

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.  
ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ  
компьютерной безопасности и  
криптографии

**Использование nikto.pl**

ОТЧЕТ ПО ДИСЦИПЛИНЕ

**«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»**

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

Преподаватель

доцент, к.п.н

\_\_\_\_\_  
подпись, дата

А. С. Гераськин

Саратов 2024

Nikto.pl - свободно распространяемый (GPL) сканнер веб серверов, предоставляющий комплексное тестирование веб сервером на разные опасности, включая 6400 потенциально опасных файлов, проверку на актуальность версии для более чем 1200 серверов и выявление проблем, присущих той или иной версии для более чем 270 серверов.

Запуск nikto.pl и обновление его:

```
root@root: /pentest/web/nikto
File Edit View Terminal Help

-mutate+          Guess additional file names
-mutate-options+  Provide extra information for mutations
-output+         Write output to this file
-nocache         Disables the URI cache
-nossl           Disables using SSL
-no404           Disables 404 checks
-port+          Port to use (default 80)
-Plugins+        List of plugins to run (default: ALL)
-root+          Prepend root value to all requests, format is /directory

-ssl             Force ssl mode on port
-Single          Single request mode
-timeout+       Timeout (default 2 seconds)
-Tuning+        Scan tuning
-update         Update databases and plugins from CIRT.net
-vhost+         Virtual host (for Host header)
-Version         Print plugin and database versions
                + requires a value

Note: This is the short help output. Use -H for full help.

root@root:/pentest/web/nikto# ./nikto.pl -update
+ ERROR (302): Unable to get www.cirt.net/nikto/UPDATES/2.1.4/versions.txt
root@root:/pentest/web/nikto#
```

Сканирование с помощью этой программы:

```
root@root: /pentest/web/nikto
File Edit View Terminal Help

root@root:/pentest/web/nikto# ./nikto.pl -host http://192.168.1.38/dvwa
- Nikto v2.1.4

-----
+ Target IP:          192.168.1.38
+ Target Hostname:    192.168.1.38
+ Target Port:        80
+ Start Time:         2024-02-17 11:21:52
-----

+ Server: Apache/2.2.16 (Fedora)
+ Retrieved x-powered-by header: PHP/5.3.3
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ ETag header found on server, inode: 130037, size: 26, mtime: 0x481ddf3a0cd80
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apache
  1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals pot
  entially sensitive information via certain HTTP requests that contain specific QUER
  Y strings.
+ OSVDB-3268: /config/: Directory indexing found.
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
```

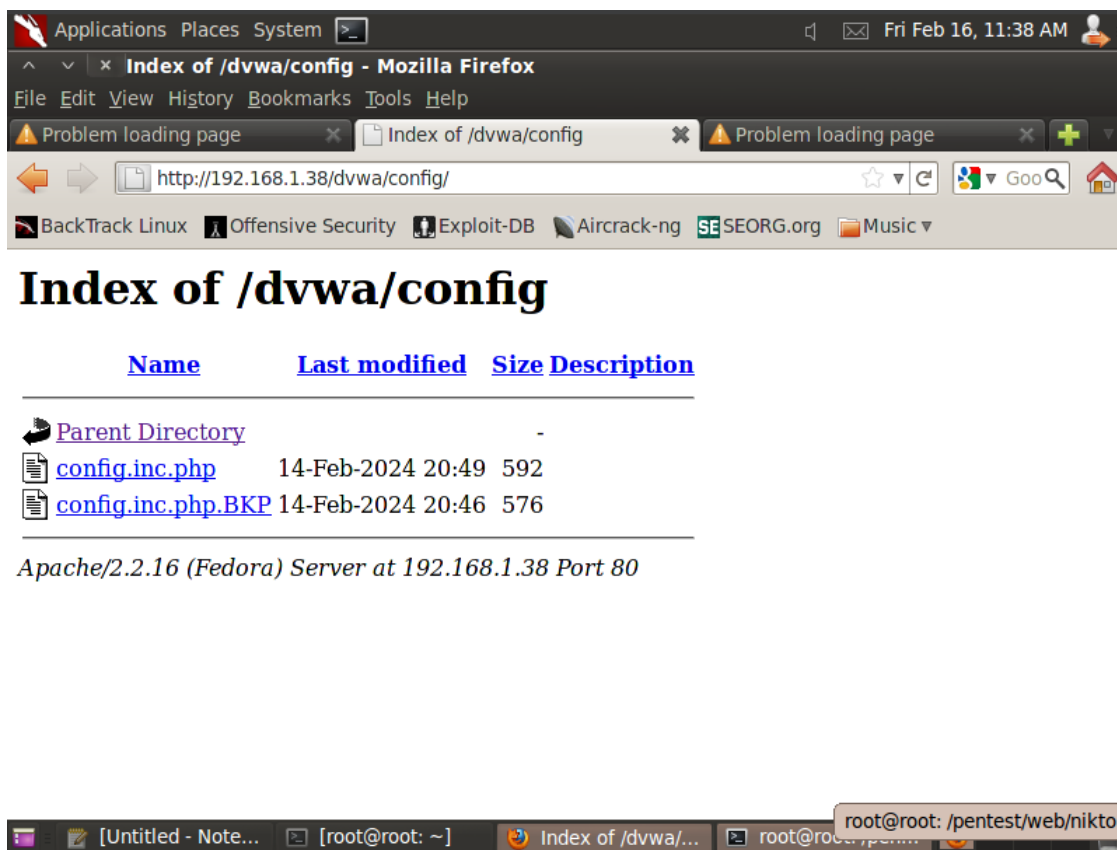
```
root@root: /pentest/web/nikto
File Edit View Terminal Help
+ Start Time: 2024-02-17 11:21:52
-----
+ Server: Apache/2.2.16 (Fedora)
+ Retrieved x-powered-by header: PHP/5.3.3
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ ETag header found on server, inode: 130037, size: 26, mtime: 0x481ddf3a0cd80
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apache
  1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals pot
  entially sensitive information via certain HTTP requests that contain specific QUER
  Y strings.
+ OSVDB-3268: /config/: Directory indexing found.
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ /login.php: Admin login page/section found.
+ 6448 items checked: 3 error(s) and 14 item(s) reported on remote host
+ End Time: 2024-02-17 11:23:04 (72 seconds)
-----
+ 1 host(s) tested
root@root: /pentest/web/nikto#
```

