

# **TUTORIAL**

# by Fancy

Email: <u>fancy@corelan.be</u> Web: http://www.corelan.be:8800

# **Table of contents**

1.	Introduction	2
2.	Installation	4
	2.1 Installation under Windows	
	2.2 Installation under BackTrack	5
3.	Using WATOBO	7
	3.1 Start WATOBO:	7
	3.2 Passive checks	9
	3.3 Active checks	10
	3.3 Session management	. 18
	3.4 Manual requests	
	Here you can change what you like in the request (e.g. id=') and send it away	.24
	See the comparison of the REQUEST	.25
	3.5 More functions	
	3.6 Fuzzing	31
	- Enumerate Usernames	
	- Fuzzing multiple values	.35
	- Generating complex values	40
4.	Conclusion	
5.	References	45





# 1. Introduction

WATOBO [1] is intended to enable security professionals to perform highly efficient (semiautomated ) web application security audits. I am convinced that the semi-automated approach is the best way to perform an accurate audit and to identify most of the vulnerabilities.

WATOBO has no attack capabilities and is provided for legal vulnerability audit purposes only. It works like a local proxy, similar to Webscarab, Paros or BurpSuite Additionally, WATOBO supports passive and active checks. Passive checks are more like filter functions. They are used to collect useful information, e.g. email or IP addresses. Passive checks will be performed during normal browsing activities. No additional requests are sent to the (web) application.

Active checks instead will produce a high number of requests (depending on the check module) because they do the automatic part of vulnerability identification, e.g. during a scan.

The most important advantages of WATOBO are:

- WATOBO has Session Management capabilities! You can define login scripts as well as logout signatures. So you don't have to login manually each time you get logged out
- WATOBO can perform vulnerability checks out of the box
- WATOBO supports Inline De-/Encoding, so you don't have to copy strings to a transcoder and back again. Just do it inside the request/response window with a simple mouse click.
- WATOBO has smart filter functions, so you can find and navigate to the most interesting parts of the application easily.
- WATOBO is written in (FX)Ruby and enables you to define your own checks
- WATOBO is free software (licensed under the GNU General Public License Version 2)

### Summarizing the functions of WATOBO:

- Supports session management.
- Detects logout and automatically takes a re-login.
- Supports filter functions
- Inline-Encoder/Decoder
- Includes vulnerability scanner
- Quick-scan for targeted scanning a URL
- Full-scan to scan a whole session





- Manual request editor with special functions
- Session information is updated
- Login can be done automatically
- Transcoder
- URL, Base64, MD5, SHA-1
- Interceptor
- Fuzzer
- Free, Stable and <u>Open source</u>!
- Script code easy to understand
- Easy to extend / adapt
- In real-world scenarios tested and developed
- Speed / usability
- Active and Passive checks
- Runs under Windows, Linux, BackTrack.

#### Screenshot:

VATOBO by siberas Settings Tools View Help									00
I I I I I I I I I I I I I I I I I I I	-								
dings Sites	Doc Filt	er Text Filter							Chat-ID: 1 🕢 Browser-View 🏠 Fuzzer 💑 Manual Rec
192.168.72.130	✓ excl	l pics 🔽 excl.	docs 🔽 excl. javascr	ipt 🔽 excl. style she	ets				
🗉 🎡 Vulnerabilities	Apply								Request:
Reflected XSS [GET]									Text Tagless
Insme] - /dvwa/vulnerab		Method	Host	Path	Parameters	Status	Set-Cookie	Comment 📥	Grep Highlight Re
	1	GET	192.168.72.130	dvwa/login.php		200 OK	PHPSESSID=34f6	.q	
E Directory Indexing		POST	192.168.72.130	dvwa/login.php		302 Found			GET http://192.168.72.130/dvwa/login.php HTTP/1.1 Host: 192.168.72.130
	5	GET	192.168.72.130	dvwa/index.php		200 OK			User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; de; rv:1.9.2)
# /dvwa/dvwa/images/	11	GET	192.168.72.130	dvwa/security.php		200 OK			Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
/dvwa/dvwa/css/	12	GET	192.168.72.130	dvwa/security.php		200 OK			Accept-Language: de-de, de; q=0.8, en-us; q=0.5, en; q=0.3
SQL-Injection	14	POST	192.168.72.130	dvwa/security.php		302 Found	security=low		Accept-Encoding: gzip, deflate Accept-Charset: ISO-8859-1, utf-8;g=0.7, ";g=0.7
[id] - /dvwa/vulnerabilitie	15	GET	192.168.72.130	dvwa/security.ph		200 OK			Keep-Alive: 115
	16	GET	192.168.72.130	dvwa/vulnerabiliti		200 OK			Proxy-Connection: keep-alive
Unencrypted Logins	17	GET	192.168.72.130	dvwa/vulnerabiliti		200 OK			Pragma: no-cache Cache-Control: no-cache
Hints	18	GET	192.168.72.130	dvwa/vulnerabiliti		200 OK			
	19	GET	192.168.72.130	dvwa/vulnerabiliti		200 OK			
HTTP Methods	20	GET	192.168.72.130		icid=aaa&Submit=				
REPLY	21	GET	192.168.72.130	dvwa/vulnerabiliti		200 OK			
I TRACK	22	POST	192.168.72.130	dvwa/vulnerabiliti		200 OK			Response:
CHECKIN	23	GET	de.start3.mozilla		client=firefox-a&				Nepolite.
PATCH	87	GET	192.168.72.130	dvwa/vulnerabiliti	ie	302 Found	PHPSESSID=fd61	k	Text Tagless
TEXTSEARCH	88	GET	192.168.72.130	dvwa/login.php		200 OK	security=high		
SEARCH	91	POST	192.168.72.130	dvwa/login.php		302 Found			Grep Highlight Re
UNCHECKOUT	92	GET	192.168.72.130	dvwa/login.php		200 OK			HTTP/1.1 200 OK
PROPPATCH	94	POST	192.168.72.130	dvwa/login.php		302 Found			Date: Wed, 24 Mar 2010 16:38:33 GMT
OPTIONS	95	GET	192.168.72.130	dvwa/index.php		200 OK			Server: Apache/2.2.12 (Ubuntu) X-Powered-Bv: PHP/5.2.10-2ubuntu6.1
UNLOCK	107	GET	192.168.72.130	dvwa/vulnerabiliti	epage=include.php				Set-Cookie: PHP/52310-2ubuntuo.1 Set-Cookie: PHPSESSID=34f6c0400d90d7909d116dc7dfd9c006; path:
VERSION_CONTROL	110	GET	192.168.72.130	dvwa/vulnerabiliti	ie	200 OK			Expires: Tue, 23 Jun 2009 12:00:00 GMT
H SHOWMETHOD	173	GET	192.168.72.130	dvwa/security.php	<b>b</b>	302 Found			Cache-Control: no-cache, must-revalidate
DEBUG	174	GET	192.168.72.130	dvwa/login.php		200 OK			Pragma: no-cache Set-Cookie: security=high
CHECKOUT	189	GET	192.168.72.130	dvwa/index.php		302 Found			Vary: Accept-Encoding
INK	190	GET	192.168.72.130	dvwa/login.php		200 OK			Content-Length: 1185
H MKCOL	200	GET	192.168.72.130	dvwa/security.php	<b>o</b>	302 Found			Connection: close Content-Type: text/html;charset=utf-8
SPACEJUMP	201	GET	192.168.72.130	dvwa/login.php		200 OK		-	
	4								J 4 >





# 2. Installation

# 2.1 Installation under Windows

## 1. Install Ruby:

Download the Ruby One-click Installer (<u>http://rubyinstaller.org/downloads/</u>) and install ruby on your computer:

RubyInstaller for Windows									
Downloads									
RubyInstallers									
B         Ruby 1.9.1-p429           B         Ruby 1.8.7-p299           B         Ruby 1.8.6-p398									
Other Useful Downloads									
7-ZIP ARCHIVES Ruby 1.9.1-p429 Ruby 1.8.7-p299 Ruby 1.8.6-p398									
RUBY CORE & STANDARD LIBRARY DOCUMENTATION         II       Ruby 1.9.1-p429 documentation (CHM format)       II       Ruby 1.8.7-p299 documentation (CHM format)         III       Ruby 1.8.6-p398 documentation (CHM format)       III       Ruby 1.8.6-p398 documentation (CHM format)									
devkit-3.4.5r3-20091110.7z									
LEGACY ONE-CLICK INSTALLER B Ruby 1.8.6-p27 (RC2) Ruby 1.8.6-p26 (Final)									
🖗 Ruby-186-27 Setup									
Choose Components Choose which features of Ruby-186-27 you want to install.									
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.									
Select components to install: V Ruby SaTE V Enable RubyGems European Keyboard mappings for IRB (creates an INPUTRC environment variable).									
Space required: 90.2MB									
Nullsoft Instell System v2.33 < Back Next > Cancel									





#### 2. Get WATOBO:

Download WATOBO (<u>http://sourceforge.net/projects/watobo/</u>) and extract the WATOBO sources to a place/directory of your choice

# 2.2 Installation under BackTrack

#### 1. Update your backtrack installation (this step is optional but always recommended)

```
apt-get update
apt-get upgrade
```

### 2.) Install fxruby

Execute the following commands:

gem uninstall rubygems-update

(ignore message "Unknown gem rubygems-update >= 0")

```
gem install rubygems-update -v 1.3.4
/var/lib/gems/1.8/bin/update_rubygems
gem install hoe
gem install fxruby
```

#### **3. Install JSSH Firefox Extension**

Follow the instructions of the firewatir projekt:

http://wiki.openqa.org/display/WTR/FireWatir+Installation

Click on "Install" and then on "Allow":





Allow 🔀

#### Rirefox prevented this site (wiki.openga.org) from asking you to install software on your computer.

#### 2) Install the JSSH Firefox Extension

The correct extension depends on your platform and your version of Firefox.

