



Ethical Hacking and Countermeasures

Version 6



Module XVII

Web Application
Vulnerabilities

Kimberly, a web application developer works for a bank, *XBank4u*. Recently *XBank4u* introduced a new service called “Mortgage Application Service”. Kimberly was assigned the task of creating the application which supported the new service.

She finds *ShrinkWarp*, an ASP based application on the Internet. The application suited perfectly for her development. She negotiates the price with the vendor and purchases the software for the firm.

She was successful in implementing the project in time. *XBank4u* was ready to serve its customers online for the new service using the application that Kimberly had designed.

A week later *XBank4u* website was defaced!

Was Kimberly’s decision to purchase the application justified?

Is it safe to trust a third party application?

Posted: 2008/01/21

Web application hacking: Inside the mind of an attacker

There's a tried and true method for seeking out the maximum number of vulnerabilities possible when testing your Web applications for security flaws. No, it's not a high-end Web application vulnerability scanner but rather a free "technique" that you can improve over time. You may not learn the methods overnight, but once you do, it's virtually guaranteed to take your Web vulnerability testing to the next level. It's stepping into the mindset of a malicious attacker and delving in to see *what else* in the Web application can be exploited.

Many people refer to this approach as penetration testing, but it's actually more than that. Technically speaking, it's called ethical hacking. This term always generates a few giggles, but it's indeed a valid form of security testing. The thing is, you'll find that by looking at your Web applications from the dark side you'll uncover and exploit weaknesses that automated scanners or checklist audits wouldn't touch in a thousand years.

The malicious mindset isn't limited to the stereotyped "hacker" as we know him. Anyone can have a malicious mindset -- not just an outsider. So, think about what an authenticated and trusted insider could do. In many cases, it's not going to be fancy cross-site scripting (XSS) or SQL injection but rather basic login mechanism tampering or URL or form field manipulation. Maybe even exploiting file transfer capabilities or disabling certain security features that no one knew he had access to.

While working on a project recently, I came across an internal Web server that hosted the security management/control application for the organisation's data centre. When trying to log in to the application, it prompted me for the password. I didn't have it. This is where most security scans and checklist audits would stop. But taking things further, I thought I'd Google the Web server and application name (which were conveniently displayed on the login page) along with the words "default password". Within about 3 seconds I had the default login ID and password, and sure enough, they worked!

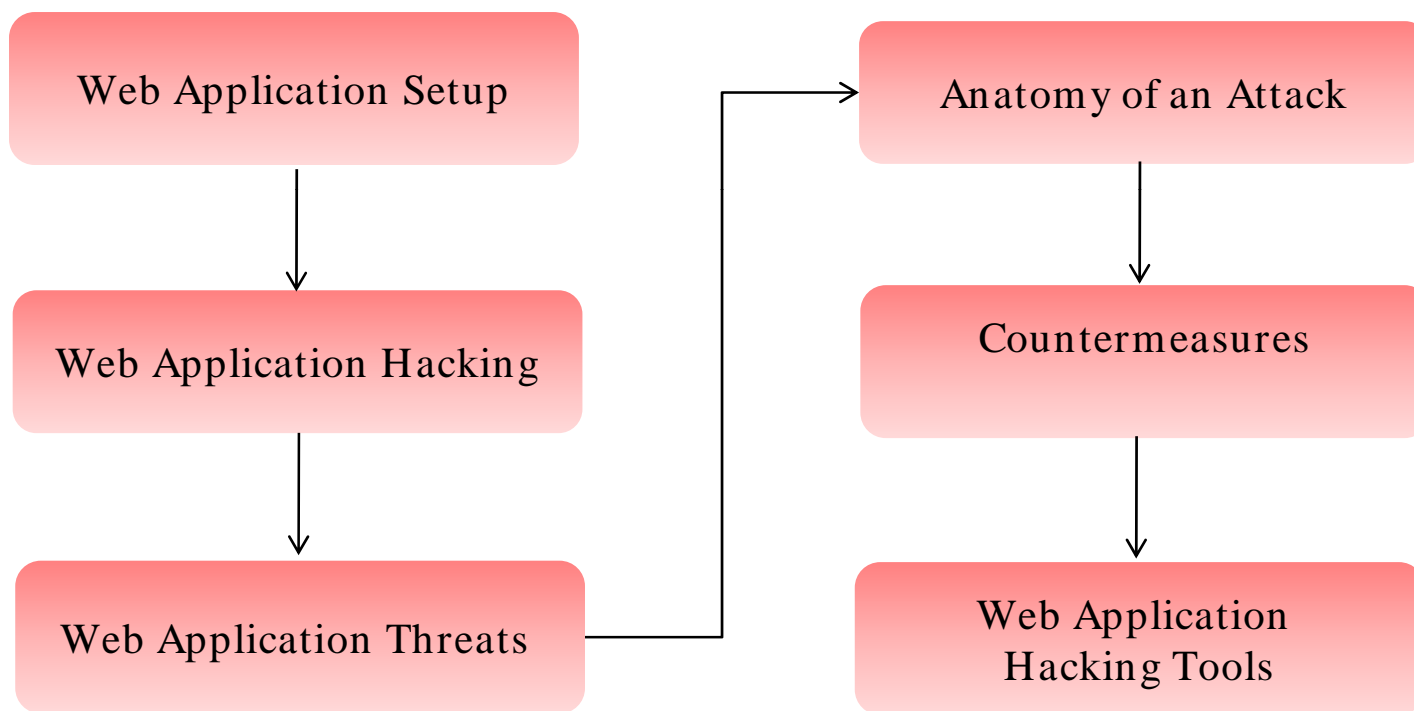
Source: <http://searchsecurity.techtarget.com.au/>

Module Objective

This module will familiarize you with :

- Web Application Setup
- Objectives of Web Application Hacking
- Anatomy of an Attack
- Web Application Threats
- Countermeasures
- Web Application Hacking Tools

Module Flow



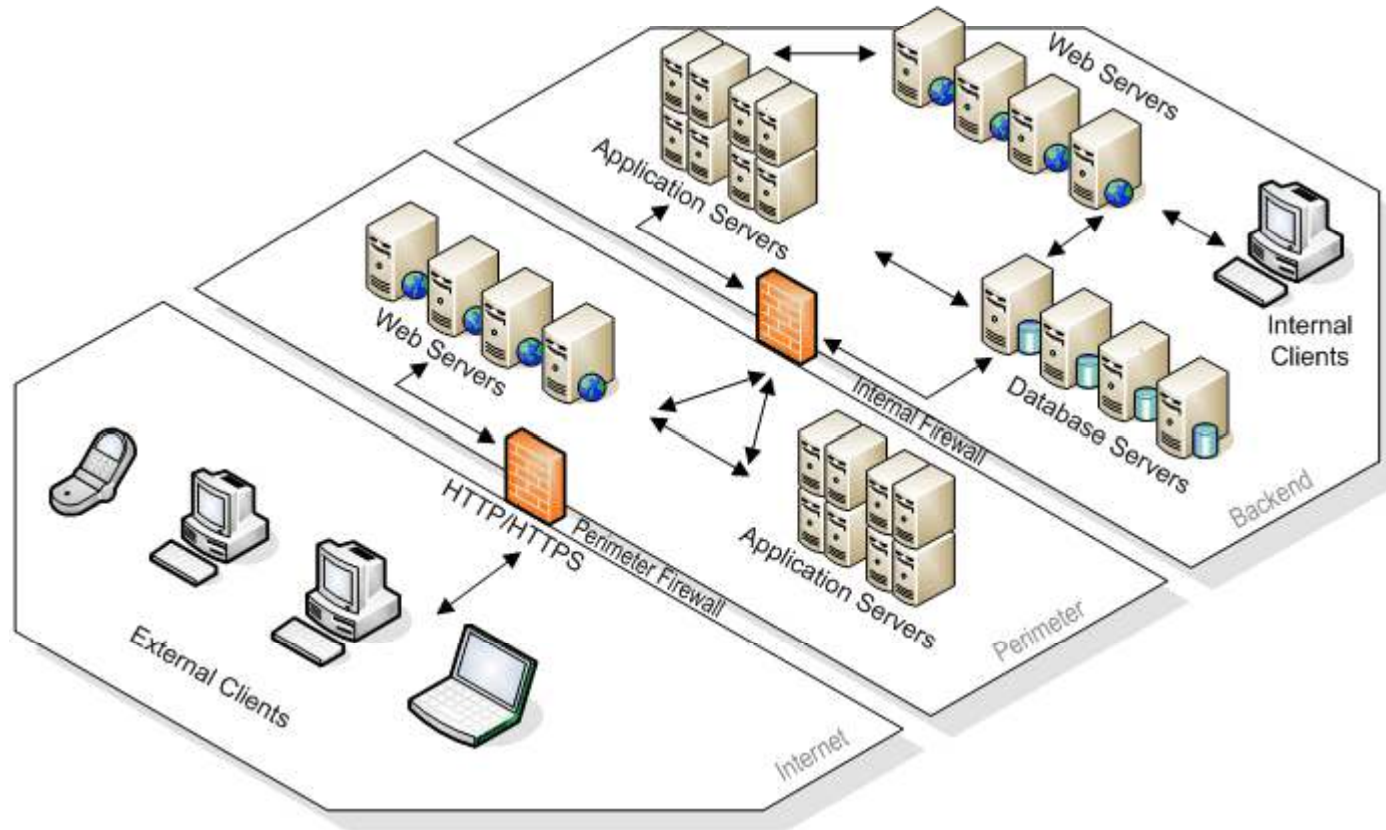
Web Application Setup

A client/server software application that interacts with users or other systems using HTTP

Modern applications are written in Java (or similar languages) and run on distributed application servers, connecting to multiple data sources through complex business logic tiers

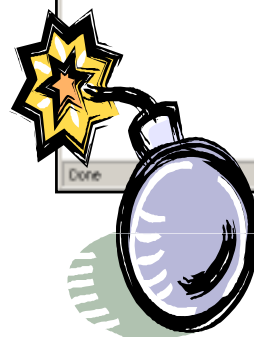
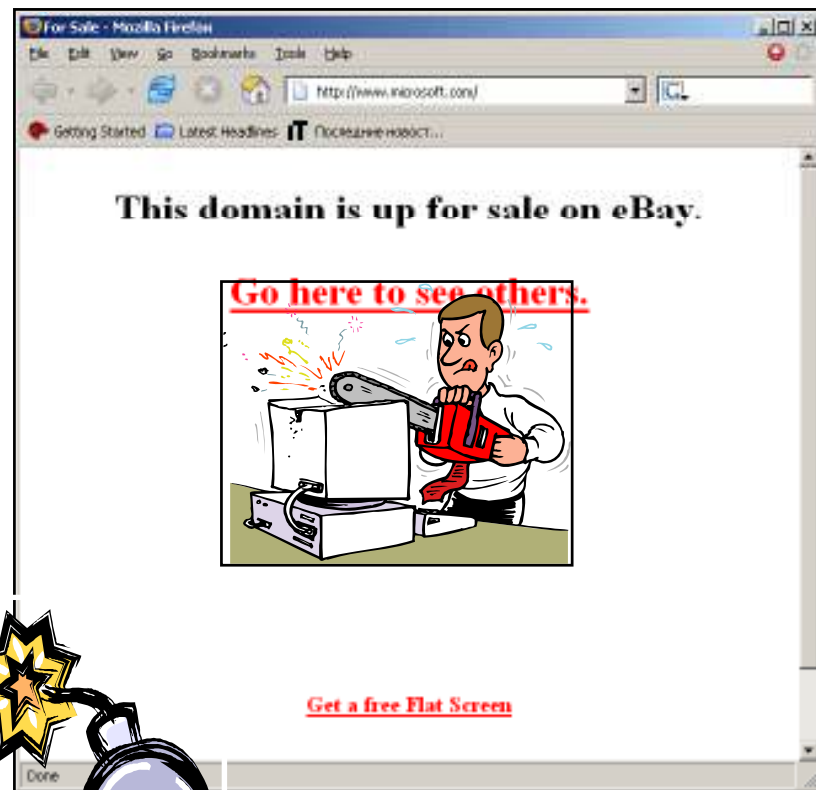


Web Application Setup (cont'd)



Exploitative behaviors

- Defacing websites
- Stealing credit card information
- Exploiting server-side scripting
- Exploiting buffer overflows
- Domain Name Server (DNS) attacks
- Employing malicious code
- Denial of Service
- Destruction of Data



Anatomy of an Attack

SCANNING



INFORMATION GATHERING



TESTING



PLANNING THE ATTACK



LAUNCHING THE ATTACK

Web Application Threats

Cross-site scripting

SQL injection

Command injection

Cookie/session poisoning

Parameter/form tampering

Buffer overflow

Directory traversal/ forceful browsing

Cryptographic interception

Cookie snooping

Authentication hijacking

Log tampering

Error message interception attack

Obfuscation application

Platform exploits

DMZ protocol attacks

Security management exploits

Web services attacks

Zero day attack

Network access attacks

TCP fragmentation

Cross-Site Scripting/ XSS Flaws

Cross-site scripting occurs when an attacker uses a web application to send malicious code; generally JavaScript

Stored attacks are those where the injected code is permanently stored on the target servers in a database

Reflected attacks are those where the injected code takes another route to the victim, such as in an email message

Disclosure of the user's session cookie allows an attacker to hijack the user's session and take over the account

In cross-site scripting, end user files are disclosed, Trojan horse programs are installed, the user to some other page is redirected, and presentation of the content is modified

Web servers, application servers, and web application environments are susceptible to cross-site scripting

An Example of XSS

A hacker realizes that the XSECURITY website suffers from a cross-site scripting bug

The hacker sends you an e-mail that claims you have just won a vacation getaway and all you have to do is "click here" to claim your prize

The URL for the hypertext link is [www.xsecurity.com/default.asp?name=<script>evilScript\(\)</script>](http://www.xsecurity.com/default.asp?name=<script>evilScript()</script>)

When you click this link, the website tries to be friendly by greeting you, but instead displays, "Welcome Back !"

What happened to your name? By clicking the link in the e-mail, you have told the XSECURITY website that your name is <script>evilScript()</script>

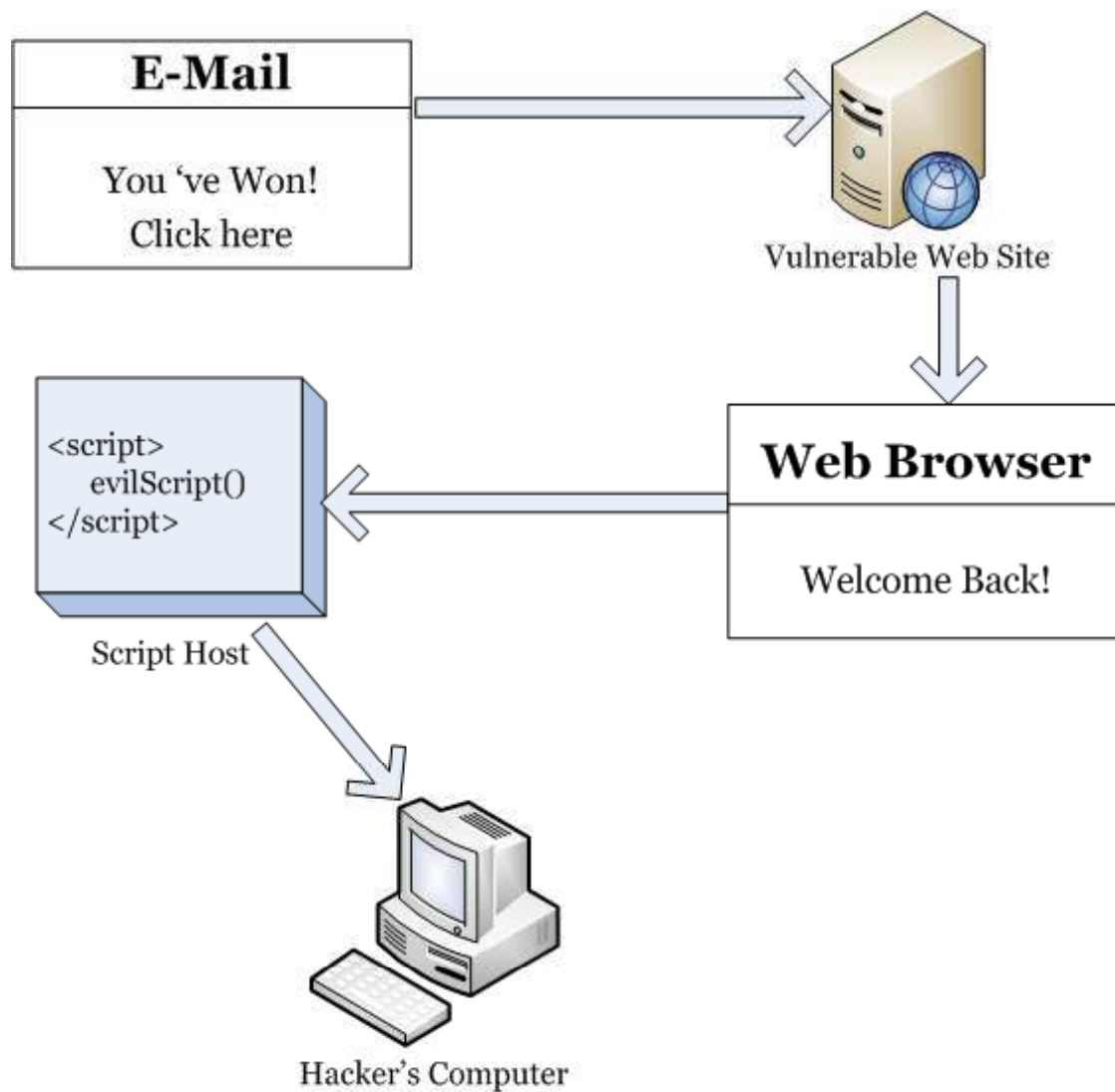
The web server generated HTML with this "name" embedded and sends it to your browser

Your browser correctly interprets this as script and runs the script

If this script instructs the browser to send a cookie containing your stock portfolio to the hacker's computer, it quickly complies

After all, the instruction came from the XSECURITY website, which owns that cookie

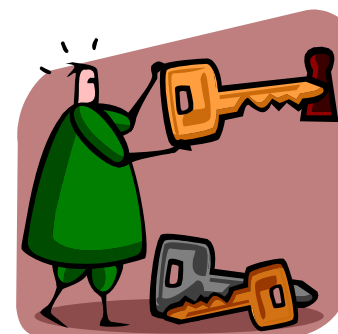
An Example of XSS (cont'd)



Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification

Adopt a stringent security policy

Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users



SQL Injection



SQL Injection uses SQL to directly manipulate database's data

An attacker can use a vulnerable web application to bypass normal security measures and obtain direct access to the valuable data

SQL Injection attacks can often be executed from the address bar, from within application fields, and through queries and searches

Countermeasure

- Check the user's input provided to database queries
- Validate and sanitize every user variable passed to the database

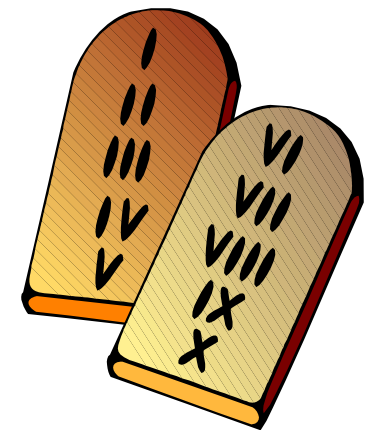


Command Injection Flaws

Command injection flaws relay the malicious code through a web application to another system

Attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to the backend databases via SQL (i.e., SQL injection)

Scripts written in Perl, python, and other languages can be injected into the poorly designed web applications



Use language-specific libraries that avoid problems due to shell commands

Validate the data provided to prevent any malicious content

Structure requests so that all supplied parameters are treated as data, rather than potentially executable content

J2EE environments allow the use of the Java sandbox, which can prevent the execution of system commands

日本語

Cookie/ Session Poisoning

Cookies are used to maintain session state in the otherwise stateless HTTP protocol

Poisoning allows an attacker to inject the malicious content, modify the user's on-line experience, and obtain the unauthorized information

A proxy can be used for rewriting the session data, displaying the cookie data, and/ or specifying a new user ID or other session identifiers in the cookie





Do not store plain text or weakly encrypted password in a cookie

Implement cookie's timeout

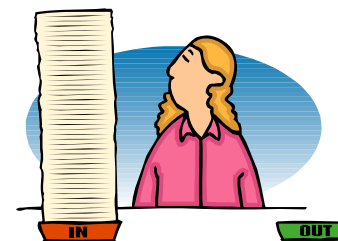
Cookie's authentication credentials should be associated with an IP address

Make logout functions available



Parameter/Form Tampering

Parameter/Form tampering takes advantage of the hidden fields that work as the only security measure in some applications



Modifying this hidden field value will cause the web application to change according to the new data incorporated



It can cause theft of services, escalation of access, and session hijacking



Countermeasure: Field validity checking

JuggyBoy.COM

About Us | What We Do | What's New | Products | Support

PRODUCTS

You can order the MCSE training slides using PayPal account or using a credit card.

