T7 - MSc Pool

T-POO-700

PENTESTING REPORT

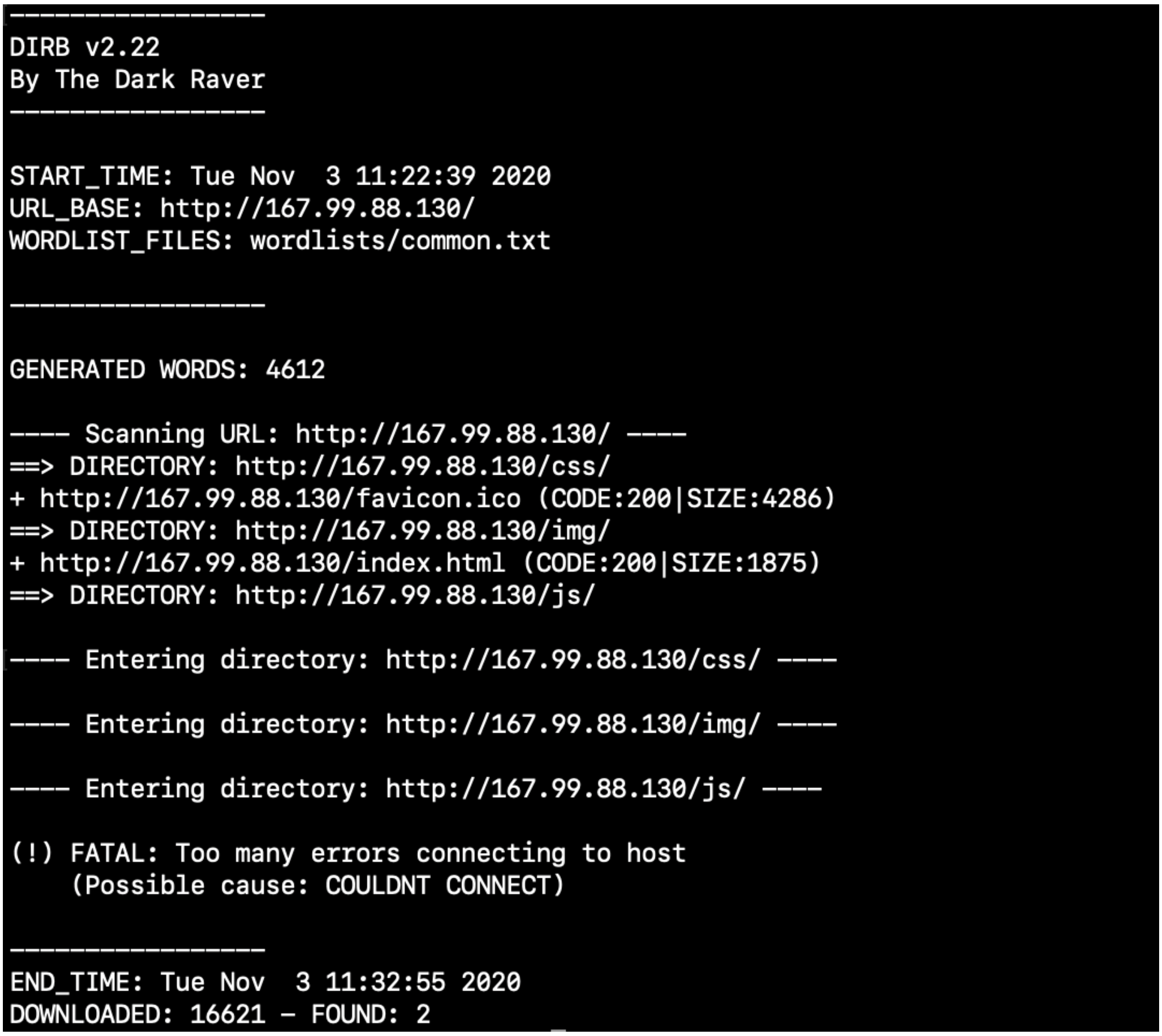
- Risk factor - security

SUMMARY

DIAGNOSTIC

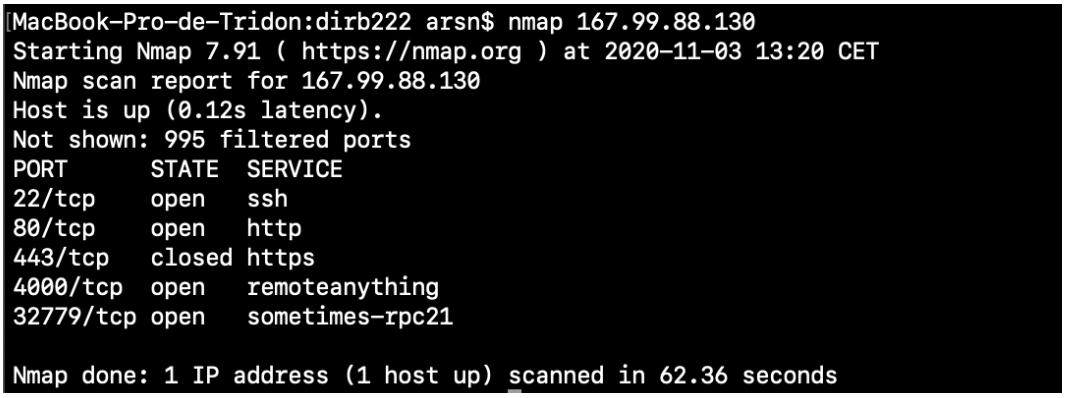
DIRB

WEB CONTENT SCANNER



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

START_TIME: Tue Nov  3 11:22:39 2020
URL_BASE: http://167.99.88.130/
WORDLIST_FILES: wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://167.99.88.130/ ----
==> DIRECTORY: http://167.99.88.130/css/
+ http://167.99.88.130/favicon.ico (CODE:200|SIZE:4286)
==> DIRECTORY: http://167.99.88.130/img/
+ http://167.99.88.130/index.html (CODE:200|SIZE:1875)
==> DIRECTORY: http://167.99.88.130/js/

---- Entering directory: http://167.99.88.130/css/ ----

---- Entering directory: http://167.99.88.130/img/ ----

---- Entering directory: http://167.99.88.130/js/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Tue Nov  3 11:32:55 2020
DOWNLOADED: 16621 - FOUND: 2
```

NMAP



```
[MacBook-Pro-de-Tridon:dirb222 arsn$ nmap 167.99.88.130
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-03 13:20 CET
Nmap scan report for 167.99.88.130
Host is up (0.12s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   closed https
4000/tcp  open   remoteanything
32779/tcp open   sometimes-rpc21