Production FireWatir									
Platform	Firefox 2.0	Firefox 3.0	Firefox 3.5	Firefox 3.6					
Windows	<u>install</u>	<u>install</u>	<u>install</u>	<u>install</u>					
Mac	<u>install</u>	<u>install</u>	<u>install</u>	<u>install</u>					
Linux	<u>install</u>	<u>install</u>	<u>install</u>	install					

#### Click on "Install now" in the following dialog box:

Software In	stallation	×								
Xari have	Install add-ons only from authors you trust. Malcious software can damage your computer or violate your privacy. asked to install the following item:									
	issh-3.6.x-Linux.xpi (Author not verified)									
	http://wiki.openqa.org/download/attachments/14188672/jssh-3.6.x-Linux.xpi?versi									
	Install Now Cancel									

Then restart firefox.

#### 4. Get WATOBO:

Download WATOBO (<u>http://sourceforge.net/projects/watobo/</u>) and extract the WATOBO sources to a place/directory of your choice





# 3. Using WATOBO

# 3.1 Start WATOBO:

 $\rightarrow$  cd into the WATOBO directory and then issue the following command:

ruby start\_watobo.rb

 $\rightarrow$  Click on the green



and create/select your workspace directory:

🙀 WATOBO by siberas	
File Settings Tools View Help	
Findings Sites     Doc Filter Text Filter Options       Image: Dec Filter Text Filter Text Filter Options       Image: Dec Filter Text	
Workspace Directory: Change	
Select Project Project Name: New	
Select Workspace Director Create New Directory	×
Directory:       watobo_0.9.2         Name       MyWorkspace	
Image: Control of the second	
Ib         File Folder         0         07/16/2010 08:22:58           modules         File Folder         0         07/16/2010 08:22:58	
Eile Name: QK	
File Filter: All Files (*)	L





 $\rightarrow$  enter project name and session name:

New Project	
Workspace Directory: k\watobo_0.9.2\MyWorkspace	Change
Select Project	
Project Name:	New
MyProject	
Cancel Back	ext Einish

New Project	
Project: MyProject	
Select Session	
Session Name: Session-1	New
Session-1	
L	
Cancel Back	Next Finish

 $\rightarrow$  change the proxy-settings of your prefered browser, e.g. firefox:

Auto-detect pro: O Use system pro>	ky settings for this net <u>w</u> ork v settings		
Manual proxy co			
<u>H</u> TTP Proxy:	localhost	Port:	8081
	$\checkmark$ Use this proxy server for	or all protocols	
<u>S</u> SL Proxy:	localhost	Port:	8081
ETP Proxy:	localhost	Po <u>r</u> t:	8081
<u>G</u> opher Proxy:	localhost	Port:	8081
SO <u>C</u> KS Host;	localhost	Por <u>t</u> :	8081
	O SOC <u>K</u> S v4 € SOCKS	⊻5	
<u>N</u> o Proxy for:			
	Example: .mozilla.org, .net.r	nz, 192.168.1.0	)/24
Automatic proxy	configuration URL:		Reload

Now you are ready to go!





# 3.2 Passive checks

 $\rightarrow$  visit the target application (all the parts you want to audit):

# Example: Mutillidae [1]:

	Mutillidae: Hack, Learn, Secur
Version 1.5	Not logged in
Core Controls <u>Home</u> <u>Login</u> <u>Login</u> <u>Logout</u> <u>Loggle hints</u> Setup/reset the DB	<b>Login</b> If you do not have an account, <u>Register</u> Enter your username and password: Name:
Show log Credits DWASP Top 10 010	testsql Password: ••••• [Submit]
<u>A1</u> - Injection SQL and Command) .ogin Jser info	
	Mutillidae: Hack, Learn, See
Version 1.5	Not logged in
Core Controls lone expister ogout ogget hints etup/reset the PB how log residts WASP Top 10	Add to your blog, leave an entry. Login, or you will be listed as "anonymous":
<u>1</u> - Injection SQL and iommand) ogin iser info INS Lookup	Submit Entries: anonymous:(2010-07-20 18:16:43) testxss anonymous:(2010-07-20 18:16:37) Hello
legister	anonymous:(2009-03-01 22:27:11) An anonymous blog? Huh?





 $\rightarrow$  when finished with browsing switch back to WATOBO and look at the first results of the passive checks:

ATOBO by siberas (Version: 0.9.2RC2)					
Settings Tools View Help					
ings Sites	Doc Filter Text Filter Options				-N/A-
192.168.178.196	🔽 excl. pics 🔽 excl. docs 🔽 e	xcl. javascript 🔽 excl. style sheets	( ) Browser-View : _ Fuzzer 🔏 Manual Re		
- <u>-</u>					🕒 Browser-View 🚊 Fuzzer 🎉 Manual Re
🖻 🚳 Vulnerabilities	Apply				Descent
🗉 🦲 Unencrypted Logins	Method Host	Path	Parameters	Status Set-Cookie Comment	Request:
mutillidae/index.php	1 GET 192.168.178.19			200 OK	Text Hex
/mutillidae/index.php	9 GET 192.168.178.19		page=add-to-your-blog.php	200 OK	Grep Highlight
E O Hints	10 POST 192.168.178.19	i mutillidae/index.php	input_from_form=Hello&Subr	nit_but 200 OK	
	11 POST 192.168.178.19	mutillidae/index.php	input_from_form=testxss⋐	mit_bu200 OK	
🗄 📋 Logins	12 GET 192.168.178.19	i mutillidae/index.php	page=browser-info.php	200 OK	
/mutillidae/index.php	13 GET 192.168.178.19	mutillidae/index.php	page=show-log.php	200 OK	
/mutillidae/index.php	14 GET 192.168.178.19	i mutillidae/index.php	page=login.php	200 OK	
Info	15 POST 192.168.178.19	i mutillidae/index.php	user_name=testsql&password	=testsq 200 OK	
<b>-</b>	16 GET 192.168.178.19	mutillidae/index.php	page=view-someones-blog.ph	p 200 OK	
IP Adress Disclosure	17 POST 192.168.178.19	i mutillidae/index.php	show_only_user=Show+All+U	sers&SL200 OK	
H [1] 127.0.0.1	18 GET 192.168.178.19		page=login.php	200 OK	
	19 GET 192.168.178.19	i mutillidae/index.php	page=register.php	200 OK	
Hotspots	20 POST 192.168.178.19	i mutillidae/index.php	user_name=hugo&password=	sanche 200 OK	
	21 GET 192.168.178.19	i mutillidae/index.php	page=login.php	200 OK	
1 index.php	22 POST 192.168.178.19		user_name=hugo&password=		
http://irongeek.com/sigs/logo.php     if register.php	23 GET 192.168.178.19			200 OK	
login.php			page=add-to-your-blog.php	200 OK	
setupreset.php	25 GET 192.168.178.19		page=login.php	200 OK	
E show-log.php	26 GET 192.168.178.19		do=logout	200 OK uid=deleted;	Response:
t credits.php				200 OK	- 1 - 1 - 1
H http://www.owasp.org/index.php	28 GET 192.168.178.19		page=login.php	200 OK	Text Tagless Hex
🖲 user-info.php	GET 192.168.178.19	i mutillidae/index.php	page=add-to-your-blog.php	200 OK	Grep Highlight
🗄 dns-lookup.php					
add-to-your-blog.php					
view-someones-blog.php					
browser-info.php					
text-file-viewer.php					
source-viewer.php					
http://www.irongeek.com/i.php     //mutillidae/index.php					
http://192.168.178.196/mutillidae/ind					
/mutilidae/index.php					
Server Headers					
Apache/2.2.14 (Win32) DAV/2 mod_s:					
Apacne/2.2.14 (WIN32) DAV/2 mod_s! /mutillidae/					
EMail Adresses					

# 3.3 Active checks

A full scan will perform an automated vulnerability analysis of all recorded chats (except the excluded ones).

