WEBGOAT and the Pantera Web Assessment Studio Project

Philippe Bogaerts

OWASP Belgium Chapter

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

Introduction

- During the day
  - Coming soon … I hope ☺
- During the night
  - Independent trainer and consultant
  - Trying to acquire a good understanding of
    - network security
    - web application, web services and XML security
    - Pen-testing

    mailto:philippe.bogaerts@radarhack.com

    http://www.radarhack.com

Why am I here ?

- A fascination for security…
- I like learning and exploring new things…
- Continuous education and awareness today is a must and must be kept big fun…

- … and this resulted in writing a paper called

  "Getting started with OWASP WebGoat4 and SOAPUI."

  (The paper is available at http://www.radarhack.com)

… and thanks to *Erwin Geirnaert* from http://www.zionsecurity.com for reviewing the paper.

ZION SECURITY
SECURING YOUR BUSINESS VALUE

What is the paper about ?

- Explain in a simple and easy way what SOAP and web services are about.

- A unique opportunity to use WebGoat 4.0 for what it is intended to do: education and awareness

- The paper is about how a web service can be exploited via simple and free available invocation tools.

Part 1:   WebGoat

WebGoat

- **WebGoat** is a deliberately insecure J2EE web application maintained by OWASP

- Designed to teach web application security

- … but also useful to test security products
  - IPS, Firewalls, Web Application Firewalls …
    - … against OWASP top 10 promise
    - … against XML and AJAX security threats

- Who already played around with WebGoat ?

WebGoat versions

- Release Quality Projects

- Current stable version: 4.0
  - http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

- A promising version 5.0 will be available 01/2007.
  - Release candidate 1 is available since 17/01/2007

Installing WebGoat

- Download available via OWASP project pages
- Windows and Unix/Linux versions

- Today we are using

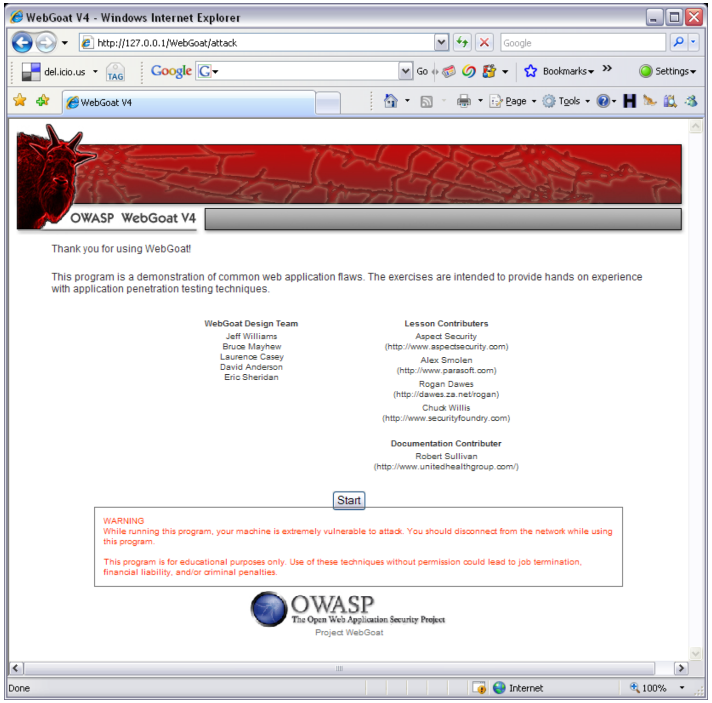
  Windows_WebGoat-4.0_Release.zip

  Windows_WebGoat-5.0-RC1_Release.zip

- Just unzip the archive and click *webgoat.bat*
  - *Some pitfalls*
    - *Make sure other web servers are stopped*
    - *Skype for some reason dares to use port 80*
    - *Verify with "netstat –an" port 80 is not used*

Connecting the first time

- http://webgoat_server/WebGoat/attack
- login with usn:guest and pwd:guest


WebGoat V4 - Windows Internet Explorer
http://127.0.0.1/WebGoat/attack
Google
del.icio.us
Bookmarks
Settings
WebGoat V4
Page
Tools
OWASP WebGoat V4

Thank you for using WebGoat!

This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

WebGoat Design Team
Jeff Williams
Bruce Mayhew
Laurence Casey
David Anderson
Eric Sheridan

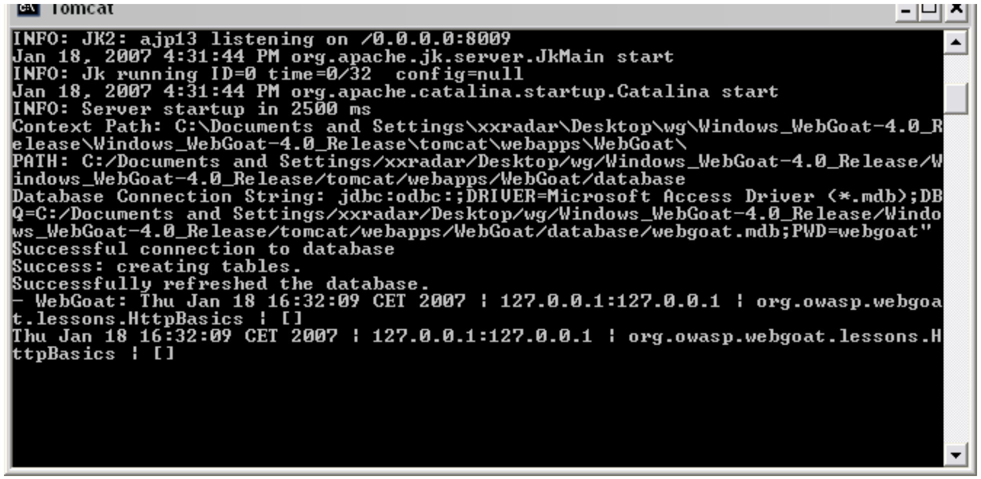
Lesson Contributers
Aspect Security
(http://www.aspectsecurity.com)
Alex Smolen
(http://www.parasoft.com)
Rogan Dawes
(http://dawes.za.net/rogan)
Chuck Willis
(http://www.securityfoundry.com)

Documentation Contributer
Robert Sullivan
(http://www.unitedhealthgroup.com/)

Start

WARNING
While running this program, your machine is extremely vulnerable to attack. You should disconnect from the network while using this program.

This program is for educational purposes only. Use of these techniques without permission could lead to job termination, financial liability, and/or criminal penalties.