1. CREDIT CARD ORDER METHOD

Click here to order using Credit Card

2. PAYPAL ORDER METHOD

Training Slide Sets

Slide Set (1) Windows 2000 Professional	USD 69.00	Add to Cart
Slide Set (2) Windows 2000 Server	USD 69.00	Add to Cart
Slide Set (3) Windows 2000 Active Directory	USD 69.00	Add to Cart
Slide Set (4) Windows 2000 Network Infrastructure	USD 69.00	Add to Cart
Complete Set (Includes all 4 sets - over 3000 slides)	USD 225.00	Add to Cart

[View Cart](#)

You will be able to download the materials immediately upon payment.

```
products[1] - Notepad
File Edit Format View Help

method="post">
<input type="image"
src="https://www.paypal.com/en_US/i/btn/x-click-but22.gif"
border="0" name="submit" alt="Make payments with PayPal -
it's fast, free and secure!">
<input type="hidden" name="add" value="1">
<input type="hidden" name="cmd" value="_cart">
<input type="hidden" name="business"
value="haja@juggyboy.com">
<input type="hidden" name="item_name" value="Slide Set (1)
Windows 2000 Professional">
<input type="hidden" name="amount" value="69.00">
<input type="hidden" name="no_note" value="1">
<input type="hidden" name="currency_code" value="USD">
<br>
&nbsp;</form></p>
</td>
</tr>
<tr>
<td width="59%" height="19"
style="border-style: none" bgcolor="#000000">
<font color="#FFFFFF" face="Garamond">Slide
Set (2) windows
2000
Server</font></td>
<td width="18%" height="19" align="right"
style="border-style: none" bgcolor="#000000">
<font face="Garamond" color="#FFFFFF">USD
69.00</font></td>
<td width="23%" height="19"
style="border-style: none" bgcolor="#000000"
align="center">
<form target="paypal"
action="https://www.paypal.com/cgi-bin/webscr"
method="post">
<input type="image"
src="https://www.paypal.com/en_US/i/btn/x-click-but22.gif"
```

Buffer Overflow

Buffer overflow is the corrupt execution stack of a web application

Buffer overflow flaws in custom web applications are less likely to be detected

Almost all known web servers, application servers, and web application environments are susceptible to attack (but not Java and J2EE environments except for overflows in the JVM itself)



```
execute error: '//bin/sh'  
This execution used shellcode that use 'Stack'.  
Its execution is very dangerous.  
Intercepting execution, This can prevent remote attack or local attack.  
  
example) Stack based Overflow, Format String attack ...  
Segmentation fault  
[root@test technic]# ./for_xp32  
AAAAAAAAAAAAAAAA4$176x%5$N%6$47x%7$N%8$256x%9$N%10$192x%11$N  
execute error: '//bin/sh'  
  
This execution used shellcode that use 'Stack'.  
Its execution is very dangerous.  
Intercepting execution, This can prevent remote attack or local attack.  
  
example) Stack based Overflow, Format String attack ...  
Segmentation fault  
[root@test technic]#
```



Validate input length in forms

Check bounds and maintain extra care when using loops to copy data

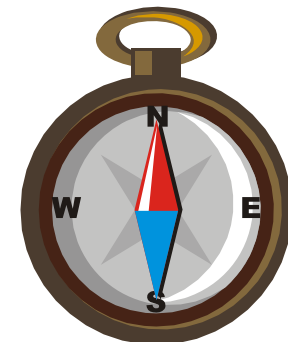
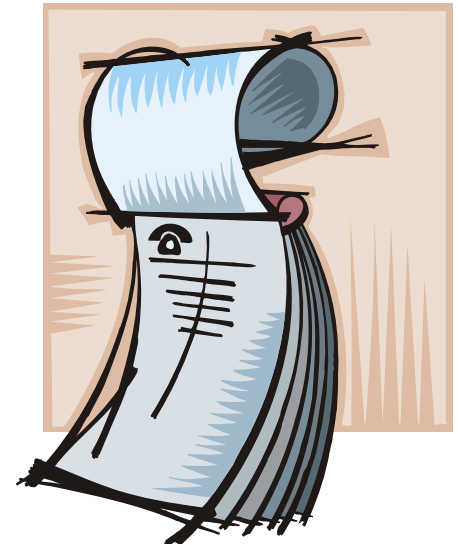
StackGuard and StackShield for Linux are tools to defend programs and systems against stack-smashing

Directory Traversal/ Forceful Browsing

Directory traversal/ forceful browsing attack occurs when the attacker is able to browse directories and files outside the normal application access

It exposes the directory structure of the application, and often the underlying web server and operating system

An attacker can enumerate contents, access secure or restricted pages, and gain confidential information, locate source code, and so on



Define access rights to the protected areas of the website

Apply checks/hot fixes that prevent the exploitation of the vulnerability such as Unicode to affect directory traversal

Web servers should be updated with security patches in a timely manner



Cryptographic Interception

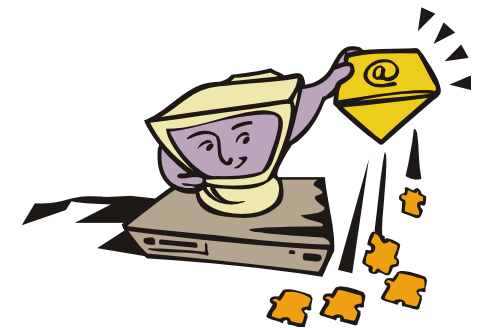
Using cryptography, a confidential message can be securely sent between two parties

Encrypted traffic flows through network firewalls and IDS systems and is not inspected

If an attacker is able to take advantage of a secured channel, he/ she can exploit it more efficiently than an open channel

Countermeasure

- Use of Secure Sockets Layer(SSL) and advanced private key protection



Cookie Snooping

In an attempt to protect cookies, site developers often encode the cookies

Easily reversible encoding methods such as Base64 and ROT13 (rotating the letters of the alphabet 13 characters) give a false sense of the security regarding the use of cookies

Cookie snooping techniques can use a local proxy to enumerate cookies

Countermeasures:

- Use encrypted cookies
- Embed source's IP address in the cookie
- Integrate cookie's mechanism fully with SSL functionality for secured remote web application access



Authentication Hijacking

Authentication prompts a user to supply the credentials that allow access to the application

It can be accomplished through:

- Basic authentication
- Strong authentication methods

Web applications authenticate in varying methods

Enforcing a consistent authentication policy between multiple and disparate applications can prove to be a real challenge

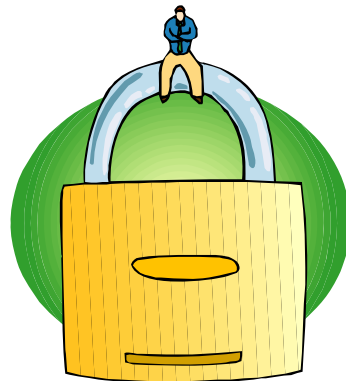
A security lapse can lead to theft of service, session hijacking, and user impersonation

The image shows a screenshot of a .NET Passport Sign-in form. The form has a blue header with the text ".NET Passport Sign-in" and a "Help" link. Below the header, there are two input fields: "E-mail Address" with the value "name@hotmail.com" and "Password" with the value "*****". There is a checkbox labeled "Sign me in automatically." and a "Sign In" button. Below the button, there is another checkbox labeled "Do not remember my e-mail address for future sign-in. (Select this when using a public computer.)". At the bottom of the form, there is a Microsoft .NET logo, a link "Don't have a .NET Passport? Get one now.", and links for "Member Services", "Terms of Use", and "Privacy Statement". The footer text reads "Some elements © 1999 - 2004 Microsoft® Corporation. All rights reserved."

Use authentication methods that use secure channels wherever possible

Instant SSL can be configured easily to encrypt all traffic between the client and the application

Use cookies in a secure manner where possible



Log Tampering

Logs are kept to track the usage patterns of the application

Log tampering allows attackers to cover their tracks or alter web transaction records

Attackers strive to delete logs, modify logs, change user information, or otherwise destroy evidence of any attack

Countermeasure

- Digitally sign and stamp logs
- Separate logs for system events
- Maintain transaction log for all application events



Error Message Interception

Information in error messages is often rich with site-specific information that can be used to:

- Determine the technologies used in the web applications
- Determine whether the attack attempt was successful
- Receive hints for attack methods to try next



Countermeasure

- Website cloaking capabilities make enterprise web resources invisible to hackers



Attack Obfuscation

Attackers often work hard to mask and otherwise hide their attacks to avoid detection

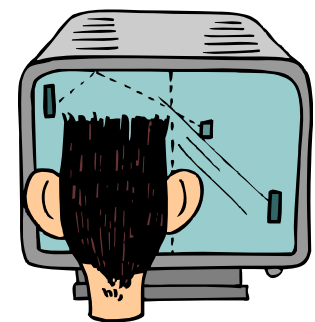
Most common method of attack obfuscation involves encoding portions of the attack with Unicode, UTF-8, or URL encoding

Multiple levels of encoding can be used to further bury the attack

It is used for theft of service, account hijacking, information disclosure, website defacement, and so on

Countermeasures:

- Thoroughly inspect all traffic
- Block or translate Unicode and UTF-8 encoding to detect attacks



Platform Exploits



Web applications are built upon application platforms, such as BEA Weblogic, ColdFusion, IBM WebSphere, Microsoft .NET, and Sun JAVA technologies

Vulnerabilities include the misconfiguration of the application, bugs, insecure internal routines, hidden processes and commands, and third-party enhancements



The exploit of application platform vulnerabilities can allow:

- Access to developer areas
- The ability to update application and site content

DMZ Protocol Attacks

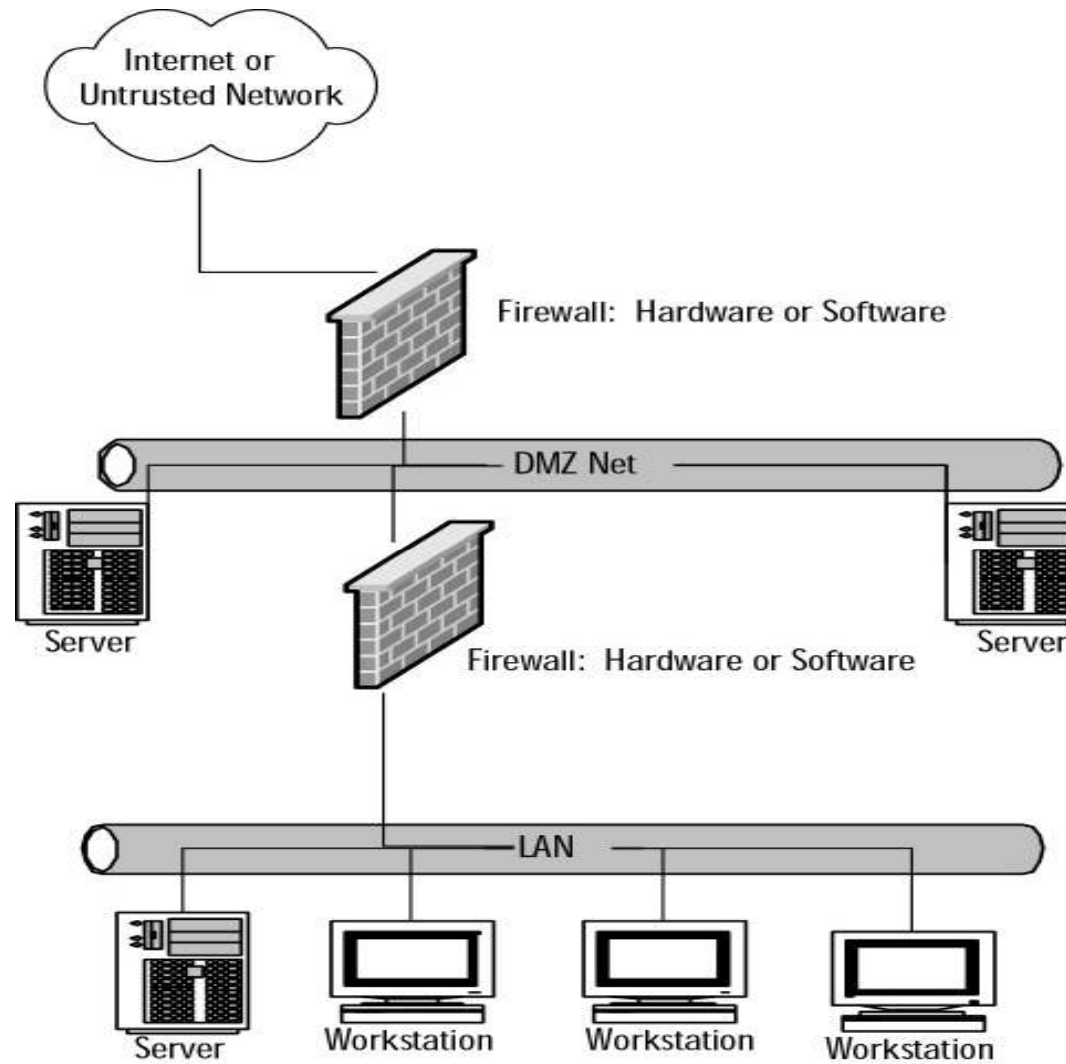
DMZ (Demilitarized Zone) is a semi-trusted network zone that separates the untrusted Internet from the company's trusted internal network

Most companies limit the protocols allowed to flow through their DMZ

An attacker who is able to compromise a system that allows other DMZ protocols, has access to other DMZ and internal systems. This level of access can lead to:

- Compromise of the web application and data
- Defacement of websites
- Access to internal systems, including databases, backups, and source code

DMZ



Deploy a robust security policy

Adopt a sound auditing policy

Use signatures to detect and block well-known attacks

- Signatures must be available for all forms of attack and must be continually updated



Security management systems are targeted to turn off security enforcement

An exploit of security management can lead to the modification of protection policies

Countermeasures

- There should be a single consolidated way to manage the security that is specific to each application
- Firewalls should be used



Web services allow process-to-process communication between web applications

An attacker can inject a malicious script into a web service that will enable disclosure and modification of the data

Countermeasures:

- Turn off web services that are not required for regular operations
- Provision for multiple layers of protection
- Block all known attack paths without relying on signature database alone



Zero-Day Attacks

Zero-day attacks take place between the time a vulnerability is discovered by a researcher or attacker and the time that the vendor issues a corrective patch

Most zero-day attacks are only available as hand-crafted exploit code, but zero-day worms have caused rapid panic

Zero-day vulnerability is the launching point for further exploitation of the web application and environment

Countermeasures:

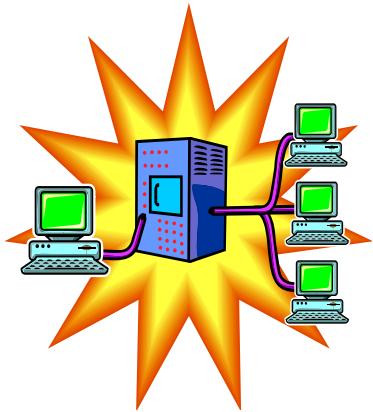
- No security solution can claim that they will totally protect against all zero-day attacks
- Enforce stringent security policies
- Deploy a firewall and enable heuristics (*heuristics*—common-sense rules drawn from experience—to solve problems) scanning

Network Access Attacks

All traffic to and from a web application traverses networks

These attacks use techniques like spoofing, bridging, ACL bypass, and stack attacks

Sniffing network traffic will allow viewing of application commands, authentication information, and application data as it traverses the network



Countermeasures

- Shut down unnecessary services thereby shutting unnecessary listening ports
- Define firewall rules to pass only legitimate traffic

TCP Fragmentation

Every message that is transferred between computers by a data network is broken down into packets

Often packets are limited to a pre-determined size for interoperability with physical networks

An attack directly against a web server would specify that the "Push" flag is set, which would force every packet into the web server's memory. In this way, an attack would be delivered piece-by-piece, without the ability to detect the attack

Countermeasure:

- Use packet filtering devices and firewall rules to thoroughly inspect the nature of the traffic directed at a web server