First you have to exclude the chats from scanning which:

- may harm our system/application
- may lock our login
- will logout our sessions
- we don't want to analyze

 $\rightarrow$  because we don't want to lock our account we exclude the login chat (15):





ATOBO by siberas (Version: 0.9.2RC2)							_	_	_	
Settings Tools View Help										
ngs Sites	Doc Fil	Iter Text	Filter Options							Chat-ID: 15
192.168.178.196	exc	:l. pics 🗟	excl. docs 🔽 excl.	javascript 🔽 e	xcl. style sheets					
*										🔄 Browser-View 🔬 Fuzzer 🔬 Manual R
🖻 鏦 Vulnerabilities	Apply									Request:
🗉 🛑 Unencrypted Logins		Metho	d Host	Path		Parameters	Status	Set-Cookie Co	mment	
Hints	1	GET	192.168.178.196	mutillidae/	ndex.php		200 OK			Text Hex
HIIIG	2	GET	192.168.178.196	mutillidae/	ndecphp	page=login.php	200 OK			Grep Highlight
🗄 👔 Logins	3	POST	192.168.178.196	mutillidae/	ndex.php	user_name=testsql&passv	0 200 OK			POST http://192.168.178.196/mutillidae/index.php?page=login.php HTTP/1.1
/mutillidae/index.php	4	GET	192.168.178.196	mutillidae/	ndex.php	page=user-info.php	200 OK			Host: 192.168.178.196
/mutillidae/index.php	5	POST	192.168.178.196	mutillidae/	ndex.php	view_user_name=testsql&	p:200 OK			User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625
	6	GET	192.168.178.196	mutillidae/	ndecphp	page=dns-lookup.php	200 OK			Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
🖻 <u>()</u> Filename Parameter	7	POST	192.168.178.196	mutillidae/		target_host=testsql&Subn	nit 200 OK			Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate
🖻 untitled	8	POST	192.168.178.196	mutillidae/		target host=sd+%26%26+				Accept-Charset: ISO-8859-1, utf-8;q=0.7, *;q=0.7
/mutillidae/index.php	9	POST	192.168.178.196	mutillidae/		target host=sd+%26+dir8				Keep-Alive: 115
E 💼 Info	10	GET	192.168.178.196	mutillidae/		page=add-to-your-blog.p				Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?page=login.php
	11	POST	192.168.178.196	mutillidae/		input from form=testxss8				Cookie: uid=5
IP Adress Disclosure	12	GET	192.168.178.196	mutillidae/		page=view-someones-blo				Content-Type: application/x-www-form-urlencoded
Hotspots	13	POST	192.168.178.196	mutillidae/		show_only_user=Show+Al				Content-Length: 51
	14	GET	192,168,178,196	mutillidae/		page=login.php	200 OK			user_name=john&password=monkey&Submit_button=Submit
	15	POST	192.168.178.196	mutillida		user_name=john&passwo		uid=3		
http://irongeek.com/sigs/logo.php	16	GET	192.168.178.196	mutillida	Send to +		200 OK			
🖲 register.php	17	GET	192.168.178.196	mutillida	Exclude from Scan 🔸	Chat (15)				
I login.php	18	POST	192.168.178.196	mutillida	Сору 🔸	input_from_form=testxss8				
setupreset.php	10	GET	192.168.178.196	mutillidae	Add to Login-Script	page=view-someones-blo				
show-log.php	20	POST	192.168.178.196	mutillidae/		show only user=admin&				Response:
🖲 credits.php	20	POST	192.168.178.196							Text Tagless Hex
http://www.owasp.org/index.php		-	192.168.178.196	mutillidae/		show_only_user=Show+Al				
user-info.php	22	GET		mutillidae/		page=browser-info.php	200 OK			Grep Highlight
dns-lookup.php	23	GET	192.168.178.196	mutillidae/		page=show-log.php	200 OK			HTTP/1.1 200 OK
add-to-your-blog.php	24	GET	192.168.178.196	mutillidae/		page=text-file-viewer.php				Date: Tue, 20 Jul 2010 17:08:21 GMT
view-someones-blog.php	25	POST	192.168.178.196	mutillidae/		text_file_name=http%3A%				Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8I mod_autoindex_ X-Powered-By: PHP/5.3.1
browser-info.php     text-file-viewer.php	26	GET	192.168.178.196	mutillidae/		page=source-viewer.php	200 OK			Set-Cookie: uid=3
text-file-viewer.php     source-viewer.php	27	GET	192.168.178.196	mutillidae/		page=source-viewer.php8				Content-Length: 5717
source-viewer.pnp     Http://www.irongeek.com/i.php	28	GET	192.168.178.196	mutillidae/			200 OK			Connection: close
/mutillidae/index.php     /mutillidae/index.php	29	GET	192.168.178.196	mutillidae/		page=show-log.php	200 OK			Content-Type: text/html
http://192.168.178.196/mutillidae/index.php	30	GET	192.168.178.196	mutillidae/		page=credits.php	200 OK			<meta content="0;url=index.php" http-equiv="refresh"/> HTML PUBLIC "</td
<ul> <li>http://192.108.178.196/mutilidae/index.php</li> <li>http://192.168.178.196/mutilidae/setupreset.p</li> </ul>	31	GET	192.168.178.196	mutillidae/	ndex.php		200 OK			<html></html>
http://localhost/mutillidae/index.php	32	GET	192.168.178.196	mutillidae/	ndex.php		200 OK			<head> <meta content="text/html; charset=utf-8" http-equiv="content-type"/></head>
redirectandlog.php	33	GET	192.168.178.196	mutillidae/	ndecphp		200 OK			<pre><meta cnarset="us-ascii" content="text/ntmi;" nttp-equiv="content-type"/> <li><li>k rel="shortcut icon" href="favicon.ico" type="image/x-icon" /&gt;</li></li></pre>
	34	GET	192.168.178.196	mutillidae/	ndex.php	do=logout	200 OK	uid=deleted;		
Server Headers	35	GET	192.168.178.196	mutillidae/	ndex.php		200 OK			<body></body>
Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14	36	GET	192.168.178.196	mutillidae/	a day a ba		200 OK			

# and exclude the logout chat (34):

WATOBO by siberas (Version: 0.9.2RC2)	Balancine and Anna	an internet regions	_	
File Settings Tools View Help				
Findings Sites	Doc Filter Text Filter Options			
E 🕢 192.168.178.196	Clear logout			Full Request Full Response
- 🎪 Vulnerabilities	Apply			
Unencrypted Logins	Method Host	Path	Parameters	Status Set-Cookie Comment
E Hints	34 GET 192.168.178.196	Send to +	do=logout	200 OK uid=deleted;
🗄 🗇 Logins		Exclude from Scan  Copy	(34)	
		Add to Login-Script		
/mutillidae/index.php				
🖻 🕦 Filename Parameter				
🖃 untitled				
/mutillidae/index.php				
info				

 $\rightarrow$  Start scan:



 $\rightarrow$  select target(s):





Start Full Scan
Select Scan Targets
Deselect All Select All
₩ 192.168.178.196
Cancel Back Next Start

 $\rightarrow$  select checks:

Start Full Scan	
Select Checks	
Default	
Misc     Directory Indexing     HTTP Methods     Lotus Domino DB Enumeration	
<ul> <li>BAP</li> <li>SQL-Injection</li> <li>SQL-Injection</li> </ul>	
Boolean SQL-Injection      XSS      Simple Cross Site Scripting Checks	
Cancel Back Next Start	

 $\rightarrow$  verify excluded Chats:

Start Full Scan	
Advanced Settings	
Scan Options	
Max. Par. Request: 20	
Enable Smart Scan 🔽	
Excluded Chats	
15, 34	
Ignore Similar Chats 🗖	View/Edit
Forwarding Proxy	
Current:	View/Edit
Session Management	
	View/Edit
Cancel Bac	k Next Start





 $\rightarrow$  press **Start**  $\rightarrow$  the findings are updated immediately:

You can watch the scan progress with the dashboard:



## Findings:

WATOBO by siberas (Version: 0.9.2RC2)	
File Settings Tools View Help	
Findings Sites	DASHBOARD
₽ 🕢 192.168.178.196	Project Information Scan Information
	Scan-Status: Finished
🗉 🛑 Unencrypted Logins	Directory Indexing
□ /mutillidae/index.php	
/mutillidae/index.php	HTTP Methods
🕀 🚱 SQL-Injection	
[show_only_user] - /mutillidae/index.php	
/mutillidae/index.php	Lotus Domino DB Enumeration
[view_user_name] - /mutillidae/index.php	
/mutillidae/index.php	Simple SQL-Injection
🖻 [password] - /mutillidae/index.php	
/mutillidae/index.php	
/mutillidae/index.php	Boolean SQL-Injection
🖻 [user_name] - /mutillidae/index.php	
/mutillidae/index.php	Simple Cross Site Scripting Checks
Reflected XSS [POST]	
🛱 [input_from_form] - /mutillidae/index.php	
/mutillidae/index.php	
🖻 [Submit_button] - /mutillidae/index.php	
- /mutillidae/index.php	
/mutillidae/index.php	
🖻 🛑 Reflected XSS [GET]	
[php_file_name] - /mutillidae/index.php	
· /mutillidae/index.php	
/mutillidae/index.php	
/mutillidae/index.php	
- /mutillidae/index.php	
/ mutillidae/index.php / mutillidae/index.php	
□ [submit] - /mutillidae/index.php	
/mutillidae/index.php	
/mutillidae/index.php	
- /mutillidae/index.php	
/mutillidae/index.php	
Reflected XSS [GET]	
🖻 [php_file_name] - /mutillidae/index.php	
/mutillidae/index.php	
🗉 💮 Hints	<b>-</b>





# Chat of SQL-injection finding:

	👩 Browser-View 🔯 Fuzzer 🔏 Manual Reque
equest:	
[ext] Hex]	
	Grep Highlight Rese
Host: 192/168.178.196 User-Agent: Mozilla/5.0 (Windo Accept: text/html, application/xł Accept-Language: de-de, de; q=; Accept-Charset: ISO-8859-1, utf- Keep-Alive: 115	-8;q=0.7,*;q=0.7 mutillidae/index.php?page=login.php ww-form-urlencoded
esponse:	
ext Tagless Hex	
	Grep Highlight Res
090110/2.7.1 mod_perl/2.0.4 Per	rl/v5.10.1
ntax; check the manual that cor	rresponds to your My <mark>SQL server</mark> version for the right syntax to use ne





#### Sites:

WATOBO by siberas (Version: 0.9.2RC2)
File Settings Tools View Help
Findings Sites
- 2192.168.178.196
🗄 📁 mutillidae
- 🄃 index.php
- 🅦 index.php?page=login.php
- 🅦 index.php?page=user-info.php
- 🅦 index.php?page=dns-lookup.php
- 🅦 index.php?page=add-to-your-blog.php
index.php?page=view-someones-blog.php
- 🏨 index.php?page=browser-info.php
- 🄃 index.php?page=show-log.php
- 🄃 index.php?page=text-file-viewer.php
- 🄃 index.php?page=source-viewer.php
ndex.php?page=source-viewer.php&php_file_name=add-to-your-blog.
index.php?page=credits.php
index.php?do=logout





#### Chats:

Clear				🗆 Full Request 🗖 Full Respo	onse
pply					
11.2	Method	Host	Path	Parameters Statu	s Se
1	GET	192,168,178,196	mutillidae/index.php	200 0	
2	GET	192,168,178,196	mutillidae/index.php	page=login.php 200 O	к
3	POST	192.168.178.196	mutillidae/index.php	user_name=testsql&passwo 200 O	К
4	GET	192.168.178.196	mutillidae/index.php	page=user-info.php 200 O	
5	POST	192.168.178.196	mutillidae/index.php	view_user_name=testsql&pa200 O	к
6	GET	192.168.178.196	mutillidae/index.php	page=dns-lookup.php 200 O	
7	POST	192.168.178.196	mutillidae/index.php	target_host=testsgl&Submit200 O	к
8	POST	192.168.178.196	mutillidae/index.php	target host=sd+%26%26+ls 200 O	
9	POST	192.168.178.196	mutillidae/index.php	target host=sd+%26+dir&S 200 O	
10	GET	192.168.178.196	mutillidae/index.php	page=add-to-your-blog.phj 200 O	к
11	POST	192.168.178.196	mutillidae/index.php	input_from_form=testxss&S 200 O	
12	GET	192.168.178.196	mutillidae/index.php	page=view-someones-blog.200 O	
13	POST	192,168,178,196	mutillidae/index.php	show_only_user=Show+All+200 O	
14	GET	192.168.178.196	mutillidae/index.php	page=login.php 200 O	
15	POST	192.168.178.196	mutillidae/index.php	user_name=john&password200 O	Ku
16	GET	192.168.178.196	mutillidae/index.php	200 0	
17	GET	192.168.178.196	mutillidae/index.php	page=add-to-your-blog.php200 O	к
18	POST	192.168.178.196	mutillidae/index.php	input_from_form=testxss&S 200 O	
19	GET	192.168.178.196	mutillidae/index.php	page=view-someones-blog.200 O	
20	POST	192.168.178.196	mutillidae/index.php	show_only_user=admin&Su 200 O	
21	POST	192.168.178.196	mutillidae/index.php	show_only_user=Show+All+200 O	
22	GET	192.168.178.196	mutillidae/index.php	page=browser-info.php 200 O	к
23	GET	192.168.178.196	mutillidae/index.php	page=show-log.php 200 O	к
24	GET	192.168.178.196	mutillidae/index.php	page=text-file-viewer.php 200 O	к
25	POST	192.168.178.196	mutillidae/index.php	text_file_name=http%3A%2I200 O	к
26	GET	192.168.178.196	mutillidae/index.php	page=source-viewer.php 200 O	к
27	GET	192.168.178.196	mutillidae/index.php	page=source-viewer.php&p200 O	к
28	GET	192.168.178.196	mutillidae/index.php	200 0	к
29	GET	192.168.178.196	mutillidae/index.php	page=show-log.php 200 O	к
30	GET	192.168.178.196	mutillidae/index.php	page=credits.php 200 O	К
31	GET	192.168.178.196	mutillidae/index.php	200 0	к
32	GET	192.168.178.196	mutillidae/index.php	200 O	к
33	GET	192.168.178.196	mutillidae/index.php	200 O	к
34	GET	192.168.178.196	mutillidae/index.php	do=logout 200 O	Ku
35	GET	192.168.178.196	mutillidae/index.php	200 0	к
36	GET	192,168,178,196	mutillidae/index.php	200 0	к





# Single chat (1):

	Browser-View	Se Fuzzer	Ă Manual Reque
equest:			
[ext Hex]			
		Gr	ep Highlight Reset
Host: 192.168.178.196 User-Agent: Mozilla/S.0 (Windows; U Accept: text/html, application/xhtml- Accept-Language: de-de, de;q=0.8,er Accept-Lanster: ISO-8859-1,utf-8;q= Keep-Alive: 115 Proxy-Connection: keep-alive Cookie: uid=5	+xml,application/xml;q=0.9,*/ n-us;q=0.5,en;q=0.3		00625 Firefox/3.6.6
		Gr	ep Highlight Reset
Text         Tagless         Hex           HTTP/1.1 200 OK         Date: Tue, 20 Jul 2010 17:07:21 GMT           Server: Apache/2.2.14 (Win32) DAV/2	2 mod_ssl/2.2.14 OpenSSL/0.9.		
Date: Tue, 20 Jul 2010 17:07:21 GMT Server: Apache/2.2.14 (Win32) DAV/2 X-Powered-By: PHP/5.3.1 Connection: close Transfer-Encoding: chunked	//DTD HTML 4.01 Transitional :us-ascii" http-equiv="conten	8  mod_autoir //EN" "http:// t-type">	ndex_color PHP/5.3





# 3.3 Session management

To demonstrate session management we need an application where you have to login first, like DVWA.

## Example: Damn Vulnerable Web App [3]:

🥹 Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox					
$      \underline{D}atei \underline{B}earbeiten \underline{A}nsicht \underline{C}hronik \underline{L}esezeichen \underline{E}_{\underline{X}tras} \underline{H}ilfe \\ \hline  \Rightarrow \bullet \underline{P} \ \hline  & & & \\ & & & & & & & & & & & & & & & $					
🗁 Aktuell 🗁 FW-ADMIN-GUIs 🗁 Info 🗁 Security 🗁 Support 🗁 LBBW 🗁 Tools 🗁 ONLINE-Tools 🗁 MyLinks 🛛 🗞 SHODAN 🛛 🔹 👋					
Damn Vulnerable Web App (DVWA) 🔅 🔹					
DVWA Username Password Login					

First we login with *admin/password* and browse the application (passive checks):

Damn Vulnerable Web App					
Home Instructions Setup	Vulnerability: Reflected Cross Site Scripting (XSS) What's your name?				
Brute Force	testxss				
Command Execution					
CSRF	More info				
File Inclusion	http://ha.ckers.org/xss.html				
SQL Injection	http://en.wikipedia.org/wiki/Cross-site_scripting				
Upload	http://www.cgisecurity.com/xss-faq.html				
XSS reflected					
XSS stored					
DVWA Security					
PHP Info					
About					
Logout					





Note: Logout from the application after browsing since we want to test session management.