Nmap done: 1 IP address (1 host up) scanned in 62.36 seconds
```

NMAP REPORT

```
PORT        STATE   SERVICE
22/tcp      open    ssh
80/tcp      open    http
443/tcp     closed  https
4000/tcp    open    remoteanything
32779/tcp   open    sometimes-rpc21
```

NESSUS

Which kernel is used by the server?

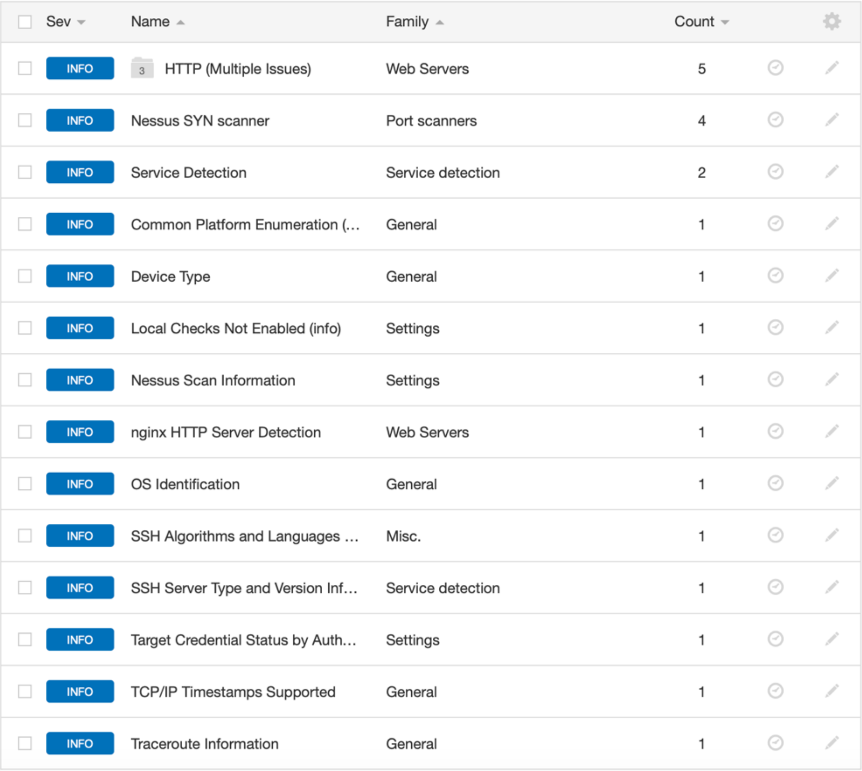
Linux Kernel 2.6

Which OS is used by the server?

Ubuntu 20.04.1 LTS

which version of Apache is used by the server?

nginx 1.16.0



□	Sev	Name	Family	Count
□	INFO	3 HTTP (Multiple Issues)	Web Servers	5
□	INFO	Nessus SYN scanner	Port scanners	4
□	INFO	Service Detection	Service detection	2
□	INFO	Common Platform Enumeration (...	General	1
□	INFO	Device Type	General	1
□	INFO	Local Checks Not Enabled (info)	Settings	1
□	INFO	Nessus Scan Information	Settings	1
□	INFO	nginx HTTP Server Detection	Web Servers	1
□	INFO	OS Identification	General	1
□	INFO	SSH Algorithms and Languages ...	Misc.	1
□	INFO	SSH Server Type and Version Inf...	Service detection	1
□	INFO	Target Credential Status by Auth...	Settings	1
□	INFO	TCP/IP Timestamps Supported	General	1
□	INFO	Traceroute Information	General	1

SQLMAP

REPORT SQLMAP in Risk 3 & Level 3

Duration of the test: 7min

```
python sqlmap.py -u 'http://167.99.88.130?id=1' --risk=3 --level=3
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage caused
by this program

[*] starting @ 15:16:17 /2020-11-03/

[15:16:17] [INFO] testing connection to the target URL
[15:16:17] [INFO] testing if the target URL content is stable
[15:16:17] [INFO] target URL content is stable
[15:16:17] [INFO] testing if GET parameter 'id' is dynamic
[15:16:18] [WARNING] GET parameter 'id' does not appear to be dynamic
[15:16:18] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be
injectable
[15:16:18] [INFO] testing for SQL injection on GET parameter 'id'
[15:16:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:16:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[15:16:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[15:16:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:16:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:16:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[15:16:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[15:16:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:16:27] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:16:29] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL
comment)'
[15:16:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:16:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:16:32] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP
BY clause'
[15:16:33] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
[15:16:35] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
[15:16:37] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[15:16:39] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[15:16:41] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:16:43] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:16:45] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:16:45] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[15:16:45] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter
replace'
[15:16:45] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[15:16:45] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[15:16:45] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[15:16:46] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[15:16:46] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[15:16:46] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[15:16:46] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[15:16:46] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:16:46] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause
(original value)'
[15:16:46] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:16:46] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[15:16:46] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[15:16:47] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
