**# EJERCICIOS ATAQUES POR FUERZA BRUTA**

**## Prerrequisitos**

**- Kali Linux**

**- Máquina OWASP BWA**

**## Ejercicio 1**

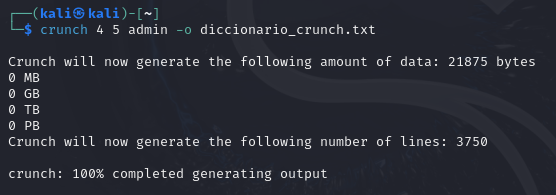
**- Creación de diccionario a medida para Mutillidae usando las herramientas vistas en clase**

**(Crunch, Cewl y Dymerge)**

#### 1. Generar un Diccionario con Crunch

Crunch te permite crear diccionarios personalizados especificando la longitud de las palabras y los caracteres a utilizar. Para generar un diccionario con palabras de 6 a 8 caracteres, usando letras y números:

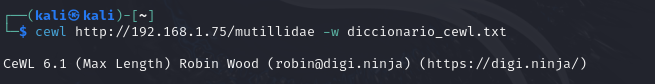
crunch 6 8 abcdefghijklmnopqrstuvwxyz0123456789 -o diccionario\_crunch.txt



#### 2. Generar un Diccionario con Cewl

Cewl permite crear diccionarios basados en el contenido de una página web. Para generar un diccionario desde una URL específica:

cewl http://IP\_OWASP\_BWA/mutillidae -w diccionario\_cewl.txt



**## Ejercicio 2**

**- Uso de Hydra con el diccionario creado para conseguir la contraseña del usuario admin en el**

**ejercicio:**

**- Mutillidae &gt; OWASP 2013 &gt; A2 &gt; Authentication Bypass &gt; Via Brute Force &gt; Login**

sudo hydra -l admin -P diccionario\_corto.txt 192.168.1.75 http-post-form "/mutillidae/index.php?page=login.php:username=admin&password=^PASS^&login-php-submit-button=Login:Not Logged In"

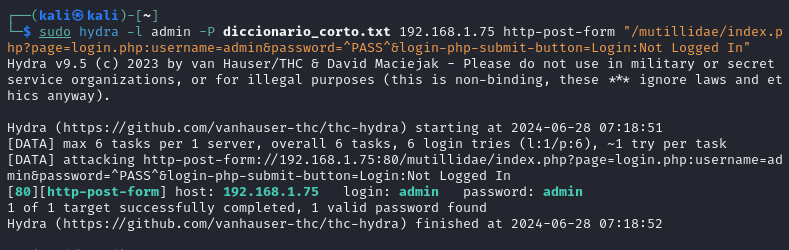
### **Resumen del Comando**

* **sudo**: Ejecuta el comando con privilegios de superusuario.
* **hydra**: Herramienta para realizar ataques de fuerza bruta.
* **-l admin**: Nombre de usuario a probar durante el ataque.
* **-P diccionario\_corto.txt**: Archivo de diccionario que contiene las contraseñas a probar.
* **192.168.1.75**: Dirección IP del objetivo, la máquina que aloja Mutillidae.
* **http-post-form "/mutillidae/index.php?page=login.php:username=admin&password=^PASS^&login-php-submit-button=Login:Not Logged In"**:
  + **http-post-form**: Método HTTP POST para enviar credenciales.
  + **"/mutillidae/index.php?page=login.php**: URL del formulario de inicio de sesión en Mutillidae.
  + **:username=admin&password=^PASS^&login-php-submit-button=Login**: Parámetros del formulario POST:
    - username=admin: Nombre de usuario estático.
    - password=^PASS^: Contraseña que será reemplazada por cada entrada del diccionario.
    - login-php-submit-button=Login: Nombre del botón de envío del formulario.
  + **:Not Logged In**: Cadena a buscar en la respuesta para identificar intentos fallidos de inicio de sesión.

### **Funcionamiento**

Hydra ejecuta un ataque de fuerza bruta contra el formulario de inicio de sesión de Mutillidae. Utiliza el nombre de usuario admin y prueba cada contraseña del archivo diccionario\_corto.txt. Para cada intento, Hydra envía una solicitud POST con el nombre de usuario y la contraseña del diccionario. Analiza la respuesta de la aplicación en busca de la cadena Not Logged In para detectar intentos fallidos de inicio de sesión.

Este comando automatiza la prueba de credenciales débiles o no válidas mediante un ataque de fuerza bruta, útil para evaluar la seguridad de contraseñas y la robustez de la autenticación en aplicaciones web como Mutillidae.