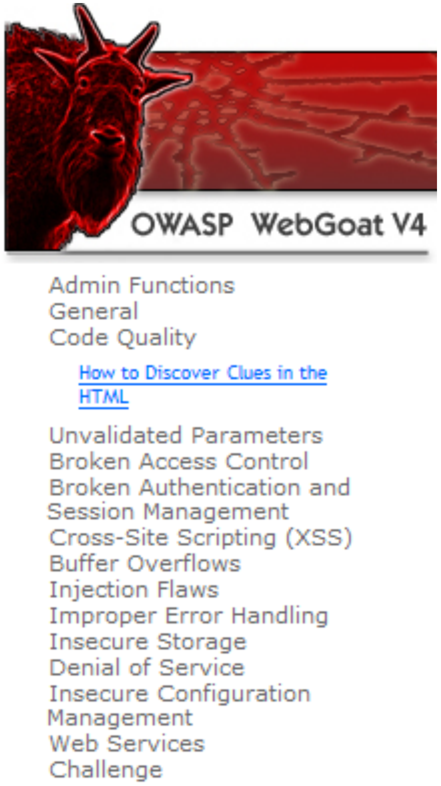
```
INFO: JK2: ajp13 listening on /0.0.0.0:8009
Jan 18, 2007 4:31:44 PM org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/32  config=null
Jan 18, 2007 4:31:44 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 2500 ms
Context Path: C:\Documents and Settings\xxradar\Desktop\wg\Windows_WebGoat-4.0_R
elease\Windows_WebGoat-4.0_Release\tomcat\webapps\WebGoat\
PATH: C:/Documents and Settings/xxradar/Desktop/wg/Windows_WebGoat-4.0_Release/W
indows_WebGoat-4.0_Release/tomcat/webapps/WebGoat/database
Database Connection String: jdbc:odbc:;DRIVER=Microsoft Access Driver (*.mdb);DB
Q=C:/Documents and Settings/xxradar/Desktop/wg/Windows_WebGoat-4.0_Release/Windo
ws_WebGoat-4.0_Release/tomcat/webapps/WebGoat/database/webgoat.mdb;PWD=webgoat"
Successful connection to database
Success: creating tables.
Successfully refreshed the database.
- WebGoat: Thu Jan 18 16:32:09 CET 2007 | 127.0.0.1:127.0.0.1 | org.owasp.webgoa
t.lessons.HttpBasics | []
Thu Jan 18 16:32:09 CET 2007 | 127.0.0.1:127.0.0.1 | org.owasp.webgoat.lessons.H
ttpBasics | []
```

Configuration tuning

- ...Windows_WebGoat-4.0_Release\tomcat\conf\server.xml
  - Port numbers of the web server
- ...Windows_WebGoat-4.0_Release\tomcat\conf\tomcat-users.xml
  - Tomcat usernames, passwords and role

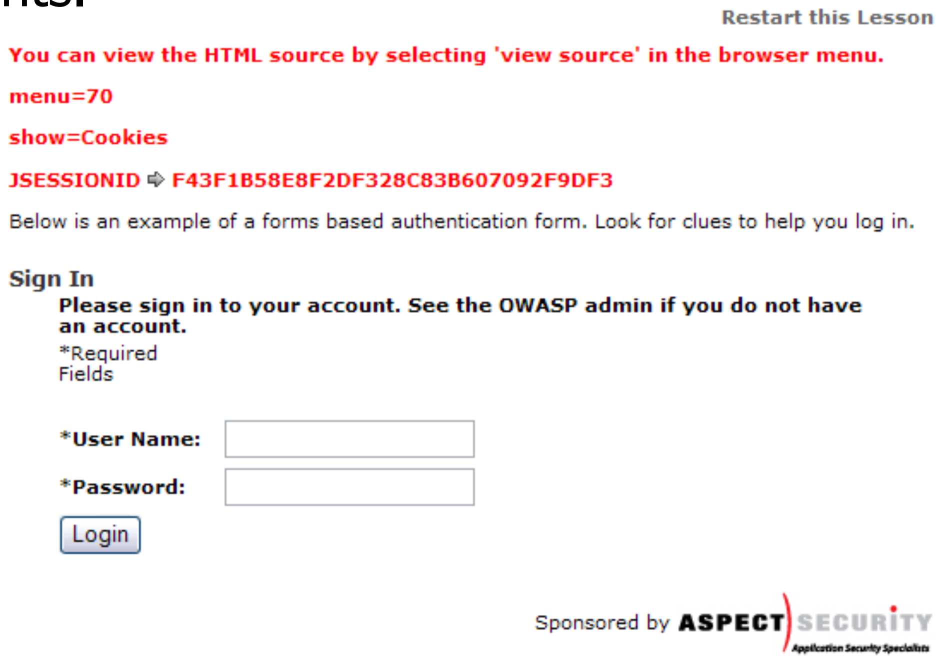
WebGoat V4

- A set of lessons and exercises to learn about basic and advanced web application security issues.
  - Coverage OWASP TOP 10
  - … and more



WebGoat is a training tool

- Tools to assist
  - Hints
    - Starting tips up to the solutions of the problem
    - Scroll through the hints.
  - Show Cookies
  - Show Java
  - Show Params
  - Report Card



Restart this Lesson

You can view the HTML source by selecting 'view source' in the browser menu.

menu=70

show=Cookies

JSESSIONID ➪ F43F1B58E8F2DF328C83B607092F9DF3

Below is an example of a forms based authentication form. Look for clues to help you log in.

Sign In

Please sign in to your account. See the OWASP admin if you do not have an account.

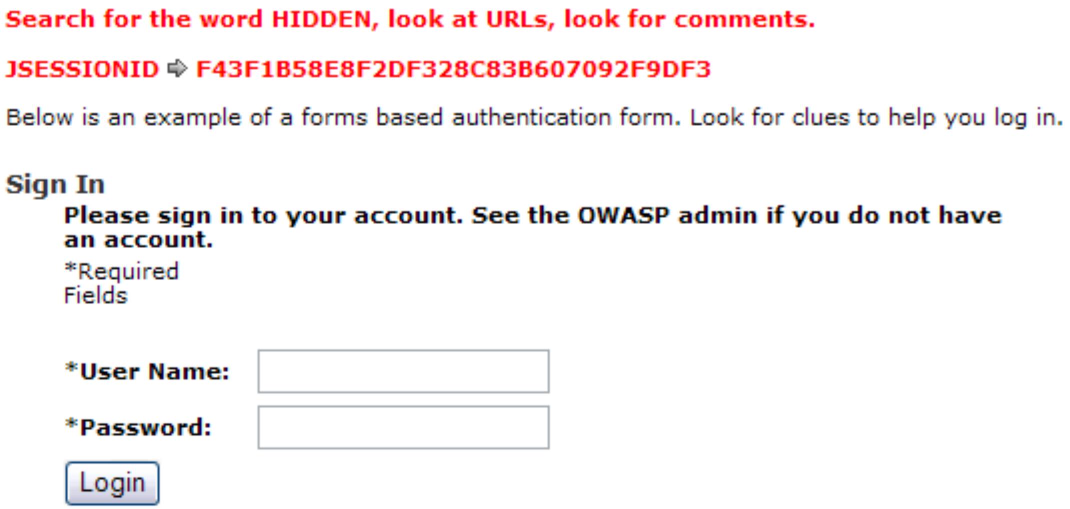
*Required Fields

***User Name:**	
***Password:**	

Sponsored by ASPECT SECURITY Application Security Specialists

Example 1

- Code Quality
  - Look in the source code
  - Use WebScarab !!!
    - Fragments module



Search for the word HIDDEN, look at URLs, look for comments.

JSESSIONID ➪ F43F1B58E8F2DF328C83B607092F9DF3

Below is an example of a forms based authentication form. Look for clues to help you log in.

Sign In

Please sign in to your account. See the OWASP admin if you do not have an account.