```

```
[15:16:47] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[15:16:48] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[15:16:49] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries
(IF)'
[15:16:49] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:16:51] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:16:52] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:16:53] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:16:55] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:16:56] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:16:58] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:16:59] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[15:17:01] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[15:17:02] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[15:17:03] [INFO] testing 'PostgreSQL OR error-based - WHERE or HAVING clause'
[15:17:05] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[15:17:06] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(IN)'
[15:17:07] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONVERT)'
[15:17:09] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONVERT)'
[15:17:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONCAT)'
[15:17:11] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONCAT)'
[15:17:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[15:17:14] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (XMLType)'
[15:17:15] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:17:16] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:17:18] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:17:19] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[15:17:20] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[15:17:21] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[15:17:23] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[15:17:24] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[15:17:25] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[15:17:27] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[15:17:27] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[15:17:27] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[15:17:27] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[15:17:27] [INFO] testing 'Oracle error-based - Parameter replace'
[15:17:27] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[15:17:28] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[15:17:28] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[15:17:28] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[15:17:30] [INFO] testing 'Generic inline queries'
[15:17:30] [INFO] testing 'MySQL inline queries'
[15:17:30] [INFO] testing 'PostgreSQL inline queries'
[15:17:31] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[15:17:31] [INFO] testing 'Oracle inline queries'
[15:17:31] [INFO] testing 'SQLite inline queries'
[15:17:31] [INFO] testing 'Firebird inline queries'
[15:17:31] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[15:17:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[15:17:33] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[15:17:34] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[15:17:34] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[15:17:35] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[15:17:36] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[15:17:37] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:17:37] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[15:17:38] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:17:39] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[15:17:39] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[15:17:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[15:17:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[15:17:42] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
```

