Password Attack: Dictionary Attack

Using dictionary attacks

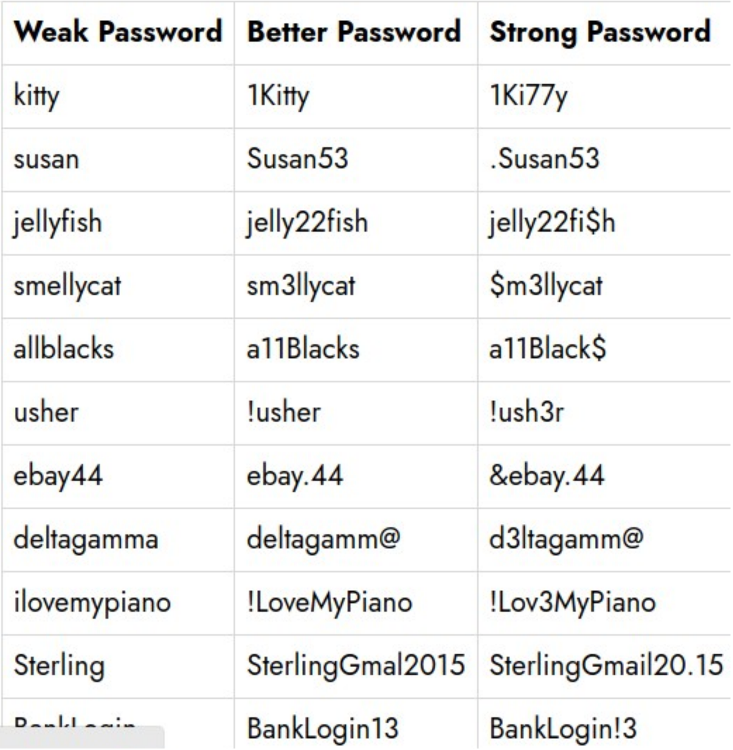
In this Lesson, we will examine dictionary or wordlist attacks. A dictionary attack uses a predetermined set of passwords and attempts to brute-force a password match for a given user against the wordlist. There are three types of dictionary lists that are generally generated:

- Username Only: Lists that contain generated usernames only
- Password Only: Lists that contain generated passwords only
- Username and Password Lists: Lists that contain both generated usernames and passwords

NB: Never use "password" as your password. A surprising number of people make this mistake.

Dictionary hacking tools that use an English dictionary list easily find words in that dictionary. If the simple word doesn't give access to an account, the device modifies the submission and tries other iterations of the same word.

Password-guessing tools submit hundreds or thousands of words per minute. If a password is anything close to a dictionary word, it's incredibly insecure. When a password does not resemble any regular word patterns, it takes longer for the repetition tool to guess it.



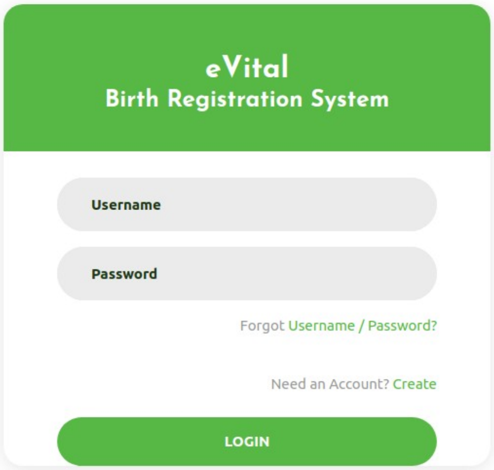
Weak Password	Better Password	Strong Password
kitty	1Kitty	1Ki77y
susan	Susan53	.Susan53
jellyfish	jelly22fish	jelly22fi$h
smellycat	sm3llycat	$m3llycat
allblacks	a11Blacks	a11Black$
usher	!usher	!ush3r
ebay44	ebay.44	&ebay.44
deltagamma	deltagamm@	d3ltagamm@
ilovemypiano	!LoveMyPiano	!Lov3MyPiano
Sterling	SterlingGmal2015	SterlingGmail20.15
BankLogin	BankLogin13	BankLogin!3

Other simple but complex to guess passwords;

- dOG.lov3r
- i7ovemydog!!
- d0gsaremybestfr13nds
- sn00pdoggyd0G
- Karm@beatsDogm@
- C@ts-and-Dogs-Living-together
- Dog.lov3r

In this Lesson we will do a dictionary Attack using popular hacking tool Burp Suite , Download it from https://portswigger.net/burp/communitydownload its available in Kali linux Distribution.

Consider below application.(Link to the application to be Provided to students).

