

Python en el mundo real



Facundo
Batista



Foto: Creativity+ Timothy K Hamilton (<http://www.flickr.com/photos/22017189@N00/60842961/>)

¿En el mundo real?

- ▶ Algunos proyectos hechos en Python
- ▶ En qué framework o lib importante nos apoyamos
 - ▶ Obviamente, además usamos la Biblioteca Estándar
- ▶ Público usuario del sistema
- ▶ Complejidad desde distintos puntos de vista
- ▶ Ventaja de usar Python en el proyecto
- ▶ Inconvenientes encontrados
 - ▶ Por haber usado Python
 - ▶ O por el tipo de proyecto en sí

w3af-gui

Web Application Attack
and Audit Framework



WizardsNewSaveStartPauseMultiple ExploitManual RequestFuzzy RequestEncode/DecodeComp

Scan configLogResultsExploit

Profiles

OWASP_TOP10
audit_high_risk
bruteforce
dav
fast_scan
full_audit_manual_disc
os
re
sitemap
sql
testfile

Target: Insert the target URL here

Plugin

serverStatus☐
sharedHosting☐
sitemapReader☐
spiderMan☒
urlFuzzer☐
userDir☐
webDiff☐
webSpider☒
wordnet☐
wsdlFinder☐

PluginActive

output

spiderMan

This plugin is a local proxy that can be used to give the framework knowledge of an application when it has a lot of client side code like Flash or Java applets. To test an application with Flash or JavaScript, the user should enable this plugin to navigate the site using the spiderMan proxy.

The proxy will extract information from the user navigation and generate audit plugins.

Another feature of this plugin is to save the cookies that are sent by the browser and use them in other plugins. So if you have a web application that has a login, you should enable this plugin, do the login through the browser and then use the cookies for the application for you. Important note: If you enable webSpider, you should also enable spiderMan.

Two configurable parameters exist:

- listenAddress
- listenPort

listenAddress

127.0.0.1

listenPort

44444

Save configurationRevert to previous values

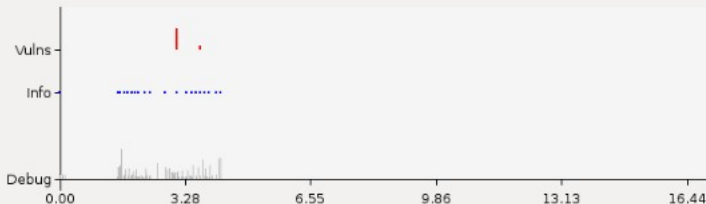
can config Log Results Exploit

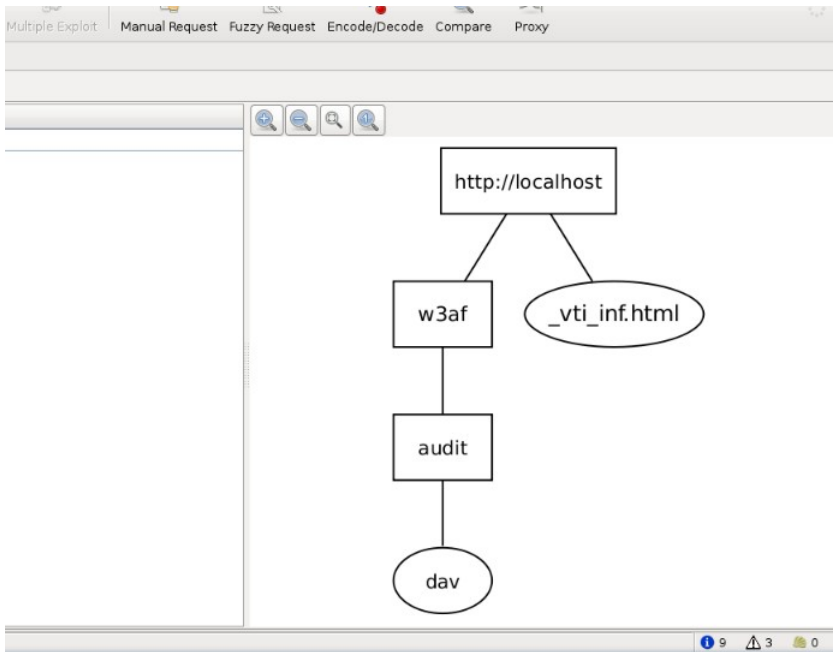
Vulnerabilities ☒ Information ☒ Error

ri 13 Feb 2009 10:51:08 PM ARST] Directory listing with HTTP PROPFIND method was found at directory: "http://localhost
ri 13 Feb 2009 10:51:08 PM ARST] Starting ssi plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting eval plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting buffOverflow plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting xss plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting xst plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] The web server at "http://localhost/w3af/audit/dav/" is vulnerable to Cross Site Tracir
ri 13 Feb 2009 10:51:08 PM ARST] Starting blindSql plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting formatString plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting preg_replace plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting globalRedirect plugin execution.
ri 13 Feb 2009 10:51:08 PM ARST] Starting LDAPi plugin execution.
ri 13 Feb 2009 10:51:09 PM ARST] Starting phishingVector plugin execution.
ri 13 Feb 2009 10:51:09 PM ARST] Starting frontpage plugin execution.
ri 13 Feb 2009 10:51:09 PM ARST] Starting responseSplitting plugin execution.
ri 13 Feb 2009 10:51:09 PM ARST] Finished scanning process.

Audit progress: 0.0 % - ETA: 00d 00h 00m

Not running.





w3af
cach
:: ap

Request Headers Request Body Response Headers Response Body Clear All Help

Id: 1 Id: 6

GET http://localhost/0 HTTP/1.1 → GET http://localhost/5 HTTP/1.1

☐ Accept-encoding: identity
Accept: */*
User-agent: w3af.sf.net
Host: www.some_host.com
Pragma: no-cache
Content-type: application/x-www-form-urlencoded

HTTP/1.1 404 Not Found
☐ date: Fri, 13 Feb 2009 21:54:41 GMT
content-length: 386
content-type: text/html; charset=iso-8859-1
server: Apache/2.2.8 (Ubuntu) DAV/2 mod_python/3.3.1 Python

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
☐ <p>The requested URL /0 was not found on this server.</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 mod_python/3.3.1 Python
</body></html>

HTTP/1.1 404 Not Found
date: Fri, 13 Feb 2009 21:54:42 GMT
content-length: 386
content-type: text/html; charset=iso-8859-1
server: Apache/2.2.8 (Ubuntu) DAV/2 mod_python/3.3.1 Python/2.5.2 PHP/5

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /5 was not found on this server.</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 mod_python/3.3.1 Python/2.5.2 PHP/5
</body></html>

Set text to compare

3 of 3 Delete

10 ok, 0 errors ☒ Fix content length header 6 of 10 Cluster Responses

HTTP Response Cluster

Zoom In

Zoom Out

Best Fit

Normal Size

54

55

51

52

56

58

w3af - Fuzzy Requests

Request

GET http://localhost/9 HTTP/1.1
Accept-encoding: identity
Accept: */*
User-agent: w3af.sf.net
Host: www.some_host.com
Pragma: no-cache
Content-type: application/x-www-form-u

w3af - HTTP Request/Response

Request

GET http://localhost/2 HTTP/1.1
Accept-encoding: identity
Accept: */*
User-agent: w3af.sf.net
Host: www.some_host.com
Pragma: no-cache
Content-type: application/x-www-form-urlencoded

Response

HTTP/1.1 404 Not Found
date: Fri, 13 Feb 2009 20:50:28 GMT
content-length: 386
content-type: text/html; charset=isc
server: Apache/2.2.8 (Ubuntu) DAV/;

<!DOCTYPE HTML PUBLIC "-//IETF//D
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>