```
[15:17:43] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[15:17:45] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[15:17:46] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[15:17:47] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'
[15:17:47] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'
[15:17:48] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP - comment)'
[15:17:49] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (heavy query)'
[15:17:50] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (heavy query)'
[15:17:51] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[15:17:53] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[15:17:54] [INFO] testing 'MySQL AND time-based blind (ELT)'
[15:17:55] [INFO] testing 'MySQL OR time-based blind (ELT)'
[15:17:57] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:17:58] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind'
[15:17:59] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[15:18:00] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'
[15:18:02] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[15:18:03] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[15:18:04] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'
[15:18:06] [INFO] testing 'Oracle AND time-based blind'
[15:18:07] [INFO] testing 'Oracle OR time-based blind'
[15:18:08] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[15:18:10] [INFO] testing 'Oracle OR time-based blind (heavy query)'
[15:18:11] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[15:18:12] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'
[15:18:14] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[15:18:15] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[15:18:16] [INFO] testing 'Informix AND time-based blind (heavy query)'
[15:18:17] [INFO] testing 'Informix OR time-based blind (heavy query)'
[15:18:19] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[15:18:20] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[15:18:20] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
(substraction)'
[15:18:20] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:18:20] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[15:18:20] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[15:18:20] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:18:21] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:18:21] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[15:18:21] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[15:18:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:18:28] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[15:18:31] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:18:34] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:18:37] [WARNING] GET parameter 'id' does not seem to be injectable
[15:18:37] [INFO] testing if parameter 'User-Agent' is dynamic
[15:18:37] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[15:18:37] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be
injectable
[15:18:37] [INFO] testing for SQL injection on parameter 'User-Agent'
[15:18:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:18:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[15:18:41] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[15:18:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:18:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:18:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[15:18:45] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[15:18:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:18:47] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:18:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL
comment)'
[15:18:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:18:50] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:18:51] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP
BY clause'
[15:18:52] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
[15:18:54] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
```

```
[15:18:56] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[15:18:58] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[15:19:00] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:19:01] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:19:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:19:04] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[15:19:04] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter
replace'
[15:19:04] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[15:19:04] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[15:19:04] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[15:19:04] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[15:19:05] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[15:19:05] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[15:19:05] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[15:19:05] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:19:05] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause
(original value)'
[15:19:05] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:19:05] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[15:19:05] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[15:19:05] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[15:19:05] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[15:19:07] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[15:19:08] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries
(IF)'
[15:19:08] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:19:10] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:19:11] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:19:12] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:19:14] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:19:15] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:19:17] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:19:18] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[15:19:19] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[15:19:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[15:19:21] [INFO] testing 'PostgreSQL OR error-based - WHERE or HAVING clause'
[15:19:23] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[15:19:24] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(IN)'
[15:19:25] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONVERT)'
[15:19:27] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONVERT)'
[15:19:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONCAT)'
[15:19:30] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONCAT)'
[15:19:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[15:19:32] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (XMLType)'
[15:19:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:19:35] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:19:36] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:19:38] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[15:19:39] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[15:19:40] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[15:19:42] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[15:19:43] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[15:19:44] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[15:19:45] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[15:19:45] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[15:19:46] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[15:19:46] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[15:19:46] [INFO] testing 'Oracle error-based - Parameter replace'
[15:19:46] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[15:19:46] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
```