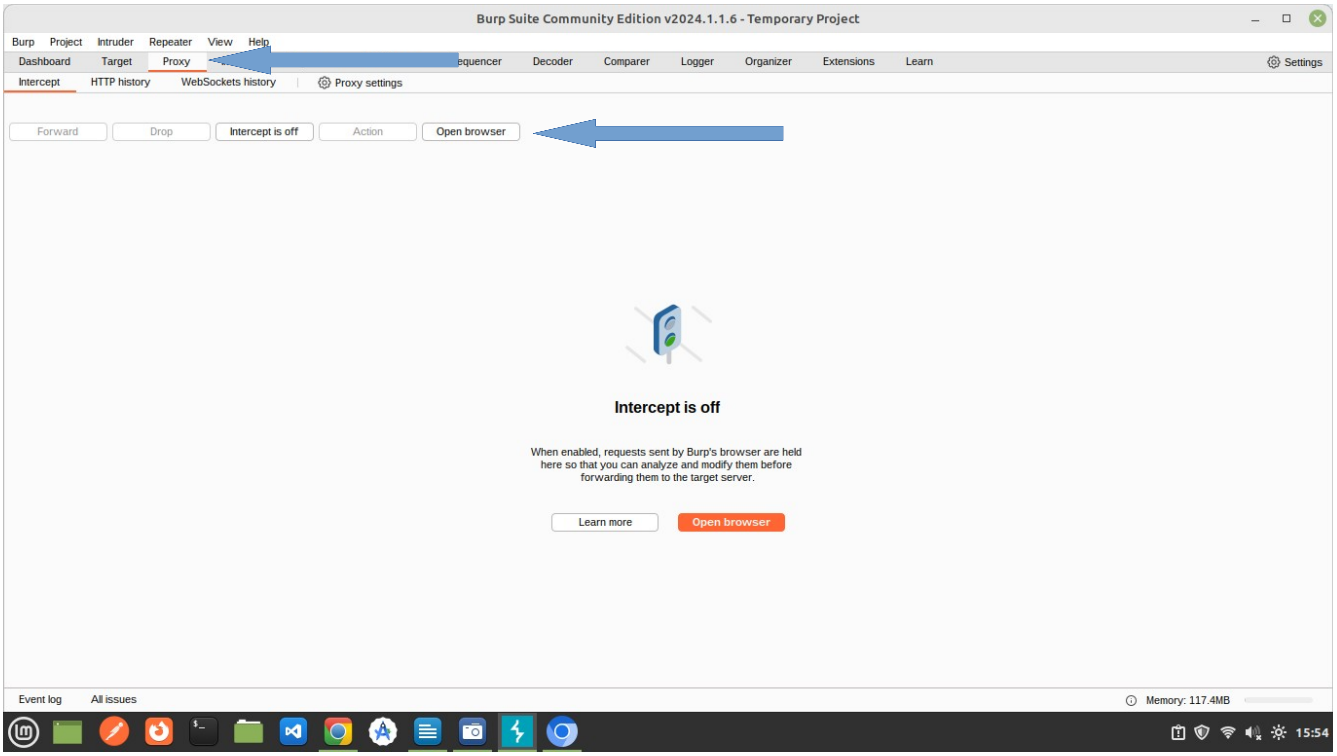


Can you try to login to the system? Did you manage to guess the passwords used? , You will try to hack above system using Dictionary Attack.

See Next Page for Practicals

Practical.

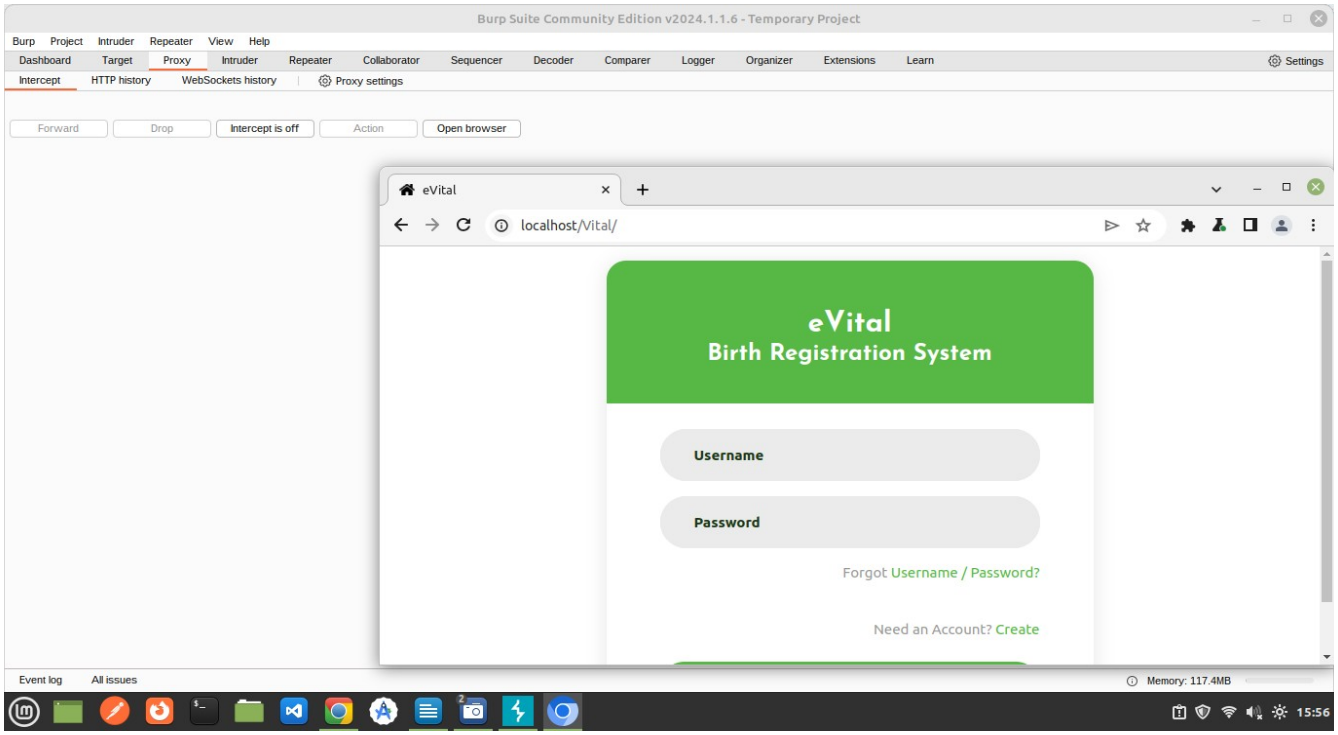
Start Burp Suite and Locate **Proxy**,   Then Click **Open Browser**


