

# HackPra



# Burp Pro: Real-life tips & tricks

**Hamburg**

**22.08.2013**

**Nicolas Grégoire**

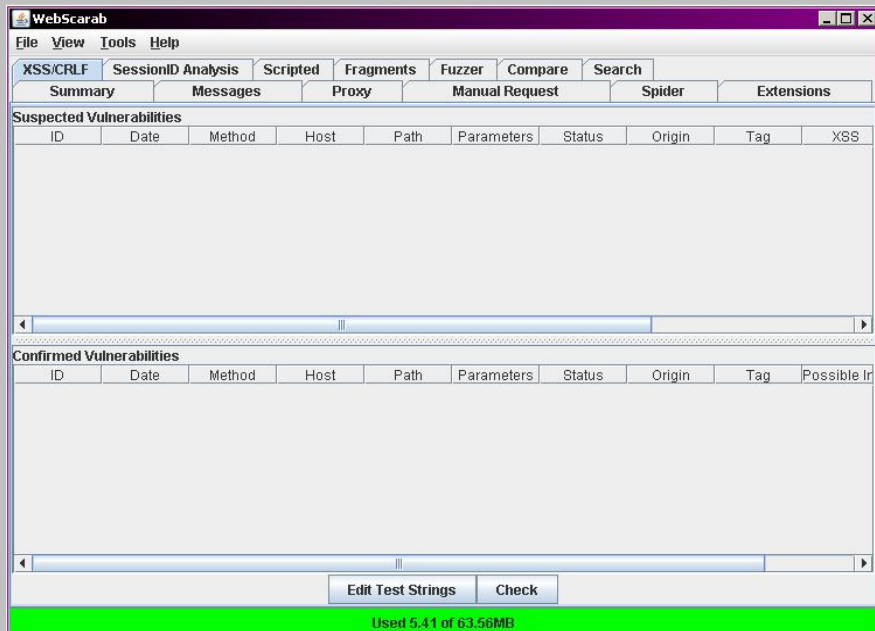
# ***Me & Myself***



**Founder & owner of Agarri**  
**Lot of Web PenTests**

**NOT affiliated with PortSwigger Ltd**

**Using Burp Suite for years**  
**And others proxies before**  
**Yes, I'm that old...**



# ***Warning***

**This is NOT about Web PenTesting methodologies**

**[http://danielmiessler.com/projects/webappsec\\_testing\\_resources/](http://danielmiessler.com/projects/webappsec_testing_resources/)**

**“Web Application Hacker's Handbook” 2nd Edition, Chapter 21**

**This is NOT “Burp 101”**

**[http://portswigger.net/burp/help/suite\\_gettingstarted.html](http://portswigger.net/burp/help/suite_gettingstarted.html)**

**<http://www.irongeek.com/i.php?page=videos/web-application-pen-testing-tutorials-with-mutillidae>**

**Everything was tested // v1.5.11 or v1.5.14**

# ***Pro vs. Free vs. Zap***

## **Burp Free:**

- no Scanner**
- speed limitations in Intruder**
- no save/restore feature**

## **Zap:**

- personal legacy: habits, extensions, ...**
- seems more buggy**

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Data visualization***

**By default**

**Via extensions**

# Parameters

Raw Params Headers Hex

POST  
/BurstingPipe/adServer.bs?cn=rsb&c=28&pli=7006784&PluID=0&w=300&h=250&ord=1766773863&ucm=true HTTP/1.1  
Host: bs.serving-sys.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:21.0) Gecko/20100101 Firefox/21.0  
Accept: \*/\*  
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://www.playboy.de/suche?suchwort=hack+in+paris  
Cookie:  
A3=RoqUeGMK0jQQ00001Sx6meS2VOiYB00001TVr2eUDN03BK00001QWLteG3S0iYB00001TRJMeSHH09Fb00001QPXYeFRo0iYB00002PyFeeGMK09ZX00000PaOxeG1B0hEp00000RqzleHyc0iYB00001Tz+5eSHH0g9Q00001QjVreHXn0GoR00000;  
B4=oSgI00000000000000000F IrdF70000000000000000Glpwb50000000000000000FNpEGn00000000000000000FMqx2A0000000000000000Ger98c0000000000000000Ggr2n10000000000000000GgoW7B00000000000000000FIp7vu00000000000000000FKpI6Q00000000000000000FKpzp.00000000000000000FH u2=e3ac62fe-7ca8-42f5-8811-cc68397b47c73T806g;  
C4=111=42; D1=x%3by%3bz  
Connection: keep-alive  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 470  
  
