2010: and still bruteforcing OWASP Webslayer

Christian Martorella

July 18th 2010

Barcelona

S21sec

Tomorrow's Digital Security, Today

internet security auditors

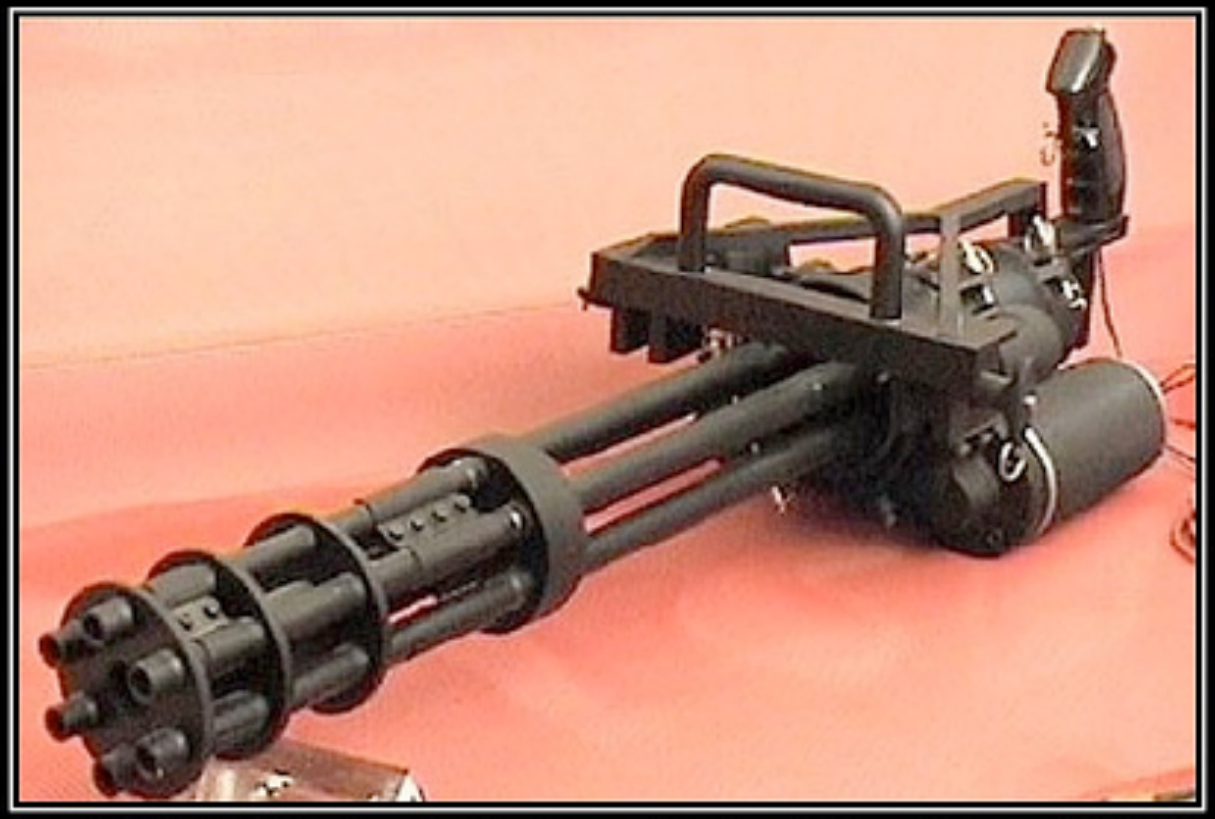
Who am I

- Manager Auditoria 

- CISSP, CISA, CISM, OPST, OPSA,CEH
- OWASP WebSlayer Project Leader
- FIST Conference, Presidente
- Edge-Security.com

Brute force attack

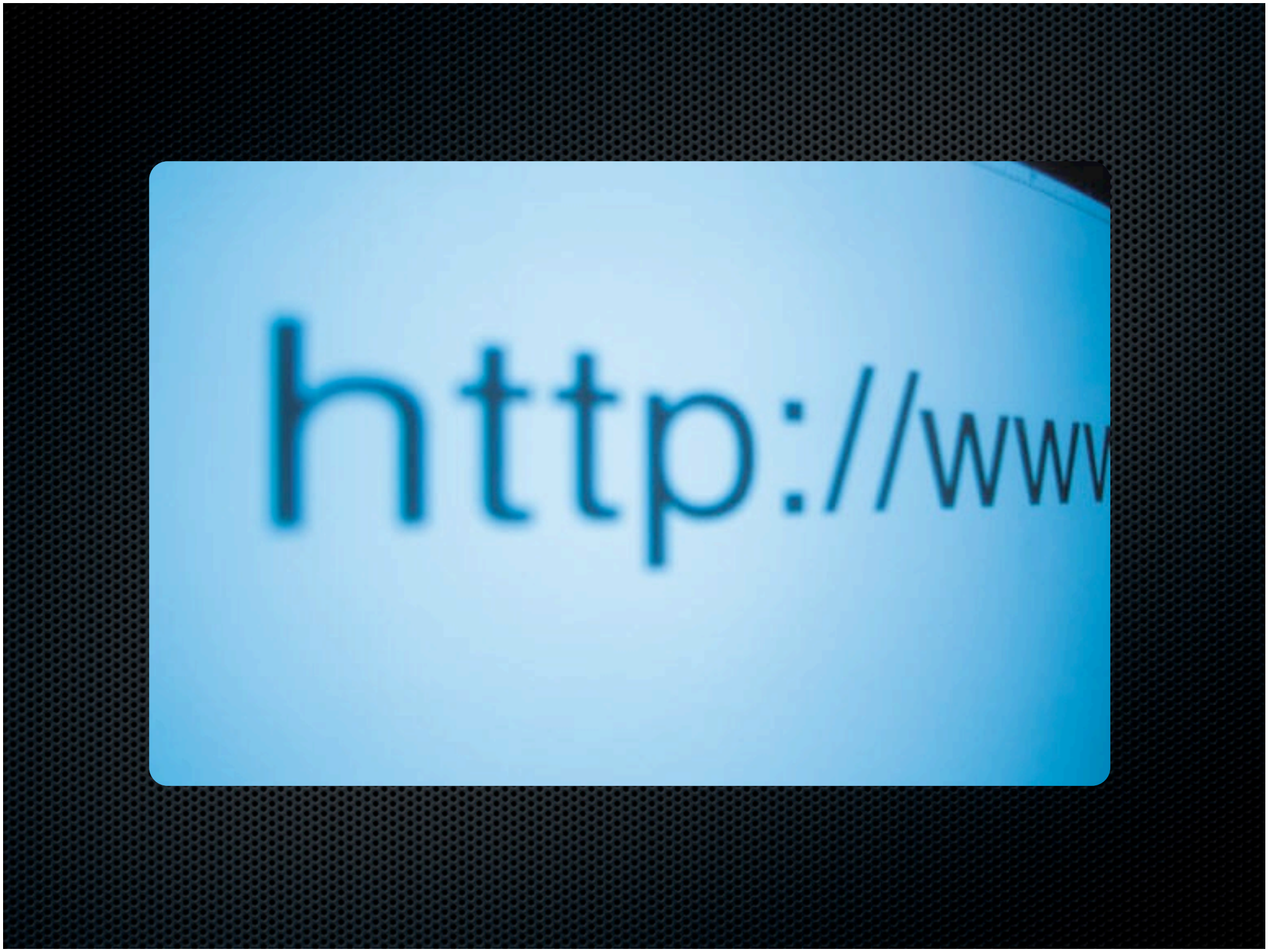
Is a method to determine an unknown value by using an automated process to try a large number of possible values.



BRUTE FORCE

If it doesn't work, you're just not using enough.


AARON LOCK
24HR SERVICE
243-7166


http://www

What can be bruteforced?

- Credentials (HTML Forms and HTTP)
- Session identifiers (session id's)
- Predictable resource location (directories and files)
- Variable values
- Cookies
- WebServices methods (rest)

Where?

- Headers
- Forms (POST)
- URL (GET)
- Authentication (Basic, NTML)

How?

- Dictionary attack
- Search attack (all possible combinations of a character set and a given length)
- Rule based search attack (use rules to generate candidates)

Why 2010 and still bruteforcing?

In 2007 Gunter Ollmann proposed a series of countermeasures to stop automated attack tools.