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy equencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Learn more
Open browser
Event log All issues
Memory: 117.4MB
15:54

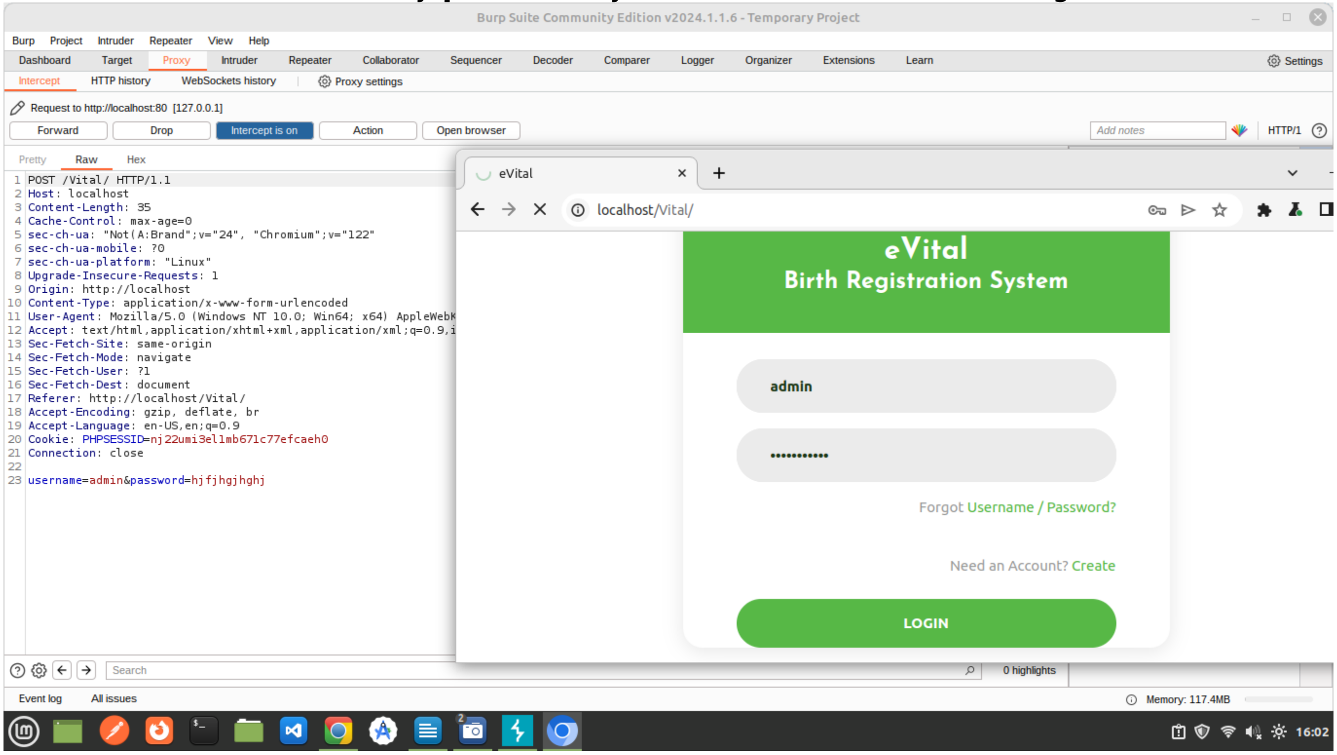
Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

On the browser that opens enter Link to eVital System , You'll have something similar to below screen. For this Practice you will use a remote Link(e.g http://192.168.43.78/Vital/) not Localhost to access eVital (Link to be provided)


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
eVital
localhost/Vital/
eVital
Birth Registration System
Username
Password
Forgot Username / Password?
Need an Account? Create
Event log All issues
Memory: 117.4MB
15:56

Ow, Set the **Intercept On** in Burp Suite, then on the browser open inn burp suite, type username as **admin** and any **password** you know.(Guess) and click Login.


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
Search
0 highlights
Event log All issues
Memory: 117.4MB
16:02

Request to http://localhost:80 [127.0.0.1]

```
POST /Vital/ HTTP/1.1
Host: localhost
Content-Length: 35
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/Vital/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=nj22umi3el1mb671c77efcaeh0
Connection: close

username=admin&password=hjfjhgjhghj
```

