti_bin/: /_vti_bin/: FrontPage directory found.
- -3233: GET /_vti_bin/cfgwiz.exe: /_vti_bin/cfgwiz.exe: Default FrontPage CGI found.
- -3233: GET /_vti_bin/contents.htm: /_vti_bin/contents.htm: Default FrontPage CGI found.
- -3233: GET /_vti_bin/_vti_cnf/: /_vti_bin/_vti_cnf/: FrontPage directory found.
- -3233: GET /_vti_pvt/authors.pwd: /_vti_pvt/authors.pwd: Default FrontPage file found, may be a password file.
- -3233: GET /_vti_pvt/service.pwd: /_vti_pvt/service.pwd: Default FrontPage file found, may be a password file.
- -3233: GET /_vti_pvt/users.pwd: /_vti_pvt/users.pwd: Default FrontPage file found, may be a password file.
- -3233: GET /help/contents.htm: /help/contents.htm: Default Netscape manual found. All default pages should be removed.
- -3233: GET /manual/ag/esperfrm.htm: /manual/ag/esperfrm.htm: Default Netscape manual found. All default pages should be removed.
- -3233: GET /com/novell/webpublisher/help/en/default.htm: /com/novell/webpublisher/help/en/default.htm: Netware web publisher documentation found. All default documentation should be removed from web servers.
- -3233: GET /servlet/gwmonitor: /servlet/gwmonitor: Netware Gateway monitor found. All default code should be removed from web servers.
- -3233: GET /servlet/SearchServlet: /servlet/SearchServlet: Novell Netware default servlet found. All default code should be removed from the system.
- -3233: GET /servlet/webacc: /servlet/webacc: Netware Enterprise and/or GroupWise web access found. All default code should be removed from Internet servers.
- -3233: GET /WebSphereSamples: /WebSphereSamples: Netware Webshere sample applications found. All default code should be removed from web servers.
- -3233: GET /doc/dspug.nsf: /doc/dspug.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /doc/internet.nsf: /doc/internet.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /doc/lccon.nsf: /doc/lccon.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /doc/npn_admn.nsf: /doc/npn_admn.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /doc/smhelp.nsf: /doc/smhelp.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /domguide.nsf: /domguide.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /help/domguide.nsf: /help/domguide.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /help/helplt4.nsf: /help/helplt4.nsf: This documentation database can be

read without authentication. All default files should be removed.
- -3233: GET /help/javapg.nsf: /help/javapg.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /help/migrate.nsf: /help/migrate.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /help/readmes.nsf: /help/readmes.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /help/srvinst.nsf: /help/srvinst.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /helpadmin.nsf: /helpadmin.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /lccon.nsf: /lccon.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /npn_admn.nsf: /npn_admn.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /readmec.nsf: /readmec.nsf: This documentation database can be read without authentication. All default files should be removed.
- -3233: GET /index.html.cz.iso8859-2: /index.html.cz.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.en: /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.es: /index.html.es: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.fr: /index.html.fr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.hr.iso8859-2: /index.html.hr.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.lu.utf8: /index.html.lu.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.nl: /index.html.nl: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.nn: /index.html.nn: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.pt: /index.html.pt: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.tw.Big5: /index.html.tw.Big5: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /index.html.var: /index.html.var: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
- -3233: GET /a/: /a/: May be Kebi Web Mail administration menu.
- -3282: GET /uploader.php: /uploader.php: This script may allow arbitrary files to be uploaded to the remote server.