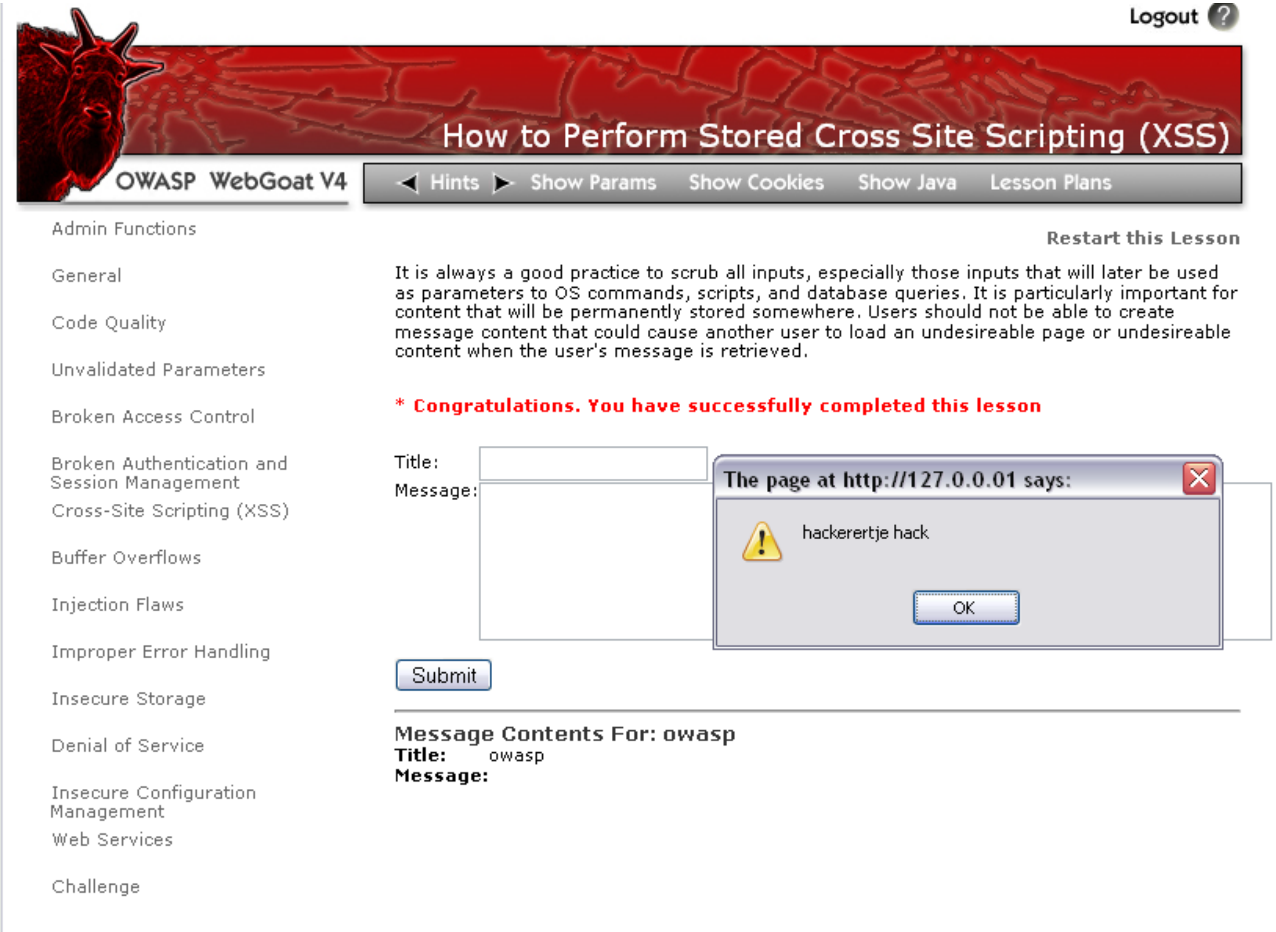
*Required Fields

***User Name:**

***Password:**

Example 2

- Stored XSS



How to Perform Stored Cross Site Scripting (XSS)

It is always a good practice to scrub all inputs, especially those inputs that will later be used as parameters to OS commands, scripts, and database queries. It is particularly important for content that will be permanently stored somewhere. Users should not be able to create message content that could cause another user to load an undesireable page or undesireable content when the user's message is retrieved.

* Congratulations. You have successfully completed this lesson

Title:

Message:

The page at http://127.0.0.01 says:

hackerertje hack

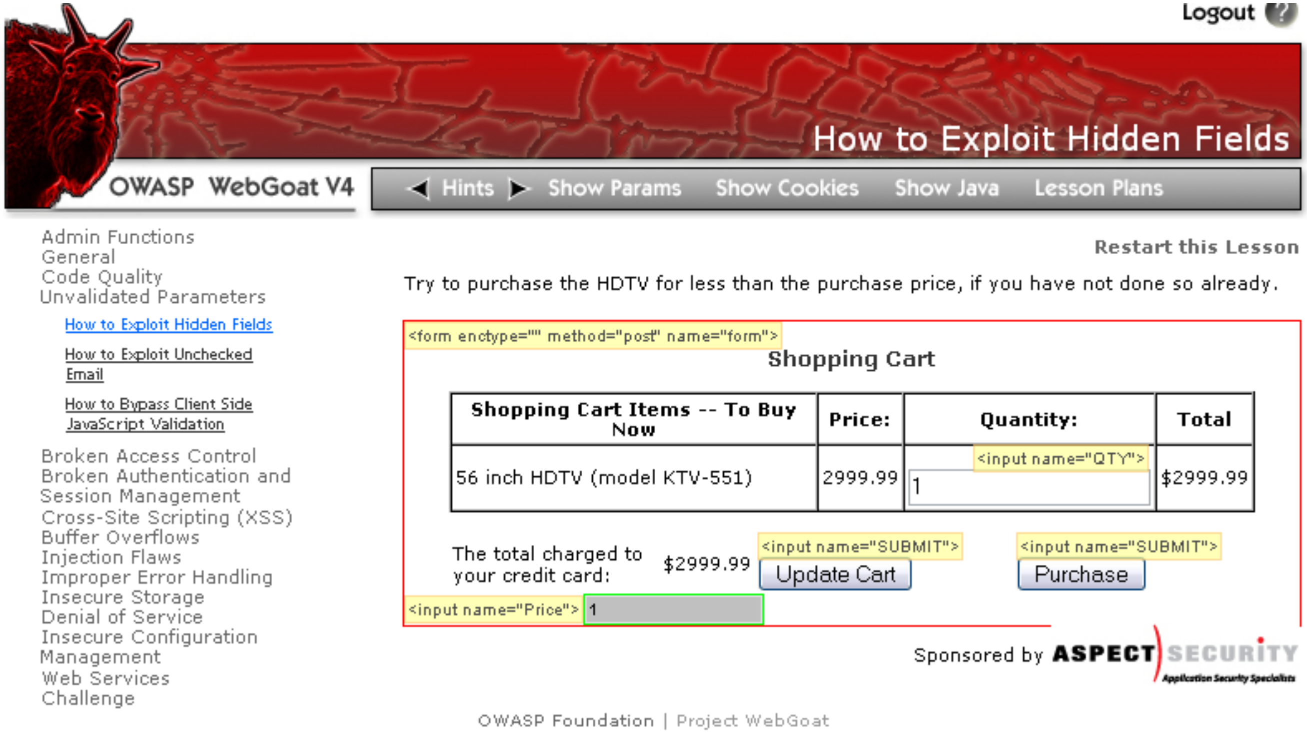
Message Contents For: owasp

Title: owasp

Message:

Example 3

- Exploiting Hidden Fields
  - Web Developer plug-in Firefox


Logout
How to Exploit Hidden Fields
OWASP WebGoat V4
Hints
Show Params
Show Cookies
Show Java
Lesson Plans
Admin Functions
General
Code Quality
Unvalidated Parameters
How to Exploit Hidden Fields
How to Exploit Unchecked Email
How to Bypass Client Side JavaScript Validation
Broken Access Control
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws
Improper Error Handling
Insecure Storage
Denial of Service
Insecure Configuration Management
Web Services
Challenge
Restart this Lesson
Update Cart
Purchase
Sponsored by ASPECT SECURITY Application Security Specialists
OWASP Foundation | Project WebGoat

Try to purchase the HDTV for less than the purchase price, if you have not done so already.