Hacking Tools

Instant Source

Wget

WebSleuth

BlackWidow

WindowBomb

Burp

cURL



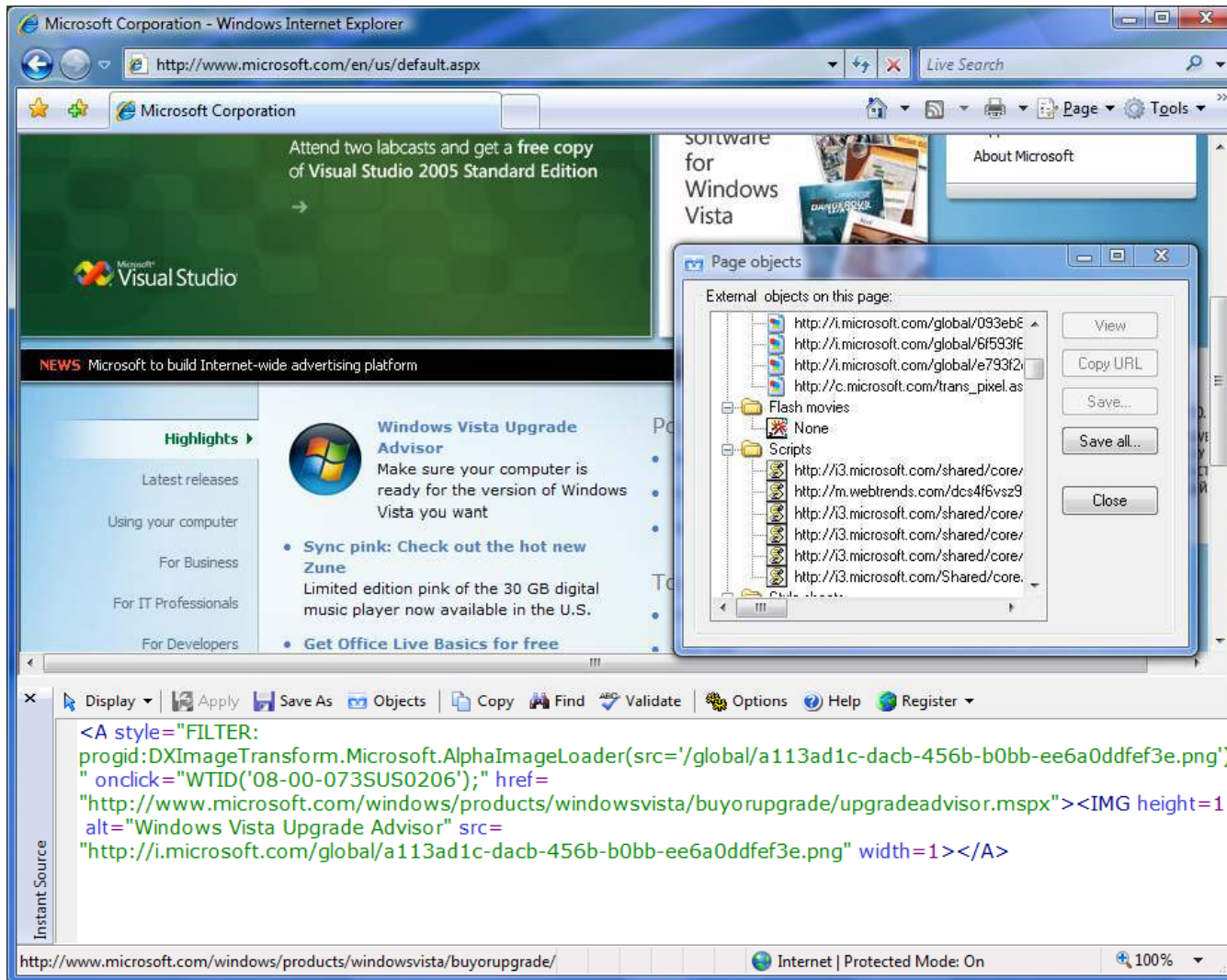
Instant Source tool allows you to see and edit the HTML source code of the web pages

It can be executed from Internet Explorer where a new toolbar window displays the source code for any selected part of the page in the browser window

```
25 </head>
26 <body text="#000000
    bgcolor="#FFFFFF">
27 <table width="1000"
28     <tr>
29         <td width="200"
30         </td>
31         <td valign="top"
32             <div align="c
33             </div>
34             <p class="Boc
35             <h1 class="He
36             <p class="Cap
Entertainment</a>
37             | <a href=
```

Source: <http://www.blazingtool.com>

Instant Source: Screenshot





Wget is a command line tool for Windows and Unix that will download the contents of a website

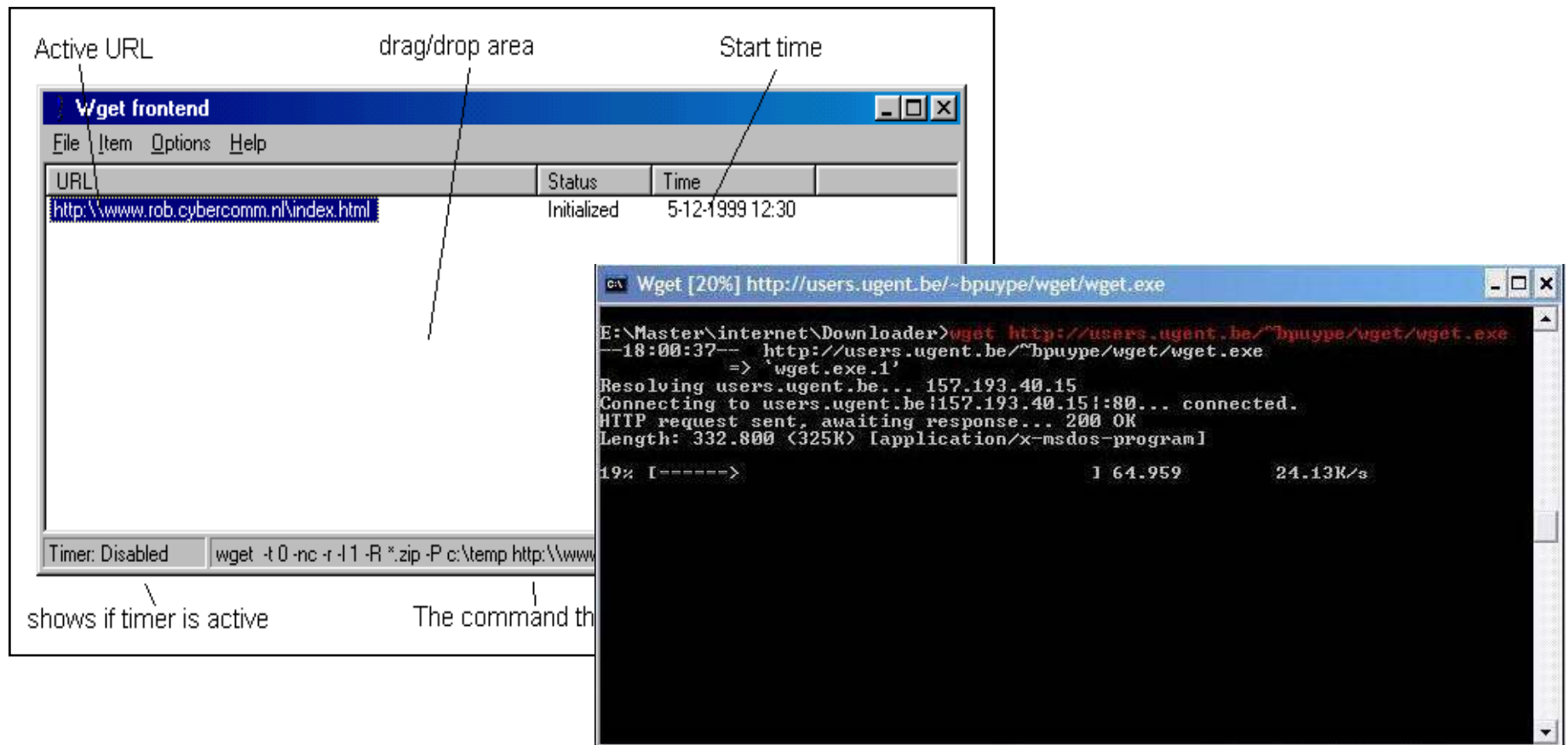
It works non-interactively in the background after the user logs off

It works particularly well with slow or unstable connections by continuing to retrieve a document until the document is fully downloaded

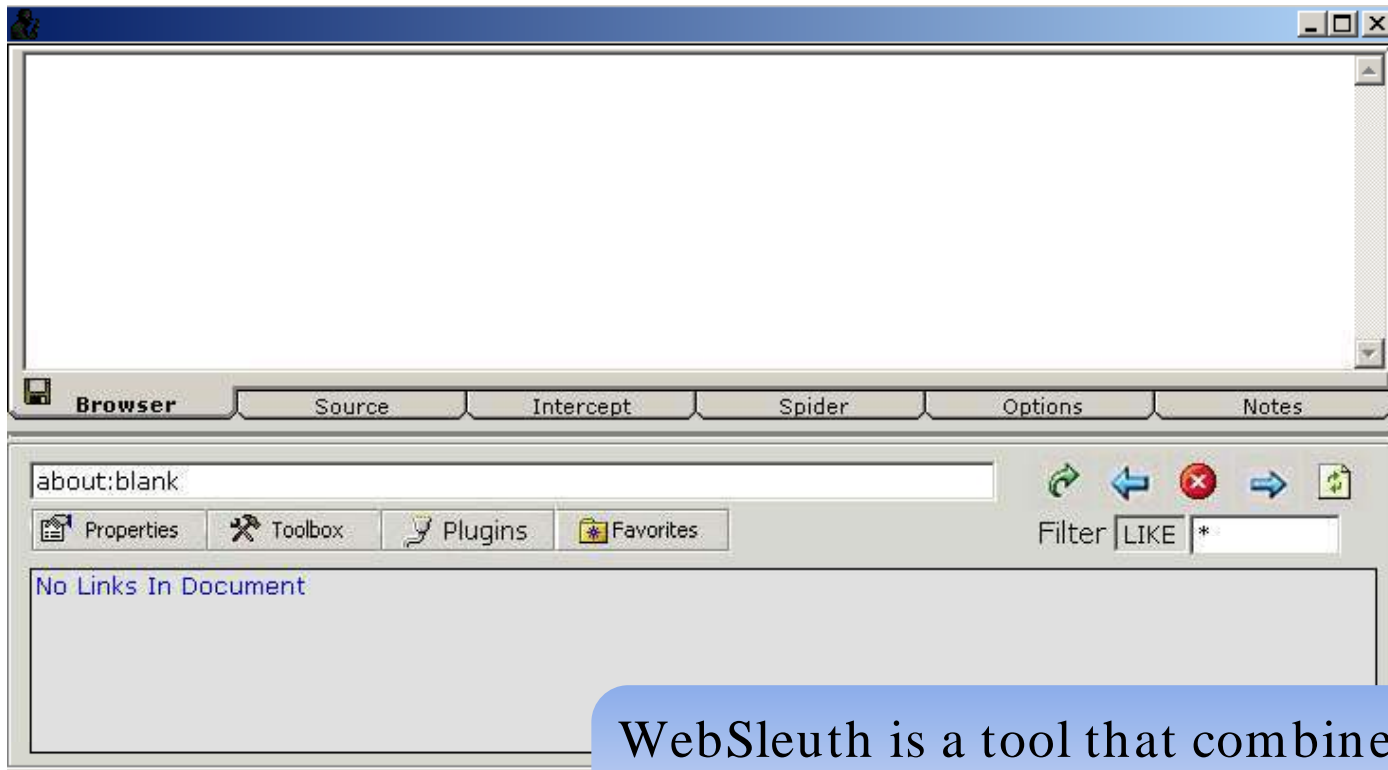
Both http and ftp retrievals can be time stamped, so Wget can see if the remote file has changed since the last retrieval and automatically retrieve the new version if it has

Source: www.gnu.org/

Wget: Screenshot



WebSleuth: Screenshot



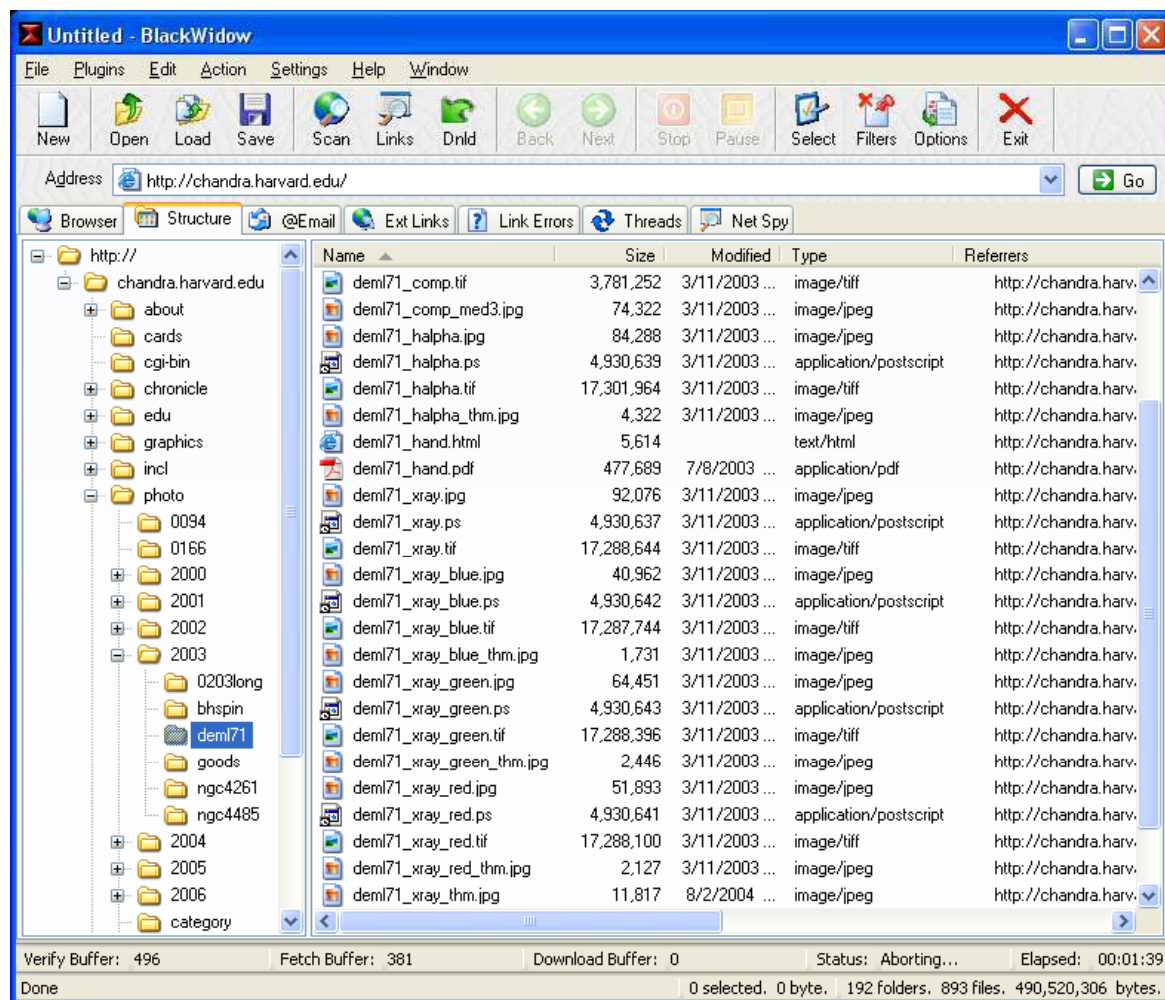
WebSleuth is a tool that combines spidering with the capability of a personal proxy such as Achilles

Picture Source: <http://sandsprite.com/sleuth/>

BlackWidow

Black widow is a website scanner, a site mapping tool, a site ripper, a site mirroring tool, and an offline browser program

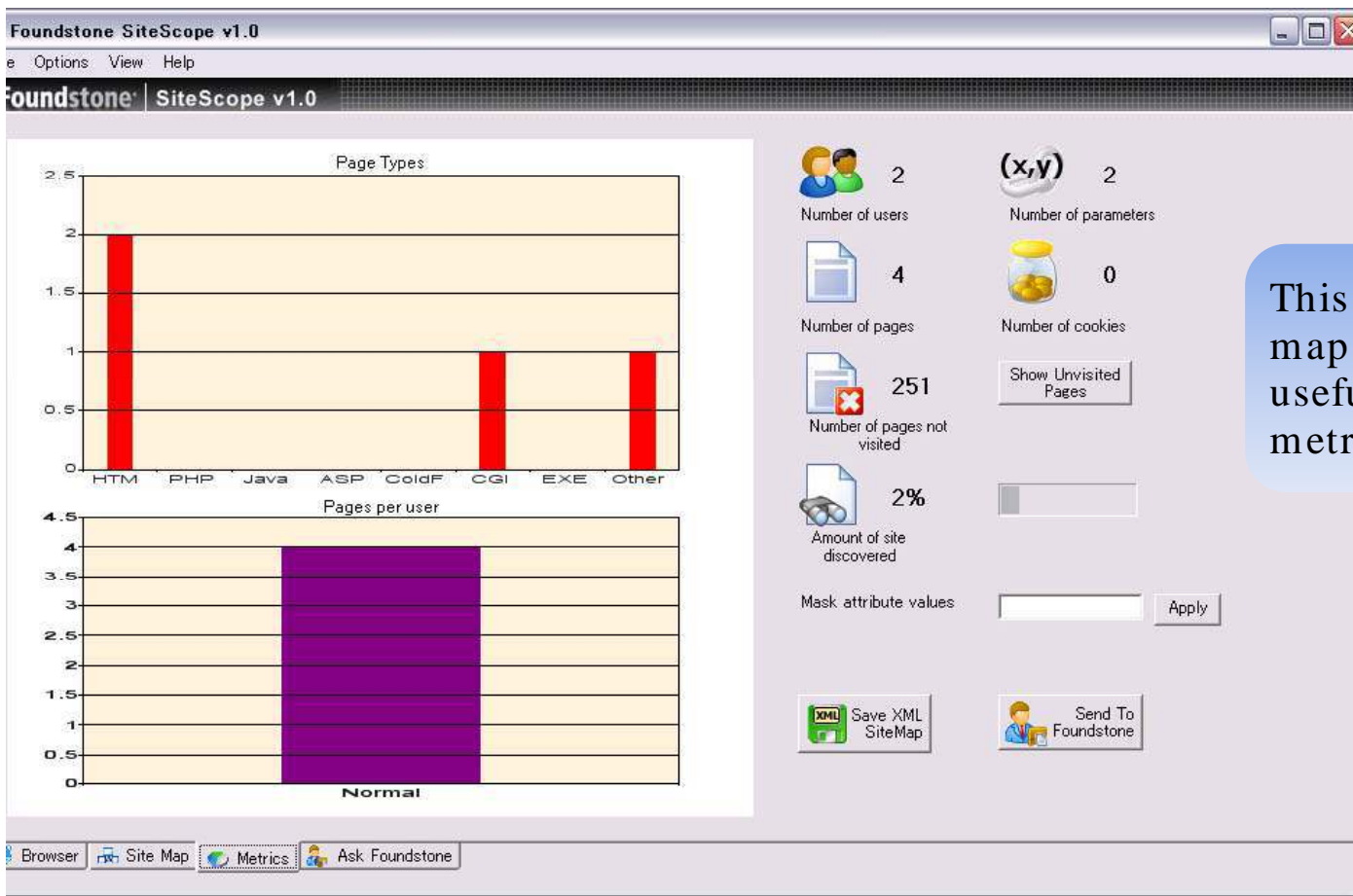
It can be used to scan a site and create a complete profile of the site's structure, files, Email addresses, external links, and even link errors



