

[New issue](#)[Jump to bottom](#)

Bypass account protection #524

[Open](#) gozan10 opened this issue 21 days ago · 0 comments

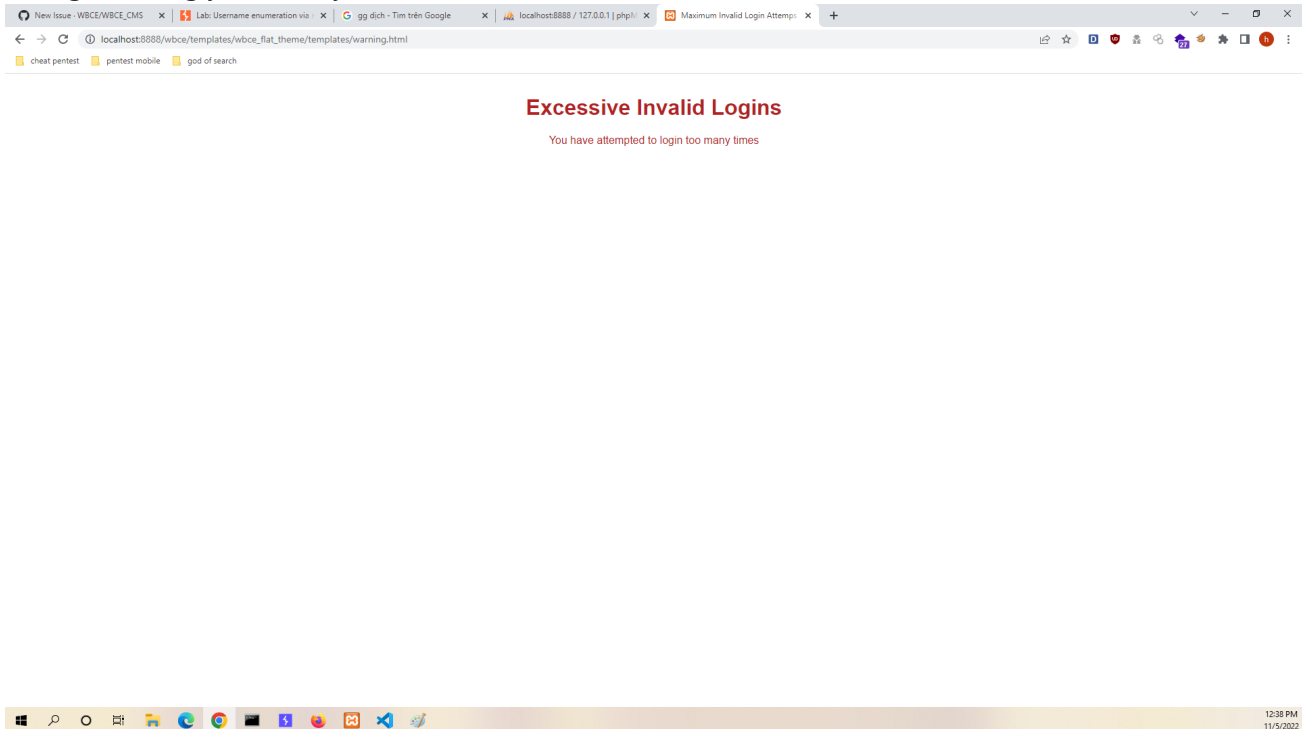
gozan10 commented 21 days ago

Hi team,

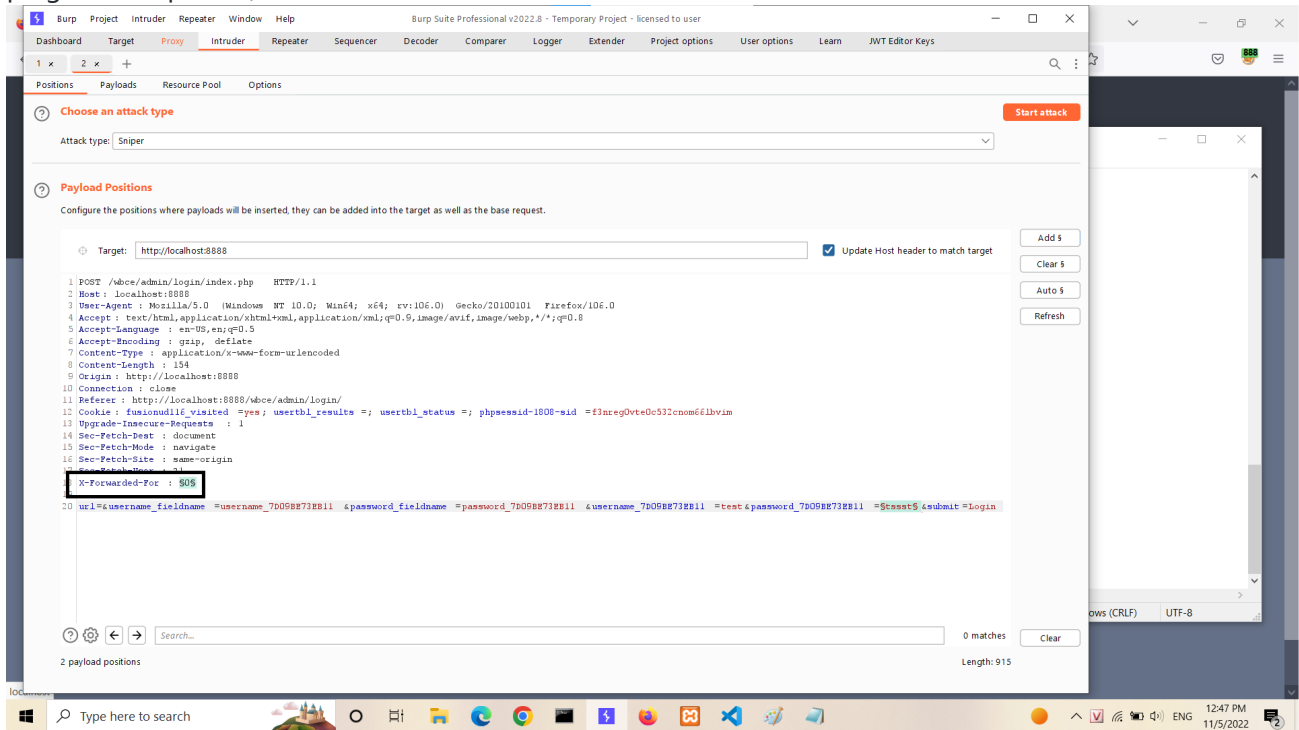
I found a way to bypass account protection (not blocked when brute-force account).

Step: *this is demo some cases

1. If I log in wrongly too many times, it will be locked



2. But i can pass it by insert X-Forwarded-For header, then brute-force without being locked (use intruder plugin of burp suite)



3. set payload to brute-force and start attack

The image displays two screenshots of the Burp Suite Professional v2022.8 interface, showing the configuration of a brute-force attack.

Top Screenshot: Payload Options [Numbers]

- Dashboard:** Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, Learn, JWT Editor Keys.
- Positions:** Payloads, Resource Pool, Options.
- 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. **Start attack** button.
- Payload set:** 1
- Payload count:** 100
- Payload type:** Numbers
- Request count:** 100
- Payload Options [Numbers]:** This payload type generates numeric payloads within a given range and in a specified format.
 - Number range:**
 - Type: ☒ Sequential ☐ Random
 - From: 1
 - To: 100
 - Step: 1
 - How many:
 - Number format:**
 - Base: ☒ Decimal ☐ Hex
 - Min integer digits:
 - Max integer digits:
 - Min fraction digits:
 - Max fraction digits: 0
 - Examples:**
1
987654321
- Payload Processing:** You can define rules to perform various processing tasks on each payload before it is used.

Bottom Screenshot: Payload Options [Simple list]