<form enctype="" method="post" name="form">

Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
56 inch HDTV (model KTV-551)	2999.99	<input name="QTY"> 1	$2999.99

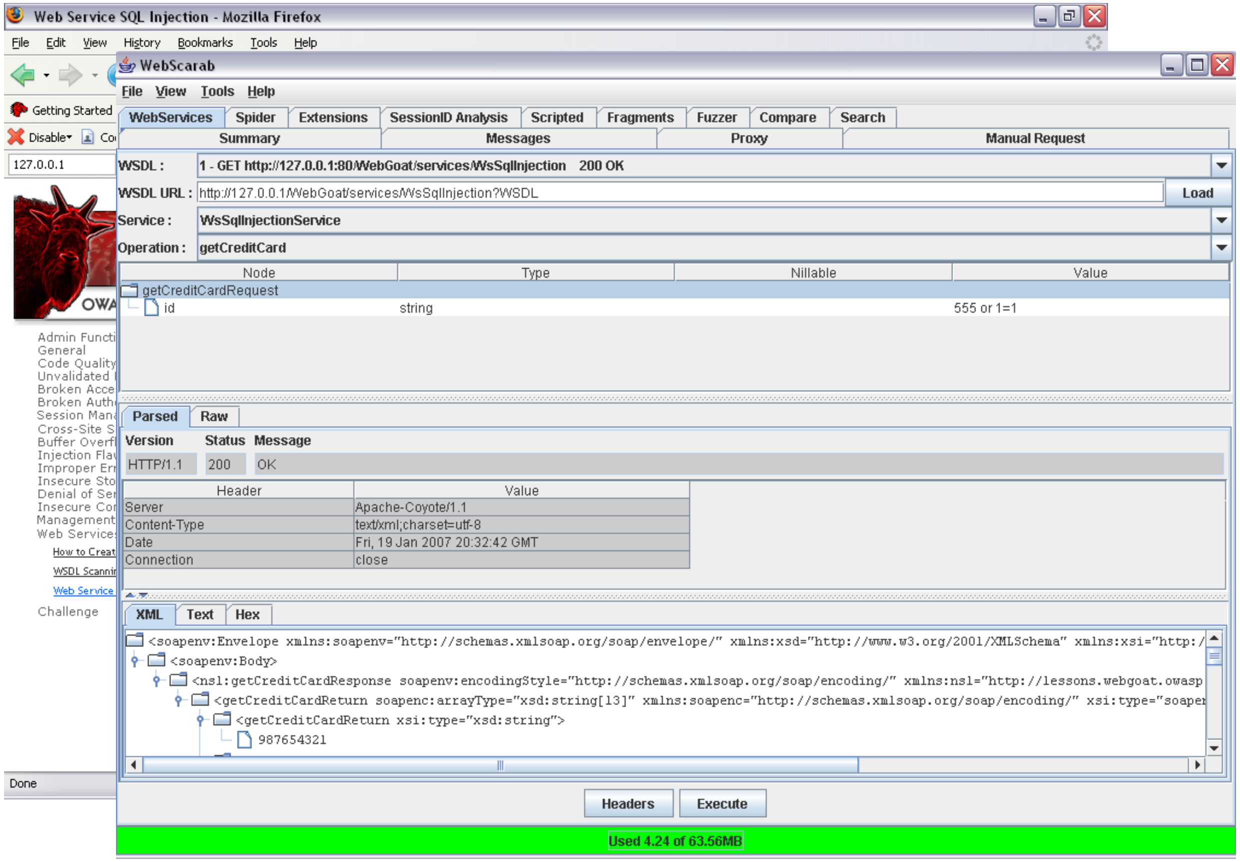
The total charged to your credit card: $2999.99

<input name="SUBMIT"> <input name="SUBMIT">

<input name="Price"> 1

Example 4

- Exploiting Web Services with SQL Injection
  - WebScarab


Web Service SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Getting Started
Disable
127.0.0.1
WebScarab
File View Tools Help
WebServices Spider Extensions SessionID Analysis Scripted Fragments Fuzzer Compare Search
Summary Messages Proxy Manual Request
Load
Parsed Raw
XML Text Hex
Headers Execute
Used 4.24 of 63.56MB
Done

WSDL : 1 - GET http://127.0.0.1:80/WebGoat/services/WsSqlInjection 200 OK

WSDL URL : http://127.0.0.1/WebGoat/services/WsSqlInjection?WSDL

Service : WsSqlInjectionService

Operation : getCreditCard

Node	Type	Nillable	Value
getCreditCardRequest			
id	string		555 or 1=1

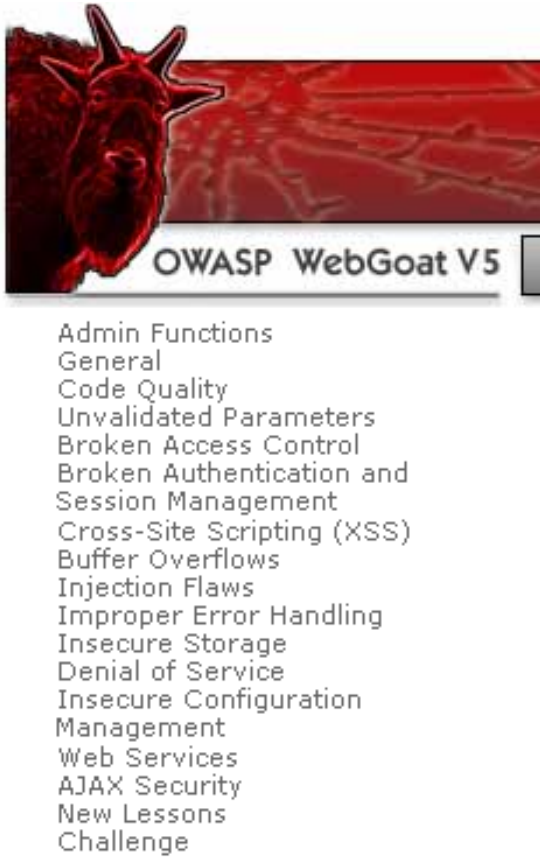
Version	Status	Message
HTTP/1.1	200	OK

Header	Value
Server	Apache-Coyote/1.1
Content-Type	text/xml;charset=utf-8
Date	Fri, 19 Jan 2007 20:32:42 GMT
Connection	close

