Server Side Attacks (Contd)

Tools in Kali Linux

Module #21

Kali Linux: Webslayer?

WebSlayer is a web application brute-force tool.
WebSlayer can be used to brute-force the Form (User/Password) , GET , and POST parameters.
WebSlayer can also be used to identify resources not linked such as scripts, files, directories, and so on.

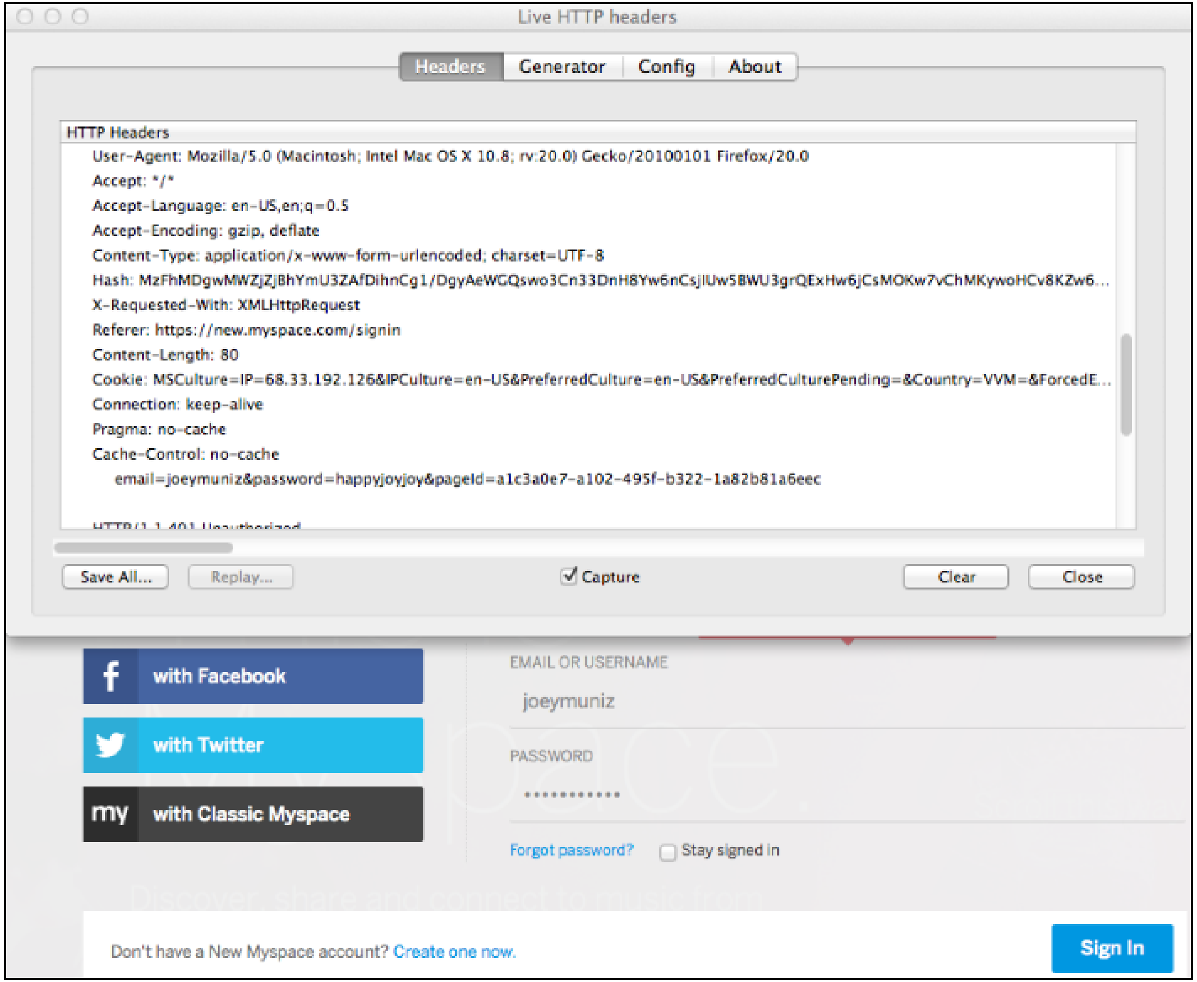
Kali Linux: Webslayer?

WebSlayer can attack any part of the HTTP request such as headers and authentication.