eVital

localhost/Vital/

eVital
Birth Registration System

admin

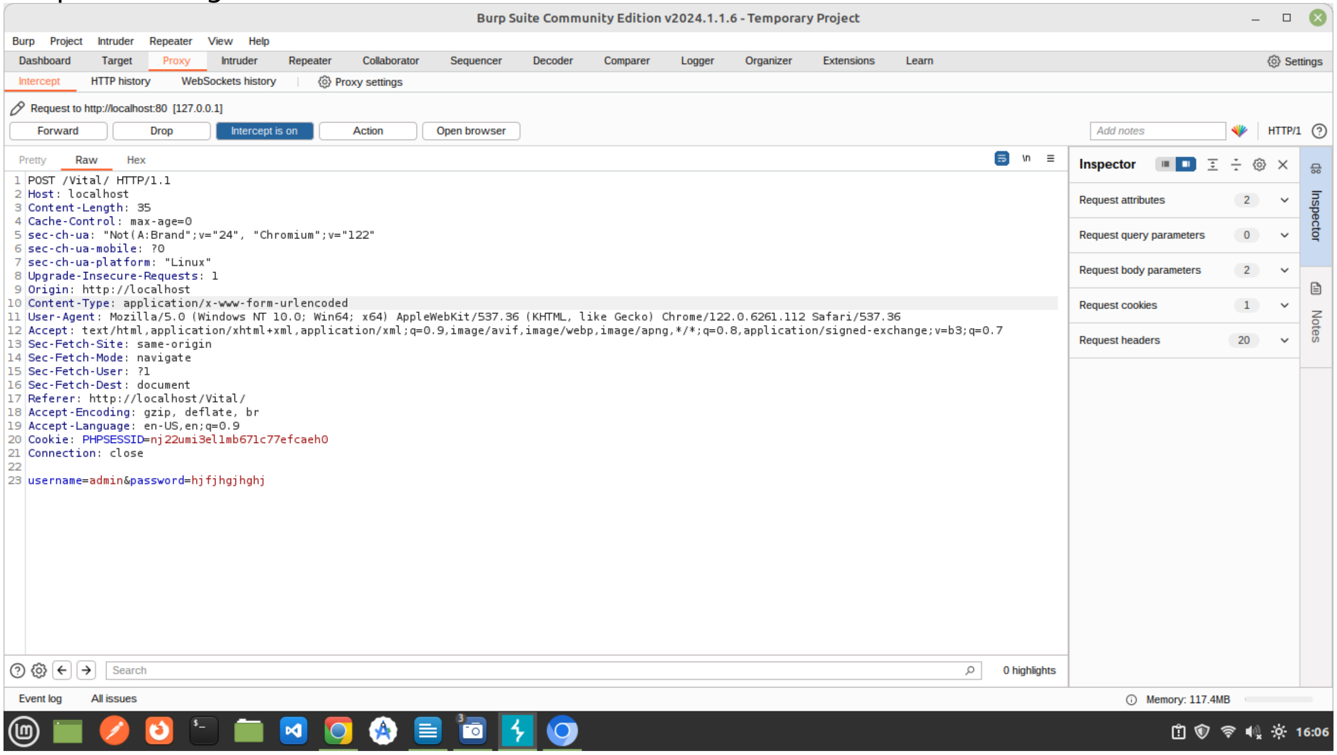
•••••••••••

Forgot Username / Password?

Need an Account? Create

LOGIN

In the Above Screen, we see on the Left, Burp Suite has captured the Request we Sent. We cam locate the username and password you submitted. Correct? Below is the Response we get.


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 117.4MB
16:06

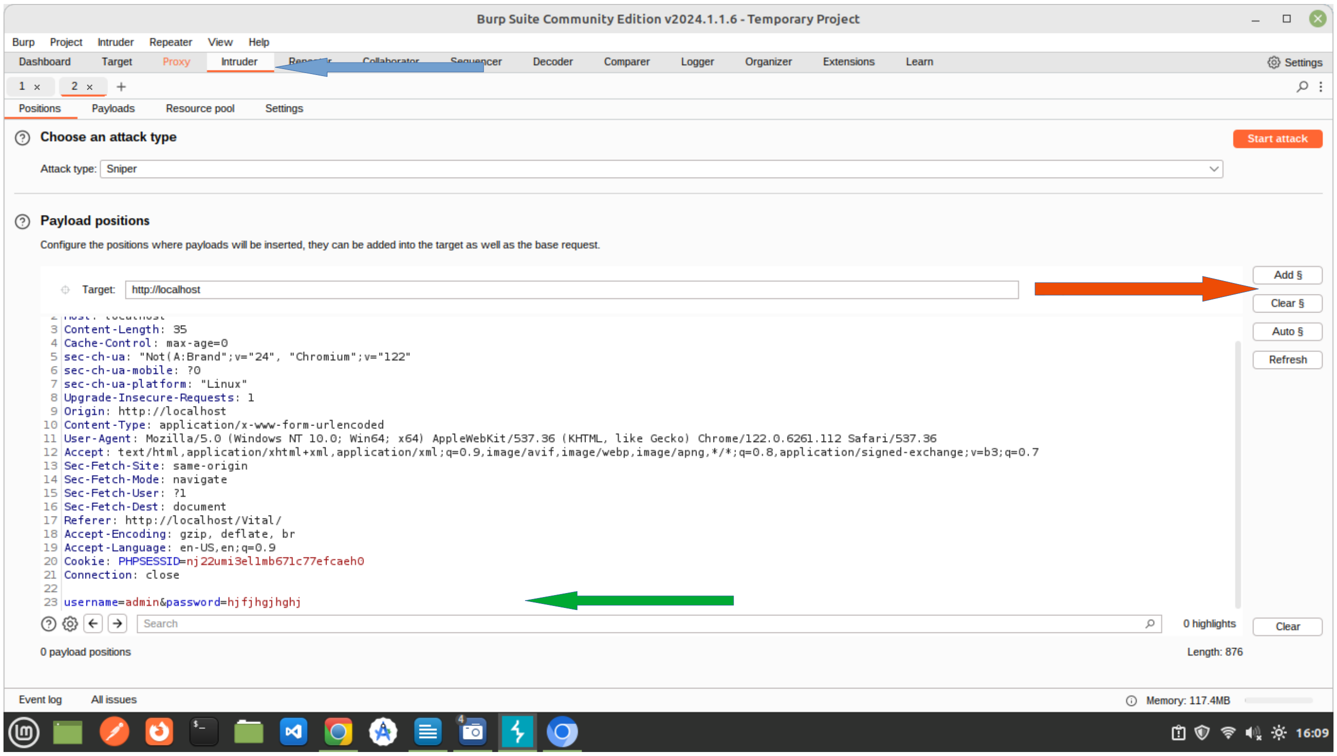
Request to http://localhost:80 [127.0.0.1]

```
POST /Vital/ HTTP/1.1
Host: localhost
Content-Length: 35
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/Vital/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=nj22umi3el1mb671c77efcaeh0
Connection: close

username=admin&password=hjfjhgjhghj
```