Countermeasures

- Block HEAD requests
- Timeouts and thresholds
- Referer checks
- Tokens

Countermeasures

- Turing tests (captchas)
- Honeypot links
- One time links
- Custom messages
- Token resource metering (Hashcash)

Countermeasures

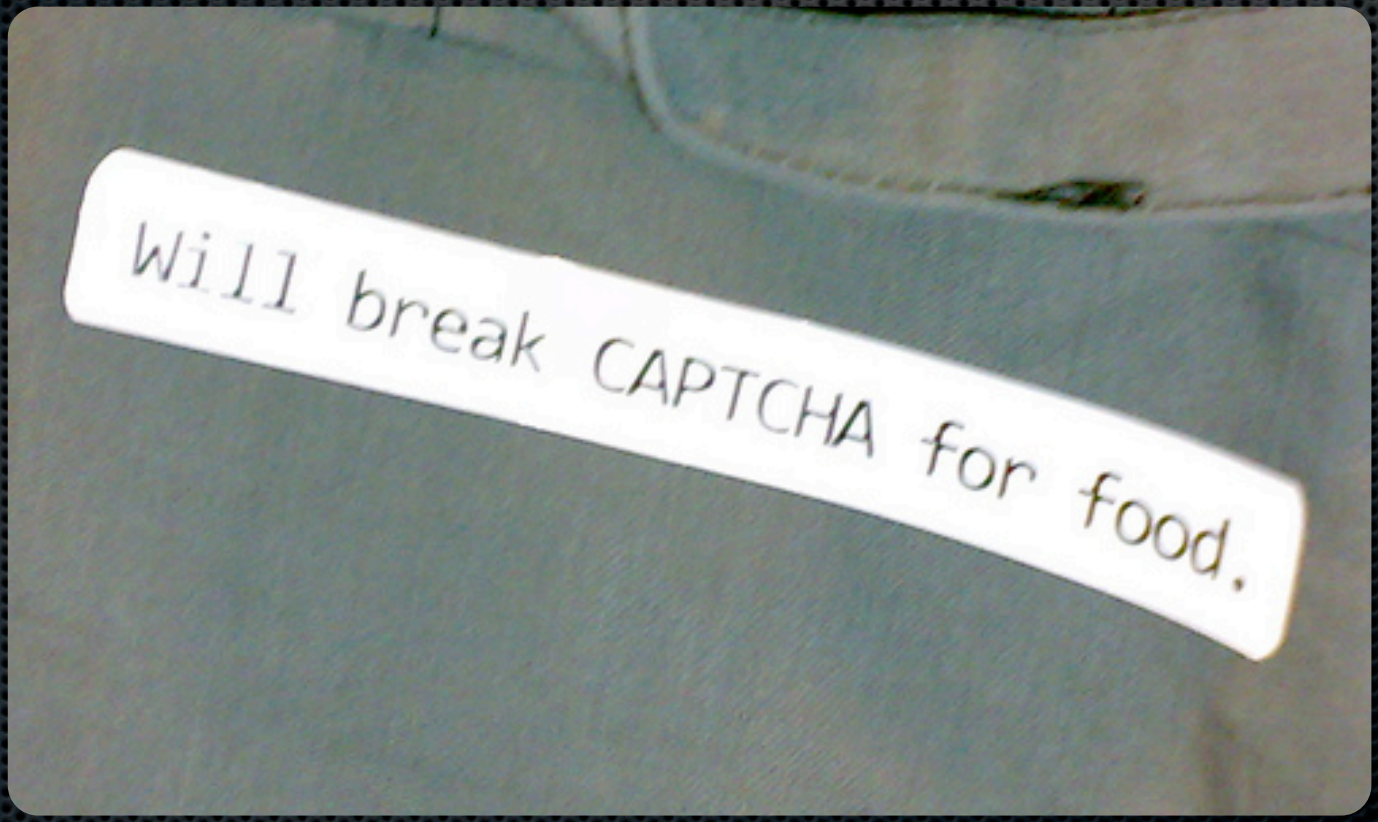
Technique	Tool Generation				Tool Classification				
Host Server Renaming	**	*				*			*
Blocking HEAD	*				*	*			
REFERER Fields	***	**	*		**	***			*
Content-Type Manipulation	***	**	*		**				
Client-side Redirection	**	*			*	*	*		*
HTTP Status Codes	**	**	**		*	*	*	*	*
Thresholds & Timeouts	***	***	**	**	*	*	***	***	**
Onetime Links	*	***	**	*	*		***	***	**
Honeypot Links	***	***			***				
Turing Tests	***	**			***				**
Token Appending	***	***	***	*	**	***	***	**	***
Token Calculators	***	***	***	*	**	***	***	**	***
Token Resource Metering	***	***	***	***	***	***	***	***	***
	1st Generation	2nd Generation	2.5 Generation	3rd Generation	Web Spidering	CGI Scanning	Brute Forcing	Fuzzers	Vuln. Scanning

Key: [] No benefit, [*] Some benefit, [**] Noticeable Benefit, [***] Valuable Protection