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http:/
  <soapenv:Body>
    <ns1:getCreditCardResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:ns1="http://lessons.webgoat.owasp
      <getCreditCardReturn soapenc:arrayType="xsd:string[13]" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="soapen
        <getCreditCardReturn xsi:type="xsd:string">
          987654321
```

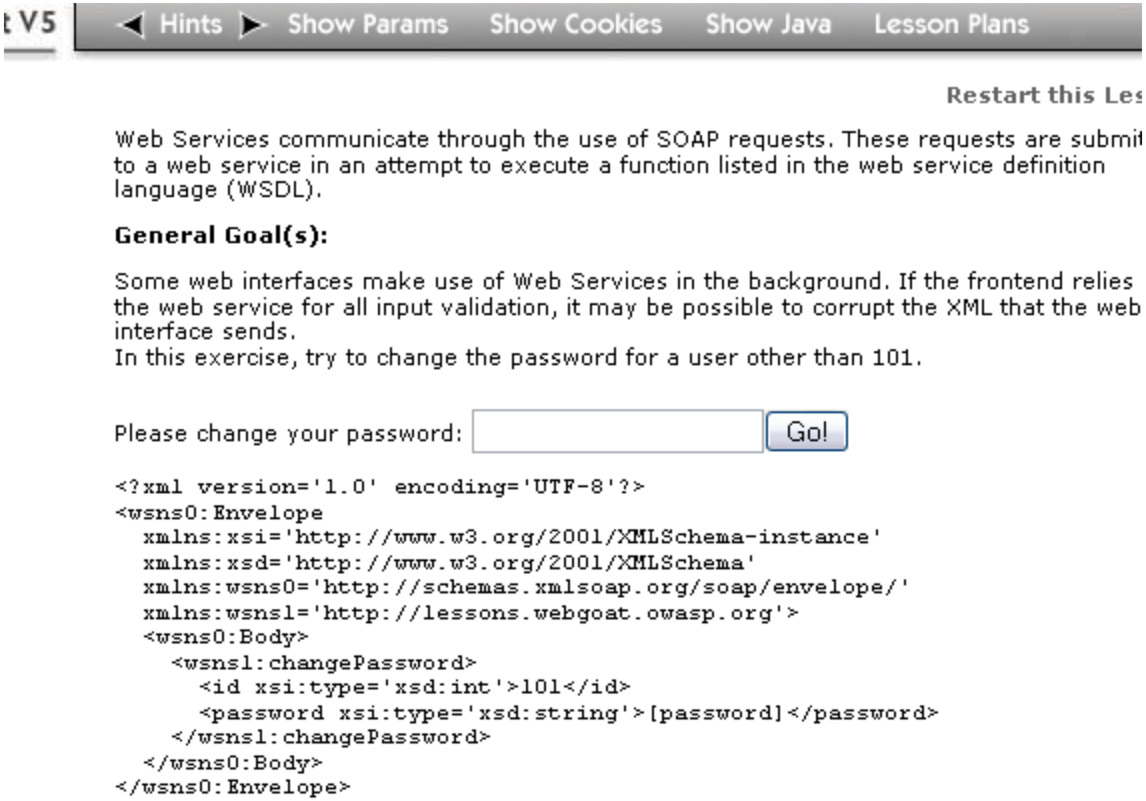
WebGoat V5 (rc1)

- What new ?
  - More XSS
    - Forced Browsing
    - How to Perform CSRF
  - More on SQL Injection
    - Blind SQL Injection
    - XPATH Injection
  - Web Services
    - SAX parser injection
  - AJAX security lessons
  - … and much more



Example 5

- Web Service SAX injection



Web Services communicate through the use of SOAP requests. These requests are submit to a web service in an attempt to execute a function listed in the web service definition language (WSDL).

General Goal(s):

Some web interfaces make use of Web Services in the background. If the frontend relies the web service for all input validation, it may be possible to corrupt the XML that the web interface sends.
In this exercise, try to change the password for a user other than 101.

Please change your password: Go!

```
<?xml version='1.0' encoding='UTF-8'?>
<wsns0:Envelope
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  xmlns:xsd='http://www.w3.org/2001/XMLSchema'
  xmlns:wsns0='http://schemas.xmlsoap.org/soap/envelope/'
  xmlns:wsns1='http://lessons.webgoat.owasp.org'>
  <wsns0:Body>
    <wsns1:changePassword>
      <id xsi:type='xsd:int'>101</id>
      <password xsi:type='xsd:string'>[password]</password>
    </wsns1:changePassword>
  </wsns0:Body>
</wsns0:Envelope>
```

Part 2: Pantera Web Assessment Studio Project

Pantera WASP, what is it ?

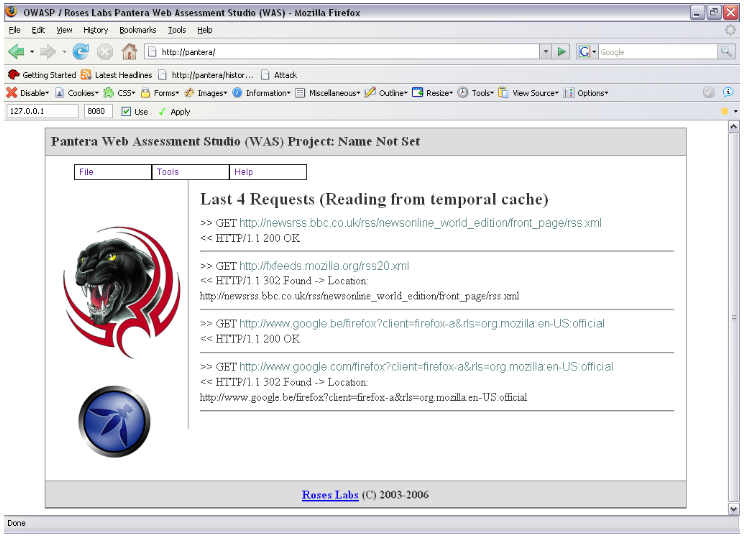
- “The primary goal of Pantera is to combine automated capabilities with complete manual testing to get the best penetration testing results.”

- penetration testing facilitation
  - Project management
  - Data mining

- Beta Status Project

Pantera

- (local) proxy
  - monitors and intercepts web traffic
  - Traffic is analyzed/modified by Pantera Passive Analyzer Plugins (PPA)
- Web based management interface
  - Project management
  - Notes



OWASP / Roses Labs Pantera Web Assessment Studio (WAS) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://pantera/
Google
Getting Started Latest Headlines http://pantera/histor... Attack
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
127.0.0.1 8080 ☑ Use ✓ Apply
File Tools Help
Done

Pantera Web Assessment Studio (WAS) Project: Name Not Set

Last 4 Requests (Reading from temporal cache)

```
>> GET http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_page/rss.xml
<< HTTP/1.1 200 OK

>> GET http://fxfeeds.mozilla.org/rss20.xml
<< HTTP/1.1 302 Found -> Location:
http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_page/rss.xml

>> GET http://www.google.be/firefox?client=firefox-a&rls=org.mozilla:en-US:official
<< HTTP/1.1 200 OK

