Python Fonksiyonları

Gönderimleri, örnekleri ve genel yürütme durumunu takip etmek için, Cuckoo SQLite, MySQL veya MariaDB, PostgreSQL ve birçok diğer SQL veritabanı sistemini kullanmanıza izin veren popüler bir Python ORM olan SQLAlchemy kullanır.

Cuckoo, daha büyük çözümlere kolayca entegre edilebilen ve tamamen otomatik hale getirilebilen bir tasarıma sahiptir. Analiz gönderimini otomatikleştirmek için REST API arayüzünü kullanmanızı öneririz (bkz. REST API), ancak kendi Python gönderim betiğinizi yazmak istiyorsanız add_path() ve add_url() işlevlerini kullanabilirsiniz.

> **`add_path`** ***(file_path[, timeout=0[, package=None[, options=None[, priority=1[, custom=None[, owner=""[, machine=None[, platform=None[, tags=None[, memory=False[, enforce_timeout=False], clock=None[]]]]]]]]]]]])***

Bekleyen analiz görevleri listesine yerel bir dosya ekler. Yeni oluşturulan görevin ID'sini döndürür.

Parametreler:

- file_path (string): Gönderilecek dosyanın yolu
- timeout (integer): Analiz süresinin maksimum saniye cinsinden miktarı
- package (string veya None): Belirtilen dosya için kullanmak istediğiniz analiz paketi
- options (string veya None): Analiz paketine iletilmesi gereken seçeneklerin listesi (key=value, key=value formatında)
- priority (integer): Belirtilen dosyaya atanacak önceliğin sayısal temsili (1 düşük, 2 orta, 3 yüksek)
- custom (string veya None): İşleme veya raporlamada kullanılmak üzere iletilmesi gereken özel değer
- owner (string veya None): Görev sahibi
- machine (string veya None): Kullanmak istediğiniz sanal makinenin Cuckoo kimliği; belirtilmezse otomatik olarak bir tane seçilir
- platform (string veya None): Çalıştırmak istediğiniz analizin işletim sistemi platformu (şu anda yalnızca Windows)
- tags (string veya None): Makine seçimi için etiketler
- memory (True veya False): Analiz makinesinin tam bellek dökümünü oluşturmak için True olarak ayarlayın
- enforce_timeout (True veya False): Süreyi tam olarak uygulamak için True olarak ayarlayın
- clock (string veya None): Analiz makinesinde ayarlanacak özel bir saat zamanı

Return type: integer

Örnek kullanım:

```
>>> from cuckoo.core.database import Database
>>> db = Database()
>>> db.add_path("/tmp/malware.exe")
1
>>>
```

add_url(*url[, timeout=0[, package=None[, options=None[, priority=1[, custom=None[, owner=""[, machine=None[, platform=None[, tags=None[, memory=False[, enforce_timeout=False], clock=None[]]]]]]]]]]]])

Bekleyen analiz görevleri listesine yerel bir dosya ekler. Yeni oluşturulan görevin ID'sini döndürür.

Parametreler:

- url (string): Analiz edilecek URL
- timeout (integer): Analiz süresinin maksimum saniye cinsinden miktarı
- package (string veya None): Belirtilen URL için kullanmak istediğiniz analiz paketi
- options (string veya None): Analiz paketine iletilmesi gereken seçeneklerin listesi (key=value, key=value formatında)
- priority (integer): Belirtilen URL'ye atanacak önceliğin sayısal temsili (1 düşük, 2 orta, 3 yüksek)
- custom (string veya None): İşleme veya raporlamada kullanılmak üzere iletilmesi gereken özel değer
- owner (string veya None): Görev sahibi
- machine (string veya None): Kullanmak istediğiniz sanal makinenin Cuckoo kimliği; belirtilmezse otomatik olarak bir tane seçilir
- platform (string veya None): Çalıştırmak istediğiniz analizin işletim sistemi platformu (şu anda yalnızca Windows)
- tags (string veya None): Makine seçimi için etiketler
- memory (True veya False): Analiz makinesinin tam bellek dökümünü oluşturmak için True olarak ayarlayın
- enforce_timeout (True veya False): Süreyi tam olarak uygulamak için True olarak ayarlayın
- clock (string veya None): Analiz makinesinde ayarlanacak özel bir saat zamanı

Return type: integer

Örnek kullanım:

```
>>> from cuckoo.core.database import Database
>>> db = Database()
```

```
>>> db.connect()
>>> db.add_url("http://www.cuckoosandbox.org")
2
>>>
```

Revision #1
Created 4 January 2024 10:39:50 by Ertan Sözer
Updated 4 January 2024 11:33:53 by Ertan Sözer