Workarounds

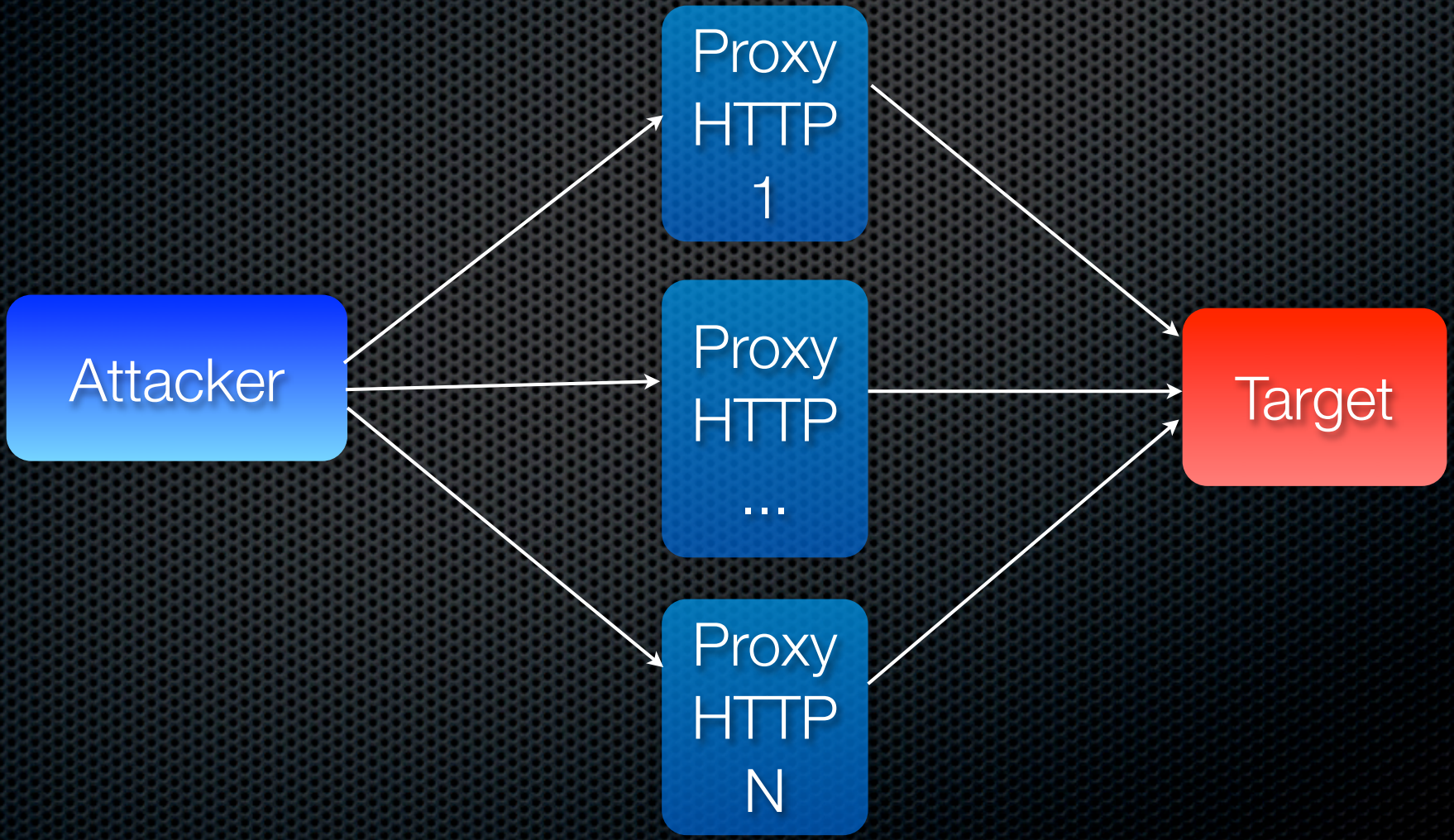
Workarounds

Captcha breakers



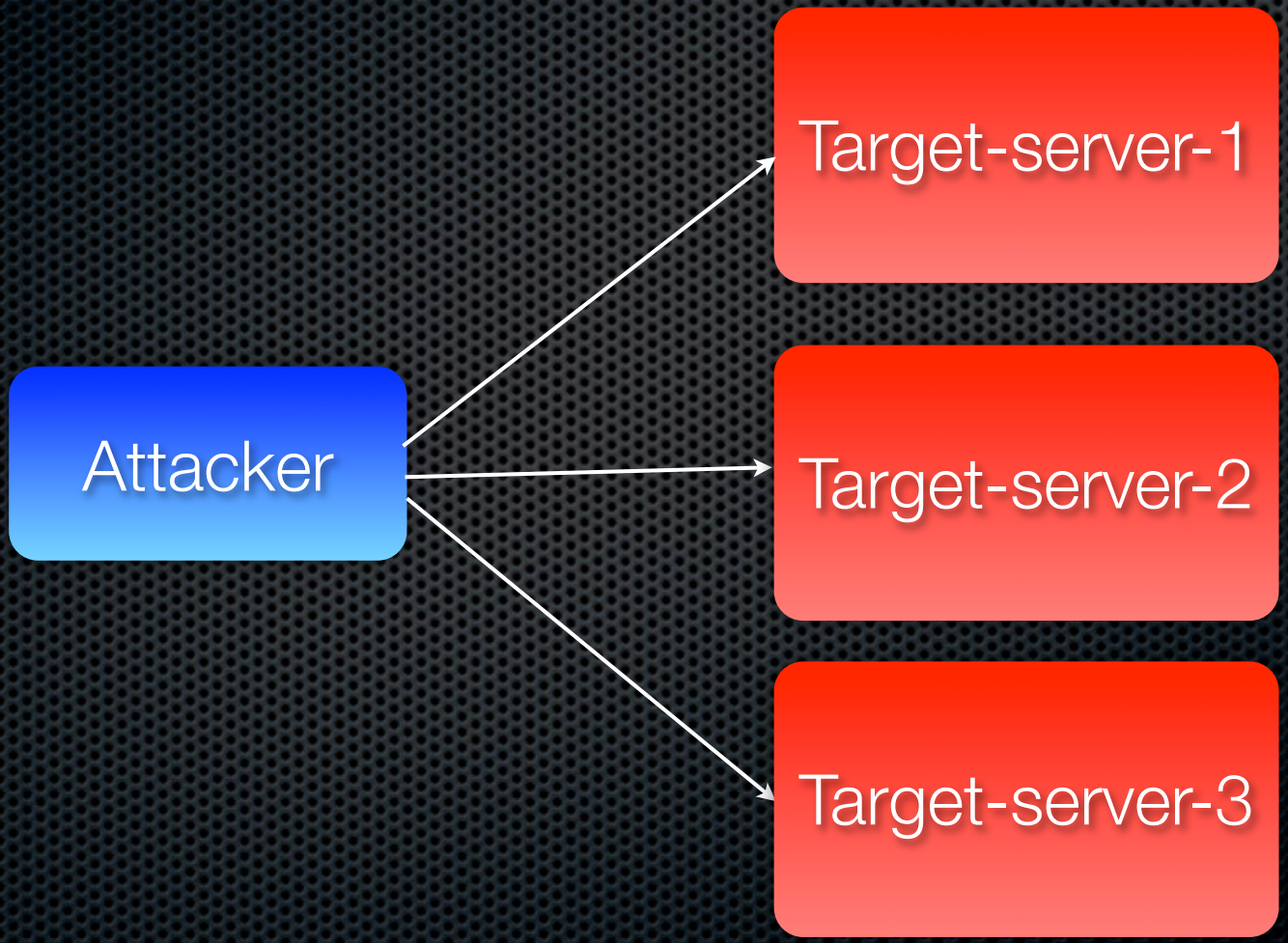
Workarounds

Distributing scanning source traffic



Workarounds

Distributing scanning on different targets



Workarounds

- **Diagonal scanning** (different username/password each round)
- **Horizontal scanning** (different usernames for common passwords)
- **Three dimension** (Horizontal,Vertical or Diagonal + Distributing source IP)
- **Four dimensions** (Horizontal, Vertical or Diagonal + time delay)


2010

2010...

114.000 emails

https://dcp2.att.com/OEPClient/openPage?ICCID=NUMBER&IMEI=0

8901410424322[redacted] : [redacted]@nytimes.com	Janet Robinson, CEO of NY Times
8901410424321[redacted] : [redacted]@time.com	Ann Moore, CEO of Time Inc.
8901410424322[redacted] : [redacted]@newscorp.com	Chase Carey, President/COO of News Corp.
8901410424331[redacted] : [redacted]@hearst.com	Cathie Black, President of Hearst Magazines
8901410424331[redacted] : [redacted]@dowjones.com	Les Hinton, CEO of Dow Jones
8901410424322[redacted] : [redacted]@weinsteinco.com	Harvey Weinstein, Co-Founder of Weinstein Co.
8901410424331[redacted] : [redacted]@bloomberg.net	Michael Bloomberg, Founder of Bloomberg LP

2010...

facebook

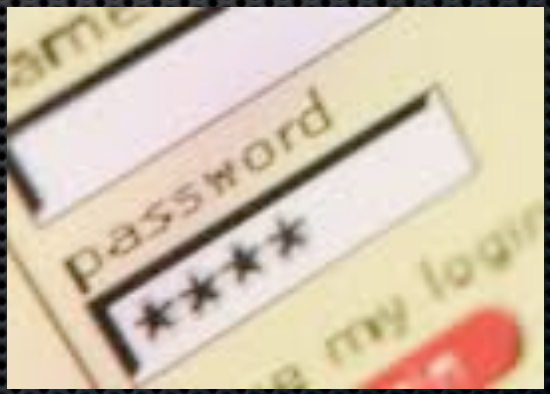
Access Any Users Photo Albums

http://www.facebook.com/album.php?aid=-3&id=1508034566&l=aad9c

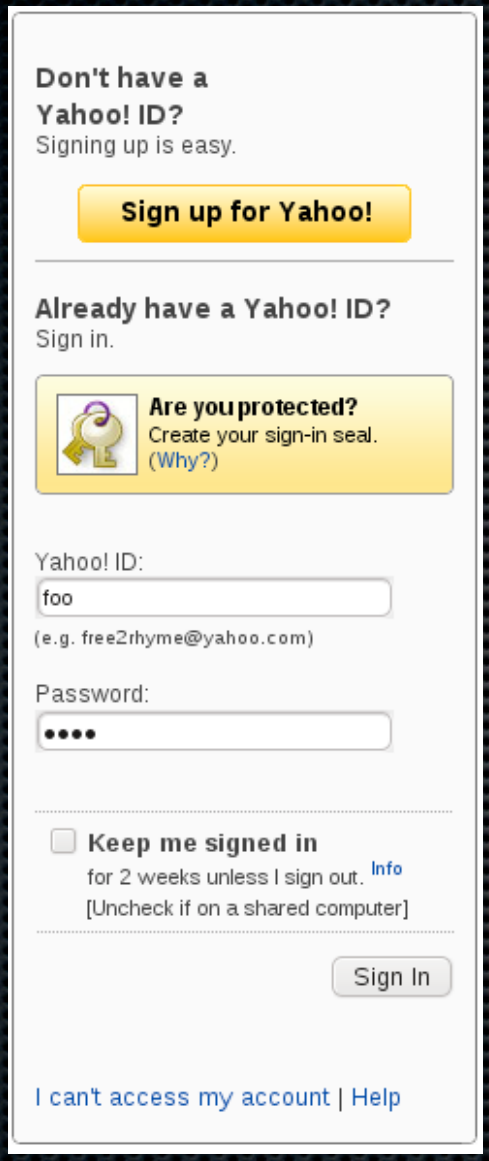
aid=-3 (-3 for every public profile album)
id=0123456789
l=? (all we know is its 5 characters from the 0123456789abcdef range)

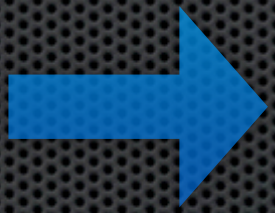
2010...