- Dashboard:** Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, Learn, JWT Editor Keys.
- Positions:** Payloads, Resource Pool, Options.
- 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. **Start attack** button.
- Payload set:** 2
- Payload count:** 100
- Payload type:** Simple list
- Request count:** 100
- Payload Options [Simple list]:** This payload type lets you configure a simple list of strings that are used as payloads.
 - Buttons:** Paste, Load ..., Remove, Clear, Deduplicate, Add, Add from list ...
 - Items:** carlos, root, admin, test, guest, info, adm, user, administrator
- Payload Processing:** You can define rules to perform various processing tasks on each payload before it is used.
 - Buttons:** Add, Edit, Remove, Up, Down
 - Rule:**

Attack

Save

Columns

Results

Positions

Payloads

Resource Pool

Options

4. Intruder attack of http://localhost:8888 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
48	48	test123	302			390	
57	57	*****	302			390	
58	58	george	302			390	
0			200			3067	
1	1	123456	200			3067	
2	2	password	200			3067	
3	3	12345678	200			3067	
4	4	qwerty	200			3067	
5	5	123456789	200			3067	
6	6	12345	200			3067	
7	7	1234	200			3067	

Request

Response

Pretty

Raw

Hex

Render

HTTP/1.1 302 Found

Server: Apache/2.4.54 (Ubuntu)

OpenSSL/1.1.1

PHP/7.4.30

X-Powered-By: PHP/7.4.30

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: http://localhost:8888/admin/start/index.php

Content-Length: 0

Connection: close

Content-Type: text/html; charset=UTF-8

🔍

🔄

🏠

🔑

🔗

Search...

0 matches

Finished



d394ba3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