In order for WebSlayer to brute-force the password of a web server, it is important to know the username or most likely WebSlayer will not work.

You will need to capture HTTP requests and attempt a login so that you can grab the user agent and content needed for the attack.

Firefox offers a plugin called Live HTTP Headers, which you can use to gather this information while attempting a login to your target server.



```
HTTP Headers
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:20.0) Gecko/20100101 Firefox/20.0
    Accept: */*
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Content-Type: application/x-www-form-urlencoded; charset=UTF-8
    Hash: MzFhMDgwMWZjZjBhYmU3ZAfDihnCg1/DgyAeWGQswo3Cn33DnH8Yw6nCsjIUw5BWU3grQExHw6jCsMOKw7vChMKywoHCv8KZw6...
    X-Requested-With: XMLHttpRequest
    Referer: https://new.myspace.com/signin
    Content-Length: 80
    Cookie: MSCulture=IP=68.33.192.126&IPCulture=en-US&PreferredCulture=en-US&PreferredCulturePending=&Country=VVM=&ForcedE...
    Connection: keep-alive
    Pragma: no-cache
    Cache-Control: no-cache
       email=joeymuniz&password=happyjoyjoy&pageId=a1c3a0e7-a102-495f-b322-1a82b81a6eec

    HTTP/1.1 401 Unauthorized
```

EMAIL OR USERNAME
joeymuniz

PASSWORD
•••••••••••

Forgot password? □ Stay signed in

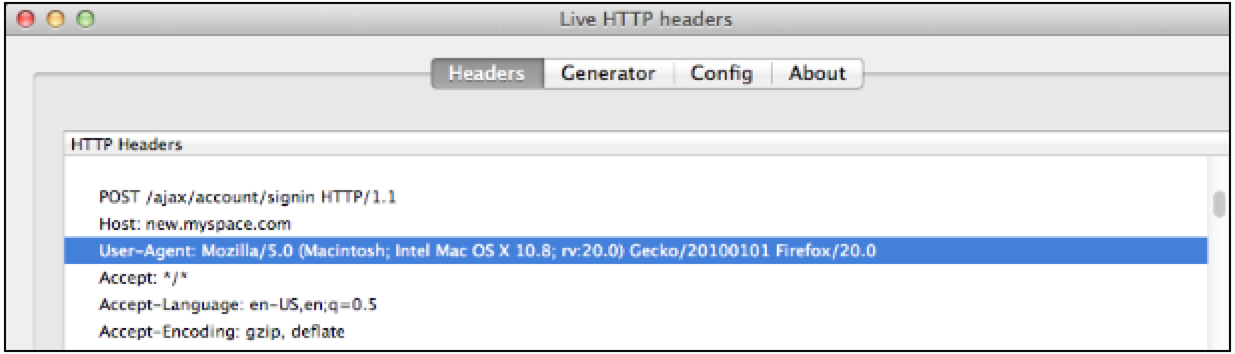
Don't have a New Myspace account? Create one now.

Kali Linux: Webslayer?