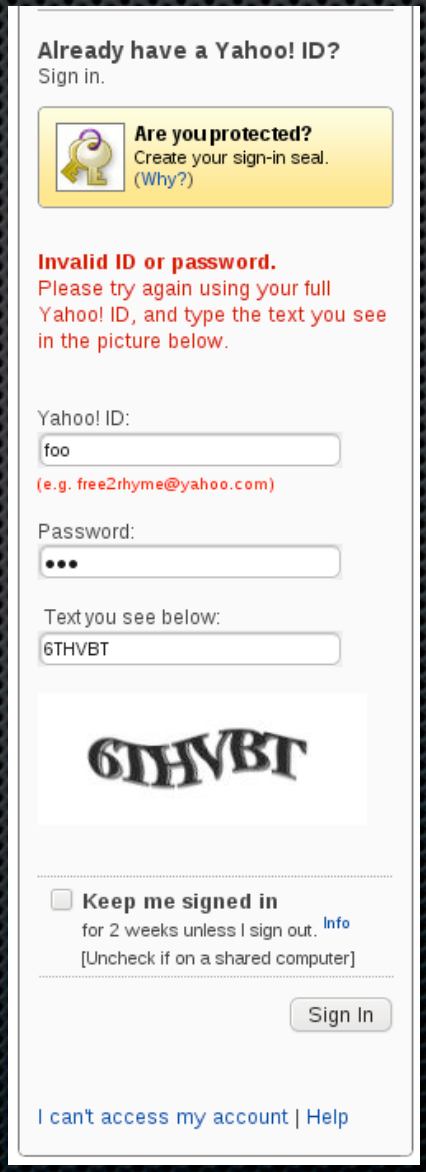
- The 500 worst passwords list
- Alyssa banned passwords list
- Cain's list of passwords
- Conficker's list
- The English dictionary
- Faithwriters banned passwords list
- Hak5's list
- Hotmail's banned passwords list
- Myspace's banned passwords list
- PHPbb's compromised list
- RockYou's compromised list
- Twitter's banned passwords list



2010...


Don't have a Yahoo! ID?
Signing up is easy.
Sign up for Yahoo!
Already have a Yahoo! ID?
Sign in.
Are you protected?
Create your sign-in seal.
(Why?)
Yahoo! ID:
foo
(e.g. free2rhyme@yahoo.com)
Password:
Keep me signed in
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]
Sign In
I can't access my account | Help




Already have a Yahoo! ID?
Sign in.
Are you protected?
Create your sign-in seal.
(Why?)
Invalid ID or password.
Please try again using your full Yahoo! ID, and type the text you see in the picture below.
Yahoo! ID:
foo
(e.g. free2rhyme@yahoo.com)
Password:
Text you see below:
6THVBT
6THVBT
Keep me signed in
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]
Sign In
I can't access my account | Help

2010...

Webservices

http://l33.login.scd.yahoo.com/config/isp_verify_user?l=USERNAME&p=PASSWORD

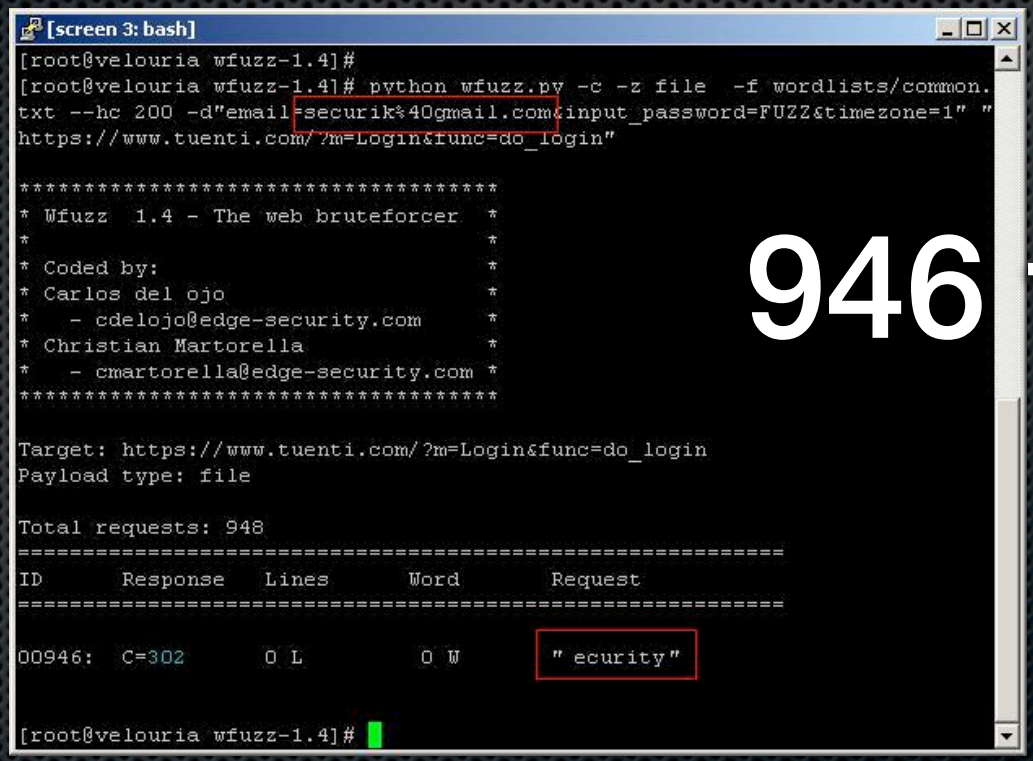
```
OK:0:username

ERROR:101:Invalid Password

ERROR:102:Invalid Login
```

2010...

Beta Privada

tuenti

Password bruteforce



946 tries

python wfuzz.py -c -z file -f wordlists/common.txt --hc 200 -d"email=securik@gmail.com&input_password=FUZZ&timezone=1" "https://www.tuenti.com/?m=Login&func=do_login"

Tools

Automated scanning tools are designed to take full advantage of the state-less nature of the HTTP protocol and insecure development techniques.

Tools

WEBSLAYER

EDGE-SECURITY

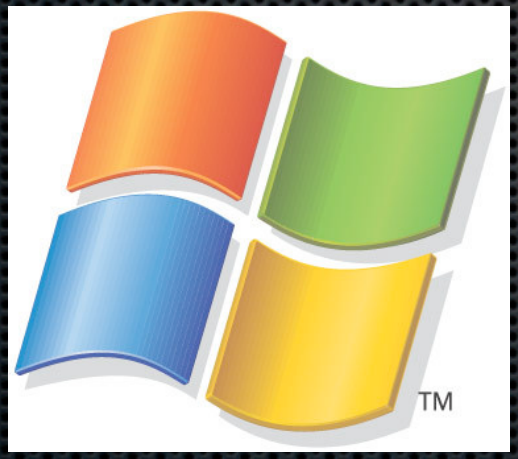
AN OWASP PROJECT

Evolution of WFUZZ

Webslayer

The main objective is to provide to the security tester a tool to perform highly customized brute force attacks on web applications, and a useful results analysis interface. It was designed thinking in the professional tester.

Webslayer



Webslayer

- Predictable credentials (HTML Forms and HTTP)
- Predictable sessions identifier (cookies,hidden fields, url)
- Predictable resource location (directories and files)
- Variables values and ranges
- Cookies
- WebServices methods
- Traversals, Injections, Overflows, etc