ncu=\$\$http://adclick.g.doubleclick.net/aclick?sa=L&ai=BGEJ2uRWyUfOtForK8APOp  
oCYDI6\_2s4FAAAAEAEgADgAWK7i-oJ6YPv58IL4CYIBF2NhLXB1YiOzNTU4NjUxNjIxODU5Njc  
2sgEOd3d3LnBsYXlib3kuZGW6AQlnZnBfaWlhZ2XIAQnaATJodHRwOi8vd3d3LnBsYXlib3kuZ  
8gGqAMB4AQBoAYf&num=0&sig=AOD64\_2Cdqstib3XwrFWJHjzCYpfJ9nzCA&client=ca-pub  
-3558651621859676&adurl=\$\$&body\_param=whatever



# *Parameters*

RawParamsHeadersHex

POST request to /BurstingPipe/adServer.bs

Type	Name	Value
URL	cn	rsb
URL	c	28
URL	pli	7006784
URL	PluID	0
URL	w	300
URL	h	250
URL	ord	1766773863
URL	ucm	true
Cookie	A3	RoqUeGMK0jQQ00001Sx6meS2V0iYB00001TVr2...
Cookie	B4	oSgl00000000000000000000FirdF700000000000000...
Cookie	u2	e3ac62fe-7ca8-42f5-8811-cc68397b47c73T806g
Cookie	C4	111=42
Cookie	D1	x;y;z
Body	ncu	\$\$http://adclick.g.doubleclick.net/aclick?sa=L
Body	ai	BGEJ2uRWyUfOtForK8AP0poCYDI6_2s4FAAAAEAE...
Body	num	0
Body	sig	AOD64_2Cdqstib3XwrFWJHjzCYpfj9nzCA
Body	client	ca-pub-3558651621859676
Body	adurl	\$\$
Body	body_param	whatever