Profiles Edit View Tools Configuration Help

Wizards New Save Clear Pause Multiple Exploit Manual Request Fuzzy Request

Scan config Log Results Exploit

Exploits

- davShell
- eval
- fileUploadShell
- localFileReader
- osCommandingShell
- remoteFileIncludeShell
- rfiProxy
- sql_webshell
- sqlmap
- xssBeef

Vulnerabilities

⚠ Cross site tracing vulnerability

Shells

< davShell

Shell - Linux brick 2.6.24-23-generic i686

Save

```
www-data@brick> w
22:51:36 up 1 day,  5:35,  7 users,  load average:
USER      TTY      FROM            LOGIN@      IDLE        CPU%
dz0       tty7     :0               Thu17       0.00s      1
dz0       pts/0    :0.0             Thu17       8:26       0
dz0       pts/1    :0.0             Thu19       1:46       0
dz0       pts/2    :0.0             Thu19       1:04m     11
dz0       pts/3    :0.0             Thu19       2:59       0
dz0       pts/4    :0.0             Thu19       2:57       0
euge      tty9     :20              08:30      14:19     15

www-data@brick> w
```

w3af-gui

- ▶ **Biblioteca:** pygtk, w3af
- ▶ **Público:** usuario final con un nivel técnico; aplicación de escritorio
- ▶ **Complejidad:** usabilidad; robustez; portabilidad
- ▶ **Ventaja:** prototipado => calidad final
- ▶ **Dificultad:** pygtk y threading en Linux y Windows; usabilidad