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	20

In above screen, right click and **send to intruder,** then click on the **Intruder Tab** in Burp Suite as shown below. You can still see the username and password in the Intruder.


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear
0 highlights
Event log All issues
Memory: 117.4MB
16:09

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

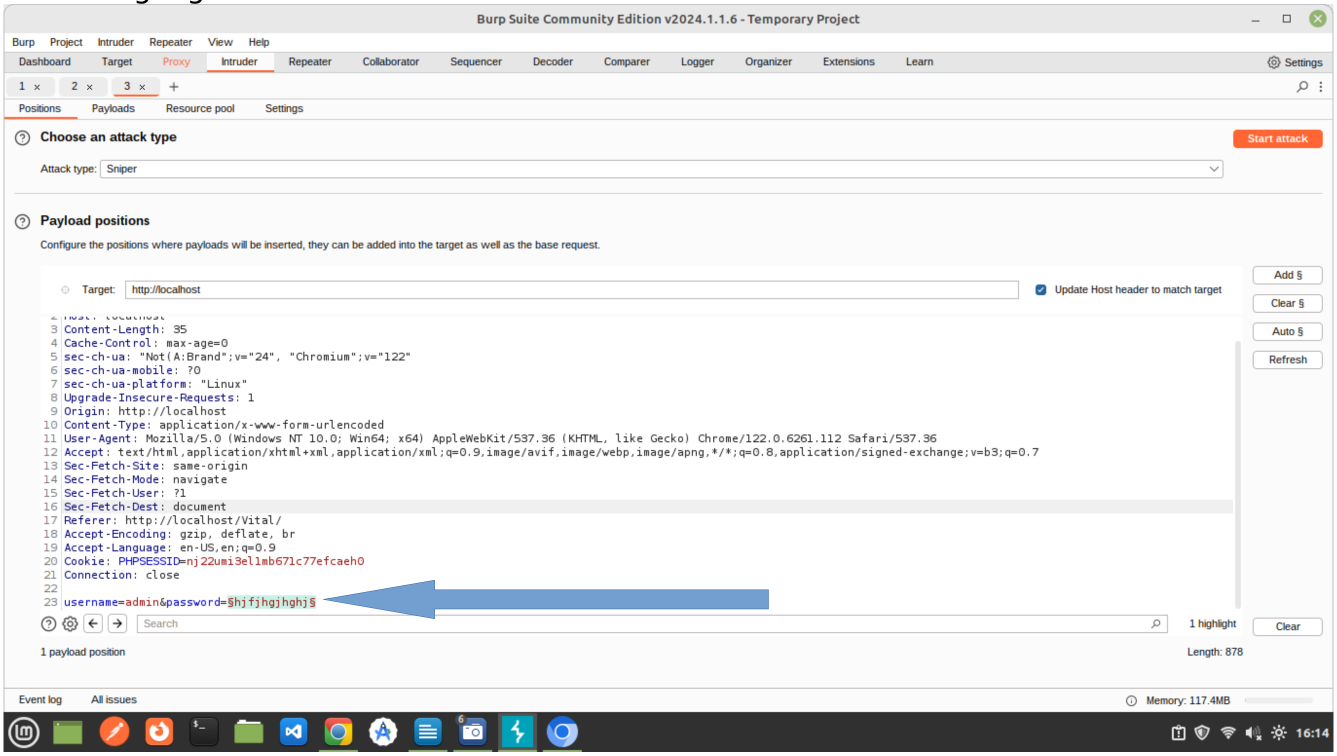
```
Host: localhost
Content-Length: 35
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/Vital/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=nj22umi3el1mb671c77efcaeh0
Connection: close

username=admin&password=hjfjhgjhghj
```

0 payload positions

Length: 876

Next, On the Right side shown in red arrow click on Clear, then double click on the Password value shown in Green Arrow, then Click Add shown in Red Arrow. The Password is now highlighted as shown below Blue Arrow


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear
1 highlight
Event log All issues
Memory: 117.4MB
16:14

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost ☑ Update Host header to match target