- -3286: GET /conspass.chl+: /conspass.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. CVE-2002-1081
- -3286: GET /general.chl+: /general.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. CVE-2002-1081
- -3396: GET /mlog.html: /mlog.html: Remote file read vulnerability 1999-0068
- -3396: GET /mlog.phtml: /mlog.phtml: Remote file read vulnerability 1999-0068
- -3396: GET /php/mlog.phtml: /php/mlog.phtml: Remote file read vulnerability 1999-0346
- -3489: GET /surf/scwebusers: /surf/scwebusers: SurfControl SuperScout Web Reports Server user and password file is available. CVE-2002-0705.
- -3501: GET /_private/form_results.htm: /_private/form_results.htm: This file may contain information submitted by other web users via forms. CVE-1999-1052.
- -3501: GET /_private/form_results.txt: /_private/form_results.txt: This file may contain information submitted by other web users via forms. CVE-1999-1052.
- -3591: GET /project/index.php?m=projects&user_cookie=1: /project/index.php?m=projects&user_cookie=1: dotProject 0.2.1.5 may allow admin login bypass by adding the user_cookie=1 to the URL.
- -379: GET /site/eg/source.asp: /site/eg/source.asp: This ASP (installed with Apache::ASP) allows attackers to upload files to the server. Upgrade to 1.95 or higher. CVE-2000-0628.
- -4013: GET /isqlplus: /isqlplus: Oracle iSQL*Plus is installed. This may be vulnerable to a buffer overflow in the user ID field. http://www.ngssoftware.com/advisories/ora-isqlplus.txt
- -4161: GET /data/member_log.txt: /data/member_log.txt: Teekai's forum full 1.2 member's log can be retrieved remotely.
- -4171: GET /ASP/cart/database/metacart.mdb: /ASP/cart/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.
- -4171: GET /mcartfree/database/metacart.mdb: /mcartfree/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.
- -4171: GET /shop/database/metacart.mdb: /shop/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.
- -4237: GET /ban.dat: /ban.dat: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected.
- -4239: GET /admin/datasource.asp: /admin/datasource.asp: Xpede page reveals SQL account name. The /admin directory should be protected.
- -4361: GET /acart2_0/admin/category.asp: /acart2_0/admin/category.asp: Alan Ward A-Cart 2.0 is vulnerable to an XSS attack which may cause the administrator to delete database information.
- -474: GET /Sites/Knowledge/Membership/Inspiredtutorial/ViewCode.asp: /Sites/Knowledge/Membership/Inspiredtutorial/ViewCode.asp: The defau

Nikto scan for chat-dev.it.tuwien.ac.at_nikto

- Target Host: chat-dev.it.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /: Uncommon header 'x-instance-id' found, with contents: GSjkGP3v3GjaWWtpF
- GET /: Uncommon header 'content-security-policy' found, with contents: default-src 'self' ; connect-src *; font-src 'self' data:; frame-src *; img-src * data:; media-src * data:; script-src 'self' 'unsafe-eval' ; style-src 'self' 'unsafe-inline'
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000

- GET /: Uncommon header 'x-xss-protection' found, with contents: 1
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
- GET /favicon.ico: Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x5e6bfbbaa9d886afe43fe8b15b3e123c8239d544
- GET /WEB-INF/web.xml: /WEB-INF/web.xml: JRUN default file found.
- -3092: GET /css: /css: This might be interesting...

Nuclei report

This is the result of the Nuclei activity. **Here you can find only the relevant information**

Remeber:

- **Green is used for low impact vulnerabilities**
- **Orange is used for medium impact vulnerabilities**
- **Red is used for high impact vulnerabilities**

Nuclei scan for ocisdev.it.tuwien.ac.at_nuclei

- [http-trace:trace-request] [http] [info] https://ocisdev.it.tuwien.ac.at

Nuclei scan for tube1.it.tuwien.ac.at_nuclei

- [ssl-issuer] [ssl] [info] tube1.it.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] tube1.it.tuwien.ac.at:443 ["tube1.it.tuwien.ac.at"]

Nuclei scan for service.it.tuwien.ac.at_nuclei

- [tls-version] [ssl] [info] service.it.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] service.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- **[weak-cipher-suites:tls-1.1] [ssl] [low] service.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- [tls-version] [ssl] [info] service.it.tuwien.ac.at:443 ["tls11"]
- [tls-version] [ssl] [info] service.it.tuwien.ac.at:443 ["tls12"]
- [tls-version] [ssl] [info] service.it.tuwien.ac.at:443 ["tls13"]

Nuclei scan for support-q.it.tuwien.ac.at_nuclei

- **[weak-cipher-suites:tls-1.0] [ssl] [low] support-q.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] support-q.it.tuwien.ac.at:443 ["tls10"]
- [tls-version] [ssl] [info] support-q.it.tuwien.ac.at:443 ["tls11"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] support-q.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] support-q.it.tuwien.ac.at:443 ["tls12"]
- **[weak-cipher-suites:tls-1.2] [ssl] [low] support-q.it.tuwien.ac.at:443 ["[tls12**

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256] "]

- [tls-version] [ssl] [info] support-q.it.tuwien.ac.at:443 ["tls13"]

Nuclei scan for infoscreen.it.tuwien.ac.at_nuclei

- **[weak-cipher-suites:tls-1.0] [ssl] [low] infoscreen.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] "]**
- [tls-version] [ssl] [info] infoscreen.it.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] infoscreen.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] "]**
- [tls-version] [ssl] [info] infoscreen.it.tuwien.ac.at:443 ["tls11"]
- [tls-version] [ssl] [info] infoscreen.it.tuwien.ac.at:443 ["tls12"]
- [tls-version] [ssl] [info] infoscreen.it.tuwien.ac.at:443 ["tls13"]