First we need to identify all chats (request/response pair) which are responsible for the login process and add them to the login script (add the chat where the cookie is set and where the login credentials are posted - "**302 found**")

In our example it is Chat 1 where the session cookie is set:

	Method	Host	Path	Para	meters		Status	Set-Cookie
1	GET	192.168.178.196	dvwa/		Send to 🕨	1	302 Found	PHPSESSID=sbeh888vm5j75a920r0s4bt
2	GET	192.168.178.196	dvwa/login.php		Exclude from Scan		200 OK	
3	POST	192.168.178.196	dvwa/login.php	use		passw	302 Found	
4	GET	192.168.178.196	dvwa/index.php		Copy •		200 OK	
5	GET	192.168.178.196	dvwa/vulnerabilities/xss_r/		Add to Login-Script		200 OK	
6	GET	192.168.178.196	dvwa/vulnerabilities/xss_r/	nam	e=testxss		200 OK	

as well as chat 3 where the login credentials are posted:

	Method	Host	Path	Parameters	Status	Set-Cookie
1	GET	192.168.178.196	dvwa/		302 Found	PHPSESSID=sbeh888vm5j75a920r0s4bk
2	GET	192.168.178.196	dvwa/login.php		200 OK	
3	POST	Send to	wa/login.php	username=admin&password=passw	302 Found	
4	GET	Exclude from Scan	wa/index.php		200 OK	
5	GET	Copy	wa/vulnerabilities/xss_r/		200 OK	
6	GET	Add to Login-Script	wa/vulnerabilities/xss_r/	name=testxss	200 OK	
7	GET	132.100.170.130	uvwa/vulnerabilities/xss_s/		200 OK	
8	POST	192.168.178.196	dvwa/vulnerabilities/xss_s/	txtName=testxss&mtxMessage=testx	200 OK	
9	GET	192.168.178.196	dvwa/vulnerabilities/sqli/		200 OK	
10	GET	192.168.178.196	dvwa/vulnerabilities/sqli/	id=testsql&Submit=Submit	200 OK	

To validate the session settings open the Session Management Menu (Settings  $\rightarrow$  Session management):

Login Script Requests: Add Request							Add Request
	Method	Host	Path	Parameters	Status	Set-Cookie	Comment
1	GET	192.168.178.196	dvwa/		302 Found	PHPSESSID=sbeh88	8v
3	POST	192.168.178.196	dvwa/login.php	username=admin&password=password&Login=Login	302 Found		
quest	Response	1					
	Response						





Open the "**Session Ids**" tab, then open the "**Response**" tab to see where the session information has been set:

Session ID Patterns:	Login Requests:
(PHPSESSID)=([0-9a-zA-Z]*)(; &)?	[1] GET http://192.168.178.196/dvwa/ HTTP/1.1
Add Remove	Request Response
name="(sessid)" value="([0-9a-zA-ZI-]")" (sessid)=([-0-9a-zA-Z_:]")( &)? (SESSIONID)=([-0-9a-zA-Z_:\.\(\)]")(; &)? (PHPSESSID)=([0-9a-zA-Z]")(; &)? (ASPSESSIONID)\w*=([0-9a-zA-Z]")(; &)? (MYSAPSSO2)=([0-9a-zA-ZI-")")(; &)? (ELEXIRSID)=([0-9a-zA-ZI-]")(; &)? (SLSID)=([0-9a-zA-ZI-]")(; &)? (sid)=([0-9a-zA-ZI-]")(; &)? (saplb_\*)=([-0-9a-zA-Z].\(\)]")(; &)? (DomAuthSessId)=([0-9a-zA-Z]")(; &)? (wgate)\/((\w]{4,}\/(\w=~]")(; &)? (session)=([-0-9a-zA-Z_:\.]")(; &)?	HTTP/1.322 Found Date: Thu, 22 Jul 2010 10:52:04 GMT Server: Apache/2.214 (Win32) DAV/2 mod_ssl/2.214 OpenSSL/0.9.81 mod_autoindex_color PHP/5.3.1 mod_apreq2- X-Powered-By: PHP/5.3.1 Set-Cookie: SPHP/5.5210 = 56:C6830m57/56:2000 EM320; path=/ Expires: Thu, 19 Nov 1981 00:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: security=high Location: login.php Content-Length: 0 Connection: close Content-Type: text/html

After we finished verifying our session management settings let's see if it really works:

#### $\rightarrow$ chose a chat and open the Manual Request Editor:

	Method	Host	Path	Parameters	Status	Set-Cookie
1	GET	192.168.178.196	dvwa/		302 Found	PHPSESSID=sbeh888vm5j75a920r0s4bk
2	GET	192.168.178.196	dvwa/login.php		200 OK	
3	POST	192.168.178.196	dvwa/login.php	username=admin&password=pa	ssw(302 Found	
4	GET	192.168.178.196	dvwa/index.php		200 OK	
5	GET	192.168.178.196	dvwa/vulnerabilities/xss_r/		200 OK	
6	GET C-	nd to	chaus (unla or shilition (vss_r/	name=testxss	200 OK	
7	6	clude from Scan	Fuzzer ss_s/		200 OK	
8	P		Manual Request	txtName=testxss&mtxMessage=t	estx: 200 OK	
9	16	opy	dvwa/vulnerabilities/sqli/		200 OK	
10	Ac	ld to Login-Script	dvwa/vulnerabilities/sqli/	id=testsql&Submit=Submit	200 OK	





# "Update Session Information" enabled:

History: < 0 >	Request: Reset	Response Request Differ	
GET http://192.168.178.196/dvwa/vulnerabilities/xss_ Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6 Accept: text/html,application/xhtml+xml,application Accept-Language: de-de,de;q=0.8, en-us;q=0.5, en;q= Accept-Encoding: gzip,deflate Accept-Enset: ISO-8859-1,utf-8;q=0.7, *;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/dvwa/vulnerabilities// Cookie: security=high; PHPSESSID=sbeh888vm5j75af	.1; de; rv:1.9.2.7) Ge /xml;q=0.9,*/*;q=0 0.3 xss_r/	Text   Tagless   Hex	Grep Highlight Reset
Request Options     Vipdate Content-Length     Vipdate Session Information     Run Login     Use Octained Research (OrticleSerge)	SEND		
Use Original Request (QuickScan) Log Chat	preview >>		
QuickScan		MD5: -N/A-	Browser-View
.ogs:			

 $\rightarrow$  Send  $\rightarrow$  we are redirected to the login page:

History: < 7 >	est: Reset Response Request Differ
GET http://192.168.178.196/dvwa/vulnerabilities/xss_r/?nam Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; Accept: text/html,application/xhtml+xml,application/xmk;q Accept: text/html,application/xhtml+xml,application/xmk;q Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/dvwa/vulnerabilities/xss_r/ Cookie: security=high; PHPSESSID=sbeh888vm5j75a920r0s4 	rv:1.9.2.7) Ge =0.9,*/*;q=0 HTTP/1.1 302 Found Date: Thu, 22 Jul 2010 11:16:23 GMT Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 Open X-Powered-By: PHP/5.3.1 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post- Pragma: no-cache
7/22/2010 @ 13:16:23: got answer 7/22/2010 @ 13:16:23: sending request 7/22/2010 @ 13:15:46: got answer 7/22/2010 @ 13:15:46: got answer	





Now check "**Run Login**" which runs the login script (chats 1 + 3) to get valid session information

 $\rightarrow$  Send  $\rightarrow$  now we successfully updated our session information:

Manual Request Toolkit	
History:       8 >         GET http://192.168.178.196/dvwa/vulnerabilities/xss_r/?name=test         Host:       192.168.178.196         User-Agent:       Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2         Accept:       text/html, application/xhtml+xml, application/xml;q=0.9,*/         Accept-Language:       de-de, de; q=0.8, en-us;q=0.5, en;q=0.3         Accept-Charset:       ISO-8859-1, utf-8;q=0.7,*;q=0.7         Keep-Alive:       115         Proxy-Connection:       keep-alive         Referer:       htp://192.168.178.196/dvwa/vulnerabilities/xss_r/         Cookie:       security=high;         PHPSESSID=sbeh888vm5j75a920r0s4bb3i5	Text       Tagless       Hex         btss HI       Grep       Highlight       Reset         2.7) Ge       HTTP/1.1 200 OK
▲         Request Options         Image: Update Content-Length         Image: Update Session Information         Image: Run Login         Image: Use Original Request (QuickScan)         Image: Log Chat	Interpretation of the second secon
QuickScan	MD5: d5b6a0f6bfde2e797a9ea94a1d01ec Browser-View
07/22/2010 @ 13:18:50: got answer 07/22/2010 @ 13:18:50: sending request 07/22/2010 @ 13:16:23: got answer 07/22/2010 @ 13:16:23: conding request	

Once you got a valid session information you can disable "**Run Login**" because the session information is still remembered

Disabling "Update Session Information" will redirect you to the login page again:





History: < 9 > Request: Reset	
GET http://192.168.178.196/dvwa/vulnerabilities/xss_r/?name=testxss H Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.7) G Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q= Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/dvwa/vulnerabilities/xss_r/ Cookie: security=high; PHPSESSID=sbeh888vm5j75a920r0s4bb3i5	e Highlight Reset
07/22/2010 @ 13:23:24: got answer 07/22/2010 @ 13:23:24: sending request 07/22/2010 @ 13:18:50: got answer 07/22/2010 @ 13:18:50: conding request	A

Now you can also try an active scan but do not forget to exclude the login- and logout chats from scanning.





