

Watobo

Information Security Inc.



Contents

- About Watobo
- Features
- Testing Environment
- Installing Watobo
- Using Watobo
- References



About Watobo

• WATABO is a security tool for testing web applications. It is intended to enable security professionals to perform efficient (semi-automated) web application security audit





Features

- Powerful 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
- Can act as a transparent proxy (requires nfqueue)
- Vulnerability checks (SQLinjectin, XSS, LFI) out of the box
- Handles Anti-CSRF-/One-Time-Tokens

WATOBO - THE WEB APPLICATION TOOLBOX



Features

- 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.
- Smart filter functions, so you can find and navigate to the most interesting parts of the application easily.
- Is written in (FX) Ruby and enables you to easily define your own checks
- Runs on Windows, Linux, MacOS every OS supporting (FX) Ruby





Testing Environment

• Kali Linux 2017

root@kali2017: # cat /etc/*rel* DISTRIB_ID=Kali DISTRIB_CODENAME=kali-rolling DISTRIB_CODENAME=kali-rolling DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling" PRETTY_NAME="Kali GNU/Linux Rolling" NAME="Kali GNU/Linux" ID=kali VERSION="2017.2" VERSION_ID="2017.2" ID_LIKE=debian ANSI_COLOR="1;31" HOME_URL="http://www.kali.org/" SUPPORT_URL="http://forums.kali.org/" BUG_REPORT_URL="http://bugs.kali.org/"



Installing Watobo

• apt-get install watobo

root@kal12017: # apt-get install watobo
Reading package lists Done
Building dependency tree
Reading state information Done
The following additional packages will be installed:
libfox-1.6-0 libfxscintilla20 libnetfilter-queue1 racc ruby-childprocess ruby-fxruby ruby-jwt ruby-mechanize ruby-net-http-pipeline ruby-nfnetlink ruby-nfqueue ruby-ntlm ruby-selenium-webdriver ruby-webrobots ruby-websocket
The following NEW packages will be installed:
libfox-1.6-0 libfxscintilla20 libnetfilter-queue1 racc ruby-childprocess ruby-fxruby ruby-jwt ruby-mechanize ruby-net-http-pipeline ruby-nfnetlink ruby-nfqueue ruby-ntlm ruby-selenium-webdriver ruby-webrobots ruby-websocket watobo
0 upgraded, 16 newly installed, 0 to remove and 158 not upgraded.
Need to get 4,106 kB of archives.
After this operation, 23.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.pe.ip/Linux/packages/kali/kali kali-rolling/main amd64 libfox-1.6-0 amd64 1.6.55-1 [876 kB]



· Starting Watobo for the first time

coot@kali2017:-# watobo

W A T O B O - THE Web Application Toolbox brought to you by siberas http://www.siberas.de

creating WATOBO's working directory /root/.watobo.* create configuration directory '/root/.watobo/conf' ...

create temp directory '/root/.watobo/tmp' ...

created workspace folder /root/.watobo/workspace

uninitialized constant Watobo::Modules::Active::Ror when loading module file /usr/share/watobo/modules/active/RoR/cve_2013_015x.rb

uninitialized constant Watobo::Modules::Active::Sap::Business_objects when loading module file /usr/share/watobo/modules/active/sap/business_objects.rb ---

None generating certificate for /C=DE/O=WATOBO/OU=WATOBO CA/CN=Watobo >> create DH key ...

DONE

loading FXRuby ... this may take some time ... [OK]



Starting Watobo





Watobo Transcoder





• Watobo: create a new project => File > New/Open





Project Name

New Project	0
Workspace Directory: //root/.watobo/workspace	Change
Project Name: Project1	New
Cancel Back No	ext Finish



Session Name

Project: Project1		
Session Name: Session1	New	
Session1		
	Cancel Back Next Fini	sh



Watobo listens on port 8081

root@kali2017: # curl -I 127.0.0.1:8081 HTTP/1.1 555 Watobo Error WATOBO: Error Date: 2017-10-15 00:36:36 -0400 Content-Length: 0 Content-Type: text/html Connection: close