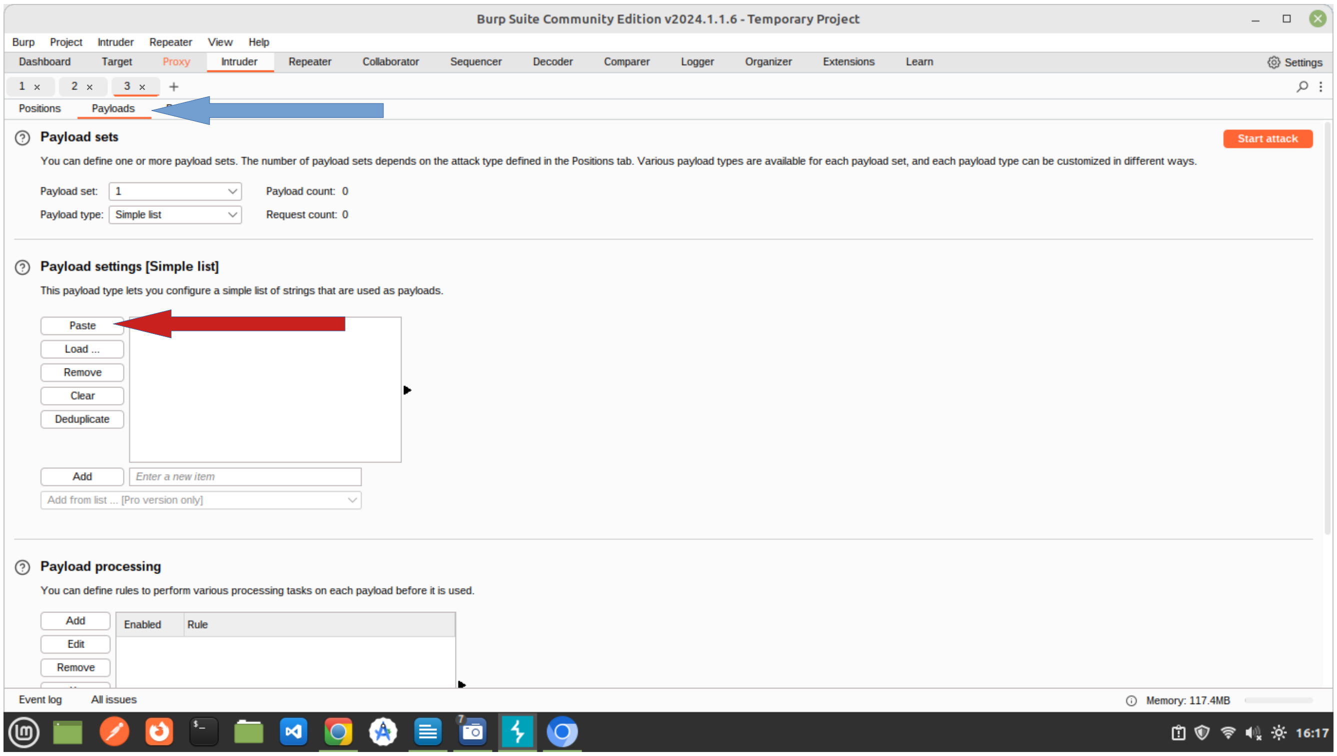
```
Host: localhost
Content-Length: 35
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/Vital/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=nj22umi3el1mb671c77efcaeh0
Connection: close

username=admin&password=§hjfjhgjhghj§
```

1 payload position

Length: 878

We selected the password only meaning our Intruder will only provide a dictionary of passwords not usernames. For username we use **admin,** This will try username admin combined with a List of Passwords. Next click on Payloads Tab as shown below Red Arrow. You can get sample password from the Link. https://justpaste.it/eka2m We got the password from 200 widely used passwords in 2023, see this LINK https://mailsafi.com/blog/top-200-most-common-passwords/


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 × +
Positions Payloads
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled Rule
Event log All issues
Memory: 117.4MB
16:17

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 0

Payload type: Simple list Request count: 0

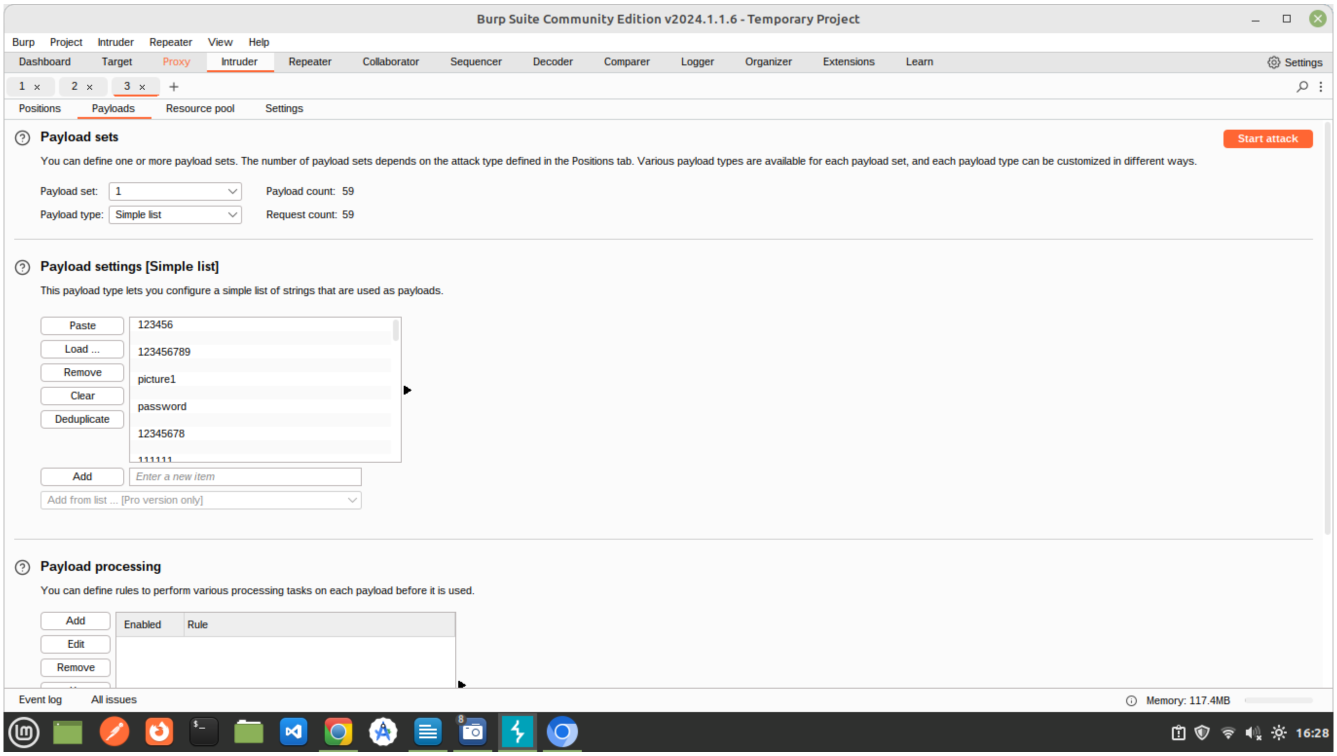
Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Below shows the pasted passwords.


Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 × +
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled Rule
Event log All issues
Memory: 117.4MB
16:28

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 59

Payload type: Simple list Request count: 59

Payload settings [Simple list]

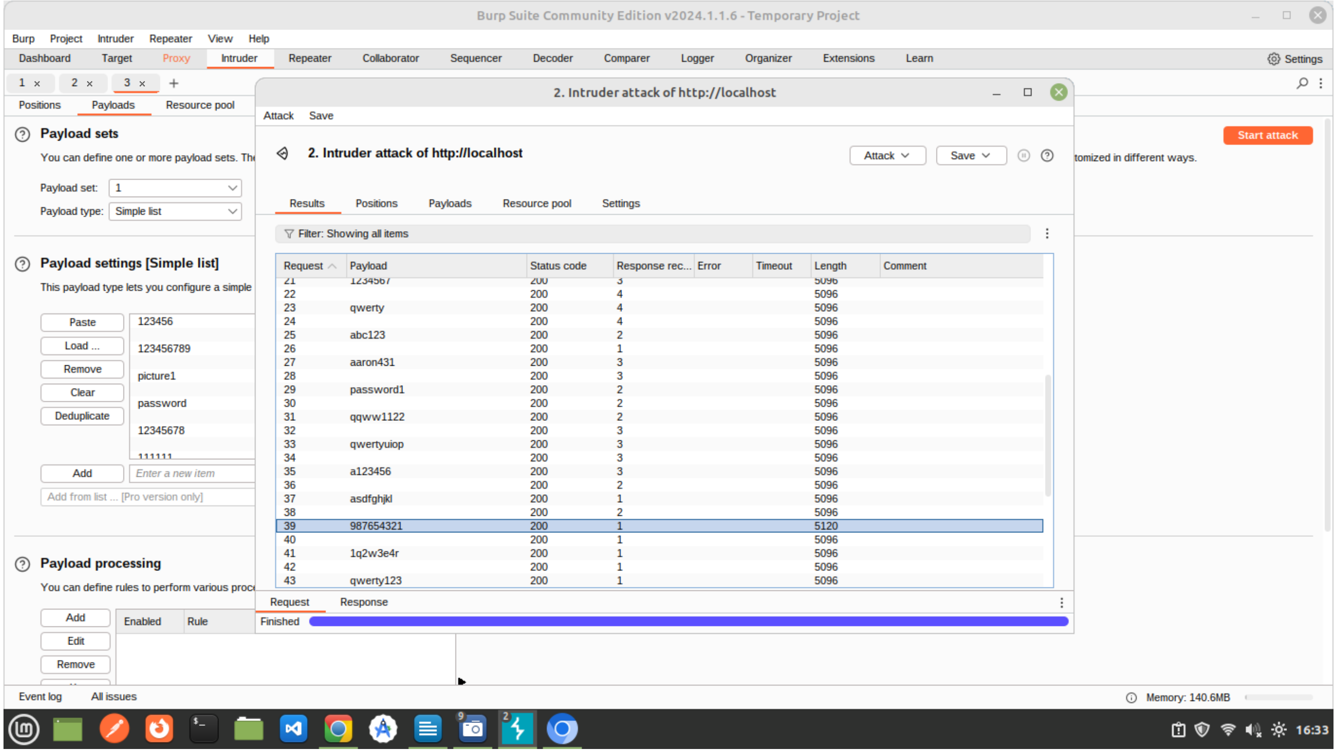
This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
123456789
picture1
password
12345678
111111
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Click on **Start Attack.** Shown in **Orange Button**. The intruder tries username **admin** with all passwords in our list we pasted(Dictionary). I get below screen showing that all passwords were tested.