AddRemoveUpDown

# KML

## Response

Raw

Headers

Hex

XML

```
<?xml version="1.0" encoding="utf-8"?><infos_diffusions total="4" nb="4"><diffusions
type="now"><diffusion debut="1370624400" utc="1370624400" chaine="france2"
bureau_regional=""><id_plurimedia>83157220</id_plurimedia><id_ftv>1718306</id_ftv><titre><![CDATA
[Mot de passe]]></titre><sous titre></date_heure><![CDATA[Vendredi 07 Juin à
19h00]]></date_heure><accroche><![CDATA[Associés à des personnalités, des candidats doivent
faire deviner un maximum de mots en un minimum de temps afin de décrocher 20 000
euros.]]></accroche><duree>28</duree><format><![CDATA[Autre]]></format><genre><![CDATA[Jeu]]></ge
nre><genre_simplifie><![CDATA[Jeu]]></genre_simplifie><nationalite/><signaletique_csa
code="TP"><![CDATA[Tous publics]]></signaletique_csa><image
url="/staticftv/ref_emissions/2013-06-07/COL_210451" format="jpg" lmt="1370588419"/><personne
id="205748" nom="Sabatier"
prenom="Patrick"><fonction>Présentateur</fonction></personne></diffusion></diffusions><diffusions
type="next"><diffusion debut="1370626080" utc="1370626080" chaine="france2"
bureau_regional=""><id_plurimedia>83157221</id_plurimedia><id_ftv>1707173</id_ftv><titre><![CDATA
[Météo 2]]></titre><sous titre></date_heure><![CDATA[Vendredi 07 Juin à
19h28]]></date_heure><accroche><![CDATA[]]></accroche><duree>2</duree><format><![CDATA[Autre]]></
format><genre><![CDATA[Météo]]></genre><genre_simplifie><![CDATA[Météo]]></genre_simplifie><natio
nalite/><signaletique_csa code="TP"><![CDATA[Tous
publics]]></signaletique_csa><image/></diffusion></diffusions><diffusions
type="prime1"><diffusion debut="1370630700" utc="1370630700" chaine="france2"
bureau_regional=""><id_plurimedia>83094226</id_plurimedia><id_ftv>1718311</id_ftv><titre><![CDATA
[Tango]]></titre><sous titre><![CDATA[Le coup du
lapin]]></sous titre><date_heure><![CDATA[Vendredi 07 Juin à
20h45]]></date_heure><accroche><![CDATA[Joana Larsen et son supérieur, le capitaine Sauvage, se
rendent à la morgue. Leur ami Salma, légiste, a signalé la disparition d'un corps arrivé la
veille. Il s'agissait de la dépouille de Nadia, décédée dans un accident de voiture maquillé. La
mort troublante de la victime éveille immédiatement les soupçons de Sauvage, qui découvre
bientôt que le cadavre en question était celui d'une autre. Pourquoi cette substitution ? Qu'est
devenue cette Nadia ? En enquêtant, les deux collègues découvrent que la jeune femme avait
```

# XML

```
Raw Headers Hex XML
<?xml version="1.0" encoding="utf-8"?>
<infos_diffusions total="4" nb="4">
  <diffusions type="now">
    <diffusion debut="1370624400" utc="1370624400" chaine="france2" bureau_regional="">
      <id_plurimedia>83157220</id_plurimedia>
      <id_ftv>1718306</id_ftv>
      <titre><![CDATA[Mot de passe]]></titre>
      <soustitre/>
      <date_heure><![CDATA[Vendredi 07 Juin à 19h00]]></date_heure>
      <accroche><![CDATA[Associés à des personnalités, des candidats doivent faire deviner un
maximum de mots en un minimum de temps afin de décrocher 20 000 euros.]]></accroche>
      <duree>28</duree>
      <format><![CDATA[Autre]]></format>
      <genre><![CDATA[Jeu]]></genre>
      <genre_simplifie><![CDATA[Jeu]]></genre_simplifie>
      <nationalite/>
      <signaletique_csa code="TP"><![CDATA[Tous publics]]></signaletique_csa>
      <image url="/staticftv/ref_emissions/2013-06-07/COL_210451" format="jpg" lmt="1370588419"/>
      <personne id="205748" nom="Sabatier" prenom="Patrick">
        <fonction>Présentateur</fonction>
      </personne>
    </diffusion>
  </diffusions>
  <diffusions type="next">
    <diffusion debut="1370626080" utc="1370626080" chaine="france2" bureau_regional="">
      <id_plurimedia>83157221</id_plurimedia>
      <id_ftv>1707173</id_ftv>
      <titre><![CDATA[Météo 2]]></titre>
```

# AMF

Raw

Headers

Hex

AMF

```
POST /gateway/helloworld HTTP/1.1
Accept-Encoding: identity
Content-Length: 73
Host: demo.pyamf.org
Content-Type: application/x-amf
Connection: close
User-Agent: PyAMF/0.6.1
```

```
         echo.echo  /1      
        (This is your typical "Hello world!" demo
```

?