```
[15:19:46] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[15:19:46] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[15:19:47] [INFO] testing 'Generic inline queries'
[15:19:47] [INFO] testing 'MySQL inline queries'
[15:19:47] [INFO] testing 'PostgreSQL inline queries'
[15:19:47] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[15:19:47] [INFO] testing 'Oracle inline queries'
[15:19:47] [INFO] testing 'SQLite inline queries'
[15:19:47] [INFO] testing 'Firebird inline queries'
[15:19:47] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[15:19:48] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[15:19:49] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[15:19:50] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[15:19:51] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[15:19:52] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[15:19:52] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[15:19:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:19:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[15:19:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:19:55] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[15:19:56] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[15:19:56] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[15:19:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[15:20:00] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[15:20:01] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[15:20:02] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[15:20:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[15:20:04] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'
[15:20:05] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'
[15:20:06] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP - comment)'
[15:20:07] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (heavy query)'
[15:20:08] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (heavy query)'
[15:20:09] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[15:20:11] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[15:20:12] [INFO] testing 'MySQL AND time-based blind (ELT)'
[15:20:13] [INFO] testing 'MySQL OR time-based blind (ELT)'
[15:20:14] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:20:16] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind'
[15:20:17] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[15:20:18] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'
[15:20:20] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[15:20:21] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[15:20:22] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'
[15:20:23] [INFO] testing 'Oracle AND time-based blind'
[15:20:25] [INFO] testing 'Oracle OR time-based blind'
[15:20:26] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[15:20:27] [INFO] testing 'Oracle OR time-based blind (heavy query)'
[15:20:29] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[15:20:30] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'
[15:20:31] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[15:20:33] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[15:20:34] [INFO] testing 'Informix AND time-based blind (heavy query)'
[15:20:35] [INFO] testing 'Informix OR time-based blind (heavy query)'
[15:20:37] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[15:20:38] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[15:20:38] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
(substraction)'
[15:20:38] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:20:38] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[15:20:38] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[15:20:38] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:20:38] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:20:38] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[15:20:39] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
[15:20:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:20:41] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[15:20:44] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:20:47] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:20:49] [WARNING] parameter 'User-Agent' does not seem to be injectable
[15:20:49] [INFO] testing if parameter 'Referer' is dynamic
[15:20:49] [WARNING] parameter 'Referer' does not appear to be dynamic
[15:20:49] [WARNING] heuristic (basic) test shows that parameter 'Referer' might not be
injectable
[15:20:49] [INFO] testing for SQL injection on parameter 'Referer'
[15:20:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

```
[15:20:51] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[15:20:54] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[15:20:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:20:56] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[15:20:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[15:20:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[15:20:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:20:59] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:21:01] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL
comment)'
[15:21:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:21:02] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access
comment)'
[15:21:04] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP
BY clause'
[15:21:05] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
[15:21:06] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause (MAKE_SET)'
[15:21:09] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[15:21:10] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[15:21:13] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:21:14] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:21:17] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:21:17] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[15:21:17] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter
replace'
[15:21:17] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[15:21:17] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[15:21:17] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[15:21:17] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[15:21:17] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[15:21:18] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[15:21:18] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[15:21:18] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:21:18] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause
(original value)'
[15:21:18] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[15:21:18] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[15:21:18] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[15:21:18] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[15:21:18] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[15:21:20] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[15:21:20] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries
(IF)'
[15:21:21] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:21:22] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:21:24] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:21:25] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
[15:21:26] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:21:27] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
[15:21:29] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
[15:21:30] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[15:21:31] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[15:21:32] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[15:21:33] [INFO] testing 'PostgreSQL OR error-based - WHERE or HAVING clause'
[15:21:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[15:21:36] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(IN)'
[15:21:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONVERT)'
[15:21:39] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONVERT)'
[15:21:40] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (CONCAT)'
```

```
[15:21:41] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause
(CONCAT)'
[15:21:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[15:21:44] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (XMLType)'
[15:21:45] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:21:46] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[15:21:48] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[15:21:49] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[15:21:50] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[15:21:52] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[15:21:53] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[15:21:54] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[15:21:56] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[15:21:57] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[15:21:57] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[15:21:57] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[15:21:57] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[15:21:57] [INFO] testing 'Oracle error-based - Parameter replace'
[15:21:57] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[15:21:57] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[15:21:58] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[15:21:58] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[15:21:58] [INFO] testing 'Generic inline queries'
[15:21:58] [INFO] testing 'MySQL inline queries'
[15:21:58] [INFO] testing 'PostgreSQL inline queries'
[15:21:59] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[15:21:59] [INFO] testing 'Oracle inline queries'
[15:21:59] [INFO] testing 'SQLite inline queries'
[15:21:59] [INFO] testing 'Firebird inline queries'
[15:21:59] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[15:22:00] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[15:22:01] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[15:22:02] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[15:22:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[15:22:03] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[15:22:04] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[15:22:04] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[15:22:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[15:22:06] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[15:22:07] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[15:22:07] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[15:22:08] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[15:22:09] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[15:22:10] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[15:22:11] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[15:22:13] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[15:22:14] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[15:22:15] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'
[15:22:15] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'
[15:22:16] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP - comment)'
[15:22:17] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (heavy query)'
[15:22:18] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (heavy query)'
[15:22:19] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[15:22:20] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[15:22:22] [INFO] testing 'MySQL AND time-based blind (ELT)'
[15:22:23] [INFO] testing 'MySQL OR time-based blind (ELT)'
[15:22:24] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[15:22:25] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind'
[15:22:27] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[15:22:30] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'
[15:22:31] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[15:22:33] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'
[15:22:34] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'
[15:22:35] [INFO] testing 'Oracle AND time-based blind'
[15:22:37] [INFO] testing 'Oracle OR time-based blind'
[15:22:38] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[15:22:40] [INFO] testing 'Oracle OR time-based blind (heavy query)'
[15:22:41] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[15:22:43] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'
[15:22:44] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[15:22:45] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[15:22:47] [INFO] testing 'Informix AND time-based blind (heavy query)'
[15:22:48] [INFO] testing 'Informix OR time-based blind (heavy query)'
[15:22:49] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[15:22:50] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
```

```
[15:22:50] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
(substraction)'
[15:22:50] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:22:51] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[15:22:51] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[15:22:51] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:22:51] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:22:51] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[15:22:51] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
[15:22:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:22:54] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[15:22:56] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:22:59] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:23:02] [WARNING] parameter 'Referer' does not seem to be injectable
[15:23:02] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase
values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that
there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use
option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 15:23:02 /2020-11-03/
```