Source: <http://softbytelabs.com>

SiteScope Tool

Foundstone SiteScope is a free tool that helps website owners, developers, and managers to easily map out the navigation of a web application



This tool creates a site map and gathers useful data for basic metrics

WSDigger Tool – Web Services Testing Tool

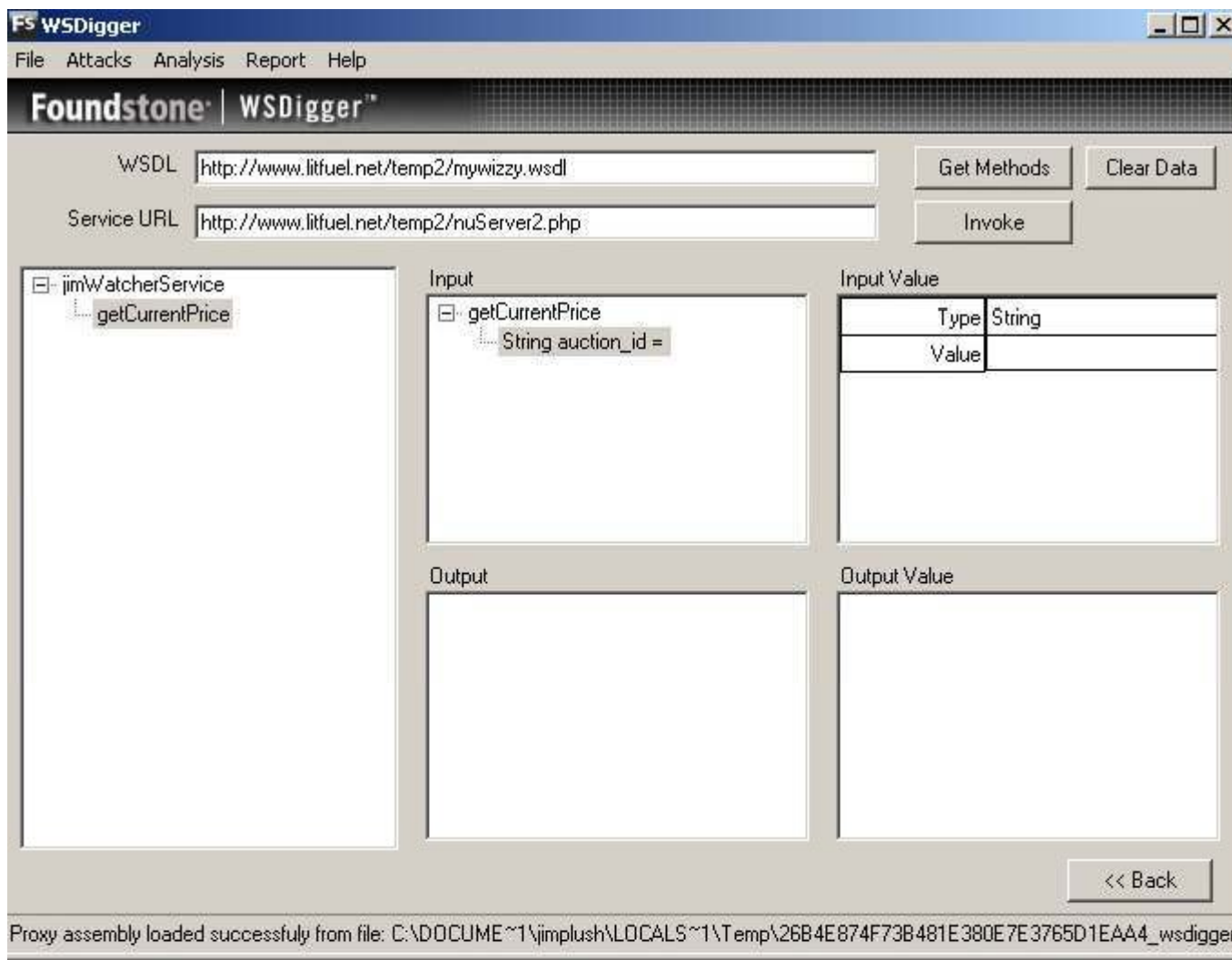
WSDigger is a free open source tool designed by Foundstone to automate black-box web services security testing

It is more than a tool; it is a web services testing framework

This framework contains sample attack plug-ins for SQL injection, cross site scripting, and XPATH injection attacks



WSDigger: Screenshot

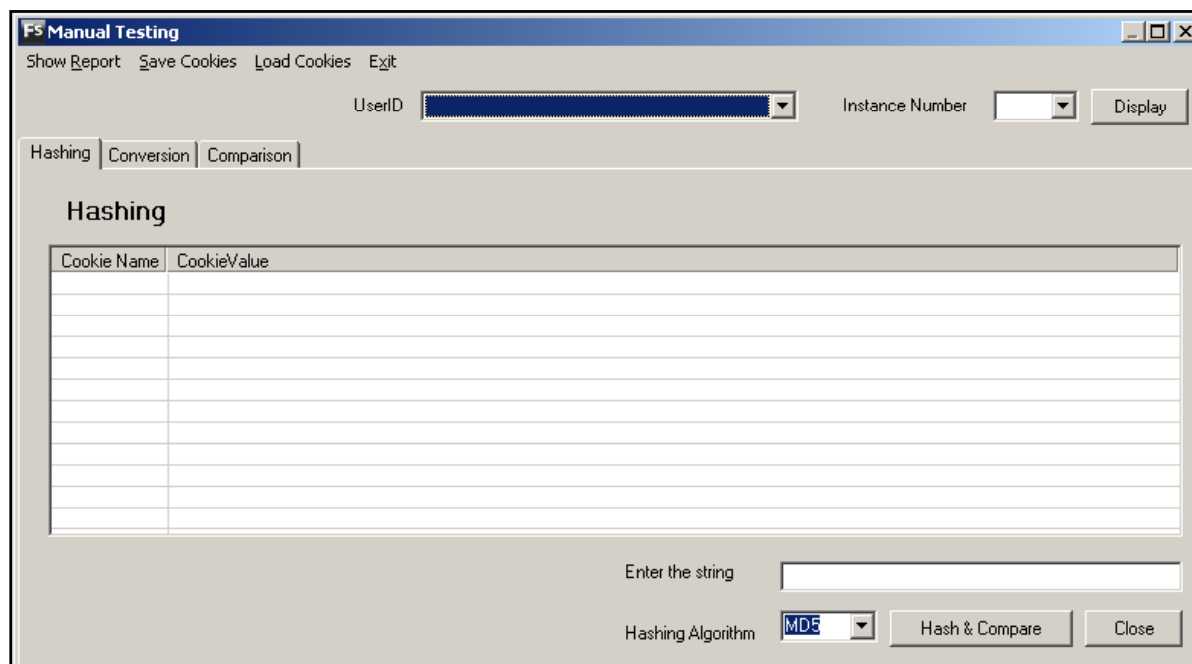


CookieDigger Tool

CookieDigger helps identify weak cookie generation and insecure implementations of the session management by web applications

The tool works by collecting and analyzing cookies issued by a web application for multiple users

The tool reports on the predictability and entropy of the cookie and whether critical information, such as user name and password, are included in the cookie values



SSL Digger Tool

SSLDigger is a tool to assess the strength of SSL servers by testing the supported ciphers

Some of these ciphers are known to be insecure

The screenshot shows the Foundstone SSLDigger tool interface. The address bar contains the URL `C:\Documents and Settings\Administrator\WINDOW\S\Desktop\SSLDigger.html`. The main content area displays the results for the server `https://www.eccouncil.org`.

Ciphers Supported

Server URL	No Security	Weak Security	Strong Security	Excellent Security	Grade
https://www.eccouncil.org	0	5	3	0	B

Detailed Results

SSL Certificate Details

Parameter	Value
Server	www.eccouncil.org
SSL Version	TLS 1.0
Key Algorithm	RSA_MD5
Key Algorithm Parameters	0500
Key Length	1024

Hacking Tool: WindowBomb

An email sent with this html code attached will create pop-up windows until the PC's memory gets exhausted

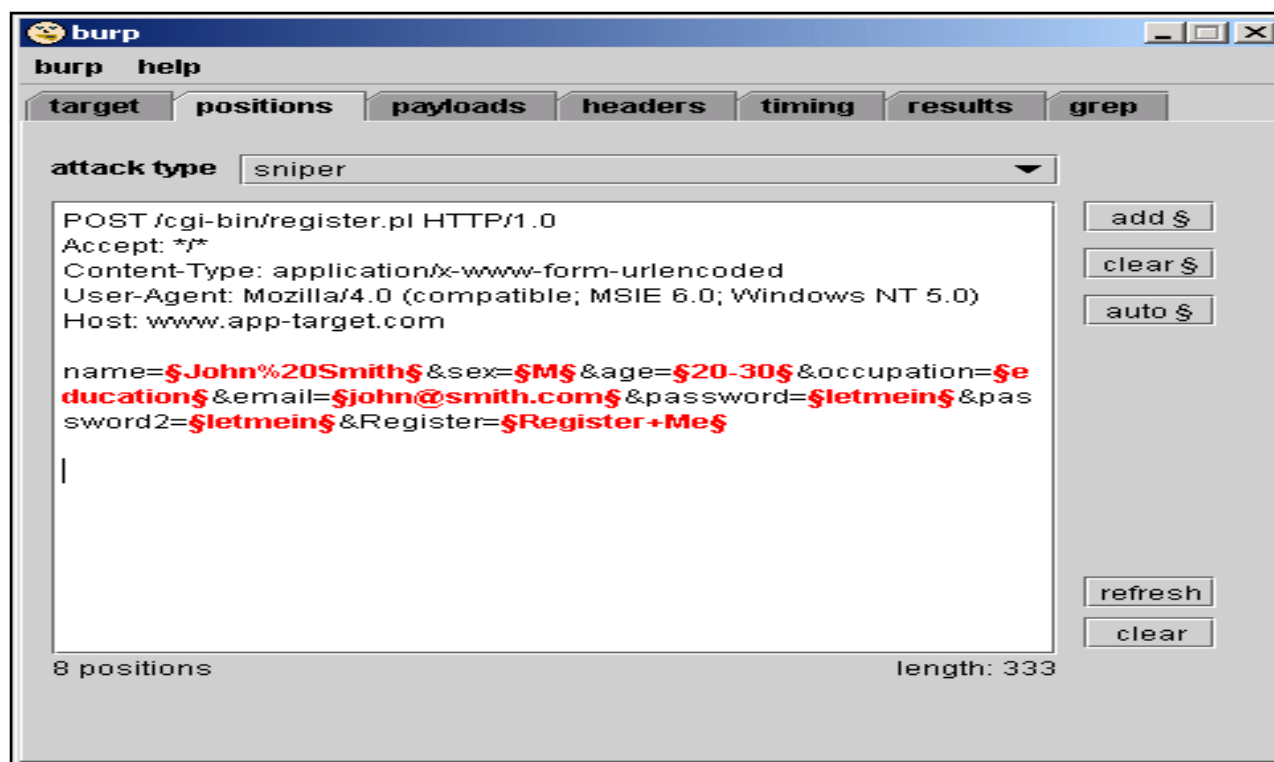
JavaScript is vulnerable to simple coding such as the example given below:

```
<HTML>
<HEAD>
<TITLE>WARNING [] INFECTING VIRUS </TITLE>
</HEAD>
<BODY ca load = "windowBomb ()">
<SCRIPT LANGUAGE= "Java Script">
{ FUNCTION WINDOW BOMB }
{ var : counter =0 // dummy counter
  while (true)
  {
    window open {"http://www.netscape.com",
"CRUSHING"
  + : counter, width=1, height=1,
resizable=90}
: counter ++
}
}
{/SCRIPT}
</BODY>
</HTML>
```



Burp: Positioning Payloads

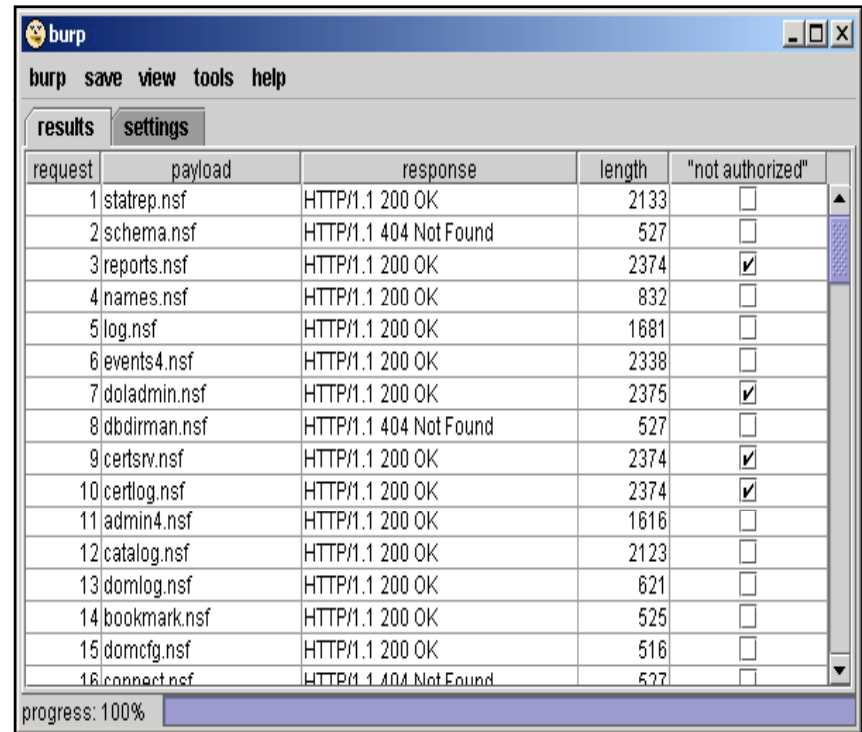
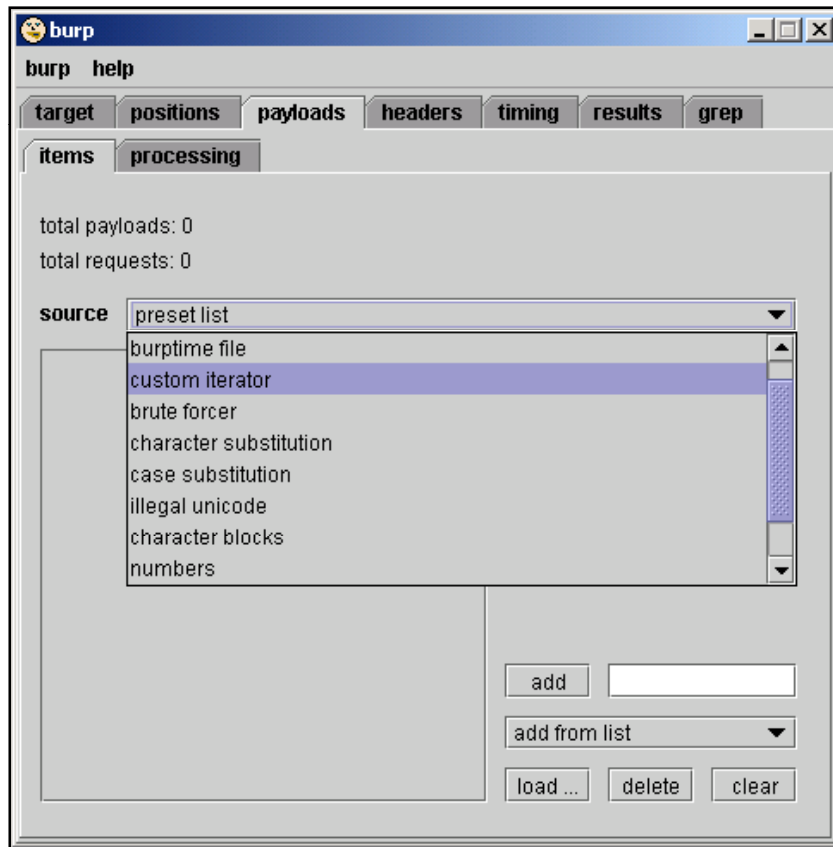
Burp is a tool for performing automated attacks against web-enabled applications



Source: <http://portswigger.net>

Burp: Configuring Payloads and Content Enumeration

Burp comes preconfigured with attack payloads and it can check for common databases on a Lotus Domino server