<

+

>

|

0 mat

## Response

Raw

Headers


Hex

AMF


```
HTTP/1.1 200 OK
Date: Sat, 15 Jun 2013 10:13:40 GMT
Server: Apache/2.2.11 (Ubuntu) DAV/2 SVN/1.6.9 PHP/5.2.6-3ubuntu4.6 with Suhosin-Patch
mod_ssl/2.2.11 OpenSSL/0.9.8g mod_wsgi/3.2 Python/2.6.4
Content-Length: 72
Connection: close
Content-Type: application/x-amf
```

```
          /1/onResult  null          (This is your typical "Hello world!" demo
```

# AMF

Raw Headers Hex AMF			
	Type	Value	
▼  body			
a target	string	echo.echo	
a response	string	/1	
a response method	string	echo.echo	
▼ [] data	array		
a [0]	string	This is your typical "Hello world!" demo	

## Response

Raw Headers Hex AMF			
	Type	Value	
▼  body			
a target	string	/1/onResult	
a response	string	null	
a response method	string	onResult	
a data	string	This is your typical "Hello world!" demo	



# ViewState

Request		Response
Raw	Headers	HexHTMLRenderViewState
		<pre>&lt;input type="hidden" name="__ctl00_QsfStyleSheetManager_TSSM" id="__ctl00_QsfStyleSheetManager_TSSM" value="" /&gt; &lt;input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" /&gt; &lt;input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" /&gt; &lt;input type="hidden" name="__LASTFOCUS" id="__LASTFOCUS" value="" /&gt; &lt;input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPMu0uAAEAAAD/////AQAAAAAAAAAMAgAAAFdUZWxlcmlrL1l1Y1V5SSwgVmVmc2lwbj0yMDEzLjIuNjExLjQwLkBDdWx0dXJlPW5ldXRyYWwzIFB1YmtpY0t1eVRva2VuPTEyMWZhZTc2MTY1Ym1ZERhdGEHAgIAAAAJAwAAAAADAAARRYAAALsvQdgHEmWJSYhbcP7f0r1StfgdKIGgATJNiQQBDswYjN5pLshW1HiymrKoHKZVZ1XWYWMQZtnb233nvvvffee++997o7nu4n99//PlxmZAFs9s5K2smeIYCC HhJf+fPdn5y/ft89zvNT3317Bf9Pr/3/E22V66/Wvzk+qc+/8nr7Lv3lxm9++2Ln/zB7Nt181M/8dWLn/q8/MH083fz/MlqPdm7X3659xMC88LBfPlsVZ1/+yeePTmdEYxXb3/q+Oz2072f+07J57/PS8H14K mnz9rqf9yev3w+vf57iv5/PPd+WTxbP1Tv/fZ5U99u6Tx7K5+HxrH9Ns/uNTi7KZOVimez+5M/u8XP/UvS8uaWyL3+f3/kn6/MUPni+e/WD67Yu7029/h979yZ+ePdldThfl1W8GLxnZxcEC4nh7/xDGN7SfC +OAtufHF199Z7pXNtnlkx9grgrGNz+1PaJufyE9OX/xguvOi+X1+7xc/ePL6J99N936fnvnu2cX0936xeP7dF5eT5avryd4VfUa/F0/4+5+6953VT52Abg/X3754dX72ky9o7N/B3D19enXw3eP5wcmTn3j1be fXGA+ysvJT+/sPP/p4/UX0/tX10bpLlvvdmZEr5ffvV/Ofu9XNL9XzdmzJ7u/D97bacv8J19dEl3XL79L/L13uvv7/OCrvS/evP3Bi8+/uvry6dunX1zv7x1+IrxzPwHNPgd/9PL44eyK4ngmun1/kJ7sH8lef