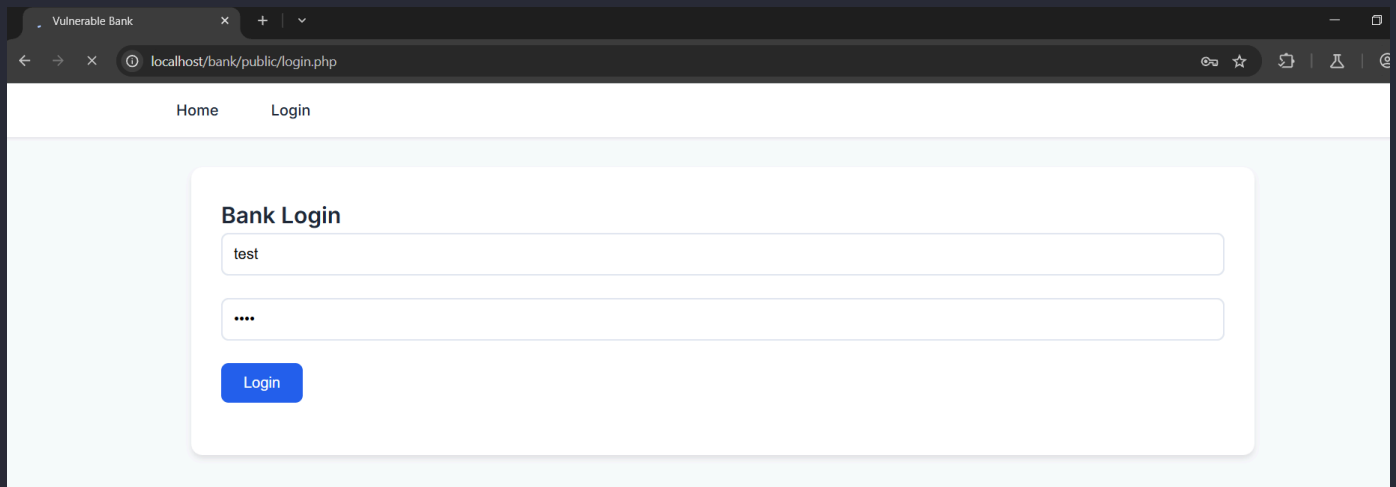


Brute Force Attack Report

Part 1: Performing the Brute Force Attack

Capturing the Login Request

1. Navigate to the Vulnerable Bank login page: `http://localhost/bank/public/login.php`
2. Enter test credentials
 - Username: `test`
 - Password: `test`



3. Click the "Login" button .
4. Burp Suite will intercept the request.



5. Right-click on the intercepted request and select "Send to Intruder"

[Burp](#)
[Project](#)
[Intruder](#)
[Repeater](#)
[View](#)
[Help](#)

[Dashboard](#)
[Target](#)
[Proxy](#)
[Intruder](#)
[Repeater](#)
[Collaborator](#)
[Sequencer](#)
[Decod](#)

[Intercept](#)
[HTTP history](#)
[WebSockets history](#)
[Match and replace](#)
[Proxy settings](#)

Intercept on
 Forward
 Drop

Time	Type	Direction	Method	URL
06:48:49 15 M...	HTTP	→ Request	POST	http://localhost/bank/public/login.php

Request

Pretty
 Raw
 Hex

```

1 POST /bank/public/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 27
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not.A/Brand";v="99", "Chromi
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
  
```

http://localhost/bank/public/login.php
 Add to scope
 Forward
 Drop
 Add notes
 Highlight
 Don't intercept requests
 Do intercept
 Scan
 Send to Intruder Ctrl+I
 Send to Repeater Ctrl+R
 Send to Sequencer
 Send to Organizer Ctrl+O
 Send to Comparer
 Request in browser

Setting Up the Intruder Attack

- Add placeholders for request parameters .
- Select Cluster Bomb Attack .

⚡ Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.3.4 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Lea

1 x 2 x **3 x** +

? Cluster bomb attack Start attack

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

Positions Add \$ Clear \$ Auto \$

```
1 POST /bank/public/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 27
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/bank/public/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=tot5lblnn2vpaink9vqrhp4ner
21 Connection: keep-alive
22
23 username=$test$&password=$test$
```

Loading Wordlists

- Specifying payload for username .
- Specifying payload for password .

Payloads



Payload position: 1 - test

Payload type: Simple list

Payload count: 7

Request count: 35

Payload configuration



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

Paste

Load...

