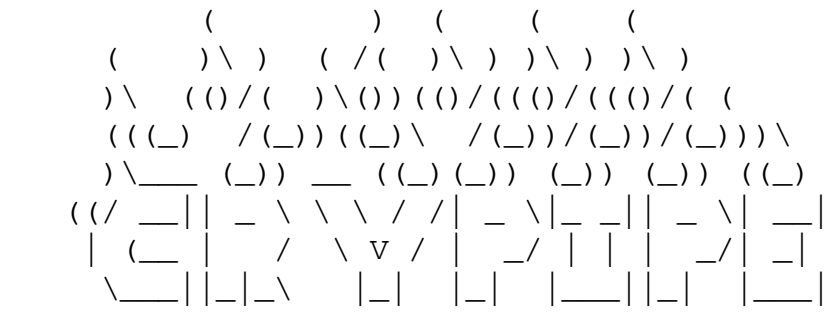

Report for domain tiss.tuwien.ac.at

Nmap report

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

Nmap scan for 128.130.32.110 : ['tiss.tuwien.ac.at', 'www.tiss.tuwien.ac.at', 'prod.tiss.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 21.55 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 tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] Joomla 1.0

[+] Core Joomla Vulnerability

[++] Joomla! 1.0.7 / Mambo 4.5.3 - (feed) Full Path Disclosure / Denial of Service

- EDB : https://www.exploit-db.com/exploits/1698/
- Joomla! 1.0.9 - (Weblinks) Blind SQL Injection
- CVE : CVE-2006-7247
- EDB : https://www.exploit-db.com/exploits/1922/
- Joomla! 1.0.x - 'ordering' Parameter Cross-Site Scripting
- CVE : CVE-2011-0005
- EDB : https://www.exploit-db.com/exploits/35167/
- Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution
- CVE : CVE-2015-8562 , CVE-2015-8566
- EDB : https://www.exploit-db.com/exploits/39033/

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://tiss.tuwien.ac.at/mbl/
- https://tiss.tuwien.ac.at/fpl/
- https://tiss.tuwien.ac.at/course/

- https://tiss.tuwien.ac.at/curriculum/
- https://tiss.tuwien.ac.at/api/
- https://tiss.tuwien.ac.at/

[+] 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 tiss.tuwien.ac.at

- Target Host: tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0xW/1cdc860c619069a652743e1354ea981d
- GET /: Uncommon header 'x-request-id' found, with contents: 78dc8fc3-6c11-4b37-9292-d7d24fe005a7
- GET /: Uncommon header 'x-runtime' found, with contents: 0.478504
- GET /: Uncommon header 'x-download-options' found, with contents: noopen
- GET /: Uncommon header 'x-rack-cors' found, with contents: miss; no-origin
- GET /: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
- GET /: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /: Uncommon header 'link' found, with contents: </assets/application-5c967972c53ee3772fc55f8cc28a99b010c2e6d23a85af13170a0761088a840d.c rel=preload; as=style; nopush,</assets/components-3698f10359890ebdc6df62bdbccdf2527e105c88b29861f9bb7d4503ae09afde.c rel=preload; as=style; nopush,</assets/modules/zur_kenntnisnahme-bd2af1277d94fad5cc3b89ec15c06f86f0eed66886a54a8ea1883e3ba5b1bea4.css>; rel=preload; as=style; nopush,</assets/application_old-b4c55fed69d9e4560bcca046f9718b726d498ac654c7f1bc987980ec210f1471.js>; rel=preload; as=script; nopush,</assets/application-b2f9e2248fdb94e81e51b191a99ab4d1b591f0f7f376da42654a04c89b95355f.js>; rel=preload; as=script; nopush,</assets/modules/zur_kenntnisnahme-915f17214635e2d213c5f667a8ac6f6de4a3acc51bdd25d95146aabc0eb rel=preload; as=script; nopush
- GET /: Uncommon header 'referrer-policy' found, with contents: strict-origin-when-cross-origin
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000;
- GET /: Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
- GET /: Cookie TISS_LANG created without the secure flag
- GET /: Cookie TISS_LANG created without the httponly flag
- GET /: Cookie _tiss_session created without the secure flag
- GET /: Cookie _tiss_session created without the httponly flag
- GET /fpl/: Cookie FPL_SESSID created without the secure flag
- GET /fpl/: Cookie FPL_SESSID created without the httponly flag
- GET /fpl/: Cookie SERVERID created without the secure flag
- GET /fpl/: Cookie SERVERID created without the httponly flag
- GET //fpl/: File/dir '/fpl/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET //course/: File/dir '/course/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

- GET //curriculum/: File/dir '/curriculum/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /api/: Uncommon header 'access-control-allow-origin' found, with contents: *
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 6 entries which should be manually viewed.
- -2946: GET /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3092: GET /access/: /access/: This might be interesting...
- -3092: GET /forum/: /forum/: This might be interesting...
- -3092: GET /library/: /library/: This might be interesting...
- -5107: GET /netutils/findata.stm?host=: /netutils/findata.stm?host=: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?: Cookie PDB_SESSID created without the secure flag
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?: Cookie PDB_SESSID created without the httponly flag
- GET /maintenance/: /maintenance/: Admin login page/section found.

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 tiss.tuwien.ac.at

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

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