mpvvmO+u3r2k/zdwbPj6vjpTz2xcM6fvGukOemT7CeIneg5P3min33x5cFNZ09+4vc6Pt77CcgH4fv7fP7tq+1EGj05/u5b+oeeb19d6GdPj3/yK/PZVycXxy/eAn/ig+8+mr98u4/zwdmPcPORrj/C9Ue4/i 7Szanf17Oyt+nuP+Tr18H9uP6i6enP3j+02frfz99+u75T//E+9mRN6fXX3z3p+Y/9Wa6/8Wb34e+P/3BTz39ie8+X/w+178WzS9ekT386smTr77T/D6w9cdkc6zt/MmTyePyC8QX+dD4D/dEfhvvvuT09PF w8aH3ms5CuQzxn28fmrxcPrn/q9X+yIX/RB4zh9tftfuclYXwNfPgP9XH4T/8c58nn83gP309ePf7ou9kF4P9M5NzxE/jNk91e75Qz+I/t1HwT/99rAU53vQKdL6LTyduHpBHKn/6pN2dXXzydBWPgfkey9E lXfTbFC/p6dBv2+y77b+6nf+zvBmIfaEH5ffBi92y9J9zaTvYcdPeh9Tvz19Cc+iF9Pv0Is1Jfj+Qz02/8g+g0pKK75vZ80PxxK8ucEn+M9xv8D5Y1g7fzUd39qNVmUox2d0EmOxjM//tDx7E6WL8quXv3c iFrtkfzD7RHP/1TK4pp5x17/t2MbNHVw/PyEx8In3ybnz676sd/vX/qu2fXXzd+H2aPKENS/j5vv9PMvvuTod3wPqe+V/th8j7/vS1f9H2yb/aDF+Hen/Ok5yke3pv+YGZzQcfK7YGPesF9fv577/bf/D57pG 7iB/1B08/1Pd3xK7+50cPd3+fvYvzk735W/GPz1hGAr+H35tRzuOn5vA/v33VLrv9Wb+G2/7U5+TnltN7PxGDK74Ij+XVtydE04LXw5/9jFdo8+Ls9/m938bgqL9wQHkr93ukXWjBgh9V4DvG+g9t9BR9/F5v /9UOZ3HxuHsGpp+svOQ8pDvLic0lth8sk2S+UR/0XFZe8Nz+1PUbvqdg8v1X0fkKbA03X73JKPdI4lrTz/sD8EX/C/+9oZzXD37q947yn9PXjPPMxmFRPujoY9Cj/1kEH9WrTD/76yd6EdpZ36PtLP67CvMSk se/Lku0TrH2TffUgxKXjyi/UXxT71Nk/XL54eN2enNG/ffrU7XXz1cLL4yV3SSfPJyRVmifRh+dOv937yPumo+qe+u/+Qcv/vKMOuX/zg4t2Ln/7J4vd58+Ltiye/z/VPcdzx+E+dPj1l/vHhRU05yjhwbMMX LZ1+pTm3saKycic27tqgWZ3sgrN319KK6Vsdm4h0XczFe9neBc61+1Hvo1ZMTht19Xh+idT2ceW3xPHL4DuvOLeExj5+Kzdz761Tru1P/Q3rz6ZNXTW9J9Dz04W4DvFIYb97ff3PvJHJZqPS9U5nn7Vtm68Q/005F 4rgy795niYnzCjXr05Jm7zPoG5of9gXM74rd7+3hS37nd+z8+zpV2/4+ru3NovT44q31N7/9FdYdf+Li+esn382++5P3vrqHdbGvLt7ce7JDTm6VL57tQAcKb5t1L/9n4Pf+opefn33yleLZ2ldYu3p6dfn7 Av3Z89eXzP10Sf2F1+9/PzValY8oX53CvrsB78P4TD9NqIH7u3TWht4310+cn17J0nPIEB+4uX3z62v/P/n72qst/7i4uf+r3nc+bl1+QdfneXlu2ekL54tvtNT9J21wddPYEt47e079764mC3Kokbrf8iV0r b/gRoUQdnn2b4hzyLUA/+p10HfWzmF7MPp+XZ6e6fkx8910/9+y14nRfOu+KcN/Jf2Ln97L9njzZmVw/WZBP/wNqc4/ktIF489niK4H1+e416e8L9nvufYdiq/s0Z5jHU/r+QNP8+8n8p/+a+usA6JXTu5MTS o2x4P30//Jb5dY051PPn936PbBcFhP/+M1pvPngV0uZwsqO3n0C27P31+Z9Zi31Fb+p101e9zj+ewOfv8/uX5AnWk+dEoDvKZ3fHw989L568IR+dYvqyBc8QjciuzKozPPEPPw+350RzRgHQydau96/oP S2c+i/8CTX9H4y8uZ9unN2U5GPEf8VGafPyMee3gd5a2n74qXbyP89Y21P2gLRJ9PSTZJfzOvvpz87SfKkZTTva8Onu+9/YRwXp9m3F5Szy4ntxjXv1Bxrh8dfftWAd+Db45U17054bmUcbJa/MBLb796pL/ 