



OWASP Pantera Unleash

Simon Roses Femerling
OWASP Pantera Project Lead
Security Technologist, Microsoft
pantera.proxy@gmail.com

OWASP
Day
Belgium - Sep 2007

Copyright © 2007 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the Creative Commons Attribution-ShareAlike 2.5 License. To view this license, visit <http://creativecommons.org/licenses/by-sa/2.5/>

The OWASP Foundation
<http://www.owasp.org/>

Intro - Who I am?

- Security Technologist at Microsoft.
- Former PwC, @Stake among others...
- Postgraduate in E-Commerce from Harvard University and a B.S. from Suffolk University at Boston, Massachusetts.
- Natural from wonderful Mallorca Island in the Mediterranean Sea.



Agenda

- Pantera Overview
- Pantera Features
- Privacy Assessments
- Demo
- Q&A





Pantera Overview

Pantera Overview (I)

- Pantera is not just another “proxy” but a Web Assessment Framework.
 - ▶ aka: Pantera – Web Assessment Studio (WAS)
- Analysis Framework.
- Born out of necessity.
- Pantera Description:
 - ▶ Pantera uses an improved version of SpikeProxy to provide a powerful web application analysis engine.

Pantera Overview (II)

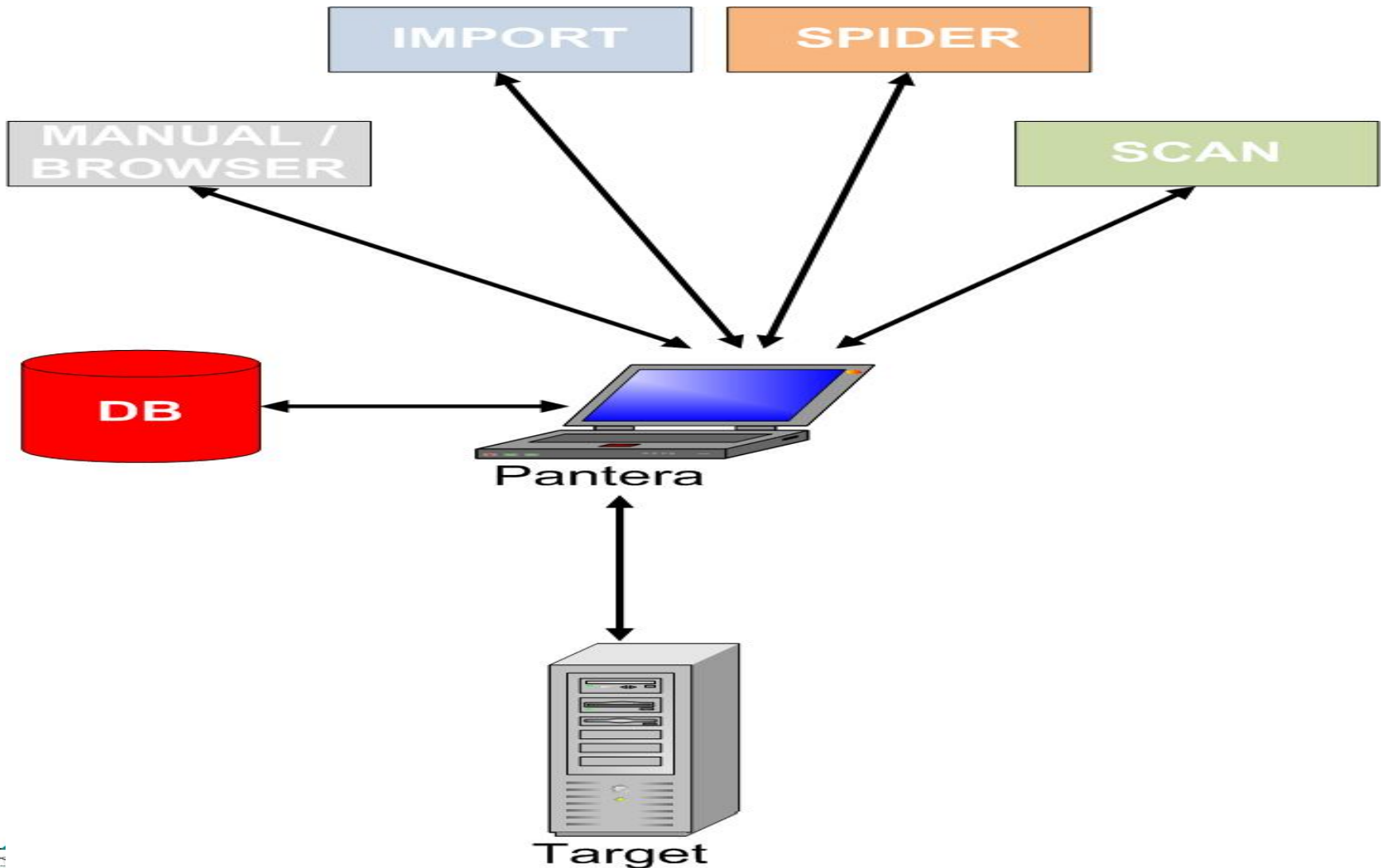
- Pantera works well with other proxies and is a complementary tool.
- Pantera is 100% python and has been tested on:
 - ▶ Windows
 - ▶ Linux
 - ▶ MacOS
 - ▶ FreeBSD