>> GET http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official
<< HTTP/1.1 302 Found -> Location:
http://www.google.be/firefox?client=firefox-a&rls=org.mozilla:en-US:official
```

Roses Labs (C) 2003-2006

How to install ?

- Pantera is available via the OWASP project pages on http://www.owasp.org
  - Current version 0.1.2

- Install the correct versions of the required software.
  - Python, MySQL, pyOpenSSL, Formbuild…

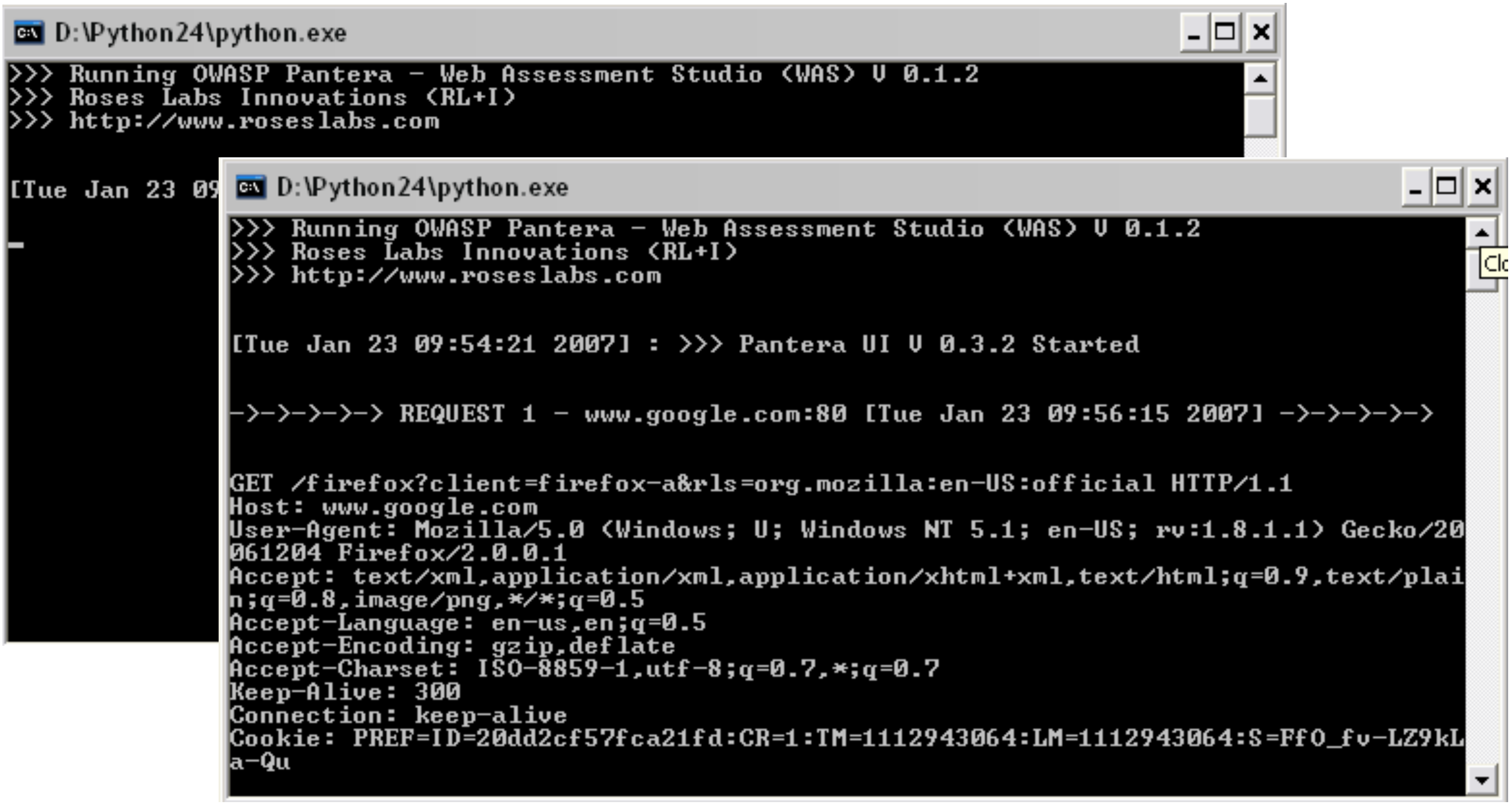
Install problems

- Installation is difficult, but it works and is well described
    - Read the INSTALL.TXT
    - Very good step by step installation instructions

- Problems ?
  - Contact the mailing list
    - VERY good response.
    - Subscribe via the project page

Starting Pantera

- python pantera.py

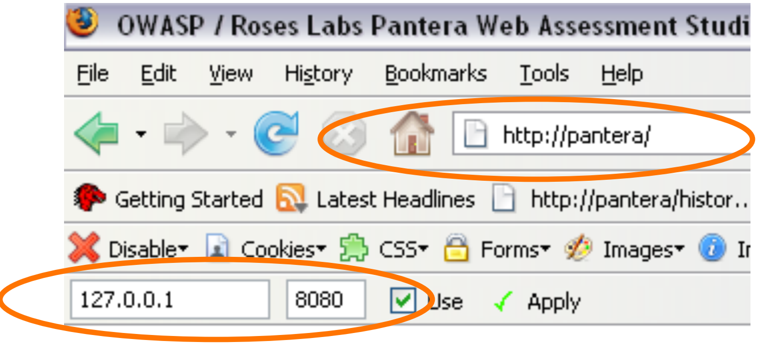


```
>>> Running OWASP Pantera - Web Assessment Studio (WAS) V 0.1.2
>>> Roses Labs Innovations (RL+I)
>>> http://www.roseslabs.com


[Tue Jan 23 09

_
```

```
>>> Running OWASP Pantera - Web Assessment Studio (WAS) V 0.1.2
>>> Roses Labs Innovations (RL+I)
>>> http://www.roseslabs.com


[Tue Jan 23 09:54:21 2007] : >>> Pantera UI V 0.3.2 Started