Burp: Password Guessing

Burp can be used for password guessing as well as data mining

burp save view tools help

results settings

request	payload	response	error	timeout	length	"login incorrect"
7091	faverias	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input type="checkbox"/>
7092	favella	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7093	fawisms	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7094	favored	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7095	favorer	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7096	favours	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7097	fawuses	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7098	fawners	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7099	fawnier	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7100	fawning	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7101	fazenda	HTTP/1.0 302 Object...	<input type="checkbox"/>	<input type="checkbox"/>	757	<input type="checkbox"/>
7102	fearers	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7103	fearful	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7104	fearing	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7105	feasing	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>
7106	feasted	HTTP/1.0 200 Ok	<input type="checkbox"/>	<input type="checkbox"/>	3733	<input checked="" type="checkbox"/>

progress: 18%

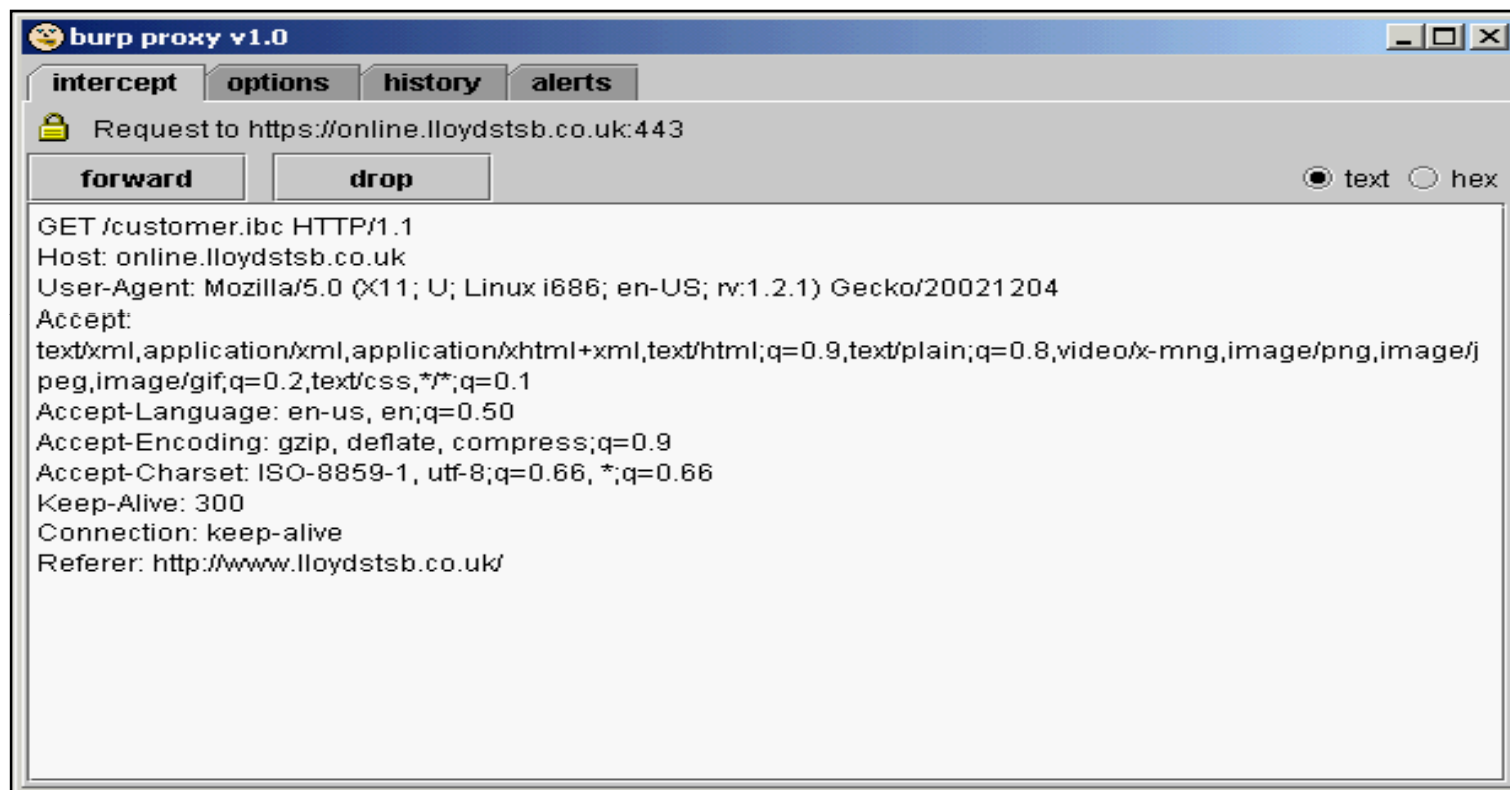
burp save view tools help

results settings

request	payload	response	length	name="username" va...	name="password" va...
285	0384	HTTP/1.0 200 Ok	1610	susanit	monday44
286	0385	HTTP/1.0 404 Not found	195		
287	0386	HTTP/1.0 200 Ok	1611	dthomas	godfather
288	0387	HTTP/1.0 200 Ok	1611	rbentley	chueh219
289	0388	HTTP/1.0 200 Ok	1612	nicholasw	password
290	0389	HTTP/1.0 200 Ok	1605	des	gateway
291	0390	HTTP/1.0 404 Not found	195		
292	0391	HTTP/1.0 404 Not found	195		
293	0392	HTTP/1.0 200 Ok	1611	richardx	richardx
294	0393	HTTP/1.0 404 Not found	195		
295	0394	HTTP/1.0 404 Not found	195		
296	0395	HTTP/1.0 404 Not found	195		
297	0396	HTTP/1.0 200 Ok	1614	administrator	infamy
298	0397	HTTP/1.0 200 Ok	1617	administrator2	firewall
299	0398	HTTP/1.0 200 Ok	1613	johnneville	teacher
300	0399	HTTP/1.0 404 Not found	195		

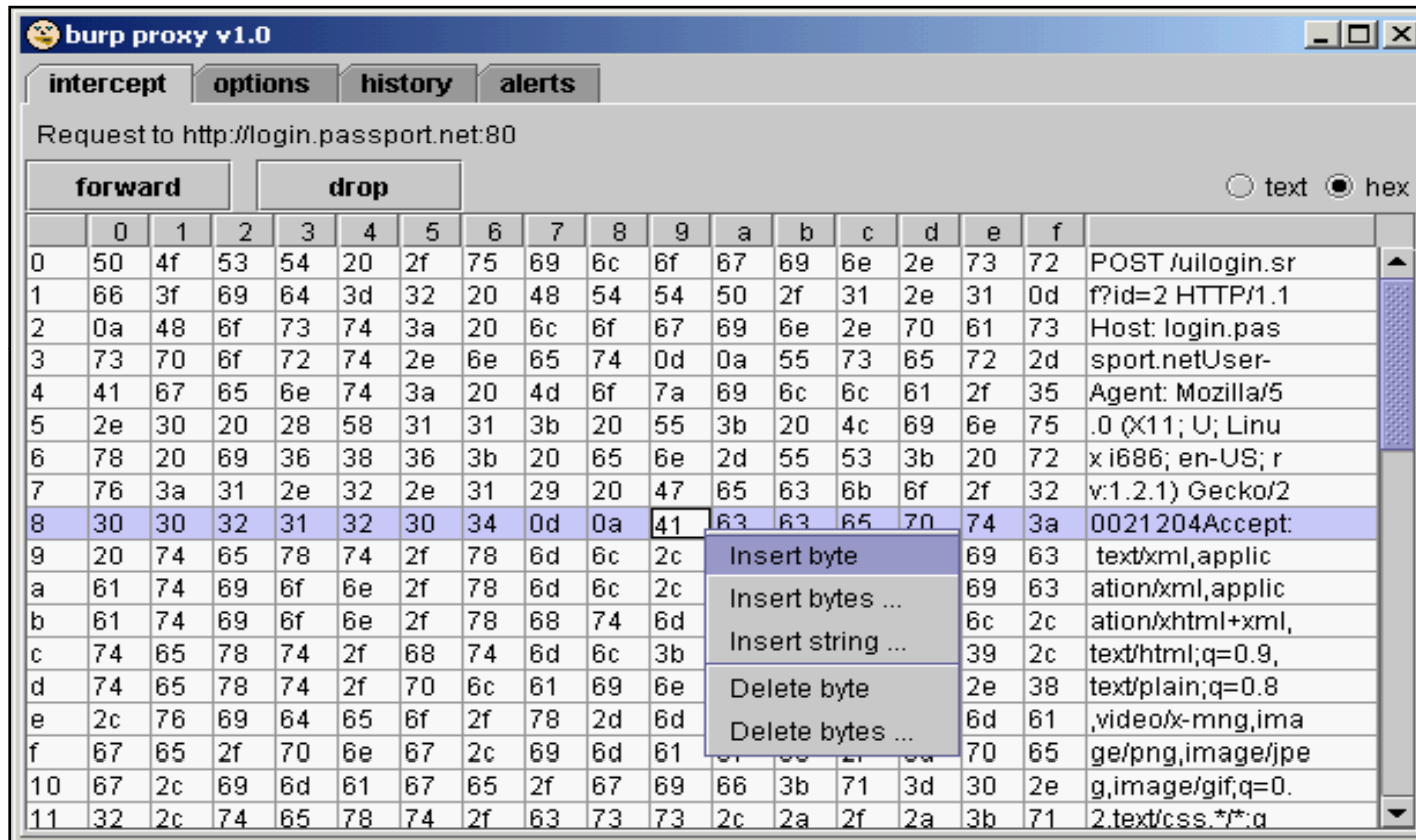
progress: 100%

Burp Proxy: Intercepting HTTP/S Traffic



Burp proxy operates as a man-in-the-middle between the end browser and the target web server, and allows the attacker to intercept, inspect, and modify the raw traffic passing in both directions

Burp Proxy: Hex-editing of Intercepted Traffic



Burp proxy allows the attacker to modify intercepted traffic in both text and hexadecimal form; so even transfers of binary data can be manipulated

Tool: Burpsuite

Burp suite is an integrated platform for attacking web applications

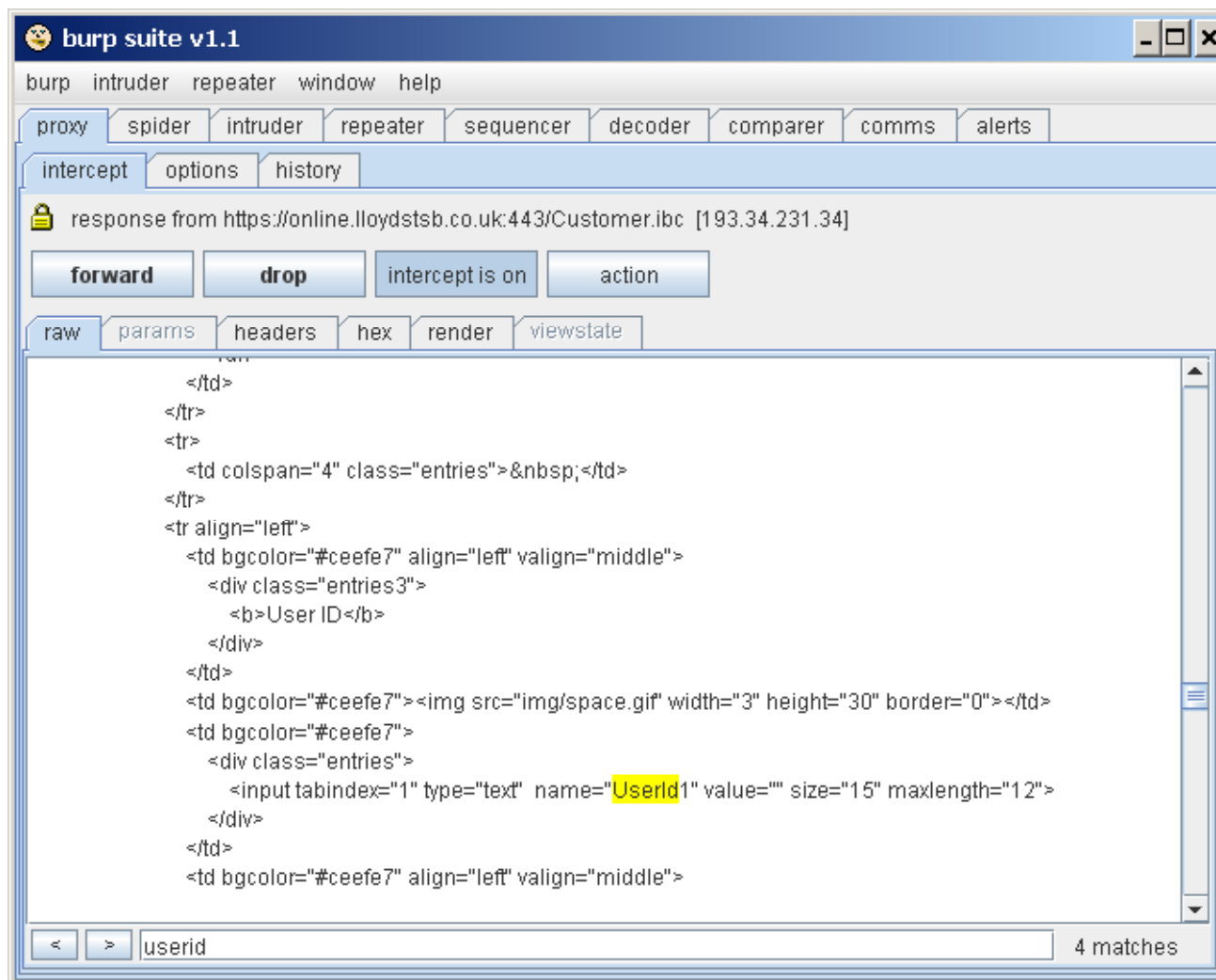
It allows an attacker to combine manual and automated techniques to enumerate, analyze, attack, and exploit web applications

The various burp tools work together effectively to share information and allow findings identified within one tool to form the basis of an attack using another

Key features include:

- Ability to passively spider an application in a non-intrusive manner
- One-click transfer of interesting requests between plug-ins, e.g. from proxy request history, or a web page form enumerated with burp spider
- Extensibility via IBurpExtender interface, which allows third-party code to extend functionality of burp suite
- Centrally configured settings for downstream proxies, web and proxy authentication, and logging
- Plug-ins can run in a single tabbed window, or be detached in individual windows
- All plug-ins and suite configuration is optionally persistent across program loads
- Runs in both Linux and Windows

Burpsuite: Screenshot 1



Burpsuite: Screenshot 2

The screenshot shows the Burp Suite v1.1 interface. The main window displays a list of intercepted requests. The selected request is a GET request to `http://amazon.co.uk/s/ref=nb_ss_w_h?url=search-alias%3Daps&field-...`. A context menu is open over this request, showing various actions such as 'send to intruder', 'send to repeater', 'copy URL to clipboard', and 'copy all URLs to clipboard'.

target	method	URL	type	SSL	IP	status	length	cookies
ecx.images-amazon.com...	GET	/images//116ofzeUJwL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	200	4,108	
ecx.images-amazon.com...	GET	/images//21H3zFHmNzL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	200	5,868	
ecx.images-amazon.com...	GET	/images//21N1rTEFcGL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	304	650	
ecx.images-amazon.com...	GET	/images//21N1rTEFcGL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	304	490	
ecx.images-amazon.com...	GET	/images//21XHFghSzeL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	304	373	
ecx.images-amazon.com...	GET	/images//21XHFghSzeL.jpg	jpg	<input type="checkbox"/>	216.38.160.117	304	426	
amazon.co.uk:80	GET	/s/ref=nb_ss_w_h?url=search-alias%3Daps&field-...		<input type="checkbox"/>	87.238.81.129	200	121,454	at-acb...
GET request to http://amazon.co.uk/s/ref=nb_ss_w_h?url=search-alias%3Daps&field-keywords=web+application+hacker%27s+handbook								
z-e send to intruder								
z-e send to repeater								
z-e send to spider								
z-e send to sequencer								
ecx send request to comparer								
ecx send response to comparer								
ad copy URL to clipboard								
ad copy all URLs to clipboard								
ad.yieldmanager.com:80	GET	/imp?z=160x600&s=225722&_salt=120503245&B=...		<input type="checkbox"/>	208.67.66.11	302	3,355	fl_inst...
ad.uk.doubleclick.net:80	GET	/adj/N3434.EType/B2564937.4;sz=160x600;ord=119...	817%...	<input type="checkbox"/>	209.62.178.57	200	4,396	
m.uk.2mdn.net:80	GET	/879366/flashwrite_1_2.js	js	<input type="checkbox"/>	216.73.84.103	304	161	
m.uk.2mdn.net:80	GET	/888452/160x600_cablecar_nov2007_uk.swf?clickT...	swf	<input type="checkbox"/>	216.73.84.103	200	14,275	
amazon.co.uk:80	GET	/favicon.ico	ico	<input type="checkbox"/>	87.238.81.129	200	1,679	

Hacking Tool: cURL

cURL is a multi-protocol transfer library

It is a client side URL transfer library supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE, and LDAP

cURL supports HTTPS certificates, HTTP POST, HTTP PUT, FTP uploading, Kerberos, HTTP form-based upload, proxies, cookies, user+password authentication, file transfer resume, http proxy tunneling, and more