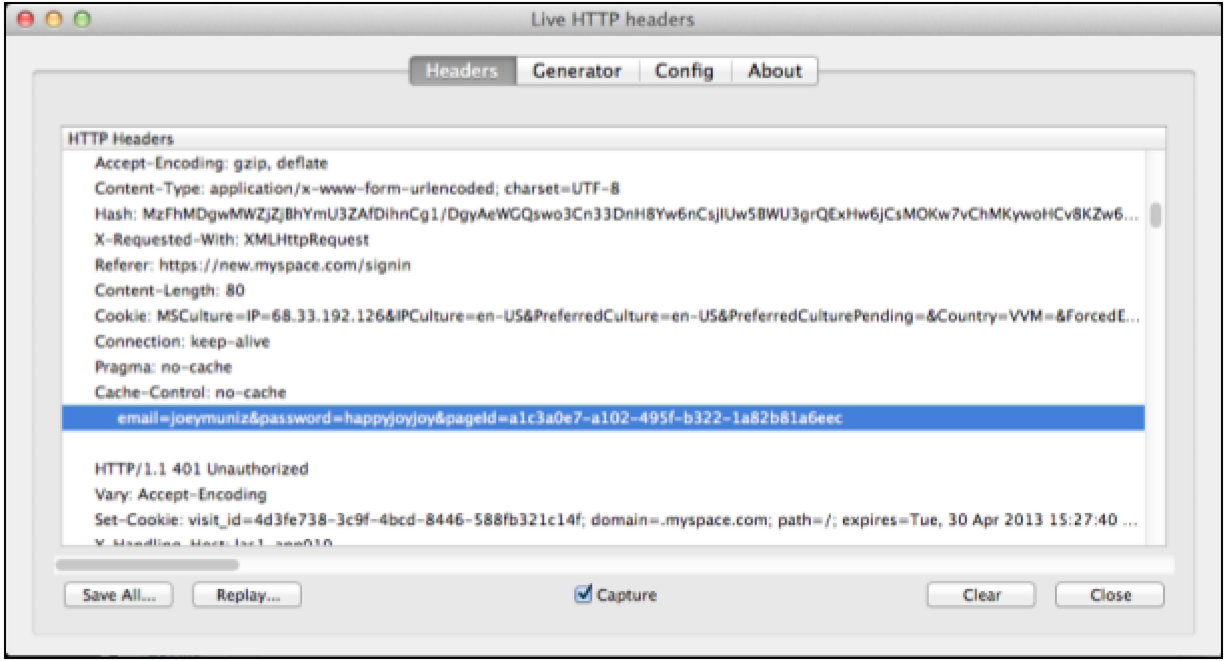
The important parts of information captured from the Live HTTP Headers used in WebSlayer are

the User-Agent and
Login Credentials

as shown in the following examples:

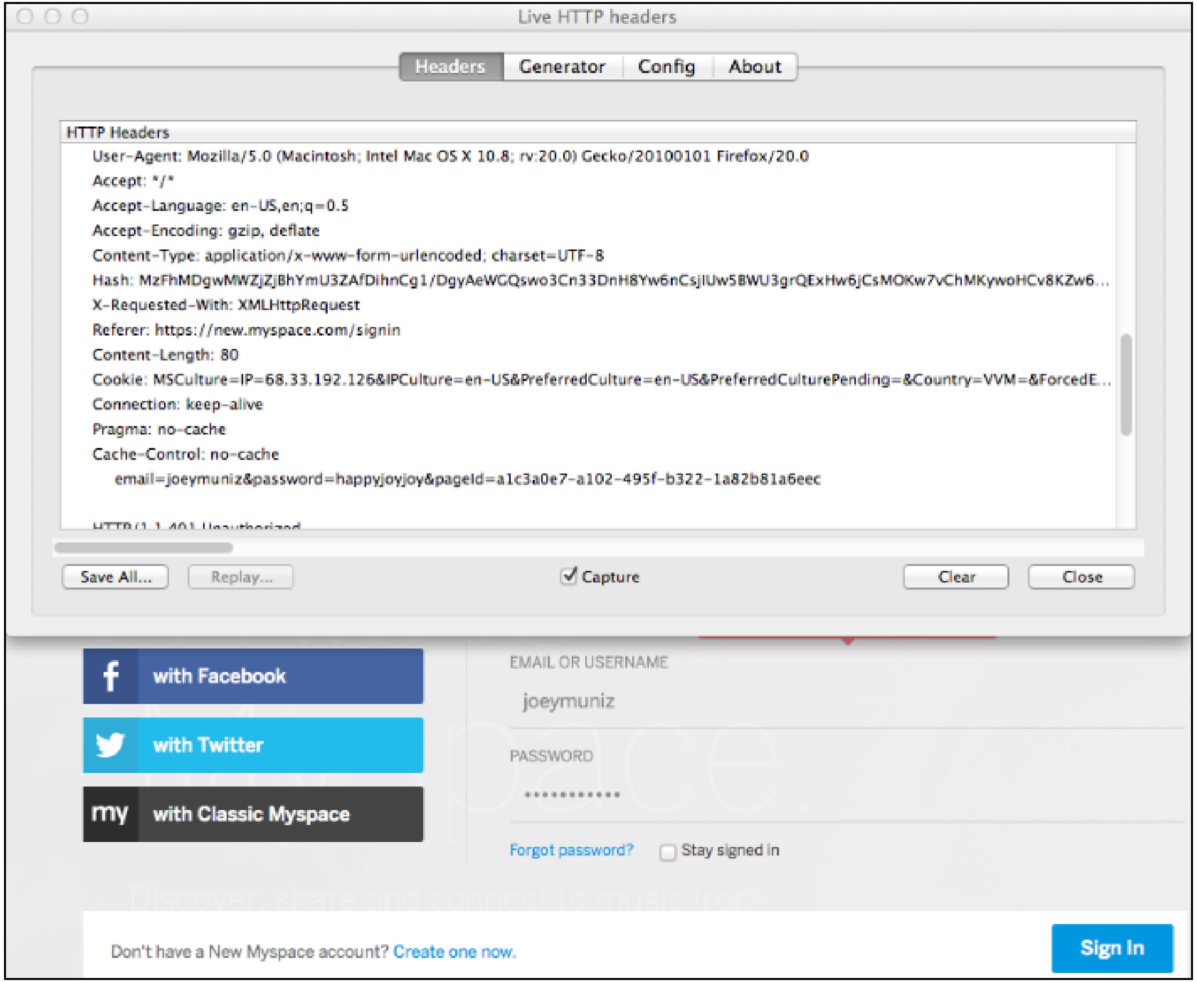


```
POST /ajax/account/signin HTTP/1.1
Host: new.myspace.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:20.0) Gecko/20100101 Firefox/20.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```