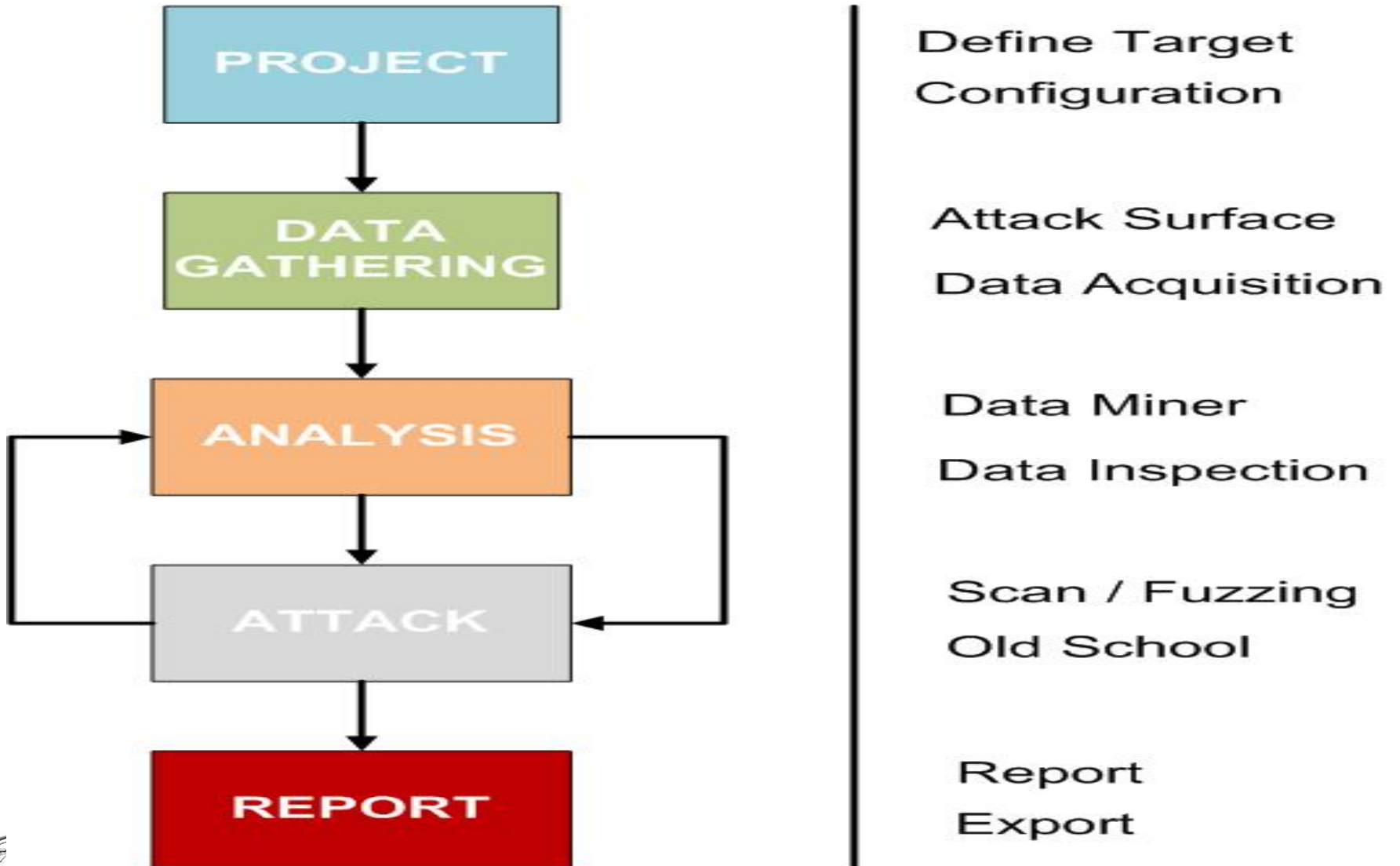
Pantera Overview (III)

- Two main operational modes:
 - ▶ Cache
 - ▶ Project Session

Pantera Architecture



Pantera Workflow



Pantera Goal

- The primary goal of Pantera is to combine automated capabilities with complete manual testing to get the best penetration testing results.