NIKTO

- which flag performs XSS injections tests? -Tuning 4

```
./nikto.pl -h 167.99.88.130 -Tuning 4
- Nikto v2.1.6
--------------------------------------------------------------------
-------
+ Target IP:          167.99.88.130
+ Target Hostname:    167.99.88.130
+ Target Port:        80
+ Start Time:         2020-11-03 16:20:03 (GMT1)
--------------------------------------------------------------------
-------
+ Server: nginx/1.16.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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.
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @CKEDITOR   val:/
Var: @CKEDITOR   val:/ckeditor/
Var: @CKEDITOR   val:/admin/ckeditor/
Var: @CKEDITOR   val:/sites/all/modules/ckeditor/
Var: @CKEDITOR   val:/resources/ckeditor/
Var: @CKEDITOR   val:/clientscript/ckeditor/
Var: @CKEDITOR   val:/wp-content/plugins/ckeditor-for-
wordpress/ckeditor/
+ 1020 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2020-11-03 16:20:42 (GMT1) (39 seconds)
--------------------------------------------------------------------
-------
+ 1 host(s) tested
```

GENERAL NIKTO REPORT

```
./nikto.pl -h http://167.99.88.130
- Nikto v2.1.6
--------------------------------------------------------------------
-------
+ Target IP:          167.99.88.130
+ Target Hostname:    167.99.88.130
+ Target Port:        80
+ Start Time:         2020-11-03 15:55:31 (GMT1)
--------------------------------------------------------------------
-------
+ Server: nginx/1.16.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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.
+ No CGI Directories found (use '-C all' to force check all possible
dirs)

+ 8106 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2020-11-03 16:00:52 (GMT1) (321 seconds)
--------------------------------------------------------------------
-------
+ 1 host(s) test
```

