```
       (        )  (    (    (
  (    )\ )  ( /(  )\ ) )\ ) )\ )
  )\  (()/(  )\())(()/((()/((()/( (
  (((_)  /(_))((_)\  /(_))/(_))/(_)))\
  )\___ (_)) __ ((_)(_)) (_)) (_)) ((_)
((/ __|| _ \ \ \ / /| _ \|_ _|| _ \| __|
 | (__ |   /  \ V / |  _/ | | |  _/| _|
  \___||_|_\   |_|  |_|  |___||_|  |___|
```

Report for domain 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 128.130.35.76 : ['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=663F5AB0%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=663F5AB7%P=x86_64-pc-linux-
SF:%r(GetRequest,198,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r
SF:ate:\x20Sat,\x2011\x20May\x202024\x2011:47:03\x20GMT\r\nx-ua-compati
SF::\x20IE=edge\r\nx-content-type-options:\x20nosniff\r\ncontent-length
```

```
SF:200\r\ncontent-type:\x20text/html;\x20charset=UTF-8\r\nstrict-transp
SF:-security:\x20max-age=63072000;\r\nx-xss-protection:\x201;mode=block
SF:nx-frame-options:\x20SAMEORIGIN\r\nset-cookie:\x20TYPO3MODE=;\x20Exp
SF:s=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20HttpOnly;\x2
SF:cure\r\nconnection:\x20close\r\n\r\n")%r(HTTPOptions,198,"HTTP/1\.1\
SF:500\x20Internal\x20Server\x20Error\r\ndate:\x20Sat,\x2011\x20May\x20
SF:4\x2011:47:03\x20GMT\r\nx-ua-compatible:\x20IE=edge\r\nx-content-typ
SF:ptions:\x20nosniff\r\ncontent-length:\x200\r\ncontent-type:\x20text/
SF:l;\x20charset=UTF-8\r\nstrict-transport-security:\x20max-age=6307200
SF:r\nx-xss-protection:\x201;mode=block\r\nx-frame-options:\x20SAMEORIG
SF:r\nset-cookie:\x20TYPO3MODE=;\x20Expires=Thu,\x2001-Jan-1970\x2000:0
SF:1\x20GMT;\x20path=/;\x20HttpOnly;\x20Secure\r\nconnection:\x20close\
SF:\r\n")%r(FourOhFourRequest,198,"HTTP/1\.1\x20500\x20Internal\x20Serv
SF:x20Error\r\ndate:\x20Sat,\x2011\x20May\x202024\x2011:47:03\x20GMT\r\
SF:ua-compatible:\x20IE=edge\r\nx-content-type-options:\x20nosniff\r\nc
SF:ent-length:\x200\r\ncontent-type:\x20text/html;\x20charset=UTF-8\r\n
SF:ict-transport-security:\x20max-age=63072000;\r\nx-xss-protection:\x2
SF:mode=block\r\nx-frame-options:\x20SAMEORIGIN\r\nset-cookie:\x20TYPO3
SF:E=;\x20Expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x2
SF:tpOnly;\x20Secure\r\nconnection:\x20close\r\n\r\n")%r(tor-versions,C
SF:HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\nCache
SF:ntrol:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20text/
SF:l\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20browser
SF:0sent\x20an\x20invalid\x20request\.\n</body></html>\n")%r(RTSPReques
SF:F,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\nCa
SF:-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20te
SF:html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20brow
SF:\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.34 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 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://it.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://it.tuwien.ac.at/fileadmin/*temp*/
- https://it.tuwien.ac.at/typo3/
- https://it.tuwien.ac.at/typo3conf/
- https://it.tuwien.ac.at/typo3/sysext/frontend/Resources/Public/*
- https://it.tuwien.ac.at/404/

[+] 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 it.tuwien.ac.at_nikto

- Target Host: it.tuwien.ac.at
- Target Port: 443
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=63072000;
- GET /: Uncommon header 'x-xss-protection' found, with contents: 1;mode=block
- GET /: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /: Cookie TYPO3MODE created without the secure flag
- GET /: Cookie TYPO3MODE created without the httponly flag
- GET /: Hostname 'it.tuwien.ac.at' does not match certificate's CN 'institute.tuwien.ac.at'
- GET /: Uncommon header 'x-ua-compatible' found, with contents: IE=edge
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- -877: TRACE /: HTTP TRACE method is active, suggesting the host is vulnerable to XST
- -3931: GET /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3931: GET /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.

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**

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**

Dirb scan for it.tuwien.ac.at_dirb

- https://www.it.tuwien.ac.at/1 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/10 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/100 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/1000 (CODE:200|SIZE:233929)
- https://www.it.tuwien.ac.at/101 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/102 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/103 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/11 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/12 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/123 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/13 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/14 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/15 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/2 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/20 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/200 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/21 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/22 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/23 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/24 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/25 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/3 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/30 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/300 (CODE:200|SIZE:233921)

- https://www.it.tuwien.ac.at/32 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/4 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/400 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/401 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/403 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/404 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/42 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/5 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/50 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/500 (CODE:200|SIZE:233921)
- https://www.it.tuwien.ac.at/51 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/6 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/64 (CODE:200|SIZE:233913)
- https://www.it.tuwien.ac.at/7 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/8 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/9 (CODE:200|SIZE:233905)
- https://www.it.tuwien.ac.at/96 (CODE:200|SIZE:233913)