

Ataque com wordlists

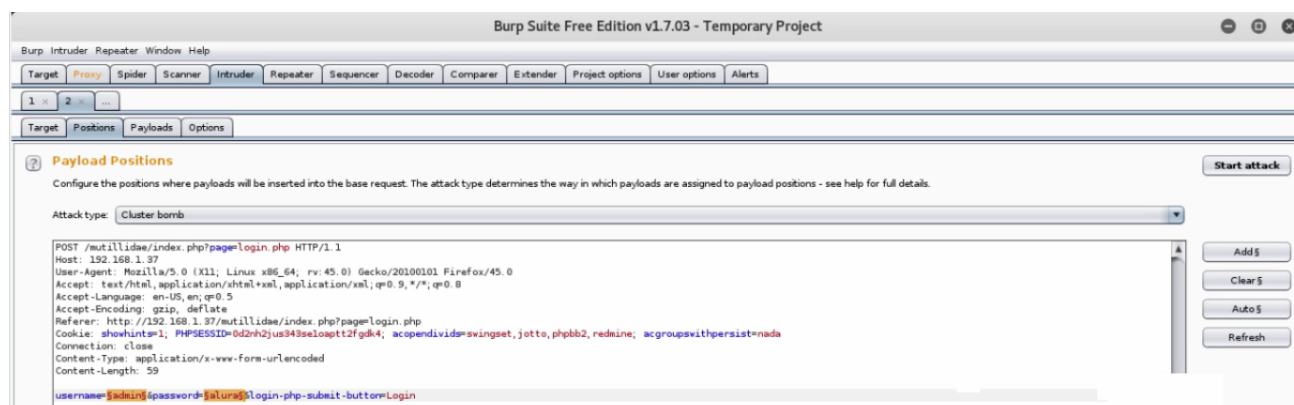
Transcrição

Vamos simular como seria um ataque de força bruta utilizando as listas. Primeiro, criamos uma nova lista baseada no site para possíveis senhas. Nós abrimos o terminal e escrevemos, o `cewl`, a URL da página, a profundidade da pesquisa `-d 1` e onde queremos salvar isso, no caso, em `-w cewl.txt`. Teremos:

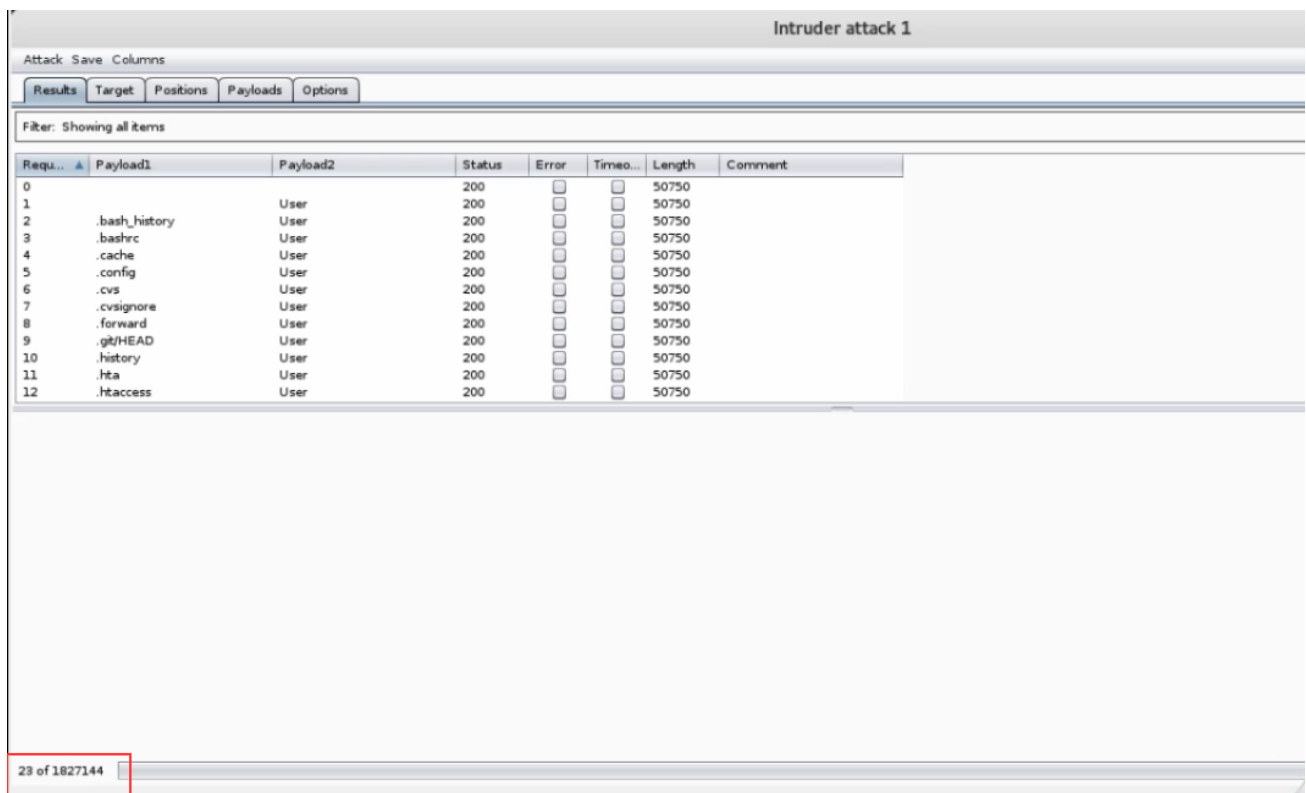
```
> cewl "http://192.168.1.37/multilidae/" -d 1 -w cewl.txt
```