# 3.4 Manual requests

	Method	Host	Path	Parameters	Status	Set-Cookie	Comment
1	GET	192.168.178.196	dvwa/login.php		200 OK		
2	POST	192.168.178.196	dvwa/login.php	username=admin&passwor	302 Four	n in the second s	
3	GET	192.168.178.196	dvwa/index.php		200 OK		
4	GET	192.168.178.196	dvwa/vulnerabilities/sqli/		200 OK		
5	GET	192.168.178.196	dvwa/vulnerabilities/sqli/	id=testsql&Submit=Submit	200 OK		
6	GET	192.168.178.196	dvwa/vulnerabilities/xss_s/		200 OK		
7	GET	192.168.178.196	dvwa/security.php		200 OK		
8	POST	192.168.178.196	dvwa/security.php	security=low&seclev_submi	302 Four	security=low	
9	GET	192.168.178.196	dvwa/security.php		200 OK		
10	GET	192.168.178.196	dvwa/vulnerabilities/xss_s/		200 OK		
11	POST	192.168.178.196	dvwa/vulnerabilities/xss_s/	txtName=hugo&mtxMessag	200 OK		
12	POST	192.168.178.196	dvwa/vulnerabilities/xss_s/	txtName=hugo&mtxMessag	200 OK		
13	GET	192.168.178.196	dvwa/vulnerabilities/fi/	page=include.php	200 OK		
14	GET	192.168.178.196	dvwa/		200 OK		

### $\rightarrow$ double-click the desired chat:

Here you can change what you like in the request (e.g. **id='**) and send it away.

🔏 Manual Request Toolkit	
History:       2         GET http://192.168.178.196/dvwa/vulnerabilities/sqli/?id='&Submit=Sut         Host:       192.168.178.196         User-Agent:       Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.7) Ge         Accept:       Language:         Accept-Language:       de-de;q=0.8,en-us;q=0.5,en;q=0.3         Accept-Charset:       ISO-8859-1,utf-8;q=0.7,*;q=0.7         Keep-Alive:       IS         Proxy-Connection:       kep-alive         Refere:       http://192.168.178.196/dvwa/vulnerabilities/sqli/         Cookie:       security=low;         PHPSESSID=nmk051skk39feidh37iabekm57         Image:       Senution         Image:       Vupdate Content-Length         Image:       Vupdate Session Information         Image:       Senution         Image:       Senution         Image:       Senution	Response Request Differ         Text Hex         GET http://192.168.178.196/dvwa/vulnerabilities/sqli/?id='&         Host: 192.168.178.196         User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de;         Accept: text/html,application/xhtml+xml,application/xml;         Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3         Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7         Keep-Alive: 115         Proxy-Connection: keep-alive         Referer: http://192.168.178.196/dvwa/vulnerabilities/sqli/         Cookie: security=low; PHPSESSID=nmk051skk39feidh37iab
QuickScan	
Logs: 07/22/2010 @ 14:26:23: got answer 07/22/2010 @ 14:26:23: sending request 07/22/2010 @ 14:26:18: got answer 07/22/2010 @ 14:26:17: conding request	 





The differ function is totally awesome - you can compare 2 chats from the same type:

History: < 3 > Ret	quest: Reset	Respons	e Request Differ		
GET http://192.168.178.196/dvwa/vulnerabilities/sqli/id= Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; dk Accept: text/html,application/xhtml+xml,application/xml Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/dvwa/vulnerabilities/sqli/ Cookie: security=low; PHPSESSID=nmk051skk39feidh37ia	e; rv:1.9.2.7) Ge ;q=0.9,*/*;q=0	URL: Leng Stati Seco Hist	ory-ID: 2 : http://192.168.1 gth: 4486 us: 200 OK nd Chat ory-ID: 3	LENGTH 4486 4486 594 178.196/dvwa/vuln	
Run Login     Use Original Request (QuickScan)     Log Chat	SEND preview >>		gth: 594 us: 200 OK		
QuickScan				Diff it!	
Logs: 17/22/2010 @ 14:30:03: got answer 17/22/2010 @ 14:30:03: sending request 17/22/2010 @ 14:26:23: got answer 17/22/2010 @ 14:26:24: conding request					

Choose the 2 chats which you want to be compared, then click on "Diff it!"

See the comparison of the REQUEST





🗾 Chat Differ		
Chat Differ          Response       Request         Type       Pos       Count         +       10       1         -       10       1	Original GET http://192.168.178.196/dvwa/vulnerabilities/sqli/?id=`&Submit=Submit 1 Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.7) Gecko 713 Firefox/3.6.7 Accept: Lext/html,application/xhtml+xml,application/xml;q=0.9;*/*;q=0.8 Accept-Language: de-de,de;q=0.8, en-us;q=0.5, en;q=0.3 Accept-Charset: ISO-8859-1,uff-8;q=0.7,*;q=0.7 Keep-Alive: 115 Referer: http://192.168.178.196/dvwa/vulnerabilities/sqli/ Cookies security=lowg PIPSESDID=nml051skE99feidh37iabekm57 Connection: Close Proxy-Connection: Close Accept-Encoding: None	New GET http://192.168.178.196/dwwa/vulnerabilities/sqli/?id='&Submit=Submit 1 Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; nv:1.9.2.7) Gecko, 713 Firefox/3.6.7 Accept text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Charset: ISO-8859-1,udf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Referen: http://192.168.178.196/dwwa/vulnerabilities/sqli/ Gookiesecutive_biologi.pt.09555510=nmid/5164/29/fedf/37/abe/sm57/ Connection: Close Proxy-Connection: Close Accept-Encoding: None
	4	4

and the RESPONSE of the chats:

Request Request	1	Original	New
Type         Pos         Co           +         1         -           -         1         -           +         5         -         -           +         5         -         -           +         8         -         -           +         10         -         10           +         12         -         12	unt 1 1 2 2 1 1 1 1 1 83 2	HTTP/1.1 200 OK Date: Thu, 22 Jul 2010 12:42:01 GMT Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.81 mod_a color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 X-Powered-By: PHP/5.3.1 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache: Control: no-score, no-cache, must-revalidate, post-check=0, pre-chr Pragma: no-cache Content-Length: 160 Connection: close Content-Type: text/html <pre>Sou have an error in your SQL syntax; check the manual that correspt your MySQL server version for the right syntax to use near """ at line 1</pre>	HTTP/1.1 200 OK 2 Date: Thu, 22 Jul 2010 12:42:12 GMT Server: Apache/2.2.14 (Win32) DAV/2 mod_ssi/2.2.14 OpenSSL/0.9.81 moc color PHP/5.31 mod aperq2-20090110/2.7.1 mod_per/2.0.4 Per/v.510.1 X-Powered-By: PHP/5.3.1 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Contok no-cache, must-revalidate Pragma: no-cache Content-Length: 4097 Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 4097 Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 4097 Connection: close Content-Type: text/html;charset=utf-8 Content-Type: text/html;charset=utf-8 Content-Type: text/html;charset=utf-8 Content-Length: 4097 Connection: close Content-Type: Text/orD X-HTML 1.0 Strict//EN**http:// html1/DTD/ahtml1=strict.dtd*> <html: ahtml1="strict.dtd*" dtd=""> <htm< th=""></htm<></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:></html:>





# 3.5 More functions

#### **Inline De-/Encoding:**

If you for example have a HTTP basic authentication you can decode the base64 encoded string immediately with WATOBO. Just select the string, right click your mouse and you can see immediately the credentials *test/test*.