Использование команды telnet для получения сведений о веб ресурсе (OSVDB-877):

```
root@root: /pentest/web/nikto
File Edit View Terminal Help
root@root: /pentest/web/nikto# telnet 192.168.1.38 80
Trying 192.168.1.38...
Connected to 192.168.1.38.
Escape character is '^]'.
GET index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.16 (Fedora) Server at ::1 Port 80</address>
</body></html>
Connection closed by foreign host.
root@root: /pentest/web/nikto#
```



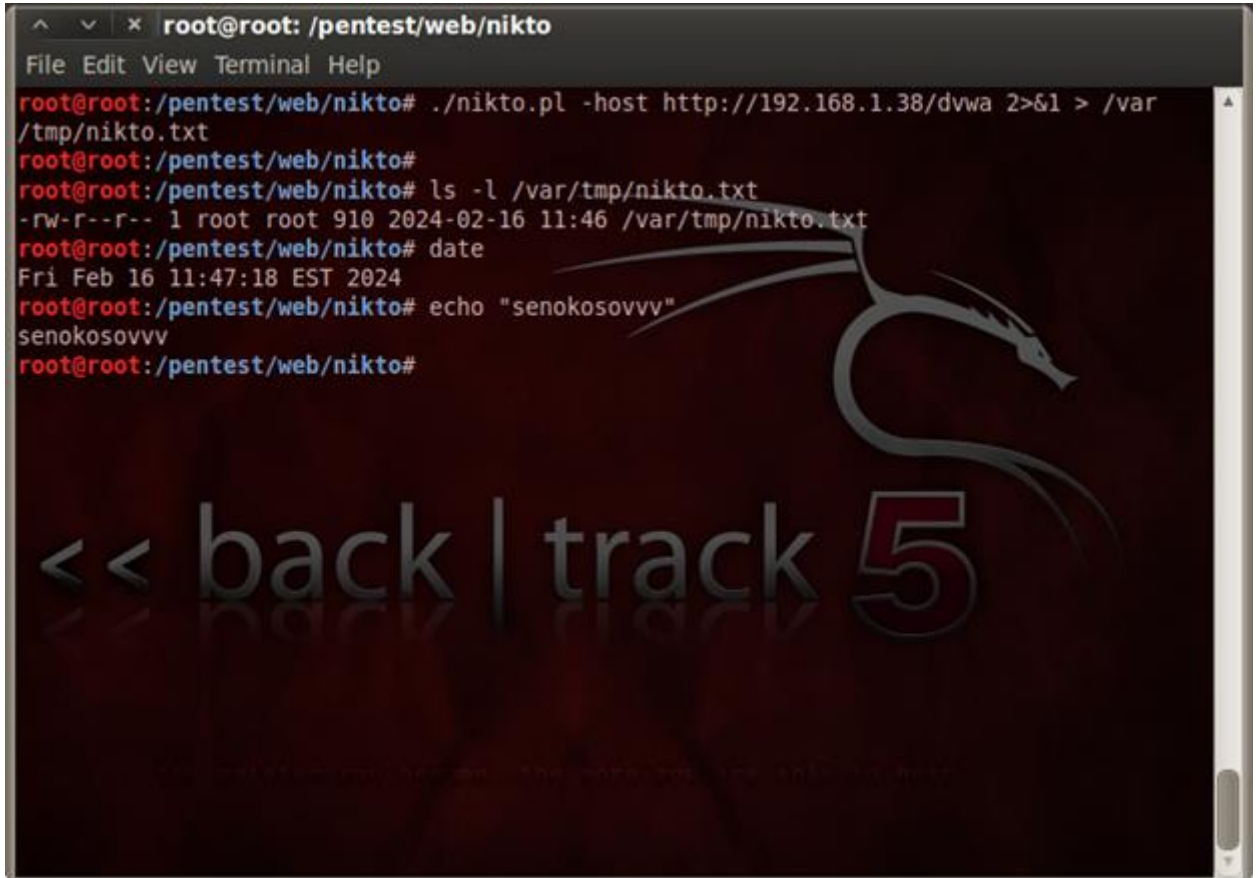
Использование OSVDB-3268 индекс директорий /dvwa/config:



Протестируйте запрос с символом ~  
( http://192.168.1.106/dvwa/config/config.inc.php~):



Отчет о проделанной работе:



```
root@root: /pentest/web/nikto
File Edit View Terminal Help
root@root:/pentest/web/nikto# ./nikto.pl -host http://192.168.1.38/dvwa 2>&1 > /var
/tmp/nikto.txt
root@root:/pentest/web/nikto#
root@root:/pentest/web/nikto# ls -l /var/tmp/nikto.txt
-rw-r--r-- 1 root root 910 2024-02-16 11:46 /var/tmp/nikto.txt
root@root:/pentest/web/nikto# date
Fri Feb 16 11:47:18 EST 2024
root@root:/pentest/web/nikto# echo "senokosovvv"
senokosovvv
root@root:/pentest/web/nikto#
```

<< back | track 5

senokosovvv