Proof of Concept

Source: <http://curl.haxx.se>

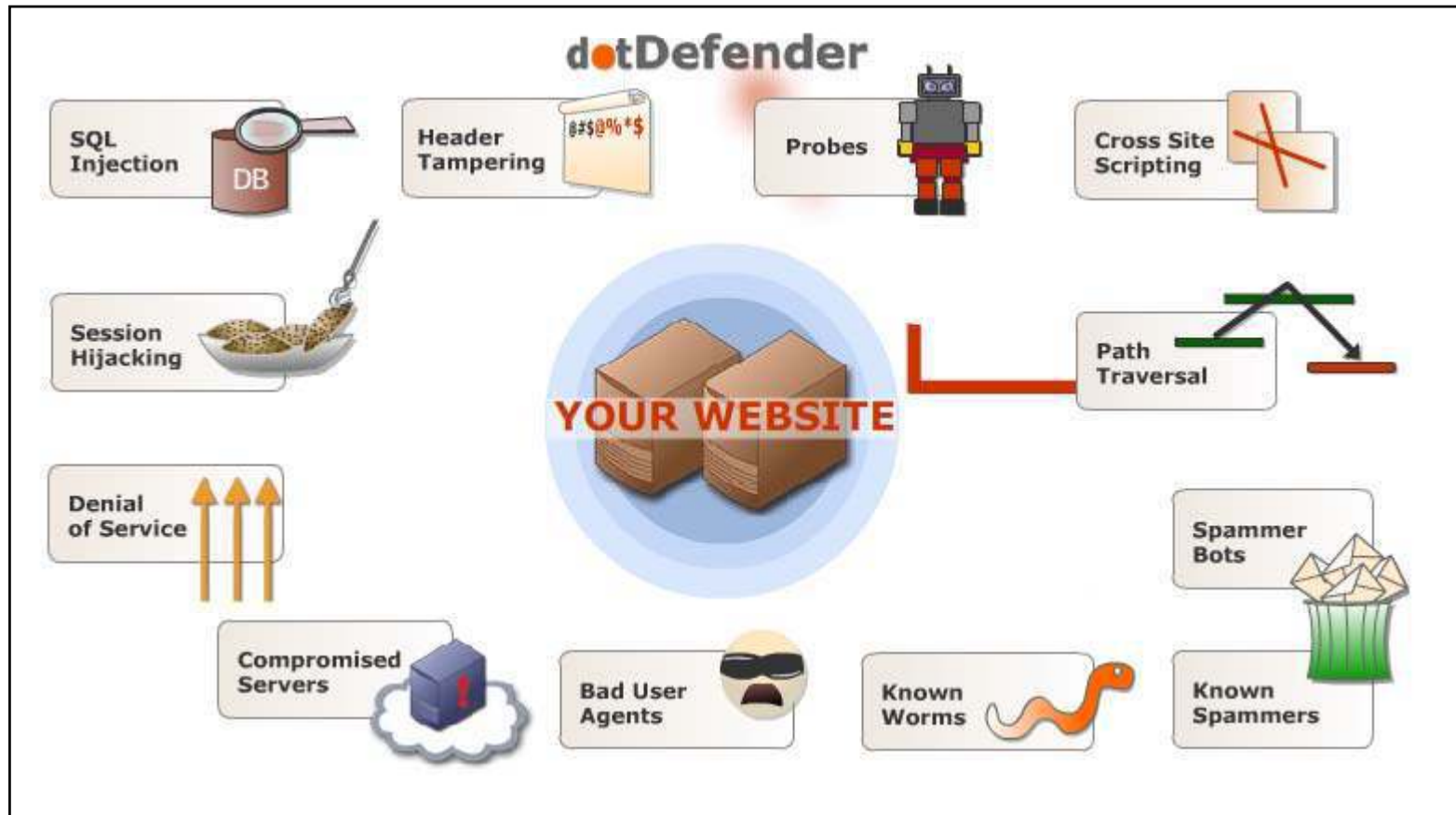
cURL: Screenshot

```
curl 7.10 (win32) libcurl/7.10
Usage: curl [options...] <url>
Options: (H) means HTTP/HTTPS only, (F) means FTP only
-a/--append          Append to target file when uploading (F)
-A/--user-agent <string> User-Agent to send to server (H)
-b/--cookie <name=string/file> Cookie string or file to read cookies from (H)
-B/--use-ascii       Use ASCII/text transfer
-c/--cookie-jar <file> Write all cookies to this file after operation (H)
-C/--continue-at <offset> Specify absolute resume offset
-d/--data <data>     HTTP POST data (H)
  --data-ascii <data> HTTP POST ASCII data (H)
  --data-binary <data> HTTP POST binary data (H)
  --disable-epsv     Prevents curl from using EPSV (F)
-D/--dump-header <file> Write the headers to this file
--egd-file <file> EGD socket path for random data (SSL)
-e/--referer         Referer page (H)
-E/--cert <cert[:passwd]> Specifies your certificate file and password (HTTPS)
  --cert-type <type> Specifies certificate file type (DER/PEM/ENG) (HTTPS)
  --key <key>         Specifies private key file (HTTPS)
  --key-type <type> Specifies private key file type (DER/PEM/ENG) (HTTPS)
  --pass <pass>       Specifies passphrase for the private key (HTTPS)
  --engine <eng>     Specifies the crypto engine to use (HTTPS)
  --cacert <file>    CA certificate to verify peer against (SSL)
  --capath <directory> CA directory (made using c_rehash) to verify
                    peer against (SSL, NOT Windows)
  --ciphers <list>   What SSL ciphers to use (SSL)
  --compressed      Request a compressed response (using deflate).
  --connect-timeout <seconds> Maximum time allowed for connection
  --crlf            Convert LF to CRLF in upload. Useful for MVS (OS/390)
-f/--fail           Fail silently (no output at all) on errors (H)
-F/--form <name=content> Specify HTTP POST data (H)
-g/--globoff       Disable URL sequences and ranges using {} and []
-G/--get           Send the -d data with a HTTP GET (H)
-h/--help          This help text
-H/--header <line> Custom header to pass to server. (H)
-i/--include       Include the HTTP-header in the output (H)
-I/--head          Fetch document info only (HTTP HEAD/FTP SIZE)
-j/--junk-session-cookies Ignore session cookies read from file (H)
  --interface <interface> Specify the interface to be used
```

dotDefender is a web application attack protection tool that blocks attacks that are manifested within the HTTP request logic such as:

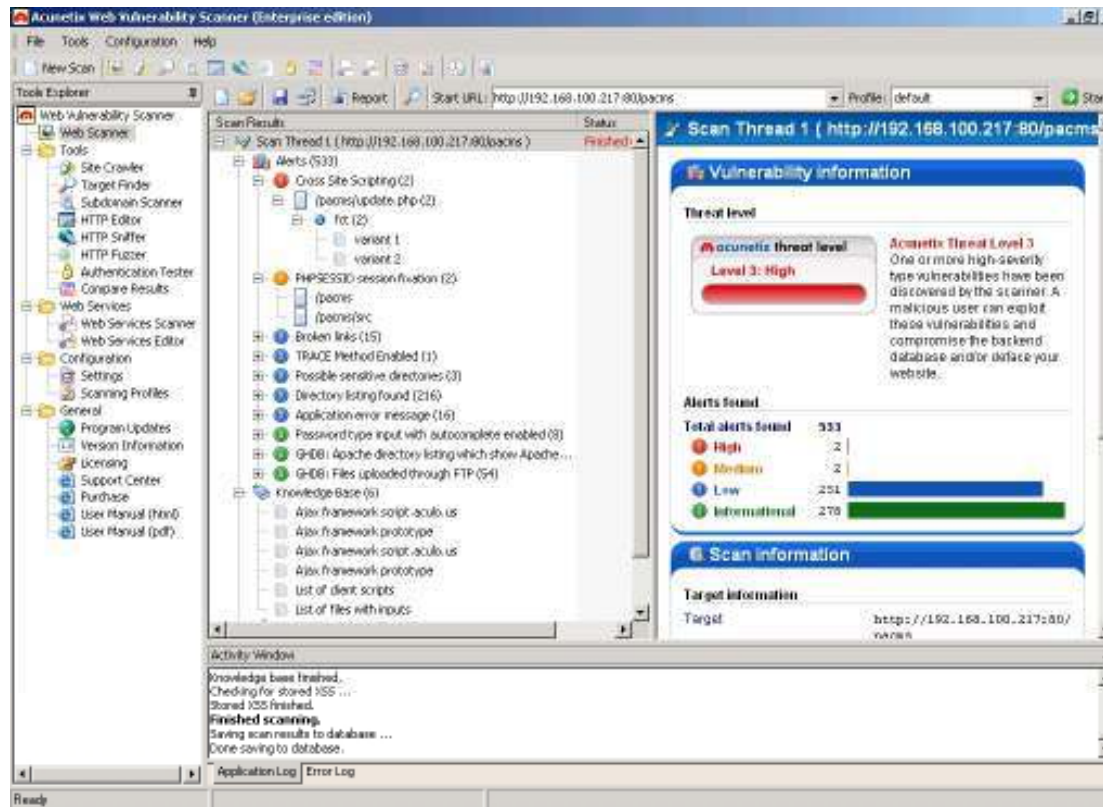
- **SQL Injection** - dotDefender intercepts and blocks attempts to inject SQL statements that corrupt or gain access to the corporate data
- **Proxy Takeover** - dotDefender intercepts and blocks attempts to divert traffic to an unauthorized site
- **Cross-site Scripting** - dotDefender intercepts and blocks attempts to inject malicious scripts that hijack the machines of subsequent site visitors
- **Header Tampering** - dotDefender identifies and blocks requests containing the corrupted header data
- **Path Traversal** - dotDefender blocks attempts to navigate through the host's internal file system
- **Probes** - dotDefender detects and blocks attempts to ferret the system's information
- **Known Attacks** - dotDefender recognizes and blocks attacks bearing known signatures

Source: <http://www.dotdefender.com>



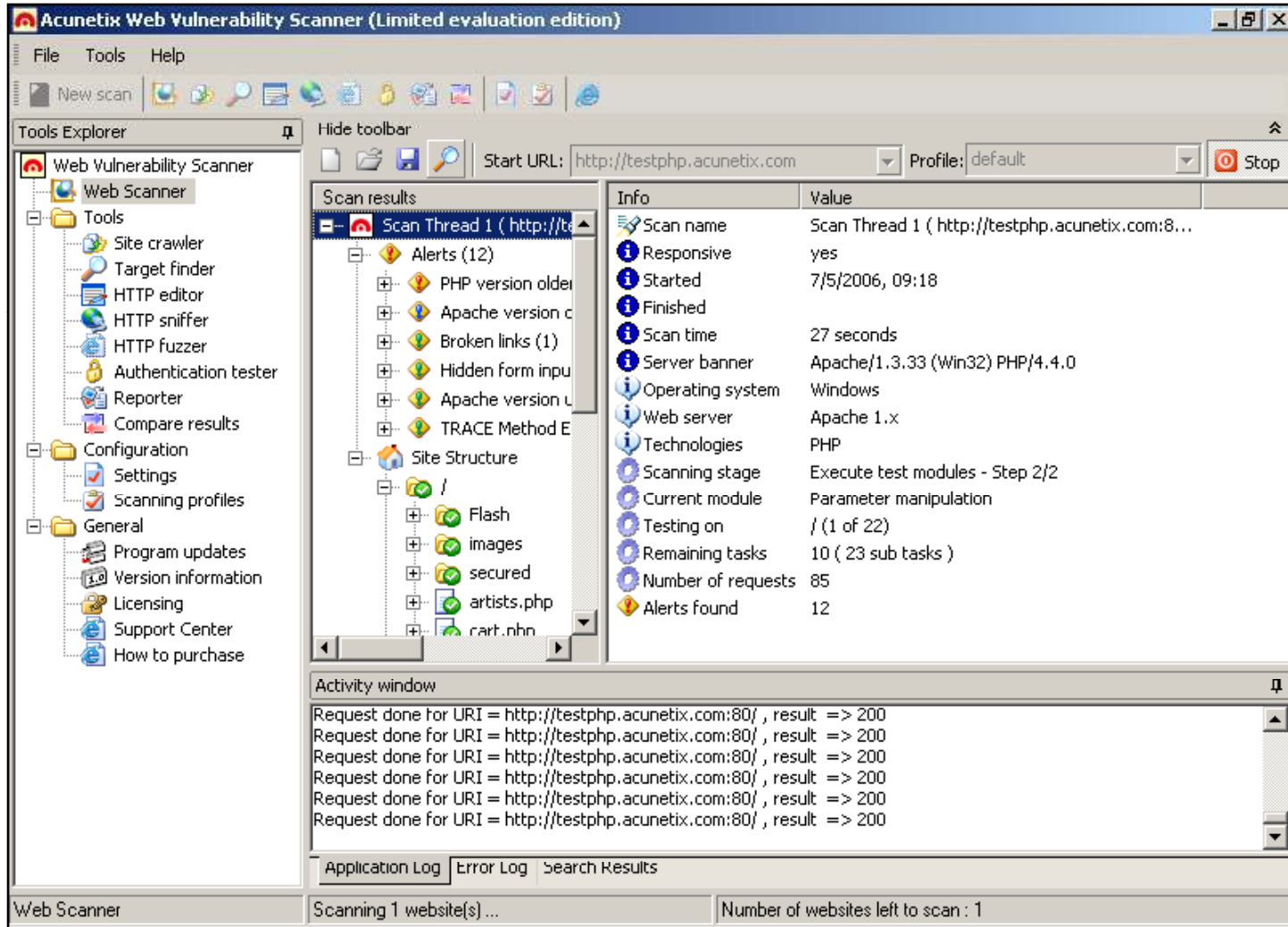
Acunetix Web Scanner

Acunetix launches all the Google hacking database queries onto the crawled content of your website, to find any sensitive data or exploitable targets before a “search engine hacker” does



Source: <http://www.acunetix.com>

Acunetix Web Scanner: Screenshot

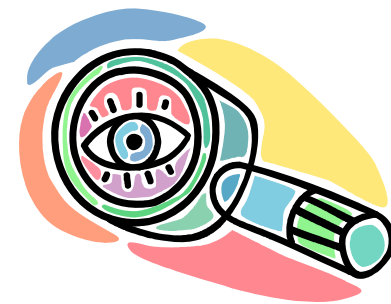


AppScan – Web Application Scanner

AppScan provides security testing throughout the application development lifecycle, which tests security assurance in the development stage

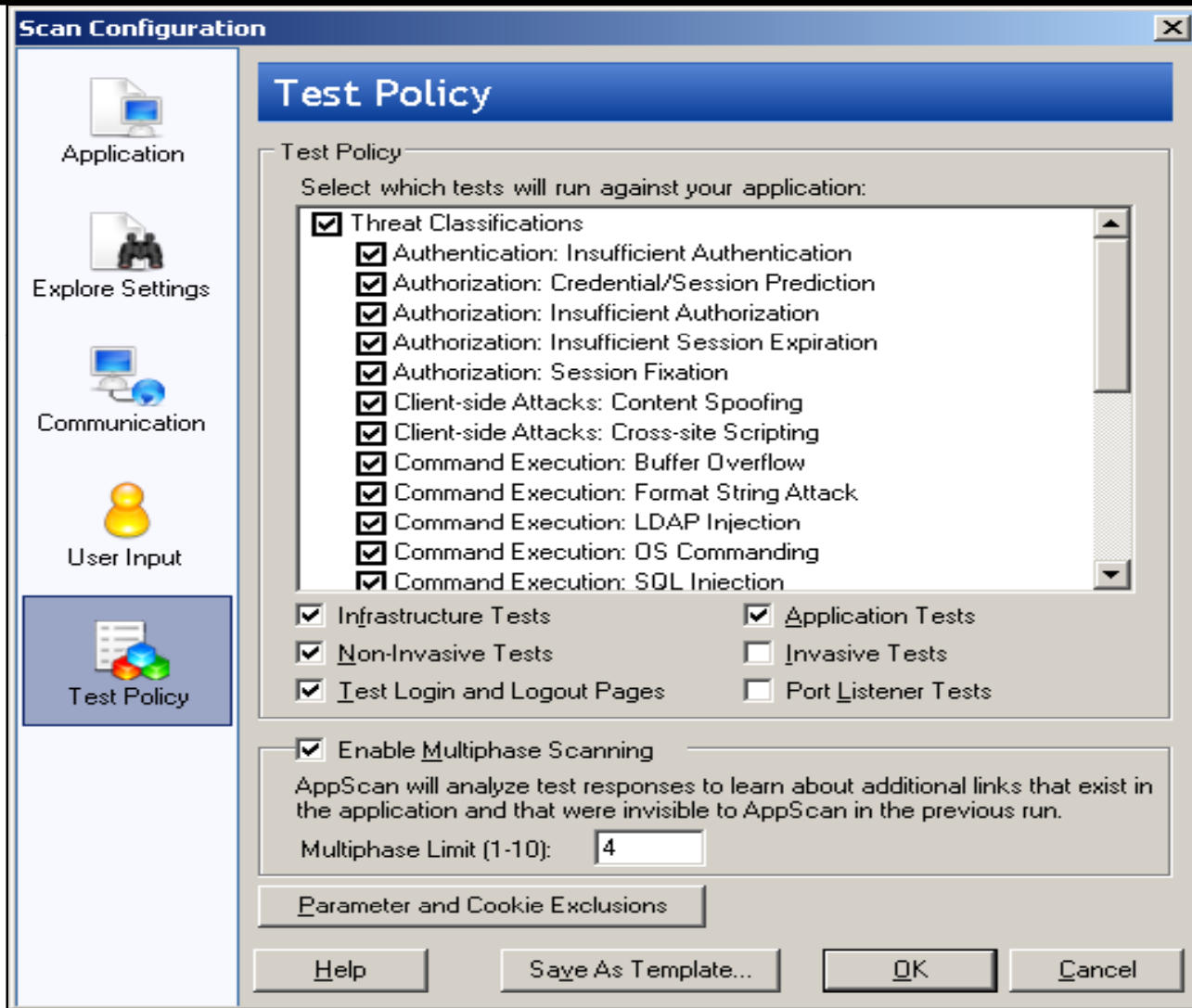
Vulnerability detects by simulating hacker attacks such as:

- Cross-Site Scripting
- HTTP Response Splitting
- Parameter Tampering
- Hidden Field Manipulation
- Backdoors/ Debug Options
- Stealth Commanding
- Forceful Browsing
- Application Buffer Overflows
- Cookie Poisoning
- Third-party misconfigurations
- Known vulnerabilities
- HTTP Attacks
- SQL Injection
- Suspicious Content
- XML/ SOAL Tests
- Content Spoofing
- LDAP Injection
- Session Fixation


















Source: www.watchfire.com







AppScan: Screenshot



AccessDiver is a security tester for WEB sites. It incorporates a set of powerful features which help you find and organize failures and weaknesses from your web site. Here is a quick list of the features available:

	Contains fast security that uses up to 100 bots to do its analysis.
	Detects directory failures by comparing hundreds of known problems to your site.
	AccessDiver is fully proxy compliant and has a proxy analyzer (speed / anonymity) and a proxy hunter built-in.
	A built-in word leecher helps you increase the size of your dictionaries to expand and reinforce your analysis.
	A powerful task automizer manages your jobs transparently. You can tackle unrelated tasks while Accessdiver is working, saving you time.
	An on-the-fly word manipulator lets you increase the strength of your dictionaries easily when doing your analysis.
	A PING tester is included to tell you the efficiency of your site and the efficiency of an Internet address you would like to access.
	A DNS resolver lets you look up the host name of an IP address and reverse the process to learn an unknown host name.
	A feature called 'HTTP debugger' helps your understanding of how actual HTTP protocol works. It opens up the process so you see what really happens during a connection problem.
	A WHOIS gadget lets you retrieve owner information of a domain name (in case you would like to buy the domain or contact the actual owner).
	An update notifier automatically tells you when a new version of AccessDiver is available.
	And I welcome you to discover the other extremely features by yourself... :)
	A leeching system allows you to collect new proxies to make better proxy lists
	n A proxy Hunting system allows you to get even more proxies by scanning IP regions...
	A file splitting and file merging system allows you to mixup files, or cut them in mutiple parts. That's good to handle wordlists or proxylists.