O arquivo `cewl.txt` salvará as senhas. O `common.txt` criado anteriormente guardará os usuários.

É preciso verificar que o **Burbsuite** está programado para interceptar, portanto, vamos em "Proxy > Intercept" e deixamos o botão *Intercept is on* pressionado. Conforme fizemos anteriormente, é preciso passar as informações para serem alteradas para vários outros parâmetros, portanto, clicamos no campo com o botão direito do mouse e selecionamos a opção "Send to Intruder". Automaticamente, a aba "Intruder" fica em destaque. Na aba "Intruder" destacamos apenas o `admin` e `alura`. Lembrando que é preciso alterar o ataque para o tipo "Cluster Bomb":



Com essa parte já configurada podemos clicar na aba "Payload". No primeiro campo "Payload Options" carregamos, através do "load", o arquivo que contem as possíveis palavras para usuário, o `common.txt`. Definida a primeira lista, podemos inserir a próxima, então, em "Payload Options" alteramos o "Payload set" para o número dois e carregamos `cewl.txt`. Agora que já temos ambas as listas carregadas podemos selecionar o "Start attack":



The screenshot shows the 'Intruder attack 1' interface. At the top, there are tabs for 'Attack', 'Save', and 'Columns'. Below these are sub-tabs for 'Results', 'Target', 'Positions', 'Payloads', and 'Options'. A filter bar indicates 'Showing all items'. The main table has columns: 'Requ...', 'Payload1', 'Payload2', 'Status', 'Error', 'Timeo...', 'Length', and 'Comment'. The table contains 12 rows of data, all with a status of 200 and a length of 50750. The payloads are listed in the 'Payload1' column, and 'User' is listed in the 'Payload2' column. At the bottom left, a red box highlights the text '23 of 1827144'.

Requ...	Payload1	Payload2	Status	Error	Timeo...	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
1		User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
2	.bash_history	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
3	.bashrc	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
4	.cache	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
5	.config	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
6	.cvs	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
7	.cvsignore	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
8	.forward	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
9	.git/HEAD	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
10	.history	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
11	.hta	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	
12	.htaccess	User	200	<input type="checkbox"/>	<input type="checkbox"/>	50750	

Bem abaixo dessa página podemos verificar a quantidade de combinações possíveis.

Uma das características do Força Bruta é que são ataques demorados, pois as combinações são diversas e é preciso esperar até que uma seja acertada. Existem alguns sistemas que estipulam um número de tentativas, por exemplo, sistemas bancários permitem no máximo 3 tentativas em um mesmo dia. Essa é uma das maneiras de justamente dificultar e proteger-se desses ataques, assim como, o uso de caracteres minúsculos e maiúsculos, até 8 dígitos, números, etc.