Remove

Clear

Deduplicate

admin123

user1

user2

user3

user4

admin

Add

Enter a new item

Add from list... [Pro version only]

Payloads

Payload position:

2 - test

Payload type:

Simple list

Payload count:

5

Request count:

35

Payload configuration

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

Paste

Load...

Remove

Clear

Deduplicate

123

password

0123

helloworld

admin123

Add

Enter a new item

Add from list... [Pro version only]

Running the Attack

- Successful login attempt will have a different status code .
- Redirection to `dashboard.php` page .

Attack
Save
2. Intruder attack of http://localhost
Attack
Save

Results
Positions

Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
24	user1	helloworld	200	20			6115	
25	user2	helloworld	200	20			6115	
26	user3	helloworld	200	20			6115	
27	user4	helloworld	200	19			6115	
28	admin	helloworld	200	17			6115	
29				15			6115	
30	admin123	admin123	200	18			6115	
31	user1	admin123	200	14			6115	
32	user2	admin123	200	12			6115	
33	user3	admin123	200	13			6115	
34	user4	admin123	200	13			6115	
35	admin	admin123	302	21			399	

Request
Response

Pretty
Raw
Hex
Render

```

1 HTTP/1.1 302 Found
2 Date: Thu, 15 May 2025 03:56:38 GMT
3 Server: Apache/2.4.62 (Win64) PHP/8.3.14 mod_fcgid/2.3.10-dev
4 X-Powered-By: PHP/8.3.14
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: /dashboard.php
9 Content-Length: 1
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14

```

Part 2: Implementing Security Measures

1. Failed Login Attempts Tracking

- Create a database table to log all login attempts, including successful and failed ones:

```
// Create table if it doesn't exist

$create_table = "CREATE TABLE login_attempts (

    id INT AUTO_INCREMENT PRIMARY KEY,

    username VARCHAR(50) NOT NULL,

    ip_address VARCHAR(45) NOT NULL,

    success TINYINT(1) DEFAULT 0,

    attempt_time DATETIME NOT NULL

)";

// Track failed attempts

function checkLoginAttempts($conn, $username, $ip) {

    // Check if there are too many failed login attempts

    $lockout_time = 15 * 60; // 15 minutes lockout

    $max_attempts = 3; // Max 3 failed attempts

```

```

$query = "SELECT COUNT(*) as attempts FROM login_attempts

        WHERE (ip_address = '$ip' OR username = '$username')

        AND success = 0

        AND attempt_time > DATE_SUB(NOW(), INTERVAL $lockout_time SECOND)";

$result = mysqli_query($conn, $query);

$data = mysqli_fetch_assoc($result);

return $data['attempts'] >= $max_attempts;
}

function logLoginAttempt($conn, $username, $ip, $success) {

    $success_val = $success ? 1 : 0;

    $query = "INSERT INTO login_attempts (username, ip_address, success, attempt_time)

            VALUES ('$username', '$ip', $success_val, NOW())";

    mysqli_query($conn, $query);
}

```

2. Account Lockout Mechanism

- temporary account lockout after a specific number of failed login attempts:
-

```

// Account Lockout after multiple failed attempts

if (checkLoginAttempts($conn, $username, $ip)) {

    $error = "Too many failed login attempts. Please try again later.";
} else {

    // Process login attempt

    // ...

}

```

Part 3: Verifying the Fixes

- Failed Attempt Even Though username and password are right .
- no redirection for `dashboard.php` .
- `login_attempts` table in database .

6. Intruder attack of http://localhost

Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
36	admin	012345678	200	13			6151	
37	user1	admin123	200	20			6151	
38	user2	admin123	200	23			6151	
39	user3	admin123	200	26			6151	
40	user4	admin123	200	25			6151	
41	user5	admin123	200	26			6151	
42	admin	admin123	200	31			6151	

Request Response

Pretty Raw Hex Render

Home Login

Bank Login

Too many failed login attempts. Please try again later.

Username

Password

Login

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all Number of rows: 25 Filter rows: Search this table Sort by key: None

Extra options

			id	username	ip_address	success	attempt_time
<input type="checkbox"/>	Edit	Copy	Delete	1	test	127.0.0.1	0 2025-05-15 07:21:26
<input type="checkbox"/>	Edit	Copy	Delete	2	user1	127.0.0.1	0 2025-05-15 07:21:26
<input type="checkbox"/>	Edit	Copy	Delete	3	user2	127.0.0.1	0 2025-05-15 07:21:26

Check all With selected: Edit Copy Delete Export