```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Hash: MzFhMDgwMWZjZjBhYmU3ZAfDihnCg1/DgyAeWGQswo3Cn33DnH8Yw6nCsjlUw5BWU3grQExHw6jCsMOKw7vChMKywoHCv8KZw6...
X-Requested-With: XMLHttpRequest
Referer: https://new.myspace.com/signin
Content-Length: 80
Cookie: MSCulture=IP=68.33.192.126&IPCulture=en-US&PreferredCulture=en-US&PreferredCulturePending=&Country=VVM=&ForcedE...
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
    email=joeymuniz&password=happyjoyjoy&pageId=a1c3a0e7-a102-495f-b322-1a82b81a6eec

HTTP/1.1 401 Unauthorized
Vary: Accept-Encoding
Set-Cookie: visit_id=4d3fe738-3c9f-4bcd-8446-588fb321c14f; domain=.myspace.com; path=/; expires=Tue, 30 Apr 2013 15:27:40 ...
X-Handling-Host: lax1-app010
```



HTTP Headers

```
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:20.0) Gecko/20100101 Firefox/20.0
    Accept: */*
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Content-Type: application/x-www-form-urlencoded; charset=UTF-8
    Hash: MzFhMDgwMWZjZjBhYmU3ZAfDihnCg1/DgyAeWGQswo3Cn33DnH8Yw6nCsjlUw5BWU3grQExHw6jCsMOKw7vChMKywoHCv8KZw6...
    X-Requested-With: XMLHttpRequest
    Referer: https://new.myspace.com/signin
    Content-Length: 80
    Cookie: MSCulture=IP=68.33.192.126&IPCulture=en-US&PreferredCulture=en-US&PreferredCulturePending=&Country=VVM=&ForcedE...
    Connection: keep-alive
    Pragma: no-cache
    Cache-Control: no-cache
      email=joeymuniz&password=happyjoyjoy&pageId=a1c3a0e7-a102-495f-b322-1a82b81a6eec