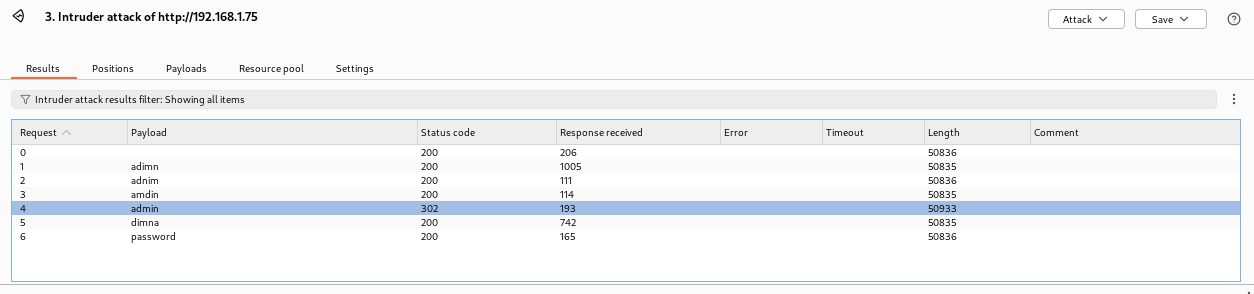
****

**## Ejercicio 3**

**- Uso de Burp Suite con el diccionario creado para conseguir la contraseña del usuario admin**

**en el ejercicio:**

**- Mutillidae &gt; OWASP 2013 &gt; A2 &gt; Authentication Bypass &gt; Via Brute Force &gt; Login**

****

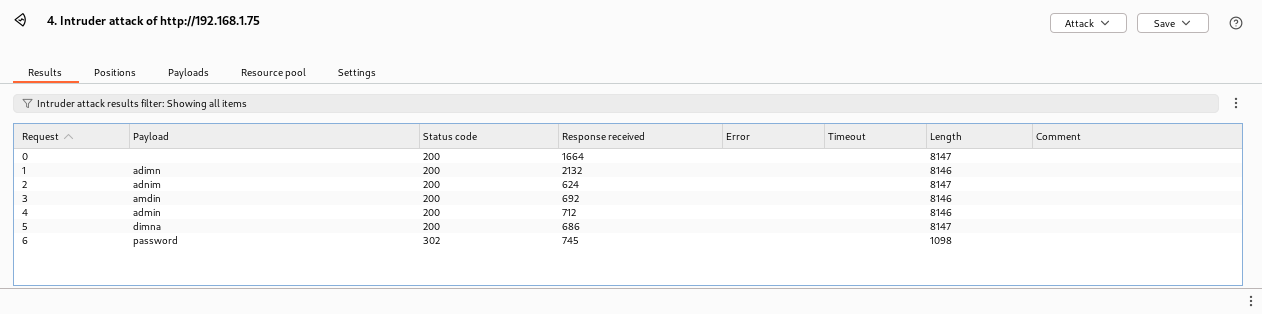
**## Ejercicio 4 Resto de Apps**

**- En OWASP BWA hay varias aplicaciones desplegadas de pruebas donde es posible realizar**

**este proceso con diferentes tecnologías y formularios de Login/Sign In. Realiza el mismo**

**procedimiento que en los ejercicios anteriores en las aplicaciones:**

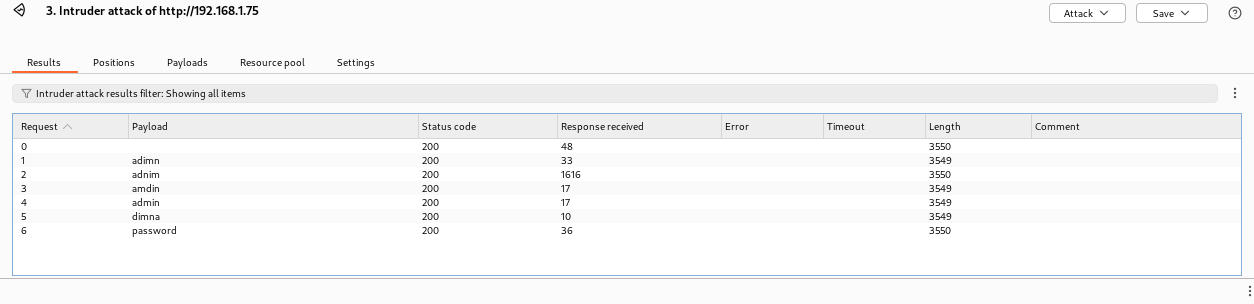
**- Cyclone:** [**http://IP\_OWASP\_BWE/cyclone/**](http://ip_owasp_bwe/cyclone/)

****

**- Google Gruyère:** [**http://IP\_OWASP\_BWE/gruyere/**](http://ip_owasp_bwe/gruyere/)

No se puede acceder a esta pagina esta en mantenimiento

**- WackoPicko:** [**http://IP\_OWASP\_BWE/WackoPicko**](http://ip_owasp_bwe/WackoPicko)

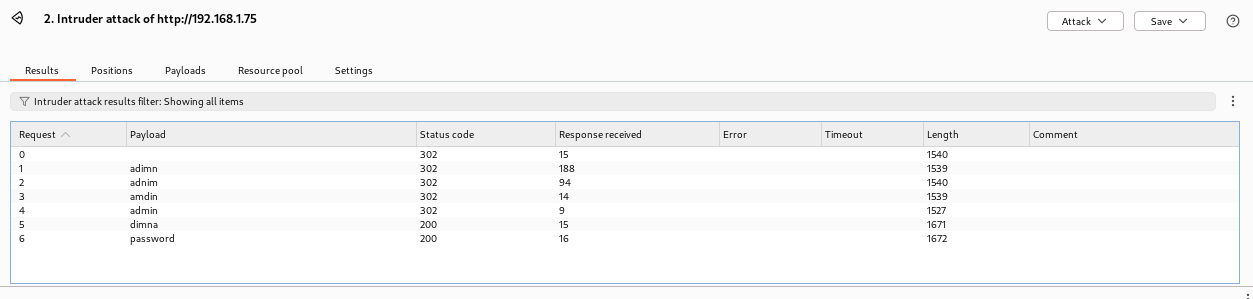
****

De aquí no he conseguido la contraseña porque ni siquiera estoy seguro de que admin sea un user válido, la página no indica nada pero bueno se haría así.

**- BodgeIt Store:** [**http://IP\_OWASP\_BWE/bodgeit**](http://ip_owasp_bwe/bodgeit)

el servidor no funciona

**- Peruggia:** [**http://IP\_OWASP\_BWE/peruggia**](http://ip_owasp_bwe/peruggia)

****