Pantera Features

Pantera Features List

- Session Management
- Database support
- Pantera Passive Analysis (PPA)
- Import / Export
- Spider
- Data Miner
- Visual Resource Icons (VRI)
- Fingerprint (Cookies / Extensions)
- Anti-IDS Generation
- Statistics
- The Snitch

Pantera Feature – Session Management

- An assessment is a project.
- Manage your projects easily.
- Under Project Session Mode you get the “whole enchilada”.

Pantera Feature – Session Management

Project Management

Home	File	Tools	Help
------	------	-------	------

New Project

Project Name:

Available Projects

Select Project: Open Delete

[Roses Labs](#) (C) 2003-2006



Pantera Feature – Pantera Passive Analysis (PPA)







- PPA is a passive analysis engine on the fly.
- PPA checks are easy to write plug-ins.
- Checks are divided into categories (17)
 - ▶ Forms / Authentication Forms
 - ▶ SSL
 - ▶ Email
 - ▶ Cookies
- More than 20+ checks available.






Pantera Feature – Pantera Passive Analysis (PPA)



Pantera Passive Analysis Summary

Home	File	Tools	Help
------	------	-------	------

- http://www.owasp.org/index.php/Main_Page
[2006-09-28 | 9:59:04]      
 - ⊙ Page has HTML comments!
 - ⊙ Page has C-Style block comments!
 - ⊙ Page has Single Line comments!

- <http://www.owasp.org/skins/common/wikibits.js>
[2006-09-28 | 9:59:08] 
 - ⊙ Page has Single Line comments!

- <http://www.owasp.org/index.php?title=-&action=raw&gen=js>
[2006-09-28 | 9:59:09]  ? 
 - ⊙ Page has C-Style block comments!

- <http://www.owasp.org/index.php?title=MediaWiki:Common.css&action=raw&ctype=text/css&smaxage=18000>
[2006-09-28 | 9:59:11]  ? 



Pantera Feature – Spider

- Pantera now includes a Spider. (still in infancy)
- Works in both operational modes.
- Uses many smart gathering techniques:
 - ▶ Parse robots.txt
 - ▶ Parse sitemap
 - ▶ Parse JavaScript
 - ▶ Request Directory Index

Pantera Feature – Data Miner

- “Get what you want”.
- Allows to get any information from the project.
 - ▶ Emails
 - ▶ IE. Query “All links with forms”
- Only place in Pantera to view all links.
- Easy to use and powerful.



Pantera Feature – Data Miner

Home	File	Tools	Help
------	------	-------	------

Add to Project Info

Type: Value: Domain:

Search on Project Info

Select:

Search Links With

Select:

Search Links

Select: Select: Criteria:

Display All Links





Project Info Data Results: target (1)

| | Select/Unselect All | [[New Search](#)]

domain: target:



Pantera Feature – Visual Resource Icons (VRI)

- The Visual Resource Icons are an easy and convenient way of quickly identify target page attributes.
- More than +10 icons:
 - ▶  Target page has an object. (ActiveX, Java Applet, etc.)
 - ▶  Target page has Authorization Forms
 - ▶  Target page sets a Session ID
 - ▶  Target page has possible attack vectors (like forms, hidden tags, URL parameters, etc.)

Pantera Feature – Fingerprint

- Pantera can fingerprint:

- ▶ File Extensions: +60 files.
- ▶ Session ID: +40 applications.

- Fingerprints are stored in XML files.

- This information is used by many other Pantera features.



Pantera Feature – Fingerprint

```
<pattern desc="MS IIS">ASPSESSIONID.*?(;| )</pattern>  
<pattern desc="ASP.NET">ASP.NET_SessionId.*?(;| )</pattern>  
<pattern desc="IBM Tivoli Policy Director WebSeal">PD-S-SESSION-  
  ID.*?(;| )</pattern>  
<pattern desc="IBM Tivoli Policy Director  
  WebSeal">PD_STATEFUL.*?(;| )</pattern>  
<pattern desc="WEBTRENDS">WEBTRENDS_ID.*?(;| )</pattern>  
<pattern desc="IBM WebSphere Application Server">sessionid.*?(;|  
  )</pattern>  
<pattern desc="IBM WebSphere Application Server or Siebel  
  CRM">_sn.*?(;| )</pattern>  
<pattern desc="BlueCoat Proxy">BCSI-.*?(;| )</pattern>  
<pattern desc="Coldfusion">CFID.*?(;| )</pattern>  
<pattern desc="Coldfusion">CFTOKEN.*?(;| )</pattern>
```