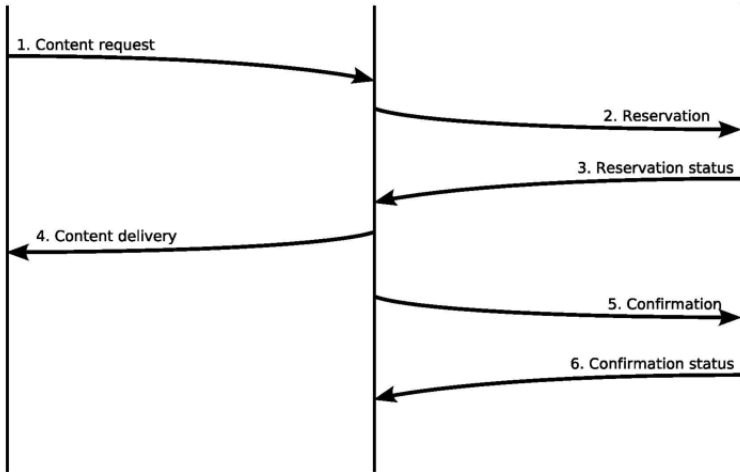
NCBS

New Cyclelogic Billing System

Subscriber

Application

Billing



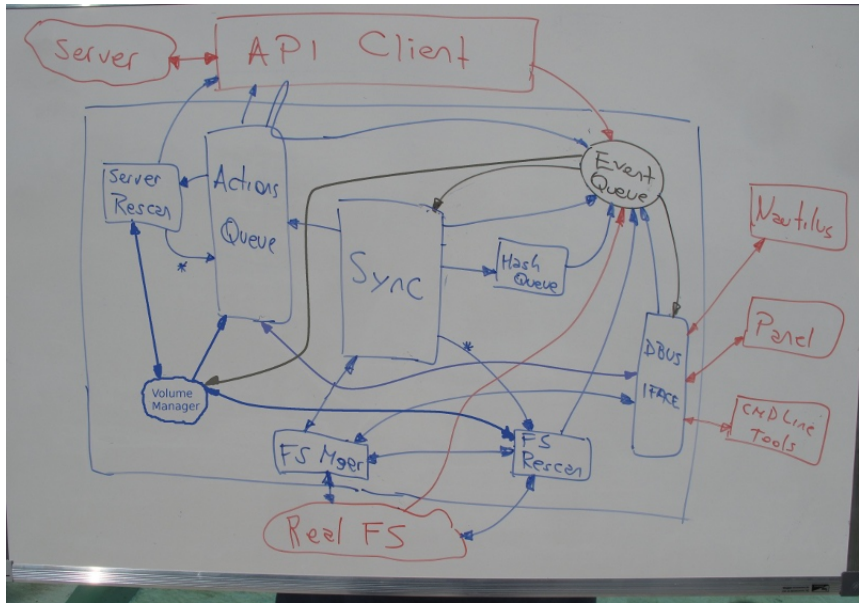
NCBS

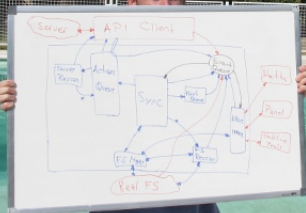
- ▶ **Biblioteca:** ninguna
- ▶ **Público:** otros sistemas vía HTTP
- ▶ **Complejidad:** velocidad; seguridad; robustez; escalabilidad
- ▶ **Ventaja:** simplicidad => seguridad/robustez; reacción ante cambios
- ▶ **Dificultad:** file descriptors por threading/gc; throttling

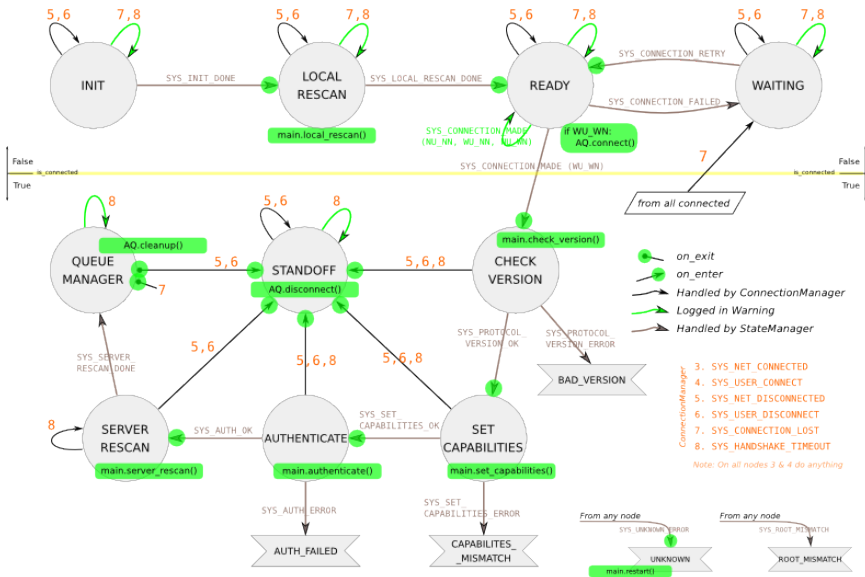
Cliente de Ubuntu One

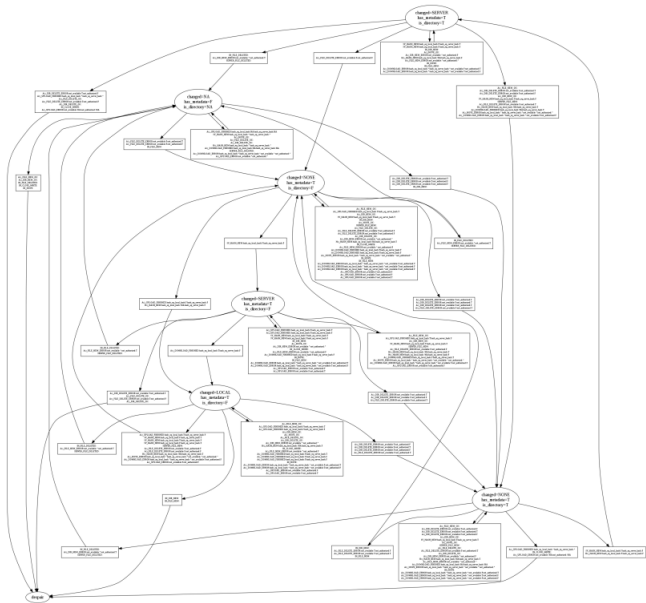
(Sync Daemon)











