



Web Application Security Payloads

Andrés Riancho – Lucas Apa
Ekoparty 2010

<http://www.bonsai-sec.com/>

andres@bonsai-sec.com\$ whoami

- **Fundador @** Bonsai Information Security
- **Director of Web Security @** Rapid7
- Programador (python!)
- Open Source Evangelist
- Con conocimientos en networking, diseño y evasión de IPS
- Líder del proyecto open source **w3af**



lucas@bonsai-sec.com\$ whoami

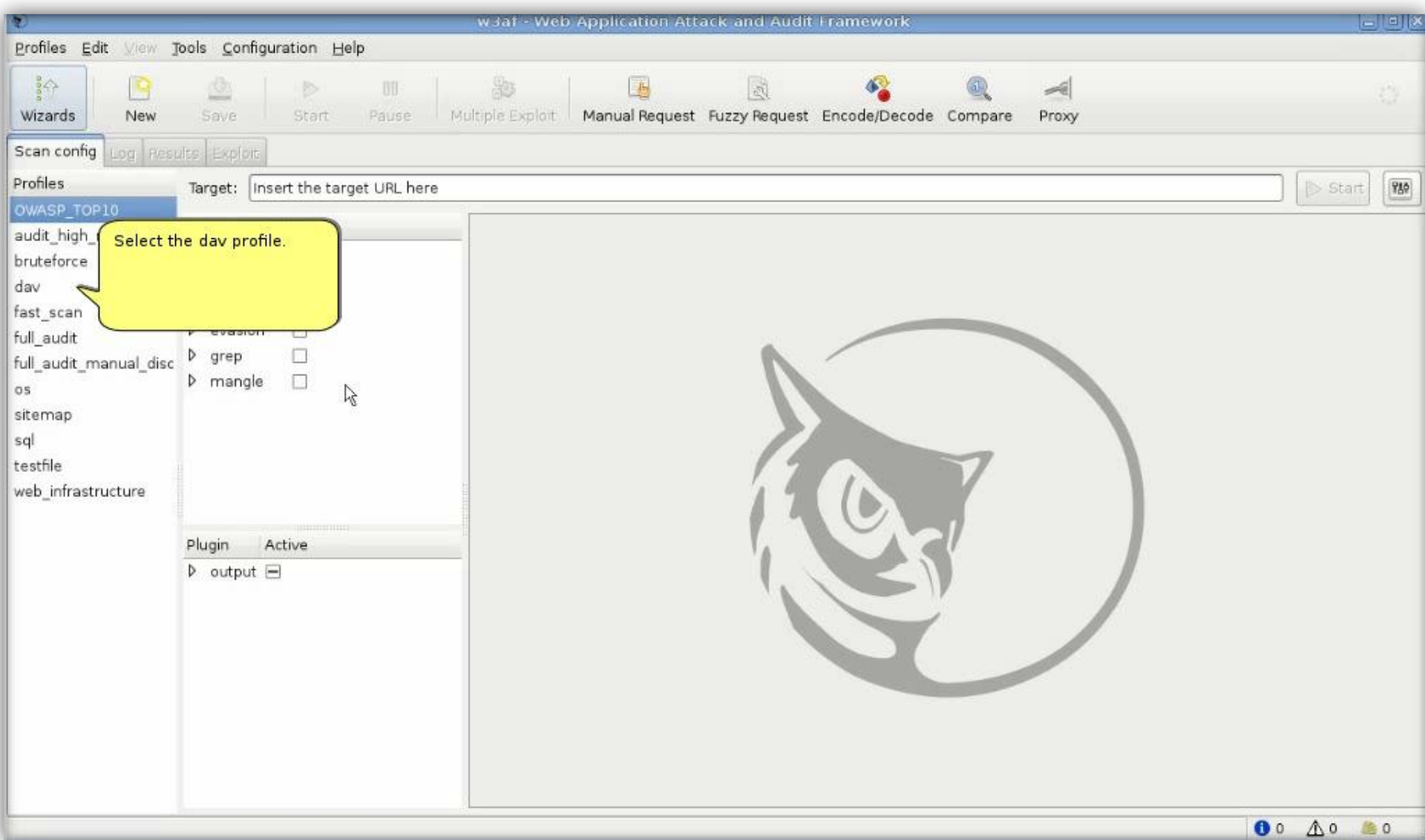
- **Consultor** @ Bonsai Information Security
- Penetration Testing y Vulnerability Research
- Web Application Security enthusiast



w3af

- w3af es un **Web Application Attack and Audit Framework**
- Herramienta Open Source (GPLv2.0) para **detectar y explotar vulnerabilidades Web.**
- Arquitectura basada en plugins, **fácilmente extensible.**
- El desarrollo se inició a finales del 2006 en mis ratos libres, y creciendo hasta la actualidad, momento en el cual tenemos **múltiples contributors alrededor del mundo y un desarrollador full time en nuestras oficinas.**

Web Application Security Payloads



Situación actual

- Los frameworks de explotación como Metasploit proveen mayormente **“payloads” para utilizar en el mejor caso**, es decir, cuando se posee control del flujo de ejecución (“exploit para buffer overflow”).
- Las aplicaciones Web nos permiten, dependiendo de la vulnerabilidad, **interactuar con el sistema de una manera particular**:
 - Lectura arbitraria de archivos
 - Escritura de archivos
 - Ejecución de sentencias SQL
 - Ejecución de comandos del sistema operativo
- Hasta hoy, ¿Que **pasos de post-explotación** podíamos hacer de manera automatizada en un entorno en el cual **no ejecutamos comandos del sistema operativo**?