Pantera Feature – Statistics

- Very helpful to get a quick status on the project.
- Divided into 5 sections:
 - ▶ General Information
 - ▶ Pages Extension Counter
 - ▶ Data gathered from Application
 - ▶ HTTP Return Codes Information
 - ▶ Links Information

Pantera Feature – Statistics

Project Assessment Statistics

Home	File	Tools	Help
----------------------	----------------------	-----------------------	----------------------

General Information

Interesting Links:	8
Total Links:	36

Pages Extension Counter

JPG	7	JPEG/JIFF Image
JS	1	JavaScript Source Code
GIF	17	Graphic Interchange Format
CSS	2	Hypertext Cascading Style Sheet
PHP	5	Perl Hypertext Pages (aka Personal Home Page Tools)
PNG	2	Portable (Public) Network Graphic
UNKNOW	1	

Data Gathered from Application

Total target:	1
Total server:	1
Total email:	1

Links Information

Links with Authentication:	0
----------------------------	---







Pantera Feature – The Snitch

- The Snitch is a gather of information.
- It can currently gather:
 - ▶ Comments
 - ▶ Scripts
 - ▶ Links


Pantera Feature – The Snitch

♦ http://www.owasp.org/index.php/Main_Page

[2006-09-28 | 9:59:04]      

```
<!-- Saved in parser cache with key owiki:pcache:idhash:1-0!1!0!0!!en!2!edit=0 and timestamp
20060928003354 -->
```

♦ http://www.owasp.org/index.php/Main_Page

[2006-09-28 | 9:59:04]      

```
<!-- end content -->
```





Privacy Assessments

Privacy Assessments (I)

■ PII – Personally Identifiable Information

- ▶ Wikipedia: “Any piece of information which can be potentially be used to uniquely identify, contact, or locate a single person.”
- ▶ Full Name
- ▶ Telephone Number
- ▶ Email Address
- ▶ Street Address

Privacy Assessments (II)

■ Sensitive PII

- ▶ Medical/health condition
- ▶ Racial origin
- ▶ Political, religious and philosophical views
- ▶ PIN
- ▶ Passwords

Privacy Assessments (III)

- Not as sexy as pen-test but necessary.
- Knowledge gap:
 - ▶ Security consultant
 - ▶ Clients
- Many countries require by law privacy assessments (kind of).
 - ▶ Spain: LSSI / LPOD

Privacy Assessments (IV)

■ Some things to look for (web apps):

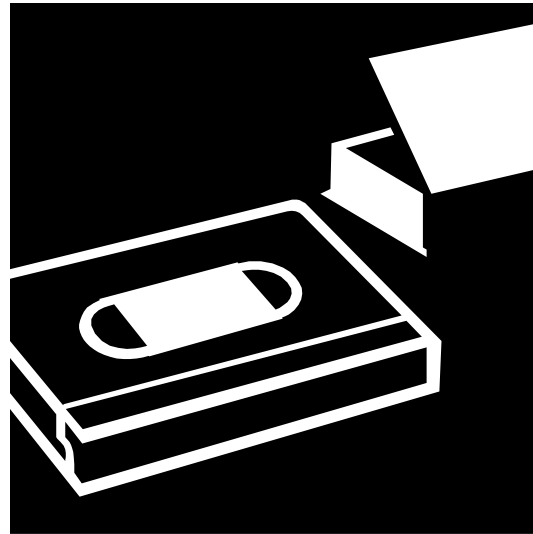
- ▶ Disclaimer
 - Site contains a disclaimer page
 - All pages link to the disclaimer
 - Is the disclaimer clear?
- ▶ Legal Notice
- ▶ What type of data is the app collecting
- ▶ How is the site managing our information
- ▶ Are we advised of any changes?
- ▶ Is Sensitive PII transfer secure?
- ▶ Why site needs Sensitive PII?



Pantera Privacy Analysis

- Pantera now includes privacy analysis feature!
- PPA Privacy Category.
- Currently 3 plugins:
 - ▶ Looks for disclaimers links
 - ▶ Checks if site uses P3P
 - ▶ Looks for US Social Security Numbers
- New Privacy Analysis Page on the UI 😊





DEMOS

The End

■ Q&A

- Important: Beer / hard liquor (Vodka Lemon, Margaritas, Mojitos, you named it...) are always welcome 😊

- Simon Roses Femerling
pantera.proxy@gmail.com



Pantera Resources

- Official Website

[http://www.owasp.org/index.php/Category:OWASP Pantera Web Assessment Studio Project](http://www.owasp.org/index.php/Category:OWASP_Pantera_Web_Assessment_Studio_Project)

- Mailing list

<https://lists.owasp.org/mailman/listinfo/owasp-pantera>

- Contact us

pantera.proxy@gmail.com