Nuclei scan for matrix-q.it.tuwien.ac.at_nuclei

- [nginx-version] [http] [info] https://matrix-q.it.tuwien.ac.at ["nginx/1.25.4"]
- [tech-detect:nginx] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:strict-transport-security] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:referrer-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:clear-site-data] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:content-security-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:permissions-policy] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:x-frame-options] [http] [info] https://matrix-q.it.tuwien.ac.at
- [http-missing-security-headers:x-content-type-options] [http] [info] https://matrix-q.it.tuwien.ac.at

- [http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://matrix-q.it.tuwien.ac.at
- [element-web-detect] [http] [info] https://matrix-q.it.tuwien.ac.at/version ["1.11.66"]
- [matrix-detect] [http] [info] https://matrix-q.it.tuwien.ac.at/.well-known/matrix/server ["matrix-q.it.tuwien.ac.at:443"]
- [matrix-homeserver-detect] [http] [info] https://matrix-q.it.tuwien.ac.at/_matrix/federation/v1/version ["Synapse","1.106.0"]
- [matrix-detect] [http] [info] https://matrix-q.it.tuwien.ac.at/.well-known/matrix/client ["https://matrix-q.it.tuwien.ac.at"]
- [waf-detect:nginxgeneric] [http] [info] https://matrix-q.it.tuwien.ac.at
- [ssl-issuer] [ssl] [info] matrix-q.it.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] matrix-q.it.tuwien.ac.at:443 ["*.matrix-q.it.tuwien.ac.at","matrix-q.it.tuwien.ac.at"]
- [wildcard-tls] [ssl] [info] matrix-q.it.tuwien.ac.at:443 ["CN: *.matrix-q.it.tuwien.ac.at","SAN: [*.matrix-q.it.tuwien.ac.at matrix-q.it.tuwien.ac.at]"]

Nuclei scan for depotm42.it.tuwien.ac.at_nuclei

- [tls-version] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] depotm42.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- **[weak-cipher-suites:tls-1.1] [ssl] [low] depotm42.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["tls11"]
- [tls-version] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["tls12"]
- [tls-version] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["tls13"]
- [ssl-issuer] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["Sectigo Limited"]
- [ssl-dns-names] [ssl] [info] depotm42.it.tuwien.ac.at:443 ["depotm42.it.tuwien.ac.at"]

Nuclei scan for owncloud.it.tuwien.ac.at_nuclei

- [http-trace:trace-request] [http] [info] https://owncloud.it.tuwien.ac.at

Nuclei scan for plesk-test.it.tuwien.ac.at_nuclei

- [tls-version] [ssl] [info] plesk-test.it.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] plesk-test.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**

- [tls-version] [ssl] [info] plesk-test.it.tuwien.ac.at:443 ["tls11"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] plesk-test.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- [tls-version] [ssl] [info] plesk-test.it.tuwien.ac.at:443 ["tls12"]

Nuclei scan for git.tuwien.ac.at_nuclei

- [gitlab-detect] [http] [info] https://git.tuwien.ac.at/users/sign_in
- [form-detection] [http] [info] https://gitlab.tuwien.ac.at/users/sign_in?auto_sign_in=false
- [robots-txt] [http] [info] https://git.tuwien.ac.at/robots.txt
- [ssh-auth-methods] [javascript] [info] git.tuwien.ac.at:22 ["["publickey","keyboard-interactive"]"]
- [ssh-server-enumeration] [javascript] [info] git.tuwien.ac.at:22 ["SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3"]
- [ssh-sha1-hmac-algo] [javascript] [info] git.tuwien.ac.at:22
- [openssh-detect] [tcp] [info] git.tuwien.ac.at:22 ["SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3"]
- [ssl-issuer] [ssl] [info] git.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] git.tuwien.ac.at:443 ["minio.it.tuwien.ac.at","registry.it.tuwien.ac.at","gitlab.tuwien.ac.at","git.tuwien.ac.at","git

Nuclei scan for www.it.tuwien.ac.at_nuclei

- [http-trace:trace-request] [http] [info] https://www.it.tuwien.ac.at
- [ssl-issuer] [ssl] [info] www.it.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] www.it.tuwien.ac.at:443 ["it.tuwien.ac.at","www.it.tuwien.ac.at"]

Nuclei scan for autoconfig.it.tuwien.ac.at_nuclei

- [tls-version] [ssl] [info] autoconfig.it.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] autoconfig.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] autoconfig.it.tuwien.ac.at:443 ["tls11"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] autoconfig.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] autoconfig.it.tuwien.ac.at:443 ["tls12"]