Sync Daemon

- ▶ **Biblioteca:** twisted; pyinotify
- ▶ **Público:** usuario final; centenares de miles (¡millones!); distribuido en todos los ubuntu's
- ▶ **Complejidad:** seguridad; robustez; sin sorpresas
- ▶ **Ventaja:** tiempo de desarrollo
- ▶ **Dificultad:** integración con Nautilus (tuvo que ser en C), supervisar filesystem y apps

Server de Ubuntu One (File Storage)



File Storage Server de Ubuntu One

- ▶ **Biblioteca:** twisted; storm
- ▶ **Público:** usuarios del cliente
- ▶ **Complejidad:** velocidad; seguridad; escalabilidad
- ▶ **Ventaja:** tiempo de desarrollo
- ▶ **Dificultad:** procesamiento multiserver

CDPedia





WIKIPEDIA
La enciclopedia libre

navegación

- [Portada](#)
- [Wikipedia en la Web](#)
- [Ayuda](#)

búsquedas:

sorprendete:

estadísticas:

Páginas 448038 (100%)
Imágenes 1292335 (99%)

presentada por



Arbeláez

Arbeláez es un municipio de [Cundinamarca \(Colombia\)](#), ubicado en la Provincia de Sabana del Sumapaz, se encuentra a 82 km de [Bogotá](#), limita con [Fusagasugá](#), [Pasca](#), [San Bernardo](#).

Tabla de contenidos [ocultar]

- 1 [Historia](#)
- 2 [Educación](#)
- 3 [Turismo](#)
- 4 [Gobierno](#)
- 5 [Enlaces externos](#)

Historia

Los primitivos habitantes de esta región fueron los Sutagaos. El sitio inicialmente se denomina Hato de [Fusagasugá](#). En 1870 se establecieron numerosos pobladores procedentes de [Guasca](#), entre ellos Vicente Rodríguez, quien cedió área para fundar pueblo e hizo la primera casa, por lo cual se le considera principal fundador. El Municipio se creó por Decreto No.32 de 16 de enero de 1886 del Gobernador del Distrito Federal General Jaime Córdoba con el nombre de Arbeláez. Por Decreto No. 53 de la misma fecha. Se hizo la división territorial de Cundinamarca y Arbeláez quedó como Distrito Integrado del Departamento de [Bogotá](#). Por Decreto 130 de 3 de marzo de 1886 se dispuso su funcionamiento a partir del 1 de abril siguiente y se dieron sus límites. Su primer Alcalde fue Ramón Rodríguez con suplencia de Gregorio Wilches nombrados por Decreto No. 124 de 2 de marzo de 1886. El 22 de octubre de 1870 se erigió en Viceparroquia por Decreto No.7 de 20 de julio de 1907 del *Arzobispo Bernardo Herrera Restrepo*; fue erigido en [Parroquia](#) con el nombre de Concepción de Nuestra Señora. Fue su primer Párroco el Padre Julio Sabogal, quien ejercía la viceparroquia desde 1904.

HECHOS NOTABLES El poblado fue incendiado y arrasado el 29 de enero de 1909 por las fuerzas revolucionarias del General Ruperto Aya durante la guerra de los Mil Días. Fue reconstruido en 1904, según consta en informe del Gobernador de Cundinamarca por Eliseo Medina de 1906. La iglesia antigua fue reconstruida a comienzos de este siglo por el Párroco Julio Sabogal. En 1905 Aureliano Castañeda organizó la segunda Banda Municipal. En 1924 se fundó la tercera bajo la dirección de Víctor José Pardo de Ubaque. Nueva iglesia se comenzó en 1932 por el cura Guillermo Garavito. Fue consagrada el 19 de marzo de 1955 por M acuerdo No. 2 de 1947, confirmado por el No.4 de 1963 presentados por el Concejal Doctor Alfonso Lozano Caballero, se creó el Hospital San F iniciada a principio de siglo por Adan Sabogal y continuada por su hermano Narciso, fue demolida en 1965, año en que se inició la actual. El 14 la Casa de la Cultura.

