

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

Bypass account protection #524

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

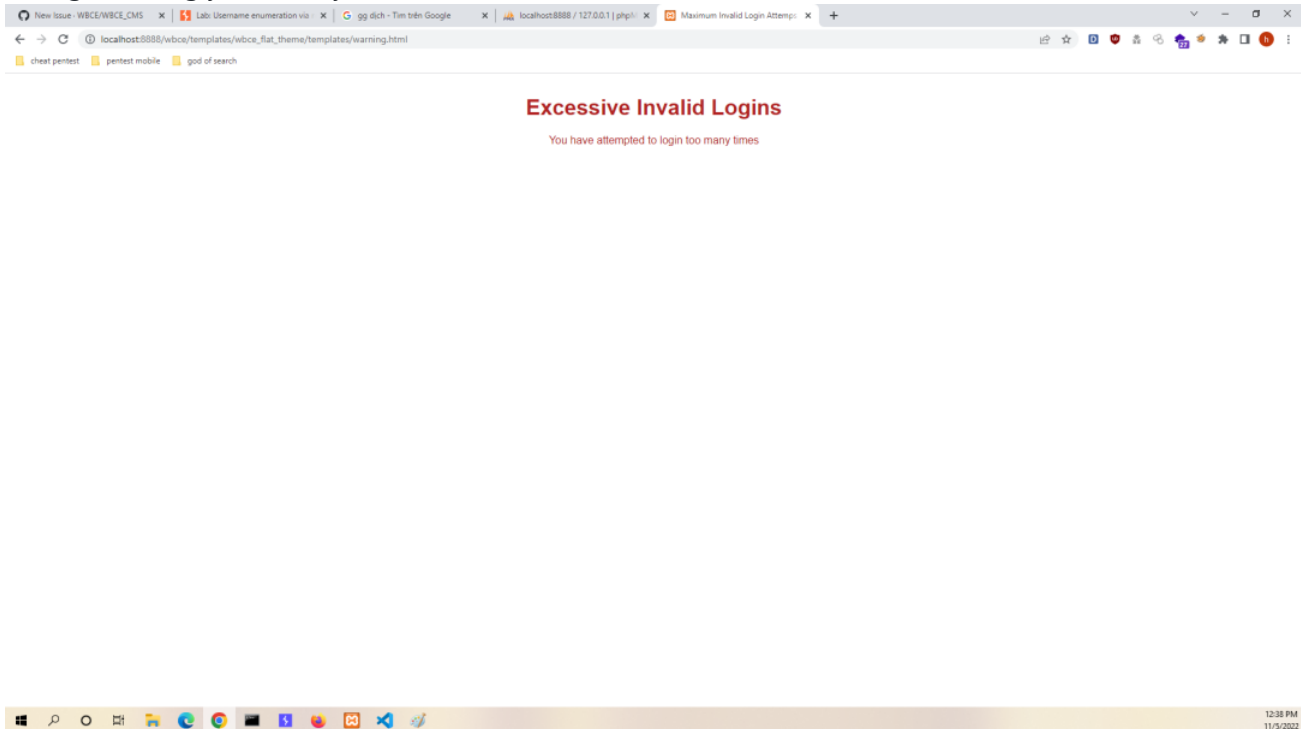
gozan10 commented 21 days ago

Hi team,

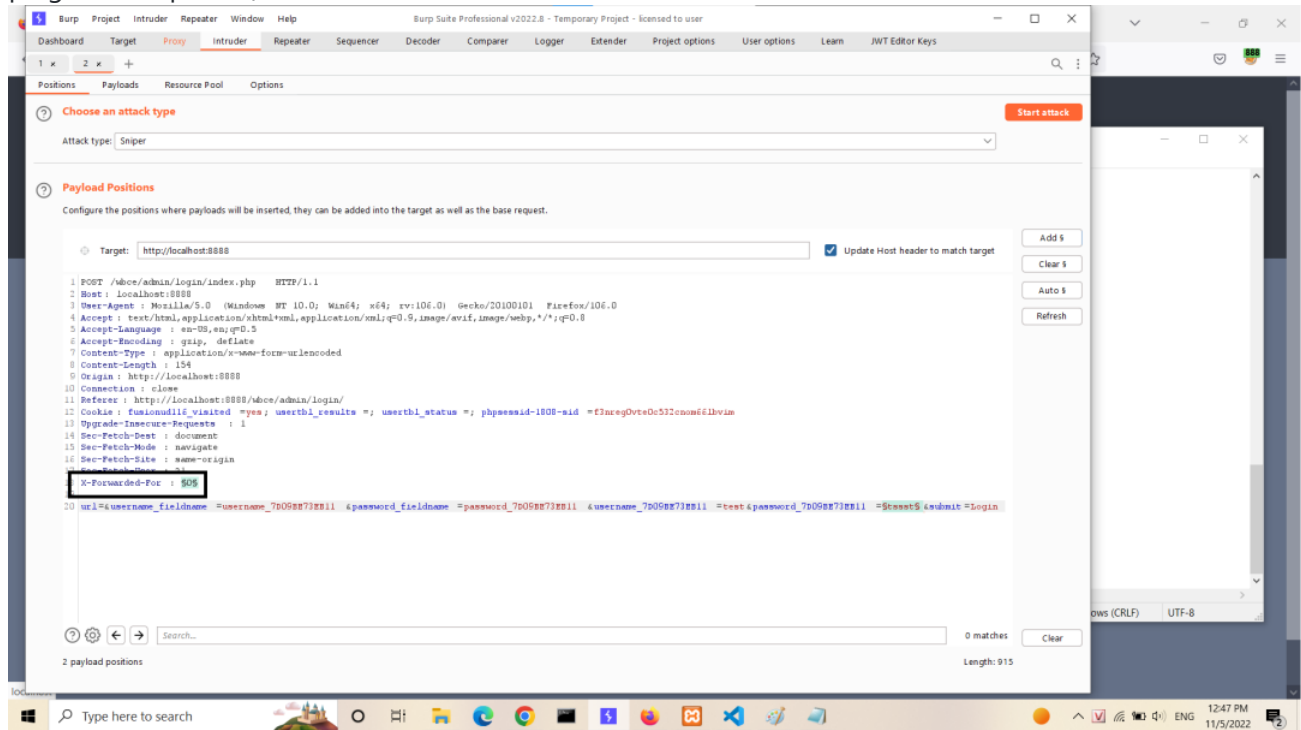
I found a way to bypass account protection (not blocked when brute-force account).

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: The "Payloads" tab is active. The "Payload Sets" section shows "Payload set: 1" and "Payload type: Numbers". The "Payload Options [Numbers]" section is expanded, showing "Type: Sequential" selected, "From: 1", "To: 100", "Step: 1", and "How many: 1". The "Number format" section shows "Base: Decimal" selected. The "Payload Processing" section is also visible.

Bottom Screenshot: The "Payloads" tab is active. The "Payload Sets" section shows "Payload set: 2" and "Payload type: Simple list". The "Payload Options [Simple list]" section is expanded, showing a list of strings: "carlos", "root", "admin", "test", "guest", "info", "adm", "user", and "administrator". The "Payload Processing" section is also visible.

4. Result find user (bypass account protection without blocked)

AttackSaveColumns

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

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---------|-----------|-----------|--------|-------|---------|--------|---------|
| 48 | 48 | test123 | 302 | | | 390 | |
| 57 | 57 | 110000 | 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 | |
| 8 | 8 | 123 | 200 | | | 3067 | |

RequestResponse

PrettyRawHexRender

HTTP/1.1 302 Found

110000 Sat, 02 Nov 2020 05:57:03 GMT

3 Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.1.1f PHP/7.4.30

4 X-Powered-By: PHP/7.4.30

5 Expires: Thu, 19 Nov 1991 08:52:00 GMT

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

7 Pragma: no-cache

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

9 Content-Length: 0

10 Connection: close

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

12

13

0 matches

Finished

 **mrbaseman** added a commit to mrbaseman/WBCE_CMS that referenced this issue 13 days ago

 fix for [WBCE#524](#) ...

d394ba3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