ANALYSIS & SOLUTIONS

NETWORK

NMAP ANALYSIS

When you read the nmap analysis, we can see the following ports open :

```
PORT         STATE    SERVICE
22/tcp       open     ssh
80/tcp       open     http
443/tcp      closed   https
4000/tcp     open     remoteanything
32779/tcp    open     sometimes-rpc21
```

Only the port 4000 is visible, so we change the configuratio of the docker-compose file and now you have this result :

```
docker-compose ps

      Name                         Command               State
Ports
--------------------------------------------------------------------
--------------------------------
api                 mix phx.server                  Up
0.0.0.0:32782->4000/tcp
app                 nginx -g daemon off;            Up
0.0.0.0:443->443/tcp, 0.0.0.0:80->80/tcp
time_manager_db_1   docker-entrypoint.sh postgres   Up
0.0.0.0:32781->5432/tcp
```

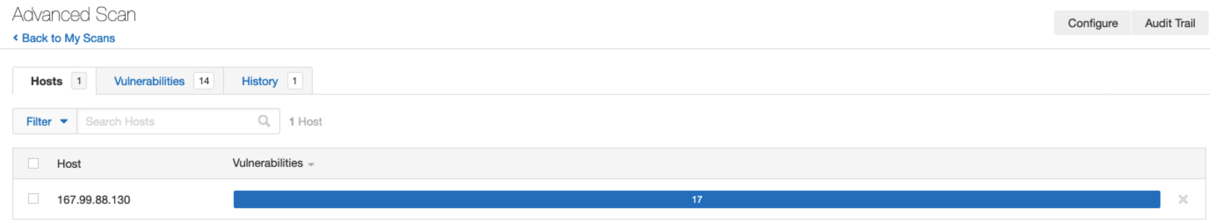
With a "docker-compose ps", we can see the redirection of the port 5432 (postgresql) in 32781 and the redirection of the port 4000 (phoenix) to 32782.

And when you make a new nmap analysis you have the following answer :

```
nmap 167.99.88.130
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-04 12:59 CET
Nmap scan report for 167.99.88.130
Host is up (0.095s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   closed https
32781/tcp open   unknown
32782/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 23.03 second
```

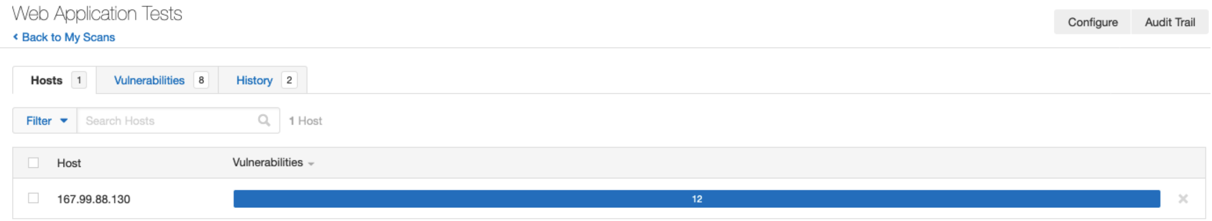
NESSUS ANALYSIS

We made 2 additional tests with Nessus, one was an advanced scan of the network and system vulnerability,



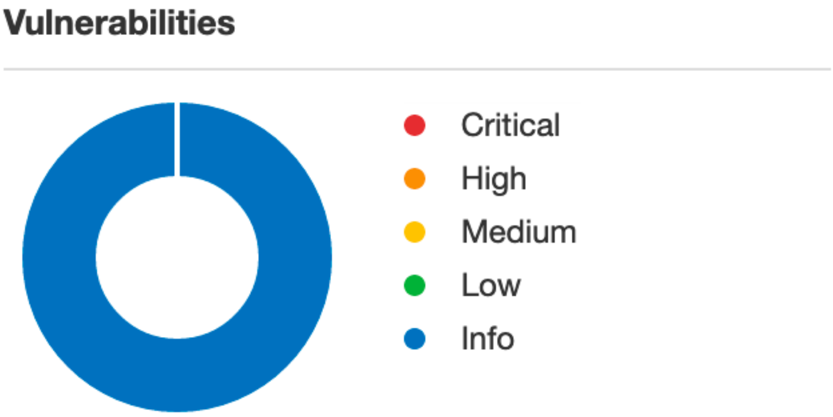
□	Host	Vulnerabilities ▾	
□	167.99.88.130	17	×

and the other one was a Web Applications Tests,



□	Host	Vulnerabilities ▾	
□	167.99.88.130	12	×

We didn't find any vulnerabilities on the both report, only "info" with basic informations. No critical or something else.