Requirements

	A PC compatible machine
	Windows 9x,Me,2000,XP,2003
	7 MB of space on your disk
	192 MB of memory (RAM)
	Pentium 200 or higher
	Screen resolution : 800x600

Source: <http://www.accessdiver.com>

AccessDiver: Screenshot

AccessDiver v4.270+

My Skill Tools Wordlist Weak History Help My other tool: HornyVision!!! Please make a donation to the author

flatus:flatus 6% 00:06:13

Test Basic authentication Stop Server http://www.juggyboy.com/ Test speed 50 Bots

Dictionary History Settings Proxy Socks Search Progression

Bot	Last UserName tried	Last Password tried	Last Response received	Proxy used & (Country Code)
1	mjb1969	mjb1969	200 - OK	None
2	tor2000	tor	200 - OK	None
3	snatch	snatch	200 - OK	None
4	boy	wonder	200 - OK	None
5	tacobell	tacobell	200 - OK	None
6	bushman	bushman	200 - OK	None
7	suck	cock	200 - OK	None
8	edyerko	bolong	200 - OK	None
9	forget	plaster	200 - OK	None
10	begood	begood	200 - OK	None
11	dcba	dcba	200 - OK	None
12	sami	sami	200 - OK	None
13	paiton	dolly	200 - OK	None
14	jackpot	jackpot	200 - OK	None
15	666666	3333332000	200 - OK	None
16	kurt	123456	200 - OK	None
17	laying	holidays	200 - OK	None
18	ultimate	ultimate	200 - OK	None
19	jamestd	kelcie	200 - OK	None
20	curtis	curtis	200 - OK	None
21	monica	blewclintski	200 - OK	None
22	otiscat	otiscat	200 - OK	None
23	starfuck	starfuck	200 - OK	None
24	roxy	roxy	200 - OK	None
25	rosemary	rosemary2000	200 - OK	None
26	obi-wan	obi-wan	200 - OK	None
27	matthew	matt	200 - OK	None
28	water123	filler	200 - OK	None

Found logins 44933 /hour

Weak logins: 0
 Speed: 44933 /hour
 Time spent: 00:00:27
 Time left: 00:06:13
 Attempts: 342
 Attempt left: 4658

Tool: Falcove Web Vulnerability Scanner

Falcove is used by web-site owners to see whether their web sites are hackable or vulnerable to attacks

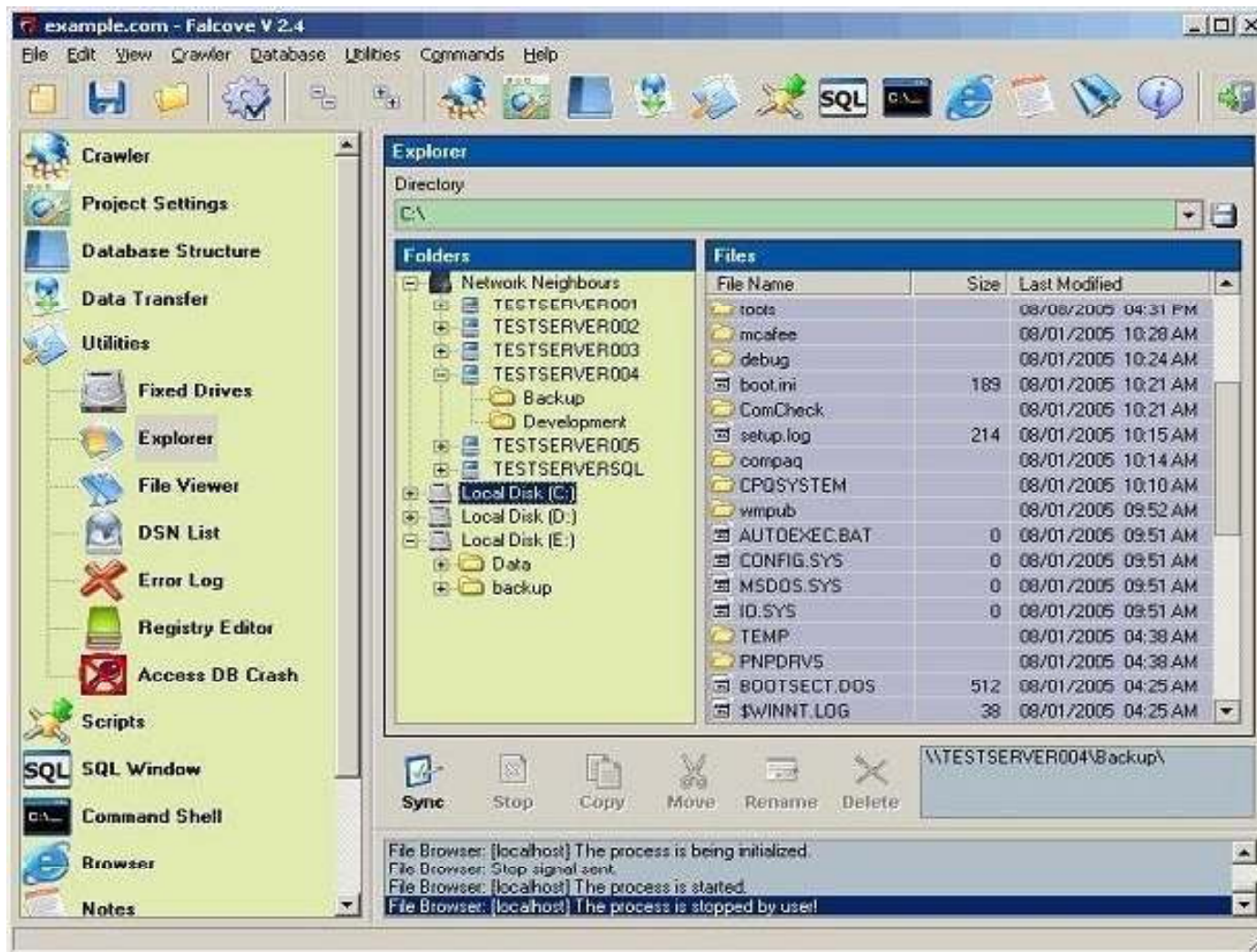
It finds vulnerabilities before hackers do and takes necessary precautions to implement the corrective actions

Features:

- Gives you an idea whether your website is secure against web attacks
- Crawler feature automatically checks for web vulnerabilities
- Audits all dynamic content including password fields, shopping carts, and other web applications
- Generates penetration reports that give you a certain idea about your websites' security level



Falcove Web Vulnerability Scanner: Screenshot



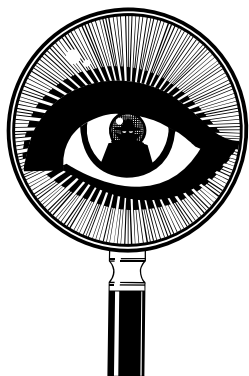
Tool: NetBrute

NetBrute scans a range of IP addresses for shared resources that have been shared via Microsoft File and Printer Sharing

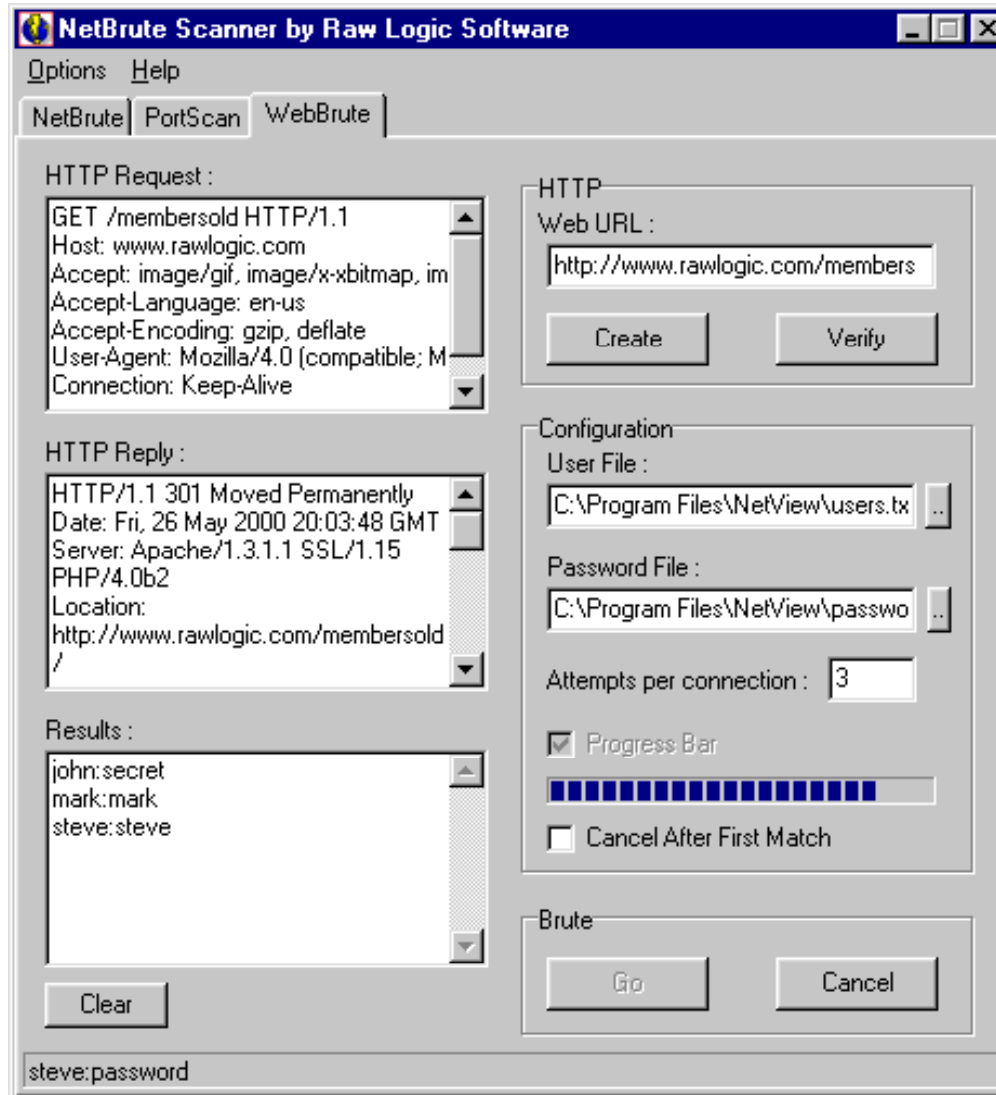
It shows any SMB compatible shared resources (i.e. Samba Servers on a Unix/Linux machine)

It is used by system administrators or home users to see what types of resources are shared and to warn the computer users if any unsecured resources are displayed

It finds all resources, whether they have passwords or not



NetBrute: Screenshot



Tool: Emsa Web Monitor

Emsa web monitor is a small web monitoring program that runs on your desktop and allows the user to monitor uptime status of several websites

It works by periodically pinging the remote sites, and showing the ping time as well as a small graph that allows the user to quickly view recent monitoring history

It is rather simple but useful in monitoring a set of websites



Tool: KeepNI

Keep an eye on your web site's functionality

It assures that your site is up and fully functional every time

Whenever a malfunction is detected, KeepNI immediately alerts you

KeepNI has an extensive logging facility to watch and alert

It logs and analyzes the collected data to present a full comprehensive view of your web site's performance



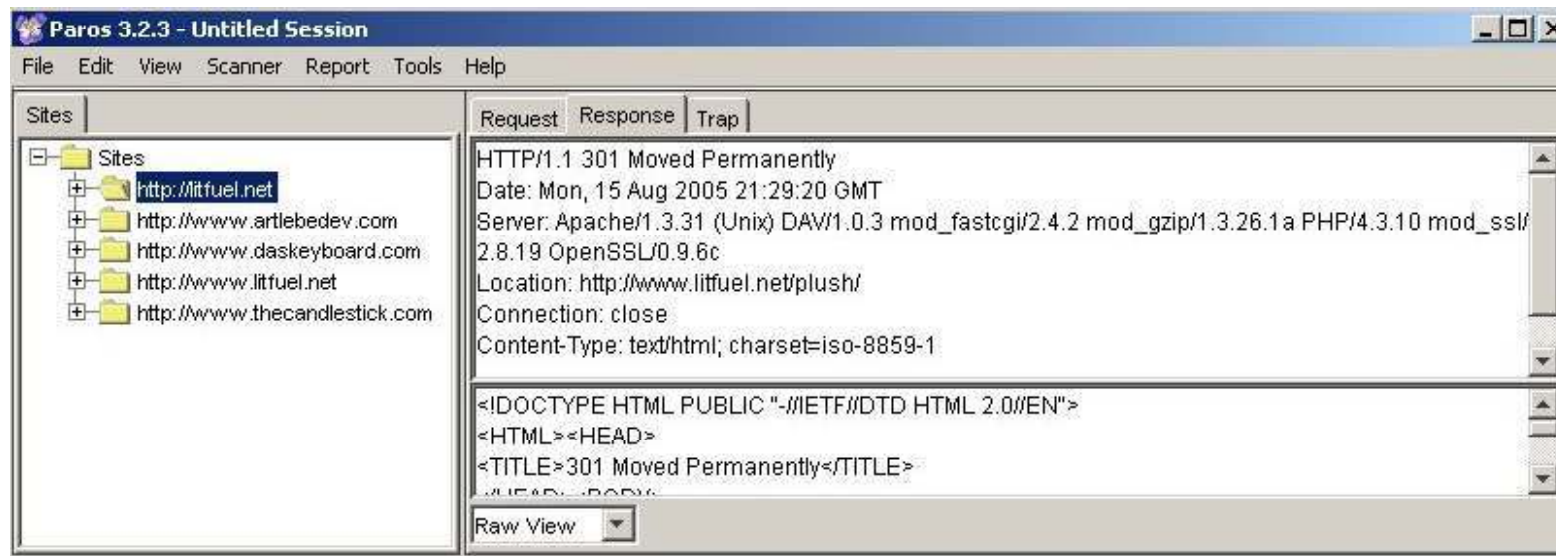
KeepNI: Screenshot



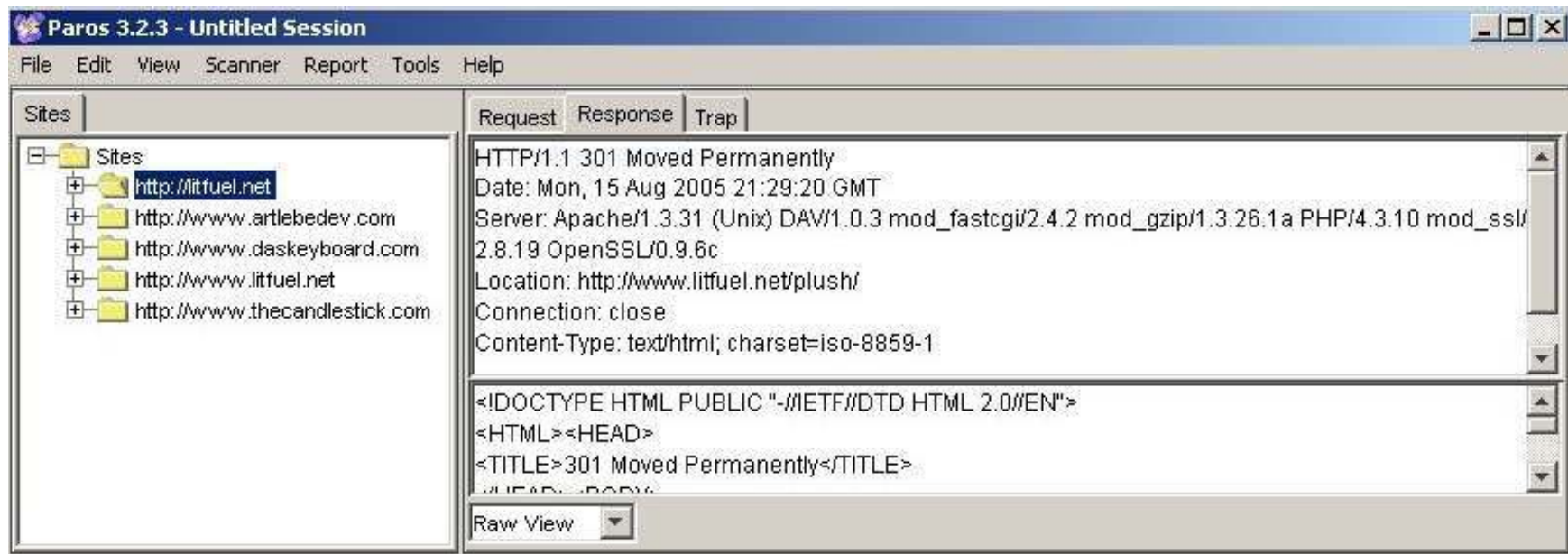
Tool: Parosproxy

Parosproxy is written in Java and useful for testing web applications and insecure sessions

Paros's proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified



Parosproxy: Screenshot



Tool: WebScarab

WebScarab is a Java framework for analyzing applications that communicate using the HTTP and HTTPS protocols

It operates as an intercepting proxy, allowing operator to review and modify requests created by the browser before they are sent to the server and vice versa

WebScarab can intercept both HTTP and HTTPS communication

Operator can also review the conversations (requests and responses) that have passed through WebScarab



WebScarab: Screenshot 1

The screenshot shows the WebScarab application window. The menu bar includes File, View, Tools, and Help. Below the menu is a toolbar with buttons for Summary, Message log, Proxy, Manual Request, WebServices, Spider, Extensions, SessionID Analysis, Scripted, Fragments, Fuzzer, and Compare. The main area is titled 'Summary' and contains a 'Tree Selection filters conversation list' with a tree view of the website structure. Below the tree is a table of request details, and at the bottom is a detailed log table.

Url	Methods	Status	Set-Cookie	Comments	Scripts
http://www.owasp.org:80/	GET	301 Moved ...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
banners/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
images/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
index.php/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Main_Page	GET	200 OK	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
skins/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main....??		200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy

5.27 / 63.56

WebScarab: Screenshot 2

The screenshot shows the WebScarab interface for a conversation. The top bar indicates the current request: "1 - GET http://www.owasp.org:80/ 301 Moved Permanently".

The interface is divided into two main sections for the request and response.