    HTTP/1.1 401 Unauthorized
```

EMAIL OR USERNAME

joeymuniz

PASSWORD

•••••••••••

□ Stay signed in

Don't have a New Myspace account? Create one now.

Kali Linux: Webslayer?

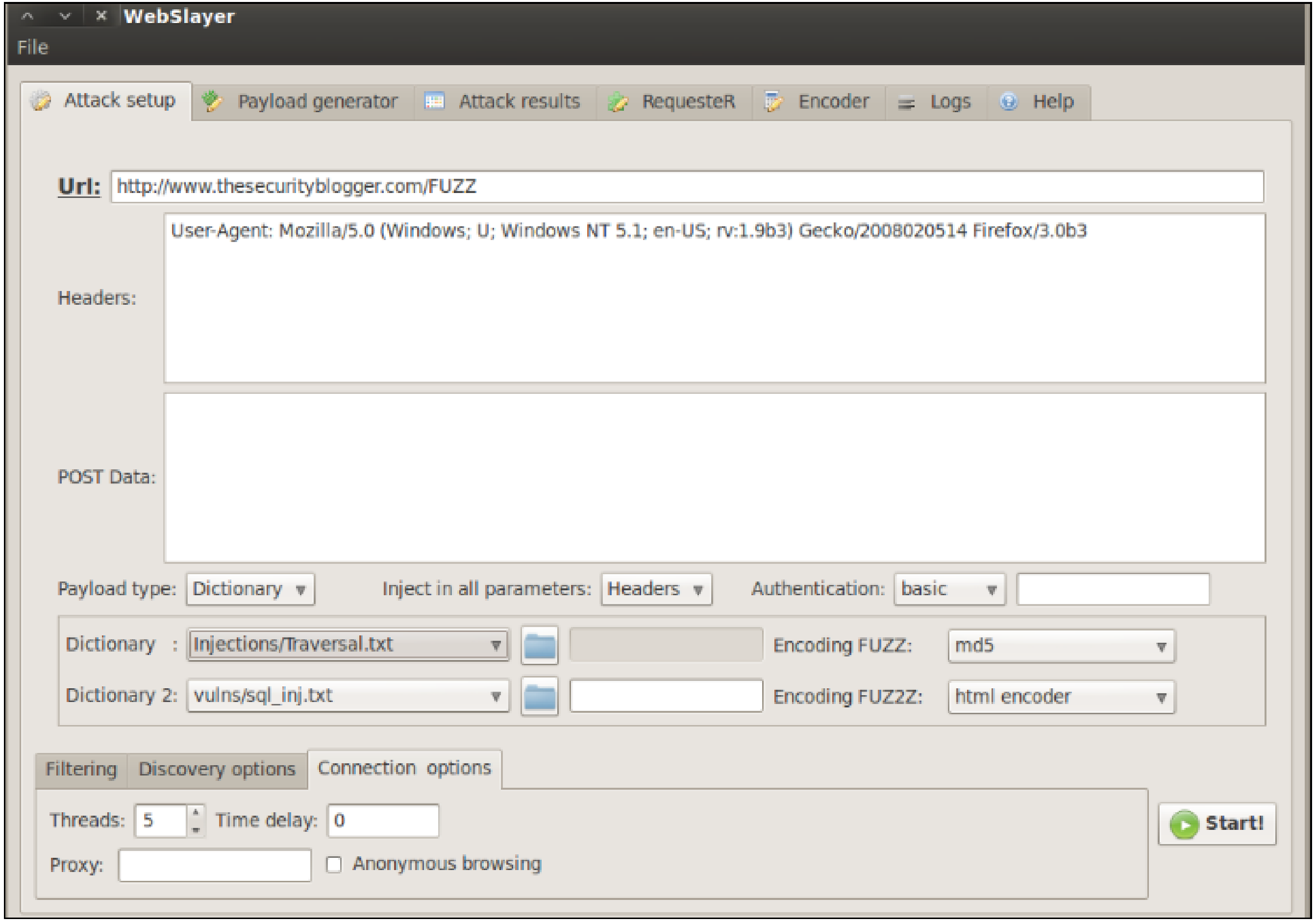
In the Attack Setup tab there is an url field, which must be filled with the target URI. Below the URL field are the Headers and POST data input fields.

There is an option to set the payload type, which can be Dictionary, Range, or Payload .

The Dictionary can be a file containing payloads, which can be a custom file or selected from a list of available dictionaries.

The Range setting can be used to specify the range for the attack.

The Payload setting can import a payload from the Payload Generator tab. Lets look at an example



Url: http://www.thesecurityblogger.com/FUZZ

Headers: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3

POST Data:

Payload type: Dictionary

Inject in all parameters: Headers

Authentication: basic

Dictionary : Injections/Traversal.txt

Encoding FUZZ: md5

Dictionary 2: vulns/sql_inj.txt

Encoding FUZ2Z: html encoder

Threads: 5

Time delay: 0

Proxy:

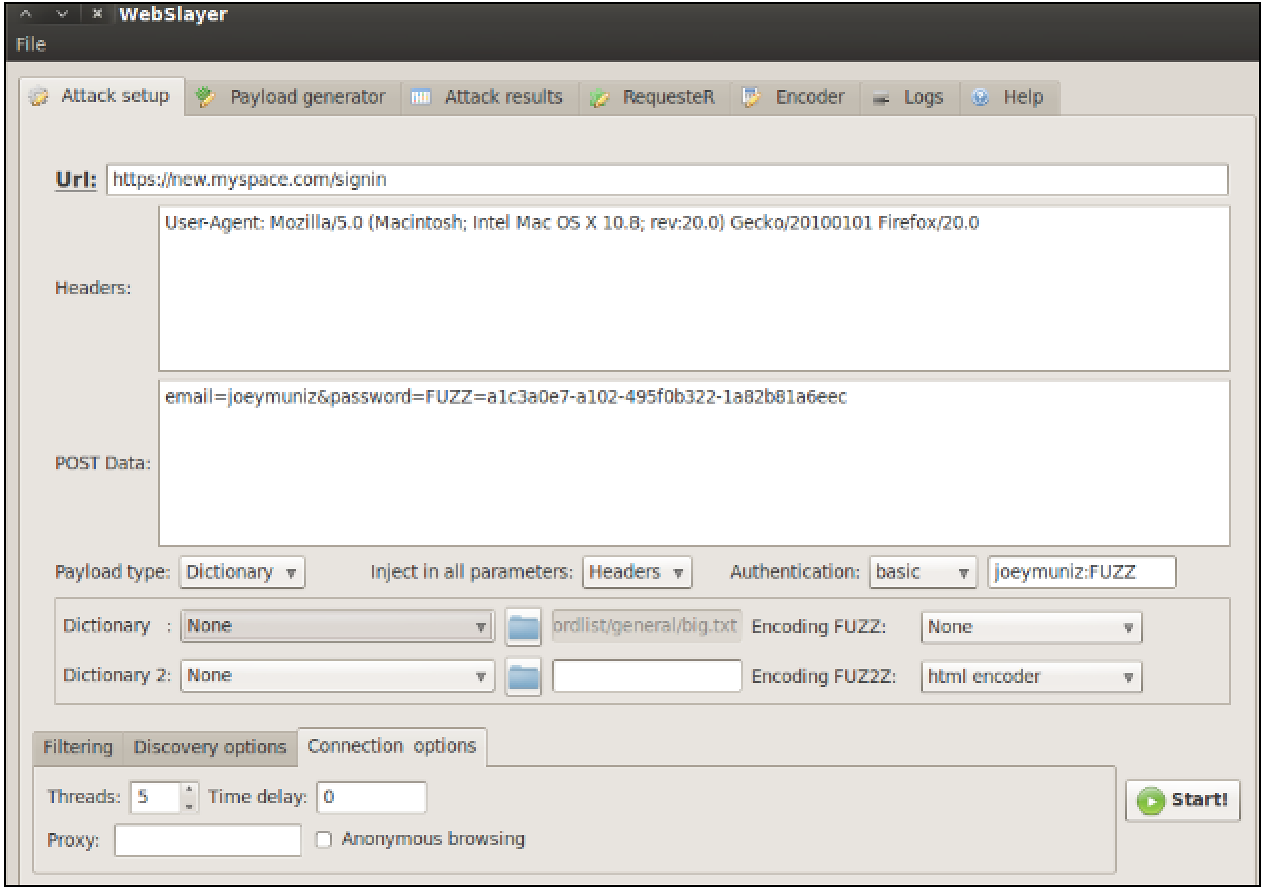