Configure browser proxy

indat proxy co	nfiguration:		
HTTP Pro <u>x</u> y:	127.0.0.1	Port:	8081
CCL Deserve	Use this proxy server for	or all protocols	0001
SS <u>L</u> Proxy:	127.0.0.1	Port:	8081
ETP Proxy:	127.0.0.1	Port:	8081
SO <u>C</u> KS Host:	127.0.0.1	Por <u>t</u> :	8081
<u>N</u> o Proxy for:	○ SOC <u>K</u> S v4 ⊙ SOCKS	<u>v</u> 5 □ Remote <u>D</u> NS	č
localhost,127.0			



Watobo Interceptor

			Bind	x x	Preferences	x +		Bing - Mozilla Firefox
			(+) ()	www.bing.com				c] Q
			All	Images Videos	Maps Nons	MSN Outlook com		the second s
					WATOBO by sib	eras (Version: 1.0.0)		000
File Settings Tools View	Winde	ow Help						
	Π							sibenas
Findings Sites	Shc 0/0	w: All / Hide	specific extension	5	Finding: Script-Parameters [Module: Passive::In_script_parameter] [Chat-ID: 14]			
Ulnerabilities		Metho	Host	Path	Parameters	Status Set-Cooki Comm	ient	Browser-View Fuzzer Manual Request
In Cooke Security (1) 호 (① Hinta R (집 Hinta R (집 Hinta	1 2 3 5 6 8 9 10 11 12 13 14 15 16 17 18 19	GET GET POST GET GET GET GET GET GET GET GET GET POST POST POST	www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com	fd/s/l fd/s/lp.aspx notifications/render notifications/render APImageArchive.aspx fd/s/lp.aspx th th th th th th fd/s/l fd/s/l fd/s/l fd/s/l fd/s/l fd/s/l fd/s/l fd/s/l fd/s/lp.aspx fd/s/lp.aspx fd/s/lp.aspx	IG=C69F1D9C39F <clentinsreque cClentInsReque ID-SERP.1006/i id=OPN.RTNews_ id=OPN.RTNews_ id=OPN.RTNews_ IG=C69F1D9C39F IG=C69F1D9C39F IG=C69F1D9C39F CG=C69F1D9C39F</clentinsreque 	2000 0K, SS-SID+ 2000 XA 0K, SS-SID+ 212240 0K, SS- 400 XA 0K, SS- 400 XA 0K, SS- 400 XA 0K, SS- 2000 0K, SS- 2140 XA 0K, SS- 2140		Text Instriction [SOM]
ab	19 20 21 22 23 24	POST POST POST POST POST POST	www.bing.com www.bing.com www.bing.com www.bing.com www.bing.com	topistip aspx (dijistip aspx) (dijistip aspx) (dijistip aspx) (dijistip aspx) (dijistip aspx) (dijistip aspx) (dijistip aspx) (dijistip aspx)	<clientinsreque <clientinsreque <clientinsreque <clientinsreque <clientinsreque< td=""><td>11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K</td><td></td><td>51228102) 5013.1'><img class="large" src="lac/bock
53.14.61/2-1.03.22m11 2<2.55.04.43-46.88-2.18.55
7027 305.2.88.23.78.62.03.23.317.2.0032/ "/>7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2022/ "></td></clientinsreque<></clientinsreque </clientinsreque </clientinsreque </clientinsreque 	11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K 11→4204 0K		51228102) 5013.1'> <img class="large" src="lac/bock
53.14.61/2-1.03.22m11 2<2.55.04.43-46.88-2.18.55
7027 305.2.88.23.78.62.03.23.317.2.0032/ "/> 7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.23.78.62.03.23.317.2.0032/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.78.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2.88.21.88.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">7027 305.2022/ ">