6Iz/+RXy7p1yMfKA/3ePwk/6FP6b1WxTIsnRU5jy0iXOLm9X1JmFAoe+mrvIfmWNJeaWTKn8/H57B16oTpeivDb/am9iwwM6U/85IufeP72/rOfPdm+fr68uPzi+V6+kdmphWtoeUX8MKvIT72QeSD9E9cfsK 4cDppPidZuYKSe+330Afm+/e5R+TtsNUNLBegOfTc5XQpvaA0em9q8B0sL2Kq1tRUnD69eWh30zvOuePwE+Q9zGe+zGraNaEv89+ynaczkK/yEwesHOAUeL/TwnO3R8gvSrfRu3L2+TvKzVksKPNv1357wf24 XtsD69gvl93f3v5uPiWd8Pw4GPP9z8ivn+ztXBD/rmai61uy7xV8mp8kntR9a/1NbOE20HywxBPgxf8ehyQX0vrVfDFiA+ha5YsOyuKsOhnoNttxv37/N4/ObW9KONysniGvNRb0sVfZ28/hG1bkGzzGiR9L3 pitWX115tvIk9w0/19ZHL4yNme7tWuaV05/2caVxv6fTa9g2GvzMpUuo136kOhjT5zIetUH3CAei9U+J/v/ps20aZ/GygG58t2zshP9uMkeeW25xeCW2+utK2pbtJ3havfN3tdCvShuRPN7/P711i/JCVS/h1 31LPp7POHMqcyJLj/5A+ePue8Secy/+3CX3pvT/CF2g3YhTcA/ogu50/MiQ6/z8OzxXnn9u3jT59fP7w3uzcl27k/z7RZ0eS5q2ZnjcyWf8Hf3+e7q31+8pD55fnvdf8mDnj1+YLBBPzf8f8r8MX9av 370068CcenpHMs0747k+OgEk66hr6n8ZtflFigy7+qck92JpnNIEIFX/iYvJdt1872e/9hOAr+IZi2jP4ZNdif4j/wX07U+H3IHYhOOFjZz1GdPpplukqk5A9yo9wxOn788znIS6ksS9dQZ95PAY7R3hBrz/8 b/Deh3rIeTzEYDvyc5PeF+9Q5yfl579YPrtiw7e8v+MBq5NL446Zyf+rczw+ffvp1/+Sm1UdMfPL8+Q1Z/71L54xP3S1BL8//e5x+e+1fLPJ6/u013vX2Hev73+bb6M96efv30H/+31i59sJ1/dKOnP/2 M9/3E+ouT/avnP/1+eb7f56en936fL50y/e/D7vvnz3BdmN4/Ov33Knb+bnre3d6EknQou++W/O+xdXfTcKNWEZ/emeH+pC+Tp48RT4PtvE10ZxyPCTTVw2yt78P3tctpy/wN11SP15++d2zey/2Tnd/nx9E z7XuH25xf0VwYe++X2u7z//qd+7FN/1J5/MyUe++KLO5r5EPA79R7747/3ip01GKU4+I3x/in190g8PXwgNaXxXFz9xj9aCvv2T1z/1ZpfG1/f3rHmOrMp38d4L9PXVZK8tJz+9W7z4wWz+4rtf7L746dP7X/ xT95GD0E04bF92PnV58/Iz2+/u5ua/mZfCr2W39Ymvf82c9d37+38COnTanP/ye8tNDn+idPPWdkf66fK5G/V16xbF/8ps+Y5fdo7WlvuTXZYa28+ffHKJacBHz+BovaT569JntHdvEn3/7eua+Sza9w6 118++pJ9V00bV/r4yfHr36fk3DNqjPwOeHO5/tv37NcU750+TL/gYmTj8J/3OnPH3y61XYtznovt/rrI+9cJH9TRBHi677uAXu80FvUJq1X8u92wL+Ref4oygcc/8ZNRf4/ep9z22fonv3q7R173J81/Iv mX11j3zXon7Q8dfGVx1P1ubvvvPh0H3707fvZ5Gf/u955f3KpILc5v9xyVfA03pUeFPXVybPTUC72VZpY2XdlciREZNXnjmldG6lvb1Zpd2VyyE11bHrUgFgnZURlbW9SZXNvdXJjZXXNDb250ZWS0BSJjdGwMCRDb2R1Vm11 GNOBdAwJGNOBdAzJGNOBdAXJFbH22VTAxp1Q29tYm9Cb3gPFCsAAgUCNTAFajUwZAVFY3RsMDAk2Q9udGvudFbsYWN1SG9sZGVyMSRYSWRHcm1kMSRjdGwWMCRjdGwWMiRjdGwWMCRQYwIdU216ZUNvbWJvQm AAxQrAAJkFwQFB18hRfNjQwLYBAU1XyFQQ291bnQCCDAULXyFJdGVtQ291bnQCCMgUJQ3VycmVudFbH22VJbmR1eGYWAh4D3XN1FgIeA19jZmRkBR1jdGwWMCRtA21uQ2hvb3N1c1RTA21uQ2hvb3N1c1cg8UKwAC &lt;/div&gt;</pre>