Chat-ID: 149		
	Browser-View	Fuzzer 🔏 Manual Request
Request:		
Text		
		Grep Highlight Reset
GET http://	/authBasic/authTest/ HT	TP/1.1
Host: handle.library.cornell.edu		
User-Agent: Mozilla/5.0 (Windows; Accept: text/html,application/xhtml		
Accept-Language: de-de,de;q=0.8,e		-0.5
Accept-Encoding: gzip, deflate		
Accept-Charset: ISO-8859-1, utf-8;q: Keep-Alive: 115	=0./,*;q=0./	
Proxy-Connection: keep-alive		
Referer: http://handle.library.cornell		
Authorization: Basic dGVzdDp0ZXN	- Info -	1
	Length: 12	
	- Decoder -	
	Base64: test:test	
	Hex(A): 0	
	Hex(Int):	
,	URL: dGVzdDp0ZXN0	
Response:	- Сору -	
	copy text: dGVzdDp0ZXN0	
Text Tagless Hex	- Transcoder -	
	send to transcoder	Grep Highlight Reset

You can also send the selected string to the **transcoder** which can do several de-/encodings:





I Transcoder	
Length: 9	
Text Hex	
testitest	
Base64 URL Encode Encode Encode MD5 Decode Decode SHA-1	

#### **Browser-View:**

A nice feature is when you click on



you can see the response in your browser (on windows only IE supported )

### **Interceptor:**

Of course, WATOBO has an interceptor too:





Interceptor	
Intercept: I▼ Requests I▼ Response	Request (1)       Response         GET http://192.168.178.196/dvwa/vulnerabilities/sqli/?id=Hugo&Submit=Submit HTTP/1.1         Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg         Refere: http://192.168.178.196/dvwa/vulnerabilities/sqli/         Accept-Language: de-DE         User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET         Accept-Encoding; gzip, deflate         Host: 192.168.178.196         Proxy-Connection: Keep-Alive         Cookie: security=low; PHPSESSID=nu8c8v6ecg368s00jf0ik3fs51         Image: Accept Discard Drop









# 3.6 Fuzzing

### - Enumerate Usernames -

Here we use the fuzzer for collecting usernames from the mutillidae web application [2]. First examine the response for the username with uid=3.

Here we have a corresponding username ("logged in as john"):

Request:			
Text Hex			
	Grep	Highlight	Reset
GET http://192.168.178.196/mutillidae/index.php?page=browser-info.php HTTP/1.1 Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.php Cookie: uid=3	8		
Response:			
Text Tagless Hex			
logged in as	Grep	Highlight	Reset

<br/>





#### Now open the fuzzer:

GET http://192.168.178.196/mutillidae/index.php?page=show-log.php Host: 192.168.178.196/mutillidae/index.php?page=show-log.php Host: 192.168.178.196/mutillidae/index.php?page=show-log.php Accept: text/html,application/xhtml+xml,application/xml;q=0,9,*/*;q= Accept: Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?page=browser-in Cookie: uid=3	Request:	Reset Settings Results
✓       Update Content-Length         ✓       Update Session Information	Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; Accept: text/html,application/xhtml-xml,application/xr Accept-Language: de-de,de;q=0.8, en-us;q=0.5, en;q=0.3 Accept-Charset: ISO-8859-1,utf-8;q=0.7, *;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?pa Cookie: uid=3	de; nv:1.9.2.6) C m;q=0.9,*/*;q= ge=browser-in
Vpdate Session Information		
I Kun Login		
	J Run Login	
	oqs:	

First we have to define a tag by which we can define the position of a generated value in the request later. Double-click on **Tags** and enter a tag name:

Create New Tag
Enter Label For Tag:
uid Note: To define the position in the request enclose the tag name between '%%', eg. '%%tag%%'. It will turn green if the given tag name is correct. Don't forget to specify a generator!
<u>Cancel</u> <u>Accept</u>

Next we have to define a generator which will produce the values we need. Double-click on "Tag: uid", select "**Counter**" and choose start=0, stop = 100, step = 0 (=1). This results in the values 0,1,2,3,...100.





Create Generator
Select Source
C File Select
C List Add Remove
<u>Cancel</u> <u>Accept</u>

To define the position of our values inside the request simply enter the tag name enclosed between "%%". That means replace **uid=3** with **uid=%%uid%%** :

E Fuzzer	
Request:       Reset         GET http://192.168.178.196/mutillidae/index.php?page=show-log.php         Host: 192.168.178.196         User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) C         Accept: text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=         Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3         Accept-Encoding: gzip,deflate         Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7         Keep-Alive: 115         Proxy-Connection: keep-alive         Referer: http://192.168.178.196/mutillidae/index.php?page=browser-in         Cookie: uid=         X%uid%%	Settings Results Tags Tag: uid Start=0/stop=100/step=1 Filters

To extract the usernames we also have to define a filter. Double-click on **Filters.** So let's define a regex. In this case the regex

# logged in as (.\*)</h2'

is just fine.

Note: the match value must be enclosed between brackets.



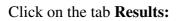


Create Filter
Filter
C Session-ID 0-9a-zA-Z!-]*)" ▼
Regex logged in as (.*)
<u>Cancel</u> <u>A</u> ccept

# Let's go $\rightarrow$ click on **Start**

GET http://192.168.178.196/mutillidae/index.php?page=show-log.php Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) G Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q= Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3	Tags Tag: uid
Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?page=browser-in Cookie: uid=%%uid%%	<ul> <li>start=0/stop=100/step=1</li> <li>Filters</li> <li>Filter: Regex</li> <li>logged in as (.*) </li></ul>
Request Options	
Vpdate Content-Length	
Update Session Information  Run Login	





equest:	Reset	Settings Result	5	
TT Lucy (102 169 179 106 (		Tag/Value	Match	
ET http://192.168.178.196/mutillidae/index.php?p lost: 192.168.178.196	age=snow-log.pnp	uid=2	adrian	
ser-Agent: Mozilla/5.0 (Windows; U; Windows NT	6.1; de; rv:1.9.2.6) G	uid=4	ed	
ccept: text/html,application/xhtml+xml,applicatio		uid=1	admin	
.ccept-Language: de-de,de;q=0.8,en-us;q=0.5,en; .ccept-Encoding: gzip,deflate	q=0.3	uid=6	hackme	
ccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7		uid=5	Fancy	
eep-Alive: 115 roxy-Connection: keep-alive		uid=3	john	
	۶			
equest Options				
itart Request Options Ø Update Content-Length		Save Matcher	1	
Start       Start       Request Options       Update Content-Length       Update Session Information       Run Login		Save Matches		

 $\rightarrow$  we found the users adrian, ed, admin, hackme, Fancy and john.

# - Fuzzing multiple values -

Here we want to enumerate a valid combination of filename + extension. In detail we want to test combinations of 3 filenames (index, test and xxx) and 3 extensions (mp3, wav and php).

First we define a tag and a list generator for the filenames we want to test.







# Create a tag for the <u>filenames</u>:

Create New Tag
Enter Label For Tag:
ААА
Note: To define the position in the request enclose the tag name between '%%', eg. '%%tag%%'. It will turn green if the given tag name is correct. Don't forget to specify a generator!
<u>Cancel</u> <u>A</u> ccept

## Create the generator:

Create Generator
Select Source
C File Select
C Counter Start 0 Stop 0 Step 0
List     Add     Remove
XXX
test
index
<u>Cancel</u> <u>Accept</u>

Create a tag for the <u>extensions</u>:

Create New Tag
Enter Label For Tag:
BBB
Note: To define the position in the request enclose the tag name between '%%', eg. '%%tag%%'. It will turn green if the given tag name is correct. Don't forget to specify a generator!
<u>Cancel</u> <u>A</u> ccept





Create the generator:

Create Gene	erator
Select So	urce
C File	Select
C Cour	nter Start 0 Stop 0 Step 0
• List	Add Remove
	wav php mp3
	<u>Cancel</u> <u>Accept</u>

Because we only want to know about valid combinations we define a filter for all

'HTTP/1.1 200 OK'

responses:

Create Filter
Filter
C Session-ID 0-9a-zA-Z!-]*)" ▼
Regex HTTP\/1.*200
<u>Cancel</u> <u>Accept</u>





# Next we place our tags:

🖄 Fuzzer	
Request:         Reset           GET http://192.168.178.196/mutillidae/%%AAAA%% %%BEB3%         ?page=browser-info.php HTTP/1.1           Host: 192.168.178.196         User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6           Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8         Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3           Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7         Keep-Alive: 115           Proxy-Connection: keep-alive         Referer: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.php           Cookie: uid=3         Second	Settings Results Tags Tags Tag: AAA List-Input 3 values Tag: BBB Filters Filter: Regex HTTP\/1.*200

Note, we have:

#### filename = % % AAA % % extension = % % BBB % %

# $\rightarrow$ Start fuzzing:

Request:	Reset	Settings Results	s]
GET http://192.168.178.196/mutillidae/ <mark>%%^^^**</mark> , <b>5%</b> , <b>188</b> , <b>198</b> , <b>1</b> 9age=browser-i Host. 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/201 Accept text/ml.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-Language: de-de;de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: grip,deflate Accept-Lincoting: grip,deflate Accept-Lincoting: grip,deflate Accept-Lincoting: grip,deflate Accept-Lincoting: grip,deflate Accept-Lincoting: grip,deflate Accept-Lincoting: grip,deflate Refere: http://192.168.178.196/mutillidae/index.php?page=view-someones-blo Cookie: uid=3	00625 Firefox/3.6.6	Taq/Value AAA=index BBB=php	Match HTTP/1.1 200 OK
Request Options ▼ Update Content-Length			
Update Session Information			1
🗆 Run Login		Save Matches	
ogs:			





 $\rightarrow$  we have only one single match.