->->->->-> REQUEST 1 - www.google.com:80 [Tue Jan 23 09:56:15 2007] ->->->->->


GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20
061204 Firefox/2.0.0.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plai
n;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=20dd2cf57fca21fd:CR=1:TM=1112943064:LM=1112943064:S=FfO_fv-LZ9kL
a-Qu
```

Managing Pantera

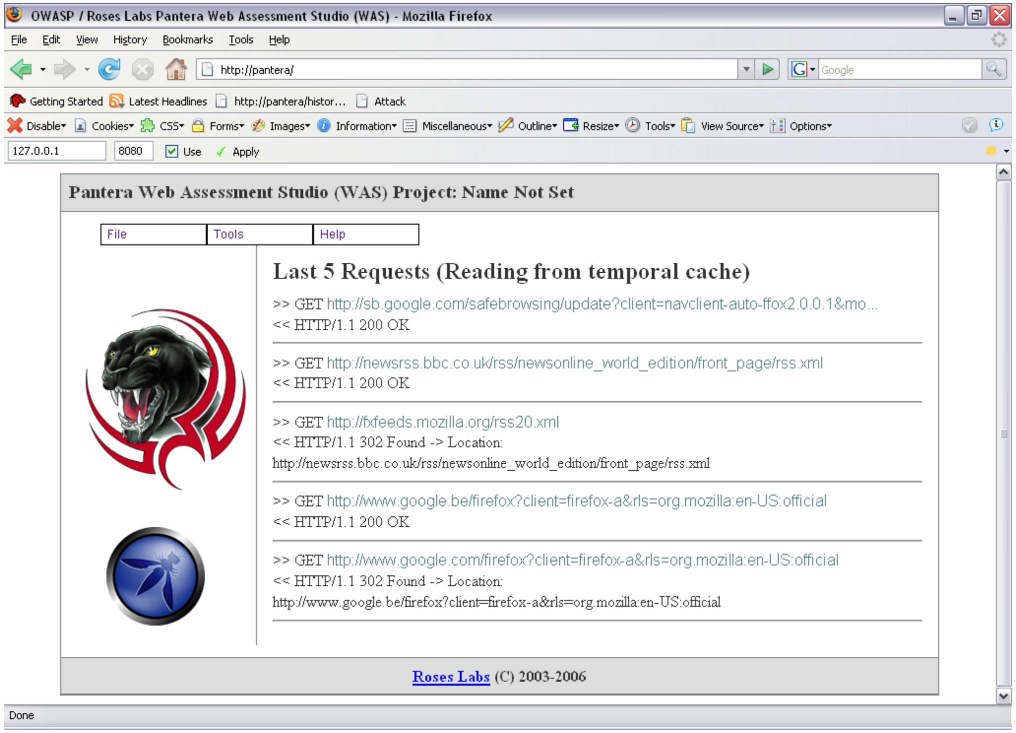
- Point your browser to the Pantera proxy instance at 127.0.0.1:8080
- Browse to http://pantera



OWASP / Roses Labs Pantera Web Assessment Studi
File Edit View History Bookmarks Tools Help
Getting Started
Latest Headlines
http://pantera/histor...
Disable▾ Cookies▾ CSS▾ Forms▾ Images▾ In

http://pantera/

127.0.0.1 | 8080 | ☑ Use | ✓ Apply



OWASP / Roses Labs Pantera Web Assessment Studio (WAS) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Getting Started
Latest Headlines
http://pantera/histor...
Attack
Disable▾ Cookies▾ CSS▾ Forms▾ Images▾ Information▾ Miscellaneous▾ Outline▾ Resize▾ Tools▾ View Source▾ Options▾
File
Tools
Help
Done

http://pantera/

127.0.0.1 | 8080 | ☑ Use | ✓ Apply

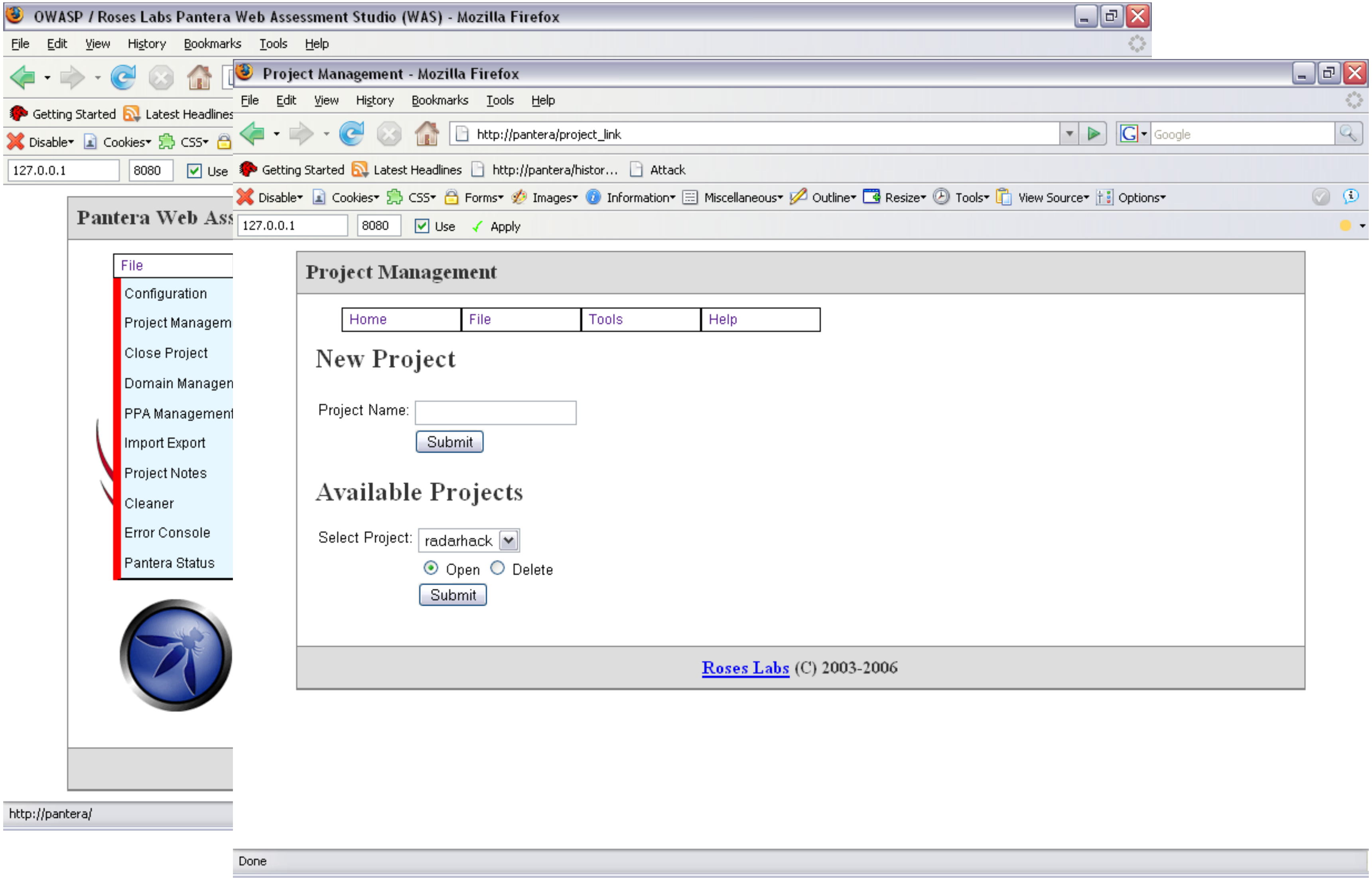
Pantera Web Assessment Studio (WAS) Project: Name Not Set

Last 5 Requests (Reading from temporal cache)