□ Anonymous browsing

Kali Linux: Webslayer?

The following example shows taking the login information captured in Live HTTP Headers while attempting to access myspace .

The wrong password is switched to the keyword FUZZ so that WebSlayer knows where to attempt the brute-force.

The Authentication tab has different security options for the example, the authentication is set to basic with the username joeymuniz followed by the keyword FUZZ



Url: https://new.myspace.com/signin

Headers: User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rev:20.0) Gecko/20100101 Firefox/20.0

POST Data: email=joeymuniz&password=FUZZ=a1c3a0e7-a102-495f0b322-1a82b81a6eec

Payload type: Dictionary

Inject in all parameters: Headers

Authentication: basic joeymuniz:FUZZ

Dictionary : None ordlist/general/big.txt

Encoding FUZZ: None

Dictionary 2: None

Encoding FUZ2Z: html encoder

Threads: 5

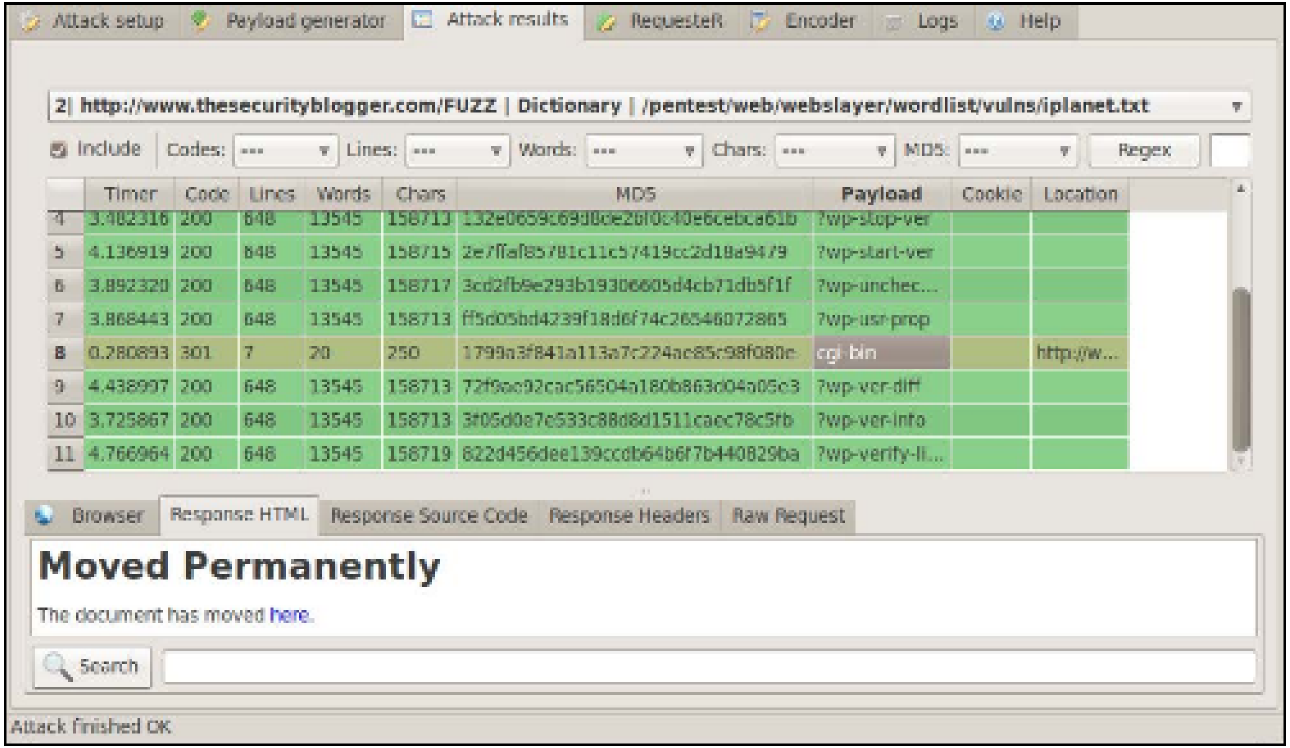
Time delay: 0

Proxy:

□ Anonymous browsing

Kali Linux: Webslayer?

After importing the payload into the attack scenario or selecting default dictionaries, you must select where the payload will be injected by WebSlayer.