Request Section:

- Method: GET
- URL: http://www.owasp.org:80/
- Version: HTTP/1.0
- Header Table:

Header	Val
Accept	image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/...
Accept-Language	en-us
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host	www.owasp.org

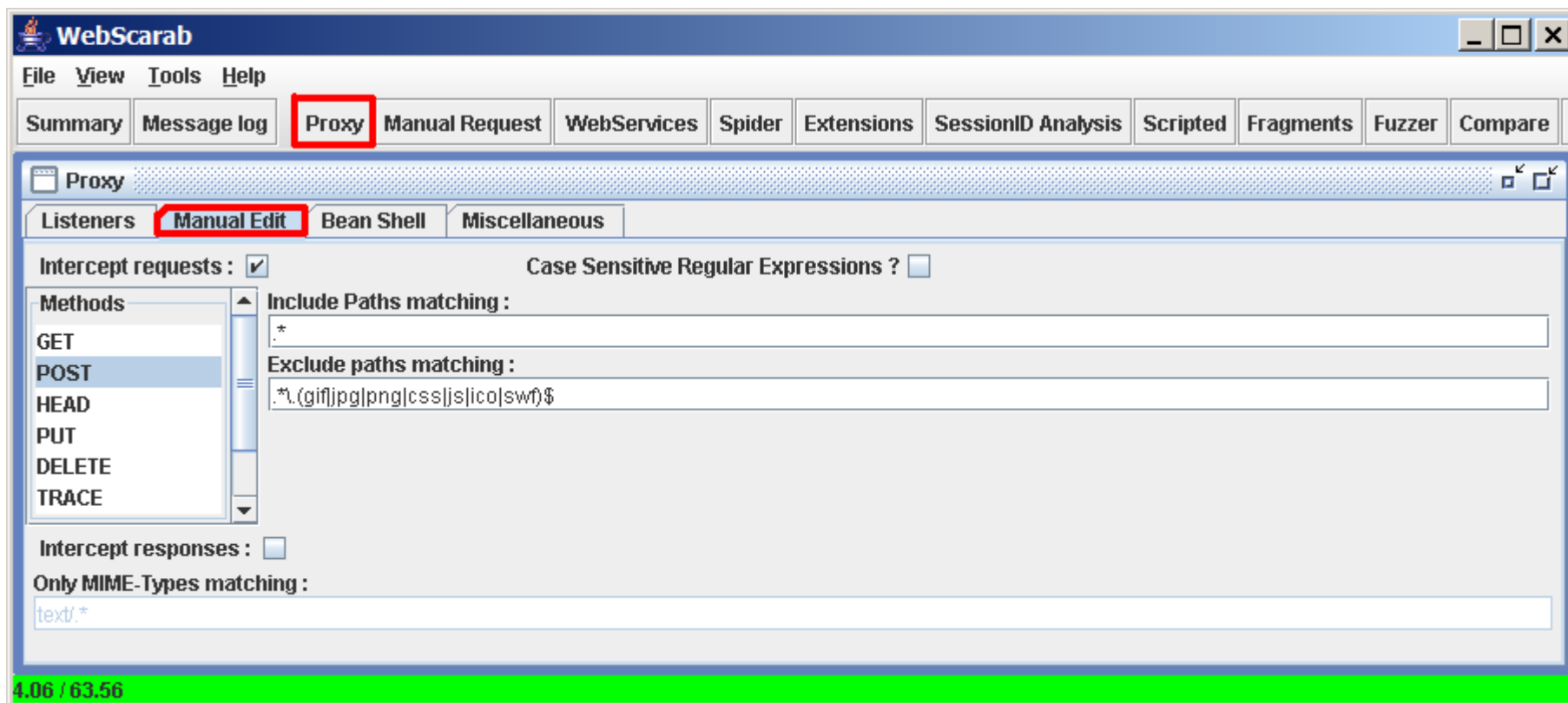
Response Section:

- Version: HTTP/1.1
- Status: 301
- Message: Moved Permanently
- Header Table:

Header	Val
Date	Fri, 23 Jun 2006 13:20:02 GMT
Server	Apache/2.0.52 (Ubuntu)

At the bottom, there are tabs for viewing the response content: HTML, XML, Text, and Hex. The Hex tab is currently selected, but the content area is empty.

WebScarab: Screenshot 3



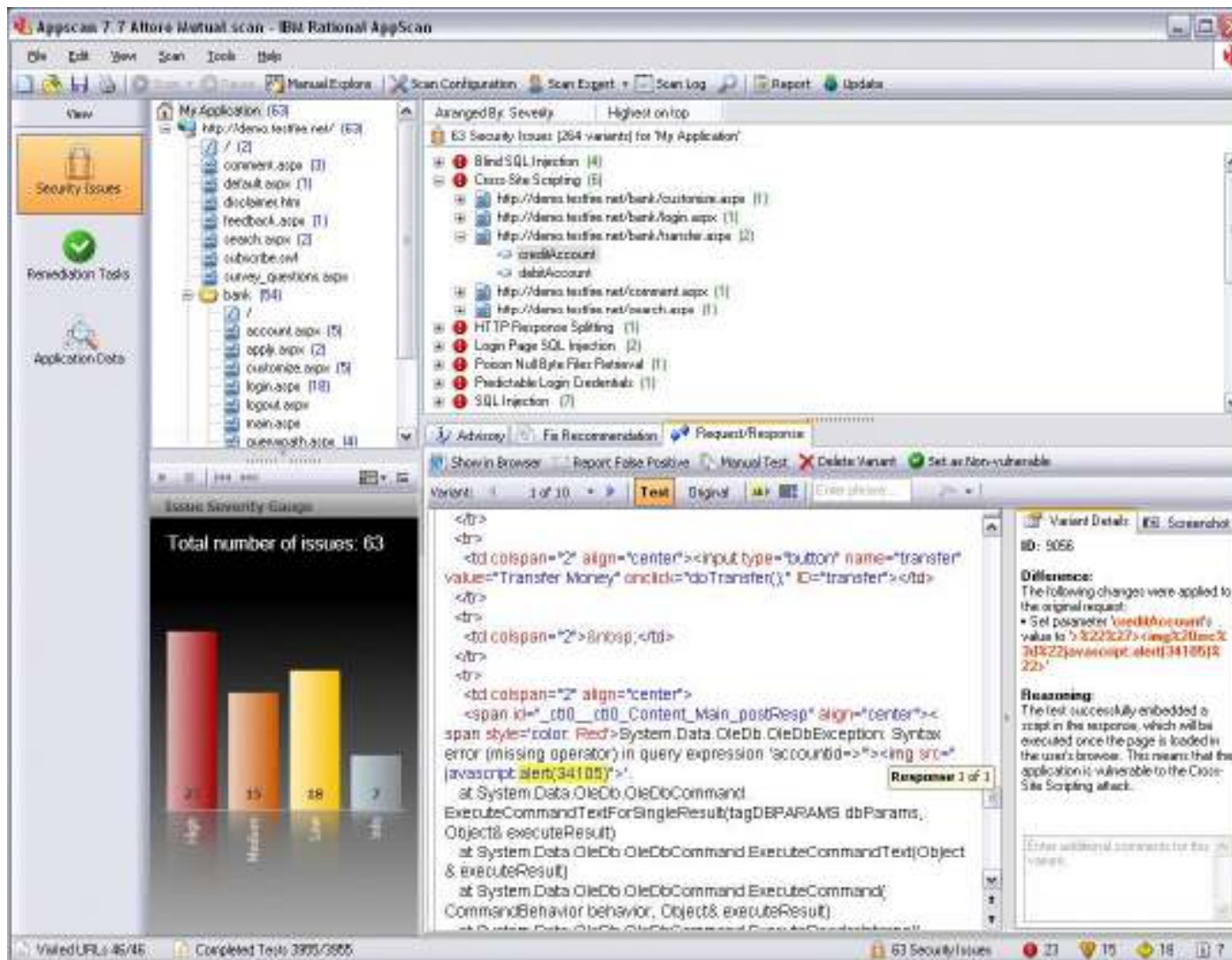
Watchfire® AppScan® automates web application security audits to ensure the security and compliance of websites

Benefits:

- Fully outsourced web application vulnerability management
- Direct access to Watchfire security experts and industry best practices
- Best path to actionable data for web application's security management
- Dramatically reduces the learning curve and adoption time
- Shields against loss of knowledge related to turnover or reorganization



Watchfire AppScan: Screenshot



Tool: WebWatchBot

WebWatchBot is a monitoring and analysis software for web sites and IP devices including Ping, HTTP, HTTPS, SMTP, POP3, FTP, Port, and DNS checks

It provides in-depth monitoring and alerting functionality as well as tools to analyze and visualize historical data with real-time charting and graphs

Additional features include an option to run as a Windows Service, customizable 3D charts with print support, SQL database storage, etc.



WebWatchBot: Screenshot

ExclamationSoft WebWatchBot - Enterprise - Application Mode - (*DEBUG *)

File Edit View Tools Reports Actions Help

New Properties Delete Run Now Run All Now Suspend Activate

Control Panel

Explorer

Watch Explorer

Filters:Status

- All
- Active
- Suspended
- Down
- Up

Filters:Types

- Ping
- HTTP
- HTTPS
- SMTP
- POP3
- FTP

Explorer

Scheduler

Dashboard

All

...	Tran...	Alar...	Watch...	Watch Item Name	Check Frequ...	Action	Last...	Avg ...	Time
	No	UP	HTTP	amazon.co.uk	1 minute	*SUSP...	4063	4063	1
	No	UP	HTTPS	bluecycle.com - HTTPS	1 minute	*SUSP...	4171	4171	1
	No	Down	FTP	bluecycle.com FTP	10 minutes	*SUSP...	906	906	1
	No	UP	HTTP	bluecycle.com New Fr...	1 minute	*SUSP...	2795	2795	1
	No	UP	HTTP	bluecycle.com/	1 minute	*SUSP...	3861	3861	1
	No	UP	HTTP	ebay	1 minute	*SUSP...	2936	2936	1
	No	UP	Ping	Example #1 - Ping	1 hour	*SUSP...	0	0	0

Log - amazon.co.uk

```

[10/28/04 19:35:09.703] Watch URL:          http://www.amazon.co.uk
[10/28/04 19:35:09.703] Watch Type:          HTTP
[10/28/04 19:35:09.703] Interval:            1 minute
[10/28/04 19:35:09.703] Times Checked:      1
[10/28/04 19:35:09.703] Times Failed:       0
[10/28/04 19:35:09.703] Failure Pct:        0.00%
[10/28/04 19:35:09.703] [DEBUG] m_hwndParentWnd: 4917528
[10/28/04 20:05:44.734] -----***[ End of Log: 10/28/2004
20:05:44]***-----
[10/28/04 20:34:01.718] -----***[ WebWatchBot 3.0 Build 0 (DEBUG) Started
]***-----
[10/28/04 20:34:01.718] Watch Name:          amazon.co.uk
    
```

Real-Time Chart Output Log Response Time Chart

WebWatchBot is Ready

1 of 22 Selected

Ratproxy is a semi-automated and largely passive web application security audit tool

It is designed specifically for an accurate and sensitive detection, and automatic annotation of potential problems

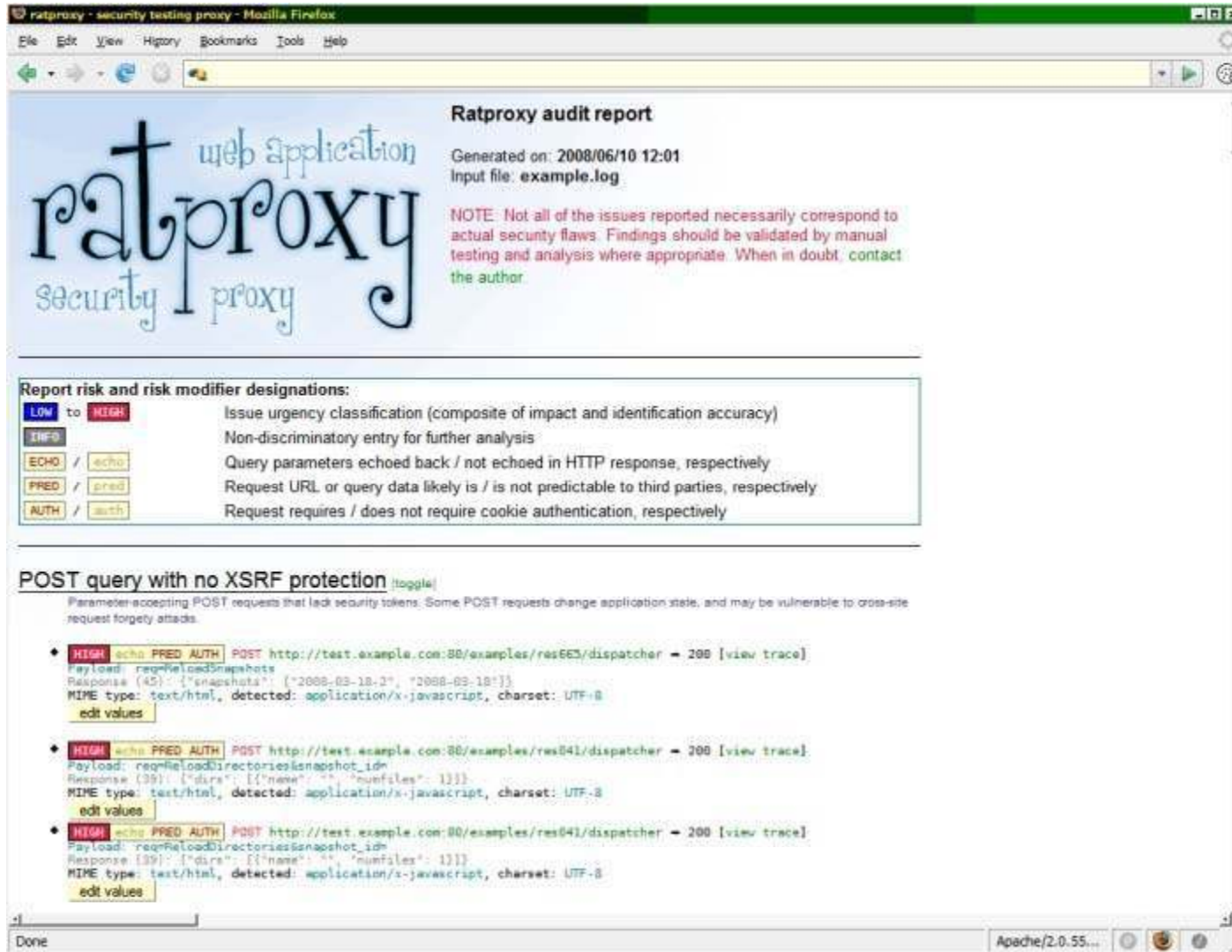
It is optimized for security-relevant design patterns based on the observation of existing, user-initiated traffic in complex web environments



How Does it Avoid False Positives?

For accurately reporting of problems and to reduce the number of false alarms, ratproxy has to considered the following points:

- What the declared and actually detected MIME type for the document is?
- How pages respond to having cookie-based authentication removed?
- Whether requests seem to contain non-trivial, sufficiently complex security tokens, or other mechanisms that may make the URL difficult to predict?
- Whether any non-trivial parts of the query are echoed back in the response, and in what context?
- Whether the interaction occurs on a boundary of a set of domains defined by runtime settings as the trusted environment subjected to the audit, and the rest of the world?





Mapper helps you map the files, file parameters, and values of any site you wish to test

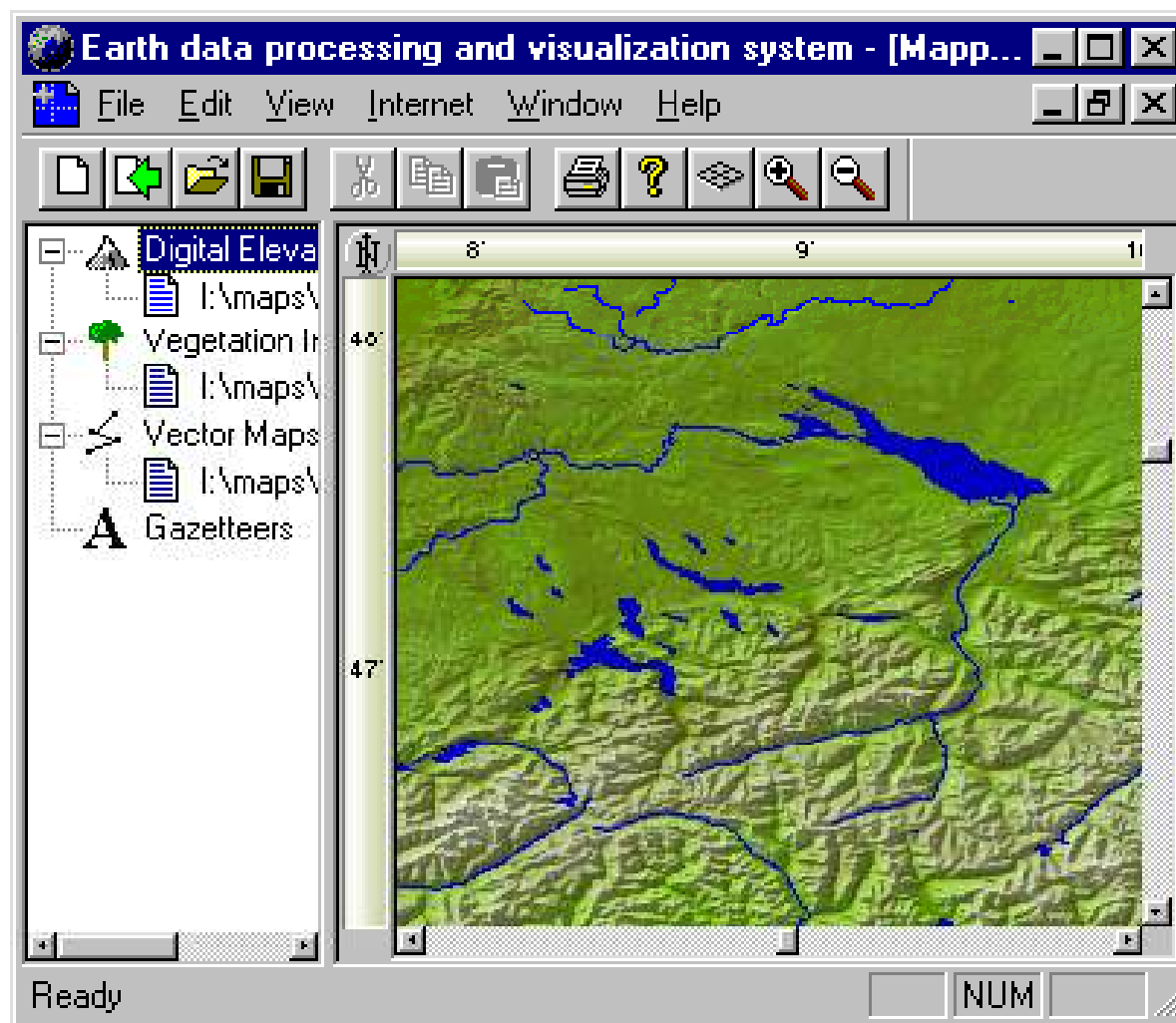
Simply browse the site as a normal user while recording your session with Achilles (Mapper supports other proxies as well), and run Mapper on the resulting log file

It will create an Excel CSV file that allows you to study the directory and file structure of the site, the parameter names of every dynamic page encountered (such as ASP/JSP/CGI), and their values for every time you request for them

It helps you to quickly locate design errors and parameters that may be prone to SQL Injection or parameter tampering problems

Supports non-standard parameter delimiters and MVC-based web sites

Mapper: Screenshot



What Happened Next

Kimberly could not solve the mystery behind the hack. Jason Springfield, an Ethical hacker was called in to investigate the case.

Jason conducted a penetration test on the website of XBank4u. The test results exposed a vulnerability in the ShrinkWarp application which could lead to web page defacement.

Some other loopholes found on the website were also fixed by Jason.

Web applications are client/ server software applications that interact with users or other systems using HTTP

Attackers may try to deface the website, steal credit card information, inject malicious codes, exploit server side scriptings, and so on

Command injection, XSS attacks, Sql Injection, Cookie Snooping, cryptographic Interception, and Buffer Overflow are some of the threats against web applications

Organization policies must support the countermeasures against all such types of attacks

© 2000 Randy Glasbergen.
www.glasbergen.com



**“Today at work, I received 650 E-mails from
feedme@homecat.com! Was that you?”**

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**“I wouldn’t say my computer skills are outdated.
I prefer to think of them as ‘classic’.”**