# ViewState

RequestResponse

RawHeadersHexHTMLRenderViewState

▼ ViewState v2.0 compatible [MAC enabled]

▼ Pair

object    ☐    yyyy☐    ☐    W Telerik.Web.UI, Version=2013.2.611.40, Culture=neutral, PublicKeyToken=121fae78165ba3d4☐☐

▼ Hashtable

name=value    \_\_ControlsRequirePostBackKey\_\_ = [ctl00\$QsfFromDecorator, ctl00\$SliderControlList\$ControlsSiteMap, ctl00\$HeaderControl\$Der

name=value    ctl00\$ContentPlaceHolder1\$RadGrid1\$ctl00\$ctl03\$ctl01\$PageSizeComboBox = pair:[array of Object,null]

name=value    ctl00\$ContentPlaceHolder1\$RadGrid1\$ctl00\$ctl02\$ctl00\$PageSizeComboBox = pair:[array of Object,null]

name=value    ctl00\$ContentPlaceHolder1\$RadGrid1\$ctl00 = pair:[array of Object,null]

name=value    ctl00\$SkinChooser\$SkinChooser = pair:[array of Object,null]

0	ff	01	0f	32	ed	2e	00	01	00
1	00	00	00	00	00	00	00	0c	02
2	65	72	69	6b	2e	57	65	62	2e
3	73	69	6f	6e	3d	32	30	31	33
4	34	30	2c	20	43	75	6c	74	75
5	72	61	6c	2c	20	50	75	62	6c
6	6b	65	6e	3d	31	32	31	66	61

# ***Data visualization***

**By default**

**Via extensions**



# JSON

# http://api.twitter.com/1/statuses/user\_timeline.json

Raw Headers Hex JSON Decoder

HTTP/1.1 200 OK  
cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0  
content-length: 30764  
content-type: application/json; charset=utf-8  
date: Fri, 07 Jun 2013 16:47:36 GMT  
expires: Tue, 31 Mar 1981 05:00:00 GMT  
last-modified: Fri, 07 Jun 2013 16:47:36 GMT  
pragma: no-cache  
server: tfe  
set-cookie: guest\_id=v1%3A137062365676699843; Domain=.twitter.com; Path=/; Expires=Sun, 03 Jun 2013 16:47:36 GMT  
status: 200 OK  
x-content-type-options: nosniff  
x-frame-options: SAMEORIGIN  
x-ratelimit-class: api  
x-ratelimit-limit: 150  
x-ratelimit-remaining: 149  
x-ratelimit-reset: 1370627256  
x-transaction: 4d10c3d6f668b0fb  
x-xss-protection: 1; mode=block  
Connection: close