Burp Suite Community Edition v2024.1.1.6 - Temporary Project

2. Intruder attack of http://localhost

Filter: Showing all items

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
21	1234567	200	3			5096	
22		200	4			5096	
23	qwerty	200	4			5096	
24		200	4			5096	
25	abc123	200	2			5096	
26		200	1			5096	
27	aaron431	200	3			5096	
28		200	3			5096	
29	password1	200	2			5096	
30		200	2			5096	
31	qqww1122	200	2			5096	
32		200	3			5096	
33	qwertyuiop	200	3			5096	
34		200	3			5096	
35	a123456	200	3			5096	
36		200	2			5096	
37	asdfghjkl	200	1			5096	
38		200	2			5096	
39	987654321	200	1			5120	
40		200	1			5096	
41	1q2w3e4r	200	1			5096	
42		200	1			5096	
43	qwerty123	200	1			5096	

Finished

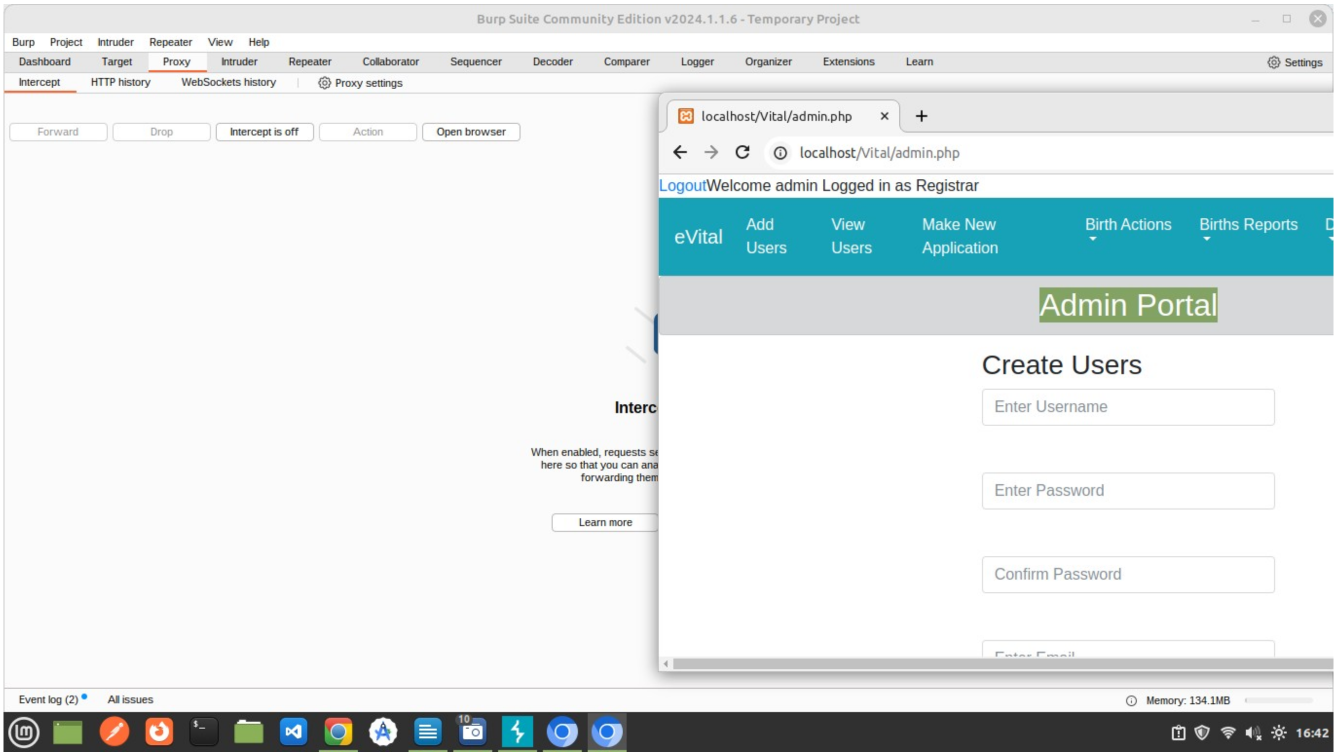
In above screen we assumed that there was an **admin** username, and we provided a dictionary of passwords, To interpret the Results in above screen, we see all passwords were tested and majority show a length of 5096 or 5095 (This is the response length after trying a given password). But one of the password has a different length of 5120? Why?

Argument: Could it be 5096 has the Majority because its wrong password, majority of passwords are wrong? Then 5120 is for a right answer because its the only one? Remember the right password can only be one for admin.

Lets try to login the system with username **admin** and password **987654321**. At this point you can t**urn off the intercept** from **Proxy Tab.**

Credentials worked. We were able to Login eVital with username **admin** and password **987654321**. This is how Hackers gain access to systems that have weak passwords like **987654321.**

See Next screen, we can access data in **eVital System admin portal.** This shows that eVital has failed to keep the users data **Confidential** in **CIA triad.**



Burp Suite Community Edition v2024.1.1.6 - Temporary Project

localhost/Vital/admin.php

LogoutWelcome admin Logged in as Registrar

Countermeasures
To avoid dictionary attacks below countermeasures can be put into prcatice.
Minimum Password Age:
The users must change the password after some time (90 days). This will reduce the risk of password cracking.

Stronger authentication method: Use stronger authentication methods such as enable Gmail one time password feature to login in a new device.

Different passwords: Use different passwords for different device or websites.

Sharing passwords: Do not share passwords with anyone or change password immediately after usage, if shared.

Storing passwords: Avoid storing passwords in an unsecured location such as desktop or mobile phones. Try to remember the passwords.

Personal Information: Do not use personal information such as date of birth, pet names, vehicle number, etc. An attacker can easily guess the password by knowing personal details through social engineering.
Login trials: The system should provide a capability to lock out users after 3 failed attempts.
Strong Passwords: Use strong passwords
Check https://www.security.org/how-secure-is-my-password/

TODO below Strong password checker.
https://github.com/modcomlearning/CyberCodes/blob/master/passwordCheck.py

Useful Links
https://www.techtarget.com/searchsecurity/definition/dictionary-attack
https://en.wikipedia.org/wiki/Dictionary_attack