Placing the keyword FUZZ on the URL being attacked does this. For example, the following screenshot shows the target http://www.thesecurityblogger.com/FUZZ in the attack URI field where FUZZ is an attack leveraging two existing dictionaries found in WebSlayer



2| http://www.thesecurityblogger.com/FUZZ | Dictionary | /pentest/web/webslayer/wordlist/vulns/iplanet.txt

☑ Include Codes: --- Lines: --- Words: --- Chars: --- MD5: --- Regex

	Timer	Code	Lines	Words	Chars	MD5	Payload	Cookie	Location
4	3.482316	200	648	13545	158713	132e0659c69d8de2bf0c40e6cebca61b	?wp-stop-ver		
5	4.136919	200	648	13545	158715	2e7ffaf8571c11c57419cc2d18a9479	?wp-start-ver		
6	3.892320	200	648	13545	158717	3cd2fb9e293b19306605d4cb71db5f1f	?wp-unchec...		
7	3.868443	200	648	13545	158713	ff5d05bd4239f18d6f74c26546072865	?wp-usr-prop		
8	0.280893	301	7	20	250	1799a3f841a113a7c224ac85c98f080e	cgi-bin		http://w...
9	4.438997	200	648	13545	158713	72f9ac92cac56504a180b863d04a05c3	?wp-ver-diff		
10	3.725867	200	648	13545	158713	3f05d0e7e533c88d8d1511caec78c5fb	?wp-ver-info		
11	4.766964	200	648	13545	158719	822d456dee139ccdb64b6f7b440829ba	?wp-verify-li...		

Moved Permanently