[{"created\_at": "Fri Jun 07 10:05:07 +0000 2013", "id": 342945306469597185, "id\_str": "342945306469597185", "text": "According to the docs. http://t.co/YW5elhSudV http://t.co/aAQ\u0026", "source": "webOS\u003c/a\u003e", "truncated": false, "in\_reply\_to\_status\_id": null, "in\_reply\_to\_status\_id\_str": null, "in\_reply\_to\_user\_id": 11, "in\_reply\_to\_user\_id\_str": "292234592", "user": {"id": 292234592, "id\_str": "292234592", "name": "Nicolas Gr\u00e9goire", "screen\_name": "nicolasg", "location": "Earth", "url": "http://www.agarri.com/", "description": "Owner of Agarri, a small XSLT", "protected": false, "followers\_count": 1170, "friends\_count": 335, "listed\_count": 2011, "favourites\_count": 6, "utc\_offset": 3600, "time\_zone": "Paris", "geo\_enabled": false, "profile\_background\_color": "131516", "profile\_background\_image\_url": "http://a0.twimg.com/themes/theme14/bg.gif", "profile\_background\_tile": true, "profile\_image\_url": "https://si0.twimg.com/profile\_images/1413753531/small\_sstic11\_normal.png", "profile\_text\_color": "333333", "profile\_use\_background\_image": true, "default\_profile": false, "coordinates": null, "place": null, "contributors": null, "retweeted\_status": {"created\_at": "Fri Jun 07 10:05:07 +0000 2013", "id": 342766988554289152, "id\_str": "342766988554289152", "text": "This is your http://t.co/aAQsZEVqpZ", "source": "\u003c a href=\"http://www.tweetdeck.com\""}]

# ***JSON***

**json.dumps(json.loads(msg), indent=4)**

**<http://128nops.blogspot.com/2013/02/json-decoder.html>**

```
Raw Headers Hex JSON Decoder
[
  {
    "contributors": null,
    "coordinates": null,
    "created_at": "Fri Jun 07 10:05:07 +0000 2013",
    "favorite_count": 0,
    "favorited": false,
    "geo": null,
    "id": 342945306469597185,
    "id_str": "342945306469597185",
    "in_reply_to_screen_name": null,
    "in_reply_to_status_id": null,
    "in_reply_to_status_id_str": null,
    "in_reply_to_user_id": null,
    "in_reply_to_user_id_str": null,
    "lang": "en",
    "place": null,
    "possibly_sensitive": false,
    "retweet_count": 168,
    "retweeted": false,
    "retweeted_status": {
      "contributors": null,
      "coordinates": null,
      "created_at": "Thu Jun 06 22:16:33 +0000 2013",
      "favorite_count": 42,
      "favorited": false,
      "geo": null,
      "id": 342766988554289152,
      "id_str": "342766988554289152",
      "in_reply_to_screen_name": null,
      "in_reply_to_status_id": null,
      "in_reply_to_status_id_str": null,
      "in_reply_to_user_id": null,
```

# JavaScript

Request		Response	
Raw	Headers	Hex	JavaScript
HTTP/1.1 200 OK Date: Fri, 07 Jun 2013 12:49:56 GMT Server: Apache Last-Modified: Thu, 22 Mar 2012 12:30:02 GMT ETag: "197407f-172a-4bbd41125e680" Accept-Ranges: bytes Content-Length: 5930 Connection: close Content-Type: application/x-javascript X-Pad: avoid browser bug			
<pre>function wp_cirrus