Watobo > send to SQLmap

inackyouraenmacroynum	31	GEI	www.bing.com	notifications/render	bnptrigger={"Partnerid 200 OK
Vulnerabilities	34	GET	www.bing.com	HPImageArchive.aspx	format-hp&idx=0&n=1200 OK
the billing	35	GET	www.bing.com	hpm	IID=SERP.1000&IG=C6200 OK
Hinds	36	GET	www.bing.com	th	id=ON.317CEBCD2DFA 200 OK
E Into	37	GET	www.bing.com	fd/ls/l	IG=C6AC33E5AA42423204 OK
🕀 🥘 Server Headers (38	GET	www.bing.com	hpm	IG=C6AC33E5AA42423200 OK
Forms (2)	39	GET	a4.bing.com	fd/ls/l	IG=C6AC33E5AA42423204 No
Hidden Fields (2)	40	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	41	POST	www.bing.com	fd/ls/lsp.aspx	1/5 0///01//////////////////////////////
	42	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK_EDGE_S=i
	43	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	44	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK_EDGE_S-i
	45	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK EDGE S-I
	46	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK_EDGE_S-i
	47	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK_EDGE_S-i
	48	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK_EDGE_S-i
	49	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	50	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK_EDGE_S=i
	51	GET	www.bing.com	AS/Suggestions	pt-page.home&mkt-ja200 OK _EDGE_S-i
	52	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	53	POST	www.bing.com	fd/ls/lsp.aspx	<clientinstrequest><e204 ok<="" td=""></e204></clientinstrequest>
	54	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK_EDGE_S=i
	55	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=r
	56	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	57	GET	www.bing.com	AS/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	58	GET	www.bing.com	A5/Suggestions	pt=page.home&mkt=ja200 OK _EDGE_S=i
	59	GET	www.bing.com	fd/ls/GLinkPing.aspx	IG=C6AC33E5AA42423200 OK
	60	POST	www.bing.com	fd/ls/lsp.aspx	<clientinstrequest><e204 ok<="" td=""></e204></clientinstrequest>
	61	GET	www.bing.com	search	q=hackyourselffirst&qs 200 OK
	62	GET	www.bing.com	fd/ls/l	IG-1415FACFB9684D0 204 OK
	63	POST	www.bing.com	fd/ls/lsp.aspx	<clientinstrequest><e204 ok<="" td=""></e204></clientinstrequest>
	64	POST	www.bing.com	fd/ls/GLinkPingPost.aspx	IG-1415FACFB9684D0 200 OK
	65	POST	www.bing.com	fd/ls/lsp.aspx	<clientinstrequest><e204 ok<="" td=""></e204></clientinstrequest>
	67	A GET	hackyourselffirst	.tr	200 OK ASP.NET_S
	68	A GET	hackyourselffirst	.tr Content/site	v=16KScglOON-KgjC5Bl200 OK
	69	A GET	hackyourselffirst	.tr bundles/bootstrap-carousel	v=rUr3jF-vnRJclo1RwL- 200 OK
	70	GET	hackyourselffirst	.trbundles/jqueryval	v=k09SZjRLUEvNZbFlw200 OK
	71	A GET	hackyourselffirst	.tr.bundles/bootstrap	v=NE-C7tK4A7Qr22gKp200 OK
	73	A GET	hackyourselffirst	.trbundles/jquery	v=yMmPM1TxecYcoWt(200 OK
	82	GET	hackyourselffirst	.trAccount/Login	200 OK
	and the second sec			Condition .	



Watobo > send to SQLmap

		SQI	LMap	00
qlmap path:	/usr/share/sqln	nap/sqlmap.py		
emp directory:	/root/.watobo/t	tmp/sqlmap		
Seneral				
Request				
Enter a test re	equest below or	use 'SEND TO -> SQLMap' fr	rom the conversation-table menu (i	right-click).
Referer: https Cookie: ASP.N Connection: c	Jage: en-US,en; s://hackyourselff VET_SessionId= lose	1=0.5 irs.troyhunt.com/ µtf3tuhyenthwlwi2emq455m	: VisitStart=10/15/2017 4:52:33 AM	; ARRAffinity=1d8f765t
•				<u>></u>
Technique:	JI	Risk: 3	▼ Level: 5	•
Manual Option	ns:			
				Cancel Start



• Watobo > send to SQLmap

sqlmap_1508043606.reg --level 5 --risk 3 --technique BE... 🖨 \otimes 1.1.10#stable [(]_|_|_|__,| http://sqlmap.org 1 17 [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon sible for any misuse or damage caused by this program [*] starting at 01:00:06 [01:00:06] [INFO] parsing HTTP request from '/root/.watobo/tmp/sglmap/sglmap_150 8043606.reg' [01:00:06] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST paramete rs through option '--data' do you want to try URI injections in the target URL itself? [Y/n/q]



References

• Kitploit

http://www.kitploit.com/2013/08/watobo-0913-web-application-toolbox.html

Kali Linux
 https://www.kali.org/downloads/

 fxruby https://github.com/larskanis/fxruby