Webslayer

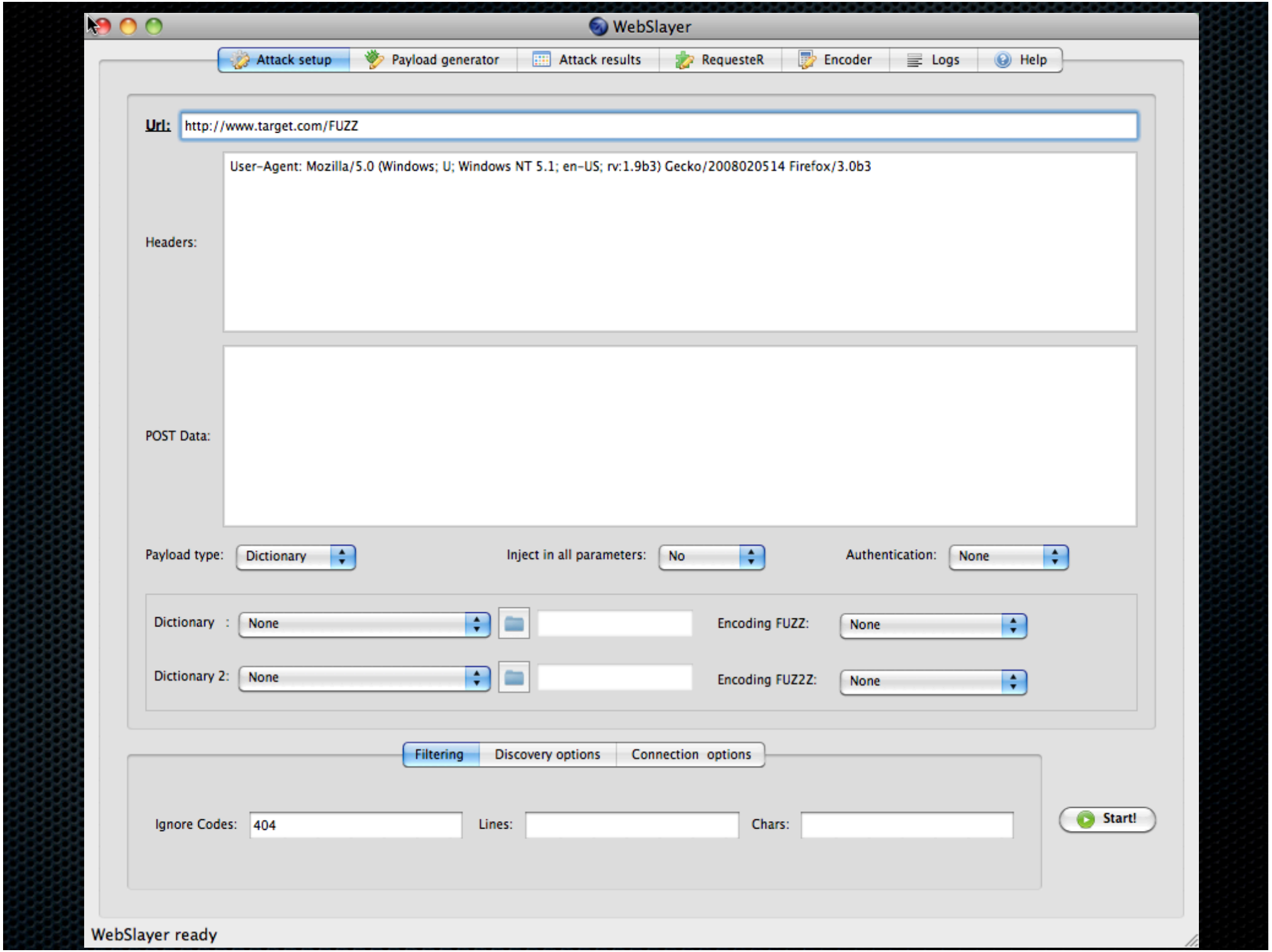
- Encodings: 15 encodings supported
- Authentication: supports Ntml and Basic (known or guess)
- Multiple payloads: you can use 2 payloads in different parts
- Proxy support (authentication supported)
- Multithreads
- Multiple filters for improving the performance and for producing cleaner results

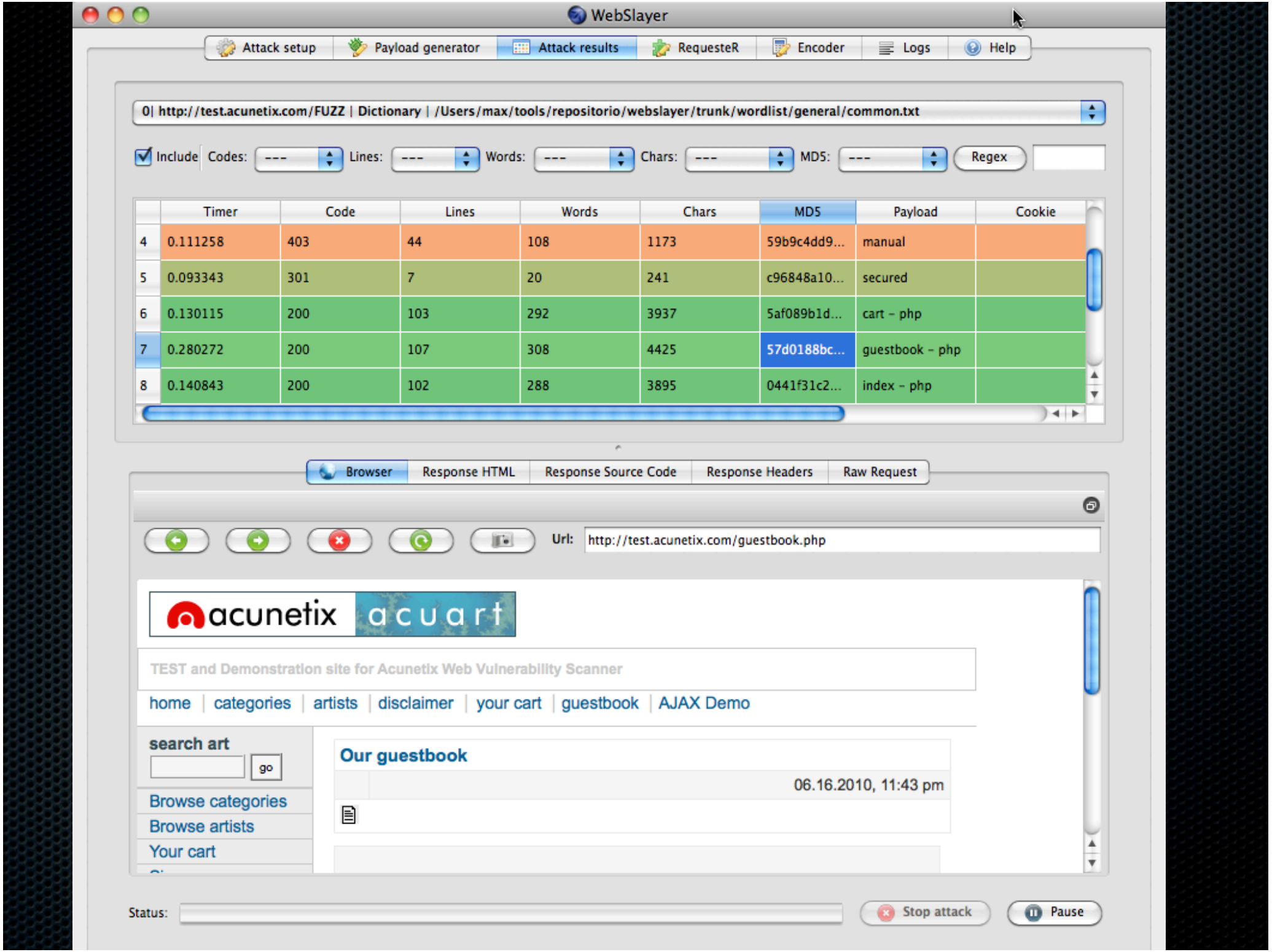
Webslayer

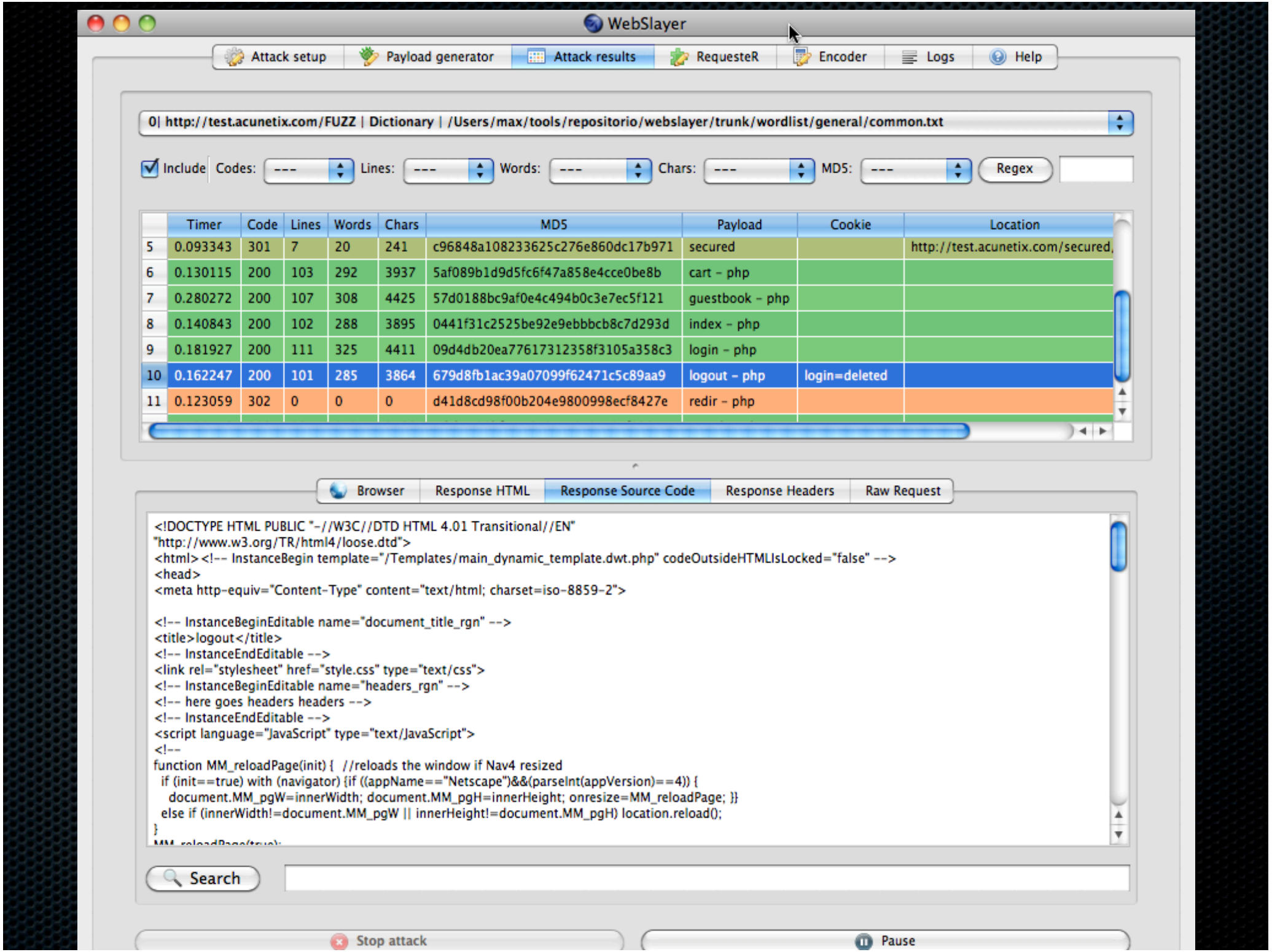
- Predictable resource location: Recursion, common extensions, non standard code detection, (Huge collection of dictionaries)
- Advanced payload generation
- Live filters
- Session saving/restoring
- Integrated browser (webKit)
- Full page screenshot