Situación actual

- Adicionalmente, las vulnerabilidades Web **mutan** cada vez mas rápidamente haciendo que su post explotación no tenga un punto de partida u objetivo final bien definido.
- Las diferentes **herramientas automatizadas** se focalizan en lo particular, en explotar una vulnerabilidad haciendo énfasis en el **cómo**.
- No definen que información se quiere comprometer. Las vulnerabilidades vencen o cambian.





Web Application Security Payloads

Diseño

- Pequeños **fragmentos** de código que corren en w3af luego de explotar una o más vulnerabilidades conocidas.
- Cada payload es **independiente** de las vulnerabilidades descubiertas, ya que el exploit exporta “**System Calls**”, los cuales son luego utilizados por los payloads:

Exploit	System calls exportados	System calls emulados
Local file read	read()	
Local file include	read()	
OS Commanding	execute()	read() , write() , unlink()
DAV Shell	write()	execute() , read(), unlink()
File Upload	write()	execute() , read(), unlink()

Diseño

- Los payloads son en general **100 líneas de código** que utilizan **un par de system calls**, como por ejemplo el de “running_vm”:

```
pci_list.append('1233')
pci_list.append('1af4:1100')
pci_list.append('80ee:beef')
pci_list.append('80ee:cafe')

for candidate in candidates:
    file = self.shell.read('/sys/bus/pci/devices/' + candidate)
    pci_id = parse_pci_id(file)
    pci_subsys_id = parse_subsys_id(file)
    for pci_item in pci_list:
        if pci_item in pci_id or pci_item in pci_subsys_id:
            result['running_vm'] = True
```


Demo #1: “users”



Sinergia entre payloads

read()

System call para leer archivos

users

Payload que lee /etc/passwd e identifica home directories

users_config_files

Payload que utiliza el conocimiento de home directories y busca allí archivos de configuración

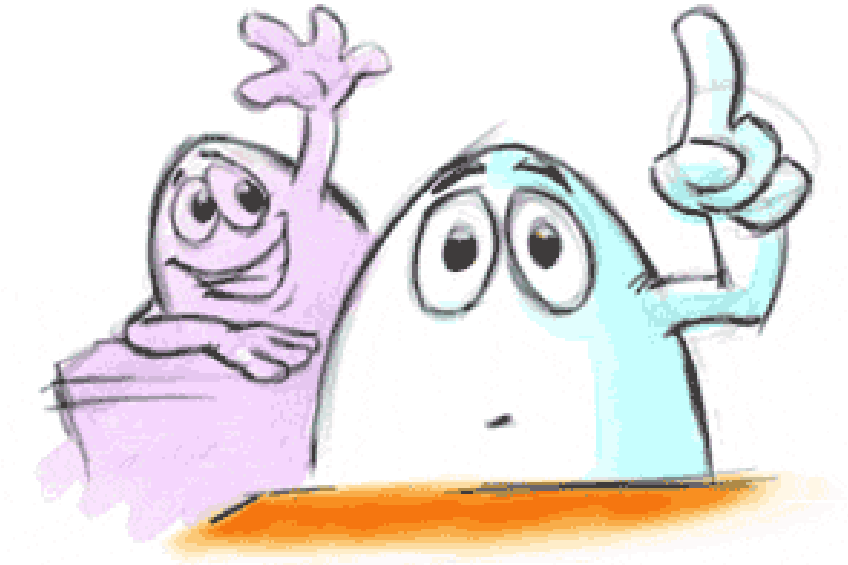
Demo #2:

Sinergia entre payloads:
“users_config_files”

Demo #3:
Integración con w3af:
“get_source_code”

Conclusiones y trabajo pendiente

- Conceptualizar esta idea como **estándar en la post-explotación** automatizada sobre aplicaciones Web.
- Desarrollar más payloads para **entornos Windows**.
- Investigar sobre **syscall hooking** y envío de syscalls al sistema remoto por medio de las web application payloads.
- **Priorización de syscalls:** cuando existe más de un syscall, cual utilizo para acceder al sistema remoto? El más rápido? El de más privilegios?
- Contribuir con la **comunidad** global descubriendo nuevas técnicas de ataque mediante **técnicas de post-explotación minimalistas**, expandiendo la información que aportan.



¿Dudas?
¿Preguntas?



Gracias!