- [tls-version] [ssl] [info] autoconfig.it.tuwien.ac.at:443 ["tls13"]

Nuclei scan for minio.it.tuwien.ac.at_nuclei

- [ssl-issuer] [ssl] [info] minio.it.tuwien.ac.at:443 ["Unspecified"]
- **[expired-ssl] [ssl] [low] minio.it.tuwien.ac.at:443 ["2024-03-17 08:18:49 +0000 UTC"]**
- **[mismatched-ssl-certificate] [ssl] [low] minio.it.tuwien.ac.at:443 ["CN: allianz-ptvap02.vm.at.nxlr.eu"]**
- **[revoked-ssl-certificate] [ssl] [low] minio.it.tuwien.ac.at:443**
- [ssl-dns-names] [ssl] [info] minio.it.tuwien.ac.at:443 ["allianz-ptvap02.vm.at.nxlr.eu"]
- **[untrusted-root-certificate] [ssl] [low] minio.it.tuwien.ac.at:443**

Nuclei scan for gitlab.it.tuwien.ac.at_nuclei

- [ssl-issuer] [ssl] [info] gitlab.it.tuwien.ac.at:443 ["Unspecified"]
- **[expired-ssl] [ssl] [low] gitlab.it.tuwien.ac.at:443 ["2024-03-17 08:18:49 +0000 UTC"]**
- **[mismatched-ssl-certificate] [ssl] [low] gitlab.it.tuwien.ac.at:443 ["CN: allianz-ptvap02.vm.at.nxlr.eu"]**
- **[revoked-ssl-certificate] [ssl] [low] gitlab.it.tuwien.ac.at:443**
- [ssl-dns-names] [ssl] [info] gitlab.it.tuwien.ac.at:443 ["allianz-ptvap02.vm.at.nxlr.eu"]
- **[untrusted-root-certificate] [ssl] [low] gitlab.it.tuwien.ac.at:443**

Nuclei scan for registry.it.tuwien.ac.at_nuclei

- [ssl-issuer] [ssl] [info] registry.it.tuwien.ac.at:443 ["Unspecified"]
- **[expired-ssl] [ssl] [low] registry.it.tuwien.ac.at:443 ["2024-03-17 08:18:49 +0000 UTC"]**
- **[mismatched-ssl-certificate] [ssl] [low] registry.it.tuwien.ac.at:443 ["CN: allianz-ptvap02.vm.at.nxlr.eu"]**
- **[revoked-ssl-certificate] [ssl] [low] registry.it.tuwien.ac.at:443**
- [ssl-dns-names] [ssl] [info] registry.it.tuwien.ac.at:443 ["allianz-ptvap02.vm.at.nxlr.eu"]
- **[untrusted-root-certificate] [ssl] [low] registry.it.tuwien.ac.at:443**

Nuclei scan for svn.it.tuwien.ac.at_nuclei

- [tls-version] [ssl] [info] svn.it.tuwien.ac.at:443 ["tls10"]

- **[weak-cipher-suites:tls-1.0] [ssl] [low] svn.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- **[weak-cipher-suites:tls-1.1] [ssl] [low] svn.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- [tls-version] [ssl] [info] svn.it.tuwien.ac.at:443 ["tls11"]
- [tls-version] [ssl] [info] svn.it.tuwien.ac.at:443 ["tls12"]
- [tls-version] [ssl] [info] svn.it.tuwien.ac.at:443 ["tls13"]

Nuclei scan for oase.it.tuwien.ac.at_nuclei

- [ssl-issuer] [ssl] [info] oase.it.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] oase.it.tuwien.ac.at:443 ["oase3.zid.tuwien.ac.at","oase4.it.tuwien.ac.at","iu.zid.tuwien.ac.at","oase.it.tuwien.ac.at",'

Nuclei scan for autodiscover.it.tuwien.ac.at_nuclei

- **[weak-cipher-suites:tls-1.0] [ssl] [low] autodiscover.it.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**
- [tls-version] [ssl] [info] autodiscover.it.tuwien.ac.at:443 ["tls10"]
- [tls-version] [ssl] [info] autodiscover.it.tuwien.ac.at:443 ["tls11"]
- [tls-version] [ssl] [info] autodiscover.it.tuwien.ac.at:443 ["tls12"]
- [tls-version] [ssl] [info] autodiscover.it.tuwien.ac.at:443 ["tls13"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] autodiscover.it.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]"]**

Dirb report

This is the result of the Dirb activity. **Here you can find only the relevant information**
Remeber: Only responses with code 200 are reported here