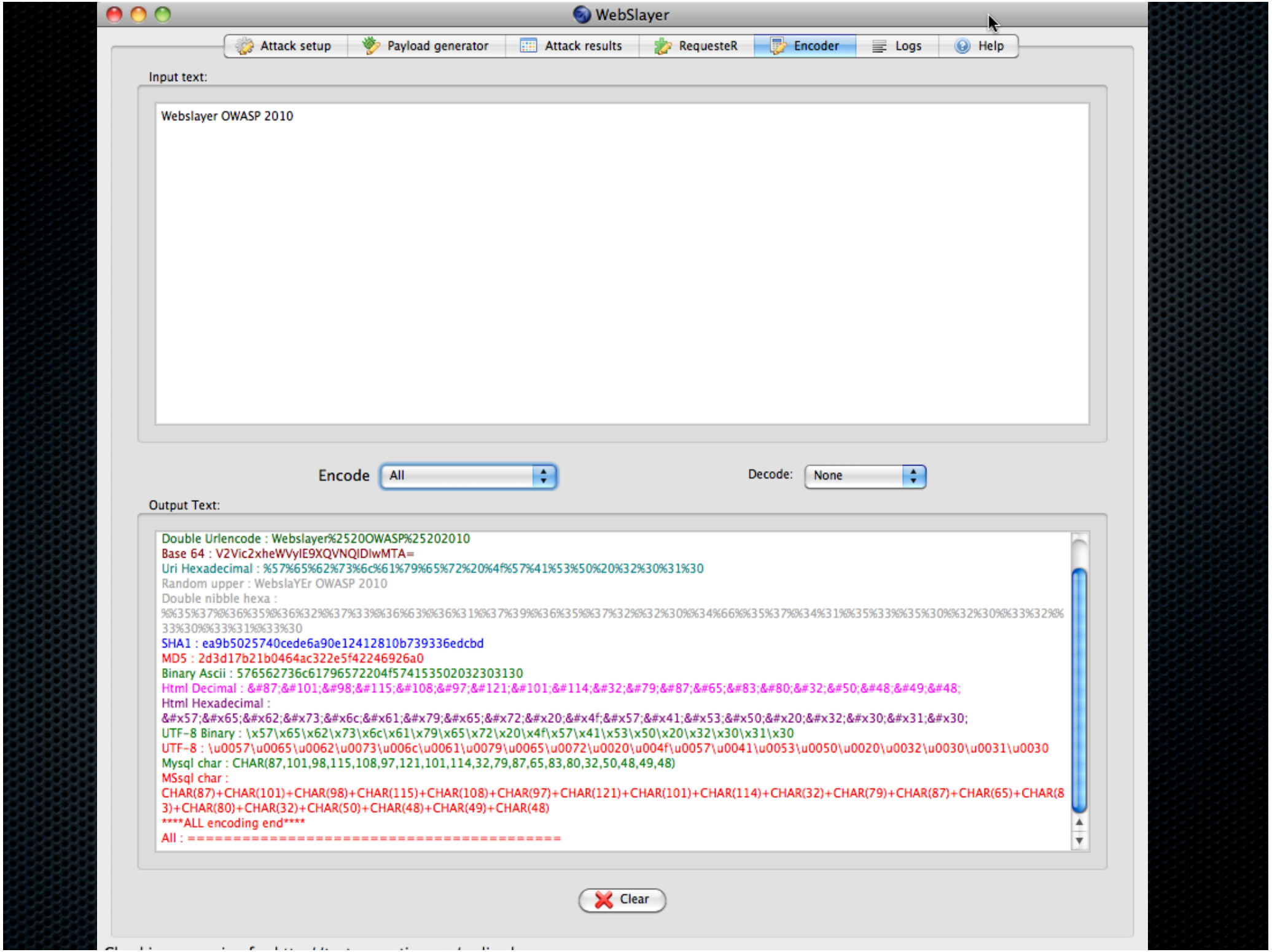
Resource location prediction

- Based on the idea of Dirb (Darkraver)
- Custom dictionaries of know resources or common passwords
  - Servers: Tomcat,Websphere,Weblogic,Vignette,etc
  - Common words: common (950), big (3500), spanish
  - CGIs (vulnerabilities)
  - Webservices
  - Injections (SQL, XSS, XML,Traversals)


WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
Url:
http://www.target.com/FUZZ
Headers:
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3
POST Data:
Payload type:
Dictionary
Inject in all parameters:
No
Authentication:
None
Dictionary :
None
Encoding FUZZ:
None
Dictionary 2:
None
Encoding FUZ2Z:
None
Filtering
Discovery options
Connection options
Ignore Codes:
404
Lines:
Chars:
Start!
WebSlayer ready