The document has moved here.

Attack finished OK

Kali Linux: Webslayer?

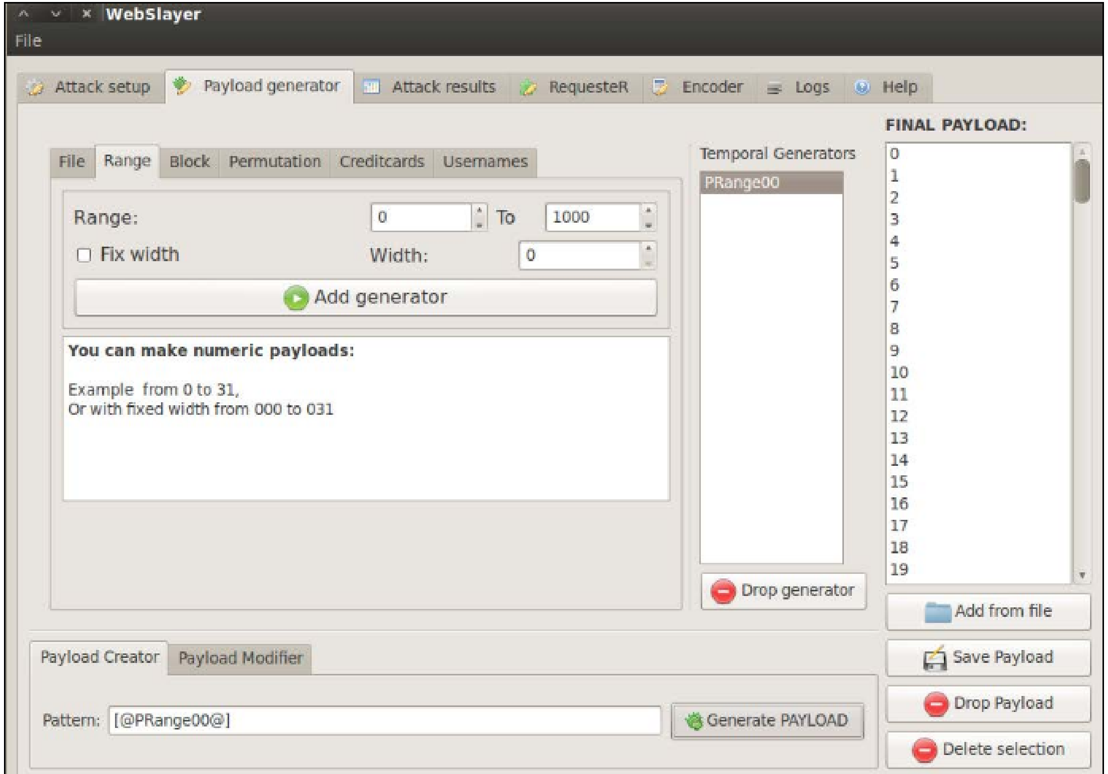
The payload generator is a tool that you can use to create custom payloads. You can load dictionaries, numeric ranges, character blocks, permutations, credit cards, usernames, and other settings.

You can concatenate and create a final payload that can be uploaded into the attack tab for a customized attack.

An example of defining a range payload in the Payload Generator tab can be seen in the following screenshot. The example shows setting the range payload from 0 to 1000 . Once the range is selected, we click on the add generator button, which will generate a Temporal Generator.

Kali Linux: Webslayer?

Drag the newly created generator to the Payload Creator at the bottom and click on Generate Payload. Now import the new payload in the Attack Setup tab



Range: 0 To 1000

□ Fix width Width: 0

You can make numeric payloads:

Example from 0 to 31,
Or with fixed width from 000 to 031

Temporal Generators: PRange00

FINAL PAYLOAD:

```
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
```

Pattern: [@PRange00@]

Thank You