```
>> GET http://sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0.0.1&mo...
<< HTTP/1.1 200 OK

>> GET http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_page/rss.xml
<< HTTP/1.1 200 OK

>> GET http://fxfeeds.mozilla.org/rss20.xml
<< HTTP/1.1 302 Found -> Location:
http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_page/rss.xml

>> GET http://www.google.be/firefox?client=firefox-a&rls=org.mozilla:en-US:official
<< HTTP/1.1 200 OK

>> GET http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official
<< HTTP/1.1 302 Found -> Location:
http://www.google.be/firefox?client=firefox-a&rls=org.mozilla:en-US:official
```

Roses Labs (C) 2003-2006

Create a project



OWASP / Roses Labs Pantera Web Assessment Studio (WAS) - Mozilla Firefox

Project Management - Mozilla Firefox

http://pantera/project_link

Pantera Web Ass

File
- Configuration
- Project Managem
- Close Project
- Domain Managen
- PPA Management
- Import Export
- Project Notes
- Cleaner
- Error Console
- Pantera Status

http://pantera/

Project Management

Home | File | Tools | Help

New Project

Project Name: ______

Submit

Available Projects

Select Project: radarhack

● Open ○ Delete

Submit

Roses Labs (C) 2003-2006

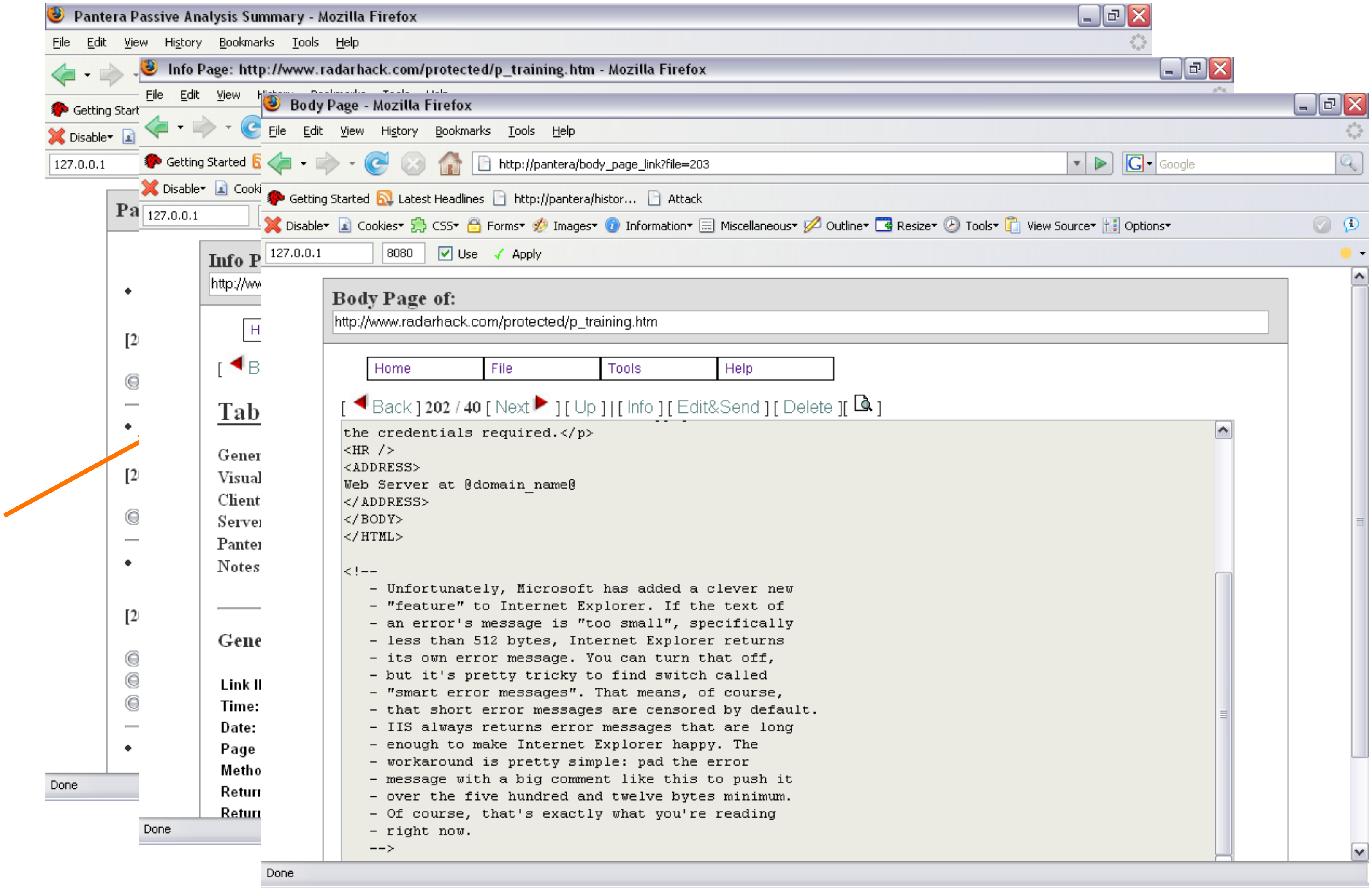
Done

File Edit View History Bookmarks Tools Help
Getting Started
Latest Headlines
http://pantera/histor...
Attack
Disable▾ Cookies▾ CSS▾ Forms▾ Images▾ Information▾ Miscellaneous▾ Outline▾ Resize▾ Tools▾ View Source▾ Options▾
127.0.0.1
8080
☑ Use
✓ Apply
Google

PPA plug-in

- PPA plug-ins are used to analyze PASSIVELY all web traffic for
  - Authentication
  - Vulnerabilities
  - Comments
  - …
- File -> Configuration
- Results are shown in
  Tools -> PPA Analysis summary

Pantera Passive Analysis Summary



Pantera Passive Analysis Summary - Mozilla Firefox

Info Page: http://www.radarhack.com/protected/p_training.htm - Mozilla Firefox

Body Page - Mozilla Firefox

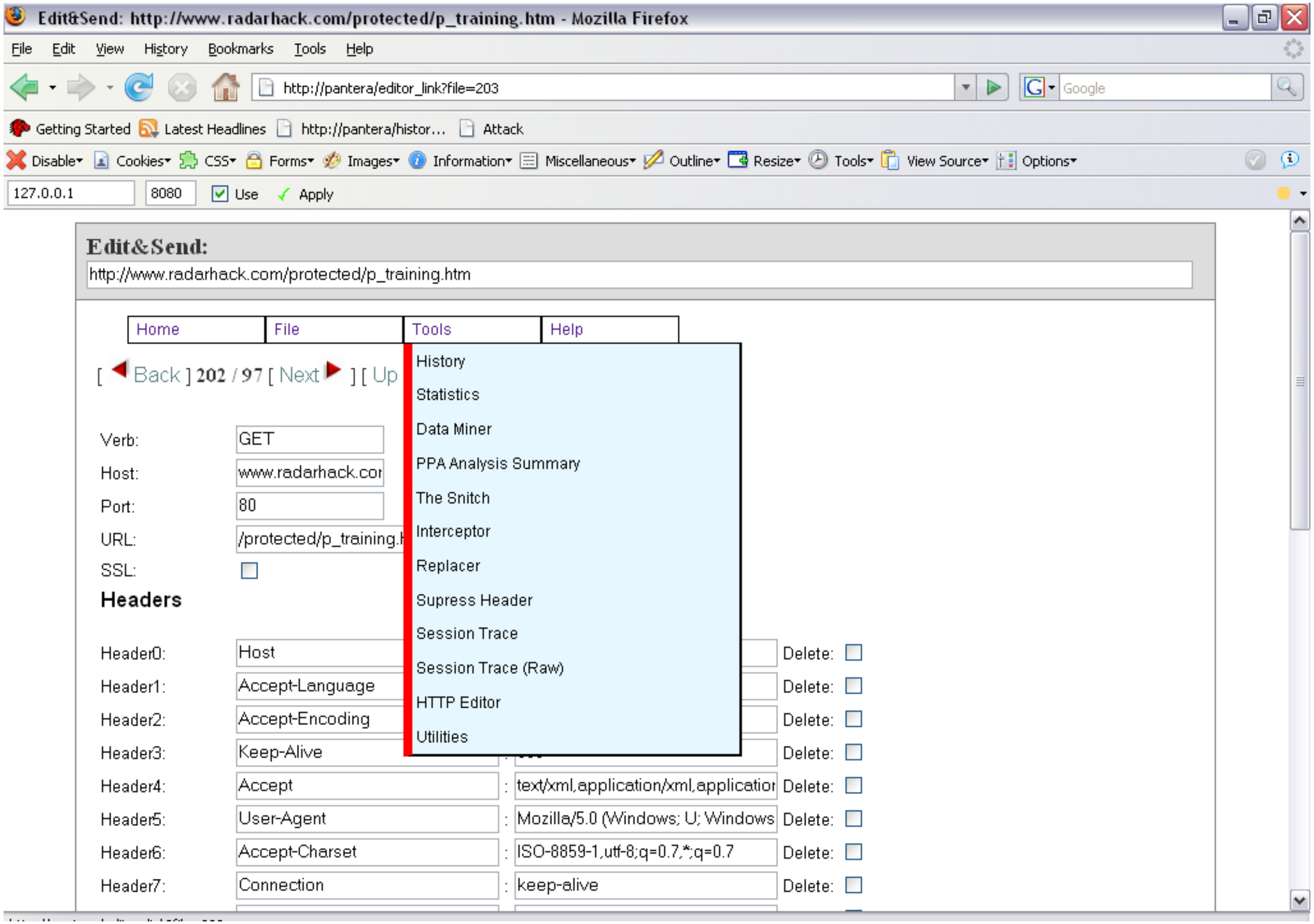
http://pantera/body_page_link?file=203

Body Page of:
http://www.radarhack.com/protected/p_training.htm

[Back] 202 / 40 [Next]][Up] | [Info] [Edit&Send] [Delete][ ]

```
the credentials required.</p>
<HR />
<ADDRESS>
Web Server at @domain_name@
</ADDRESS>
</BODY>
</HTML>

<!--
   - Unfortunately, Microsoft has added a clever new
   - "feature" to Internet Explorer. If the text of
   - an error's message is "too small", specifically
   - less than 512 bytes, Internet Explorer returns
   - its own error message. You can turn that off,
   - but it's pretty tricky to find switch called
   - "smart error messages". That means, of course,
   - that short error messages are censored by default.
   - IIS always returns error messages that are long
   - enough to make Internet Explorer happy. The
   - workaround is pretty simple: pad the error
   - message with a big comment like this to push it
   - over the five hundred and twelve bytes minimum.
   - Of course, that's exactly what you're reading
   - right now.
   -->
```

Tools



Edit&Send:

http://www.radarhack.com/protected/p_training.htm

Verb:	GET
Host:	www.radarhack.cor
Port:	80
URL:	/protected/p_training.h
SSL:	□

Headers

Header0:	Host		Delete:	□
Header1:	Accept-Language		Delete:	□
Header2:	Accept-Encoding		Delete:	□
Header3:	Keep-Alive		Delete:	□
Header4:	Accept	text/xml,application/xml,applicatior	Delete:	□
Header5:	User-Agent	Mozilla/5.0 (Windows; U; Windows	Delete:	□
Header6:	Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7	Delete:	□
Header7:	Connection	keep-alive	Delete:	□

Tools

- Stats and Data Mining
- Interceptor, Replacer, Supress Headers
- Session Trace and HTTP Editor
- Utilities
  - En/decode, Hashing...

- Demo

Thank You