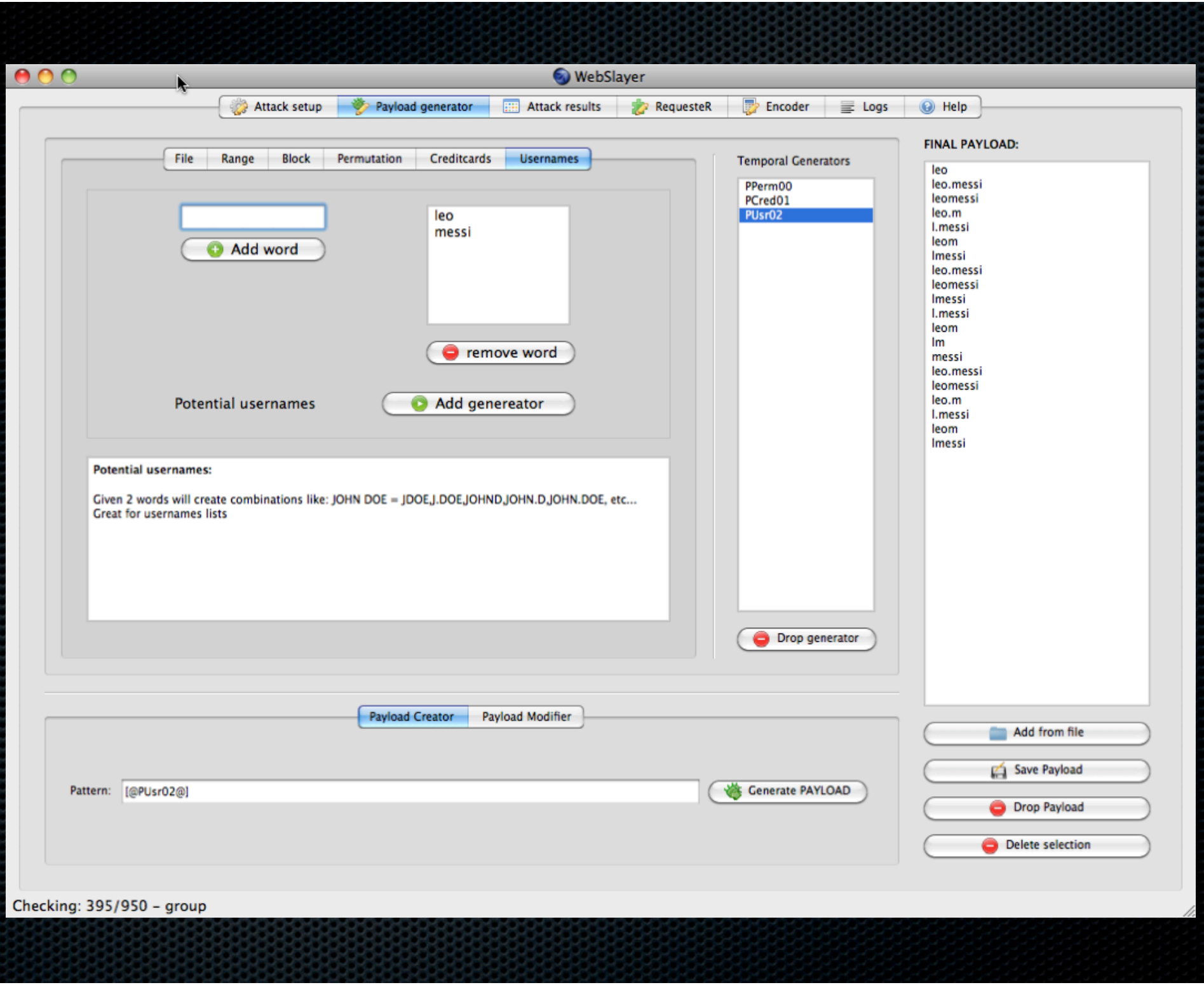

WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
0| http://test.acunetix.com/FUZZ | Dictionary | /Users/max/tools/repositorio/webslayer/trunk/wordlist/general/common.txt
Include
Codes: ---
Lines: ---
Words: ---
Chars: ---
MD5: ---
Regex
Timer Code Lines Words Chars MD5 Payload Cookie
4 0.111258 403 44 108 1173 59b9c4dd9... manual
5 0.093343 301 7 20 241 c96848a10... secured
6 0.130115 200 103 292 3937 5af089b1d... cart - php
7 0.280272 200 107 308 4425 57d0188bc... guestbook - php
8 0.140843 200 102 288 3895 0441f31c2... index - php
Browser
Response HTML
Response Source Code
Response Headers
Raw Request
Url: http://test.acunetix.com/guestbook.php
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Our guestbook
06.16.2010, 11:43 pm
Status:
Stop attack
Pause

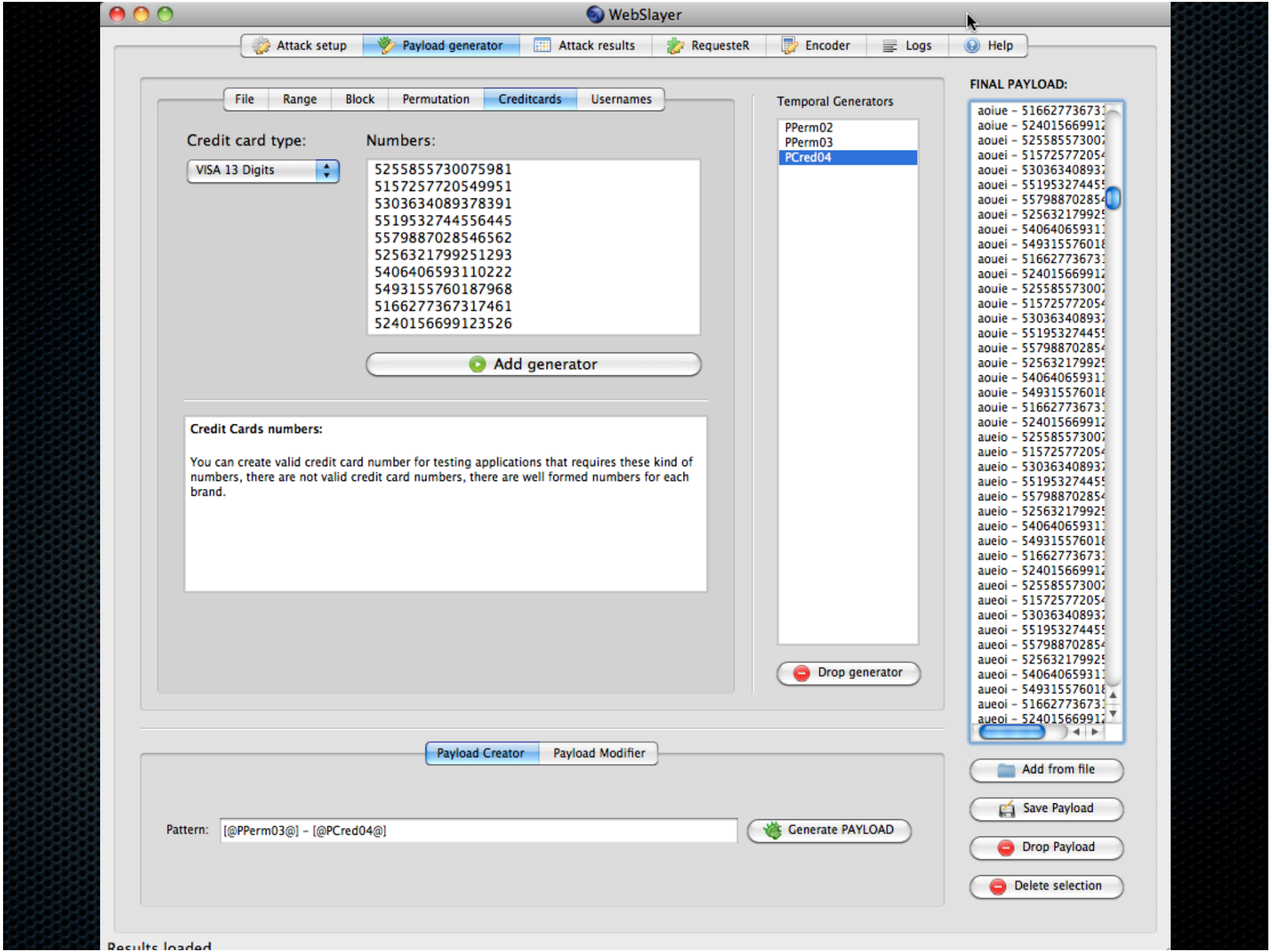

WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
0| http://test.acunetix.com/FUZZ | Dictionary | /Users/max/tools/repositorio/webslayer/trunk/wordlist/general/common.txt
Include
Codes: ---
Lines: ---
Words: ---
Chars: ---
MD5: ---
Regex
Timer Code Lines Words Chars MD5 Payload Cookie Location
5 0.093343 301 7 20 241 c96848a108233625c276e860dc17b971 secured http://test.acunetix.com/secured/
6 0.130115 200 103 292 3937 5af089b1d9d5fc6f47a858e4cce0be8b cart - php
7 0.280272 200 107 308 4425 57d0188bc9af0e4c494b0c3e7ec5f121 guestbook - php
8 0.140843 200 102 288 3895 0441f31c2525be92e9ebbbcb8c7d293d index - php
9 0.181927 200 111 325 4411 09d4db20ea77617312358f3105a358c3 login - php
10 0.162247 200 101 285 3864 679d8fb1ac39a07099f62471c5c89aa9 logout - php login=deleted
11 0.123059 302 0 0 0 d41d8cd98f00b204e9800998ecf8427e redir - php
Browser
Response HTML
Response Source Code
Response Headers
Raw Request
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>logout</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
Search
Stop attack
Pause


WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
Input text:
Webslayer OWASP 2010
Encode
All
Decode:
None
Output Text:
Double Urlencode : Webslayer%2520OWASP%25202010
Base 64 : V2Vic2xheWVyIE9XQVNQIDIwMTA=
Uri Hexadecimal : %57%65%62%73%6c%61%79%65%72%20%4f%57%41%53%50%20%32%30%31%30
Random upper : WebslaYEr OWASP 2010
Double nibble hexa :
%%35%37%%36%35%%36%32%%37%33%%36%63%%36%31%%37%39%%36%35%%37%32%%32%30%%34%66%%35%37%%34%31%%35%33%%35%30%%32%30%%33%32%%33%30%%33%31%%33%30
SHA1 : ea9b5025740cede6a90e12412810b739336edcbd
MD5 : 2d3d17b21b0464ac322e5f42246926a0
Binary Ascii : 576562736c61796572204f574153502032303130
Html Decimal : Webslayer OWASP 2010
Html Hexadecimal :
Webslayer OWASP 2010
UTF-8 Binary : \x57\x65\x62\x73\x6c\x61\x79\x65\x72\x20\x4f\x57\x41\x53\x50\x20\x32\x30\x31\x30
UTF-8 : \u0057\u0065\u0062\u0073\u006c\u0061\u0079\u0065\u0072\u0020\u004f\u0057\u0041\u0053\u0050\u0020\u0032\u0030\u0031\u0030
Mysql char : CHAR(87,101,98,115,108,97,121,101,114,32,79,87,65,83,80,32,50,48,49,48)
MSsql char :
CHAR(87)+CHAR(101)+CHAR(98)+CHAR(115)+CHAR(108)+CHAR(97)+CHAR(121)+CHAR(101)+CHAR(114)+CHAR(32)+CHAR(79)+CHAR(87)+CHAR(65)+CHAR(83)+CHAR(80)+CHAR(32)+CHAR(50)+CHAR(48)+CHAR(49)+CHAR(48)
****ALL encoding end****
All : ==========
Clear

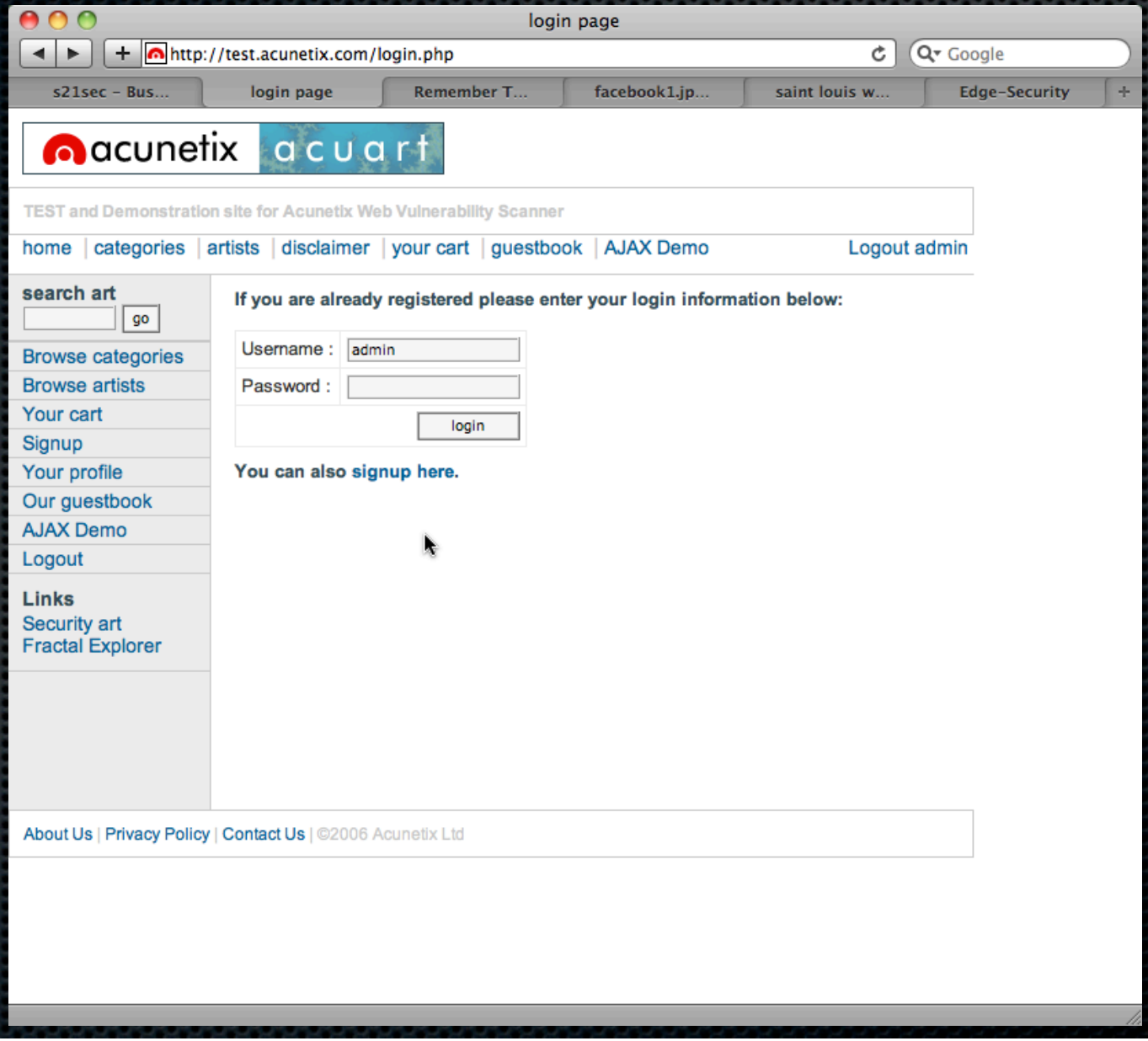
Payload Generation

- Payload generator:
  - Usernames
  - Credit Card numbers
  - Permutations
  - Character blocks
  - Ranges
  - Files
  - Pattern creator and regular expression (encoders)


WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
File
Range
Block
Permutation
Creditcards
Usernames
Add word
leo
messi
remove word
Potential usernames
Add genereator
Potential usernames:
Given 2 words will create combinations like: JOHN DOE = JDOE,J.DOE,JOHND,JOHN.D,JOHN.DOE, etc...
Great for usernames lists
Temporal Generators
PPerm00
PCred01
PUsr02
Drop generator
FINAL PAYLOAD:
leo
leo.messi
leomessi
leo.m
l.messi
leom
lmessi
leo.messi
leomessi
lmessi
l.messi
leom
lm
messi
leo.messi
leomessi
leo.m
l.messi
leom
lmessi
Payload Creator
Payload Modifier
Pattern:
[@PUsr02@]
Generate PAYLOAD
Add from file
Save Payload
Drop Payload
Delete selection
Checking: 395/950 - group


WebSlayer
Attack setup
Payload generator
Attack results
RequesteR
Encoder
Logs
Help
File
Range
Block
Permutation
Creditcards
Usernames
Credit card type:
VISA 13 Digits
Numbers:
5255855730075981
5157257720549951
5303634089378391
5519532744556445
5579887028546562
5256321799251293
5406406593110222
5493155760187968
5166277367317461
5240156699123526
Add generator
Credit Cards numbers:
You can create valid credit card number for testing applications that requires these kind of numbers, there are not valid credit card numbers, there are well formed numbers for each brand.
Temporal Generators
PPerm02
PPerm03
PCred04
Drop generator
FINAL PAYLOAD:
Payload Creator
Payload Modifier
Pattern:
[@PPerm03@] - [@PCred04@]
Generate PAYLOAD
Add from file
Save Payload
Drop Payload
Delete selection
Results loaded

Demo


login page
http://test.acunetix.com/login.php
Google
s21sec - Bus...
login page
Remember T...
facebook1.jp...
saint louis w...
Edge-Security
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout admin
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
Fractal Explorer
If you are already registered please enter your login information below:
Username : admin
Password :
login
You can also signup here.
About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Advanced uses

Sweep an entire range with a common dictionary

HTTP://192.168.1.FUZZ/FUZ2Z

FUZZ: RANGE [1-254]

FUZ2Z: common.txt

Advanced uses

Scanning through proxies

me ----> Server w/proxy ---->LAN

wfuzz -x serverip:53 -c -z range -r 1-254 --hc XXX -t 5 http://10.10.1.FUZZ

-x set proxy
--hc is used to hide the XXX error code from the results, as machines w/o webserver will fail the request.

Future features

- Time delay between request
- Multiple proxies (distribute attack)
- Diagonal scanning (mix dictionaries)

Contact

- cmartorella _at_s21sec.com
- cmartorella_at_edge-security.com
- http://twitter.com/laramies
- http://laramies.blogspot.com
- http://www.edge-security.com

References

- http://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)
- http://projects.webappsec.org/Predictable-Resource-Location
- http://projects.webappsec.org/Credential-and-Session-Prediction
- http://projects.webappsec.org/Brute-Force
- http://www.technicalinfo.net/papers/StoppingAutomatedAttackTools.html
- http://gawker.com/5559346/
- http://tacticalwebappsec.blogspot.com/2009/09/distributed-brute-force-attacks-against.html
- http://praetorianprefect.com/archives/2010/06/114000-ipad-owners-the-script-that-harvested-their-e-mail-addresses/
- http://www.securitybydefault.com/2009/07/no-no-uses-captchas-ni-ningun-otro.html
- http://nukeit.org/facebook-hack-access-any-users-photo-albums/