Educación

País

- [Departamento](#)
- [Región](#)

Localiza

- [Latitud](#)
- [Longitud](#)

Altitud

Temperatura

Población

- [Total](#)
- [Densidad](#)
- [A. Metr](#)

Gentilicio

IDH

CDPedia

- ▶ **Biblioteca:** ninguna
- ▶ **Público:** usuario final; distribución física
- ▶ **Complejidad:** procesamiento de datos; facilidad de uso; portabilidad
- ▶ **Ventaja:** portabilidad
- ▶ **Dificultad:** índice; compresión de datos

Typus Pocus



Hijo mío, este será un
día clave para ti.





Typus Pocus

Tu posición es:

David Copperfield

Puntaje

29

8: David Copperfield

9: Lord Zedd

10: Orko

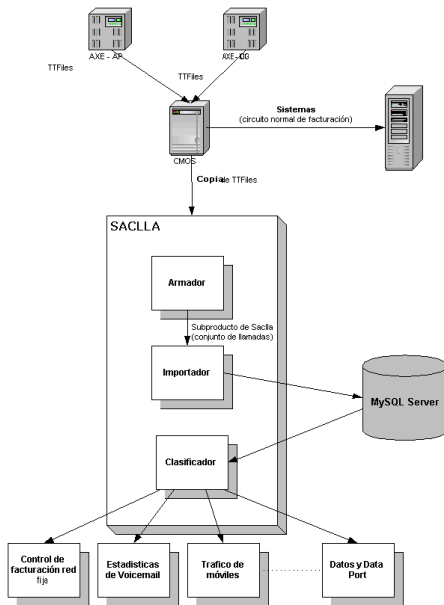
Typus Pocus

- ▶ **Biblioteca:** pygame
- ▶ **Público:** final
- ▶ **Complejidad:** facilidad de uso; portabilidad;
- ▶ **Ventaja:** en 7 días!
- ▶ **Dificultad:** jugabilidad

SACLLA

Sistema de Armado y
Clasificación de LLAmadas

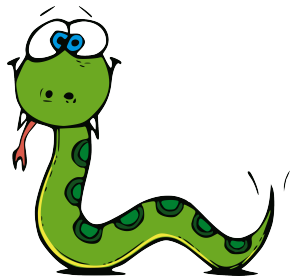




SACLLA

- ▶ **Biblioteca:** MySQLdb
- ▶ **Público:** admin
- ▶ **Complejidad:** velocidad; procesamiento de datos; escalabilidad; robustez
- ▶ **Ventaja:** adaptabilidad
- ▶ **Dificultad:** uptime crítico; no specs

Conclusiones







Powered by
Python



Conclusiones

- ▶ No es la herramienta ideal para todos los casos
 - ▶ Es suficiente la mayor parte del tiempo
- ▶ Es la mejor para prototipar, y entender el problema
 - ▶ *"Premature optimization is the root of all evil"* (Donald Knuth)
- ▶ Hay que usar Python
 - ▶ Pero siempre hay que saber C (aunque no lo usemos)
- ▶ Y sus bibliotecas, incluídas o no
 - ▶ ¡No reinventar la rueda!

¡Muchas gracias!

¿Preguntas?

¿Sugerencias?

Facundo Batista

facundo@taniquetil.com.ar

<http://www.taniquetil.com.ar>



Licencia: Creative Commons

Atribución-NoComercial-CompartirDerivadasIgual 2.5 Argentina

http://creativecommons.org/licenses/by-nc-sa/2.5/deed.es_AR