If you want to see all combinations of values simply remove the filter:

equest:	Reset Setti	ngs Results	
SET http://192.168.178.196/mutillidae/%%AAA%%%%BBB%%%?page=browser-infg	Tag	/Value	Match
er nup/152.106.176.196 lost: 192.108.178.196 ser-Agent: Mozilla/5.0 (Windows: U: Windows NT 6.1; de; nv:1.9.2.6) Gecko/20100	AAA	A=xxx =mp3	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
<pre>kccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 kccept-Language: de-de_de;q=0.8,en-us;q=0.5,en;q=0.3 kccept-Encoding: gzip,deflate kccept-Charset: ISO-8859-1,ut-8;q=0.7,*;q=0.7</pre>	AAA	A=xxx =php	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
		A=xxx =wav	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:46 GMT
:ep-Alive: 115 oxy-Connection: keep-alive ferer: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.p	DDD	=test =wav	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
rerer: http://192.106.176.196/mutilildae/index.php:page=view-someones-biog.p iokie: uid=3	. AAA	a=index =wav	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
		l=test =mp3	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
		A=test =php	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
		A=index =mp3	HTTP/1.1 404 Not Found Date: Fri, 23 Jul 2010 09:47:47 GMT
		=index =php	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 09:47:47 GMT Server:
itart lequest Options 7 Update Content-Length 7 Update Session Information 7 Run Login		re Matches	
gs: 23/2010 @ 11:47:47: Finished Fuzzing 23/2010 @ 11:47:47: Started Fuzzing (6 Requests)			





### - Generating complex values -

Here we only generate more complex values without really fuzzing the web application so we neither place a tag at the request nor we need to define a filter.

First we create a tag called 'FANCY' and a simple generator which produces the values 0,1,2,....20 and start the fuzzing process. In the Result tab we can see our values:

equest:	Reset	Settings Result	
		Tag/Value	Match
ET http://192.168.178.196/mutillidae/index.php?page=browser-info.php HTTP/1.1 lost: 192.168.178.196		FANCY=4	HTTP/1.1 200 OK
ser-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6		FANCY=6	HTTP/1.1 200 OK
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8		FANCY=5	HTTP/1.1 200 OK
		FANCY=7	HTTP/1.1 200 OK
		FANCY=8	HTTP/1.1 200 OK
Keep-Alive: 115		FANCY=9	HTTP/1.1 200 OK
		FANCY=10	HTTP/1.1 200 OK
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7		FANCY=12	HTTP/1.1 200 OK
		FANCY=11	HTTP/1.1 200 OK
		FANCY=15	HTTP/1.1 200 OK
		FANCY=14	HTTP/1.1 200 OK
		FANCY=13	HTTP/1.1 200 OK
		FANCY=17	HTTP/1.1 200 OK
		FANCY=16	HTTP/1.1 200 OK
		FANCY=19	HTTP/1.1 200 OK
		FANCY=20	HTTP/1.1 200 OK
		FANCY=18	HTTP/1.1 200 OK
		FANCY=3	HTTP/1.1 200 OK
		FANCY=0	HTTP/1.1 200 OK
		FANCY=2	HTTP/1.1 200 OK
		FANCY=1	HTTP/1.1 200 OK

Next we work on the values we get from the generator (input). We want to build values like **"<input\*10>:<input\*10** 

For example for *input=3* we want the resulting value "30:3". Therefore right-click Counter and choose Add Action, select "Ruby Proc" and add the following line of ruby code:

## (input.to\_i\*10).to\_s + '':'' + input





Create Action	
Select Action C Encode Base64 C Encode URL C Hash MD5 Ruby Proc proc { [input] # place your code betweenhere # e.g. 'input + "TAIL" (input.to_i*10).to_s + ":" + input # and here }	
<u>Cancel</u> <u>A</u> ccept	

 $\rightarrow$  Start fuzzing and check the results:

equest: R	eset Settings Res	ults
	Tag/Value	Match
ET http://192.168.178.196/mutillidae/index.php?page=browser-info.php HTTP/1.1 lost: 192.168.178.196	FANCY=40:4	4 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
ser-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6	FANCY=30:3	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	FANCY=60:6	5 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
ccept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 ccept-Encoding: gzip,deflate	FANCY=50:5	5 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
ccept-Charset: ISO-8859-1, utf-8;q=0.7,*;q=0.7	FANCY=70:7	7 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
eep-Alive: 115	FANCY=80:8	8 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
roxy-Connection: keep-alive	FANCY=90:9	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
eferer: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.php ookie: uid=3	FANCY=100	:10 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=110	:11 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=120	:12 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=140	:14 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=160	:16 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=150	:15 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=130	:13 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=170	:17 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=180	:18 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=190	:19 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=200	:20 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=10:1	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=20:2	2 HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G
	FANCY=0:0	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:12:00 G





In the next step we want to base64 encode this value by simply adding another action:

Create Action	
Select Action	
• Encode Base64	
C Encode URL	
C Hash MD5	
C Ruby Proc	
proc {  input  # place your code betweenhere # e.g. 'input + "TAIL"	
# and here }	
<u>Cancel</u> <u>Accept</u>	

 $\rightarrow$  Start fuzzing and check the results:

		Settings Results		
TT http://100.169.179.106/constilling a finder a barran harmonia for a bar LITTD /1.1		Tag/Value	Match	
GET http://192.168.178.196/mutillidae/index.php?page=browser-info.php HTTP/1.1 Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept: Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Proxy-Connection: keep-alive Referer: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.php Cookie: uid=3	.6	FANCY=MTA6MQ==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MjA6Mg==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MDow	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=NDA6NA==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MzA6Mw==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=NjA6Ng==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=NTA6NQ==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=NzA6Nw==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=ODA6OA==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MTAwOjEw	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=OTA6OQ==	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MTEwOjEx	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MTIwOjEy	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
		FANCY=MTMwOjEz	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
equest Options		FANCY=MTQwOjE0	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	
7 Update Content-Length		FANCY=MTUwOjE1	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:15:20	





In the final step the value should look like this:

### "WATOBO:"<base64>":pwned"

We create another action by adding the following ruby code:

"WATOBO:" + input.strip + ":pwned"

Create Action	
Create Action Select Action Encode Base64 Encode URL Hash MD5 Ruby Proc proc {  input  # place your code betweenhere # e.g. 'input + "TAIL"	,
<u>Cancel</u> <u>Accept</u>	





# $\rightarrow$ Start fuzzing and check the results:

Request:	Reset	Settings Results	gs Results	
		Tag/Value	Match	
GET http://192.168.178.196/mutillidae/index.php?page=browser-info.php HTTP/1.1 Host: 192.168.178.196 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 Accept: text/html,application/xhtml=xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: de-de_de_q=0.8,en-us;q=0.5,en;q=0.3 Accept: Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: I15 Proxy-Connection: keep-alive Refere: http://192.168.178.196/mutillidae/index.php?page=view-someones-blog.php Cookie: uid=3		FANCY=WATOBO:MjA6Mg==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MzA6Mw==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:NzA6Nw==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:NjA6Ng==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:NTA6NQ==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:NDA6NA==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:ODA6OA==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:OTA6OQ==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTAwOjEw:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTEwOjEx:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTIwOjEy:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTMwOjEz:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTUwOjE1:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTQwOjE0:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTcwOjE3:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTkwOjE5:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTgwOjE4:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTYwOjE2:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MjAwOjIw:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MDow:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
		FANCY=WATOBO:MTA6MQ==:pwned	HTTP/1.1 200 OK Date: Fri, 23 Jul 2010 10:3	
Start				
Request Options				
✓ Update Content-Length		•	1	
✓ Update Session Information				
🗆 Run Login		Save Matches		
ogs:	]			
7/23/2010 @ 12:33:41: Finished Fuzzing				
7/23/2010 @ 12:33:41: Finished Fuzzing 7/23/2010 @ 12:33:40: Started Fuzzing (20 Requests)				

Perfect !!!!!





# 4. Conclusion

WATOBO is a really awesome tool which doesn't need an installation and can be quickly adapted to new requirements. I think the semi-automated approach of WATOBO is the best way to perform an accurate audit and to identify most of the vulnerabilities.

The session management feature is totally leet and rarely found in free tools of this genre. Most of the functions are self explanatory and easy to perform which makes WATOBO an important tool in the pentester's arsenal. Since it's written in ruby you can add your own checks.

The implemented fuzzer is very valuable in exploring a web application and finding more information and vulnerabilities.

All these great features and functions make WATOBO one of the top free web assessment tools.

# 5. References

- [1] WATOBO Homepage (by Siberas) http://sourceforge.net/apps/mediawiki/watobo/index.php?title=Main\_Page
- [2] Mutillidae by Irongeek http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10
- [3] Damn Vulnerable Web App http://www.dvwa.co.uk/