APPLICATION

– **are they injectable (XSS, Script, HTML, . . .)?**

Tuning 4: Injection (XSS/Script/HTML)

```
./nikto.pl -h http://167.99.88.130 -Tuning 4
- Nikto v2.1.6
--------------------------------------------------------------------
-------
+ Target IP:          167.99.88.130
+ Target Hostname:    167.99.88.130
+ Target Port:        80
+ Start Time:         2020-11-04 10:08:45 (GMT1)
--------------------------------------------------------------------
-------
+ Server: nginx/1.16.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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.
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: name    val:Nikto
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @MAGENTO    val:/
Var: @MAGENTO    val:/magento/
Var: @MAGENTO    val:/shop/
Var: @CKEDITOR   val:/
Var: @CKEDITOR   val:/ckeditor/
Var: @CKEDITOR   val:/admin/ckeditor/
Var: @CKEDITOR   val:/sites/all/modules/ckeditor/
Var: @CKEDITOR   val:/resources/ckeditor/
Var: @CKEDITOR   val:/clientscript/ckeditor/
Var: @CKEDITOR   val:/wp-content/plugins/ckeditor-for-
wordpress/ckeditor/
+ 1020 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2020-11-04 10:09:26 (GMT1) (41 seconds)
--------------------------------------------------------------------
-------
+ 1 host(s) tested
```

- **are they vulnerable to sql injections, nosql?**

```
[10:12:54] [CRITICAL] connection dropped or unknown HTTP status code received. sqlmap is going to retry the request(s)
[10:12:54] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[10:12:58] [WARNING] GET parameter 'id' does not seem to be injectable
[10:12:58] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment')
```

- **are there accessible configuration files?**

Plugins 1: Test all files with all root directories

```
./nikto.pl -h http://167.99.88.130 -Plugins 1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          167.99.88.130
+ Target Hostname:    167.99.88.130
+ Target Port:        80
+ Start Time:         2020-11-04 10:32:01 (GMT1)
---------------------------------------------------------------------------
+ Server: nginx/1.16.0
+ 239 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2020-11-04 10:32:10 (GMT1) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- **are password hashes difficult to break?**

Yes, bcrypt with a salt.

- **are routes accessible by unauthorized users?**

No.

- **are endpoints accessible by unauthorized users?**

No.

- **is it possible to fill the database and cause a denial of service when rendering the page?**

Tuning 6: Denial of Service

```
./nikto.pl -h http://167.99.88.130 -Tuning 6 -C all
- Nikto v2.1.6
--------------------------------------------------------------------
-------
+ Target IP:          167.99.88.130
+ Target Hostname:    167.99.88.130
+ Target Port:        80
+ Start Time:         2020-11-04 11:22:08 (GMT1)
--------------------------------------------------------------------
-------
+ Server: nginx/1.16.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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.
+ 2385 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2020-11-04 11:23:40 (GMT1) (92 seconds)
--------------------------------------------------------------------
-------
+ 1 host(s) tested
```

- **are JWT tokens http-only? If not, how to recover these tokens?**

we don't have a JWT Tokens, instead we have a Bearer Token. Most common, it's a JWT with an XSS.

- **are the passwords sent in clear? If so how do you recover them?**

Yes, our passwords are send in clear, but it's in HTTPS, so their are protected by the protocols.

- **is the application available only in https? if not, how could a malicious user intercept a client's requests to your server?**

Yes, the application is only in HTTPS.

Between the test phase of the tuesday 4th november, and the next day. We implement the HTTPS protocol, to prevent big vulnerabilities. It resolved a lot of problems. That's the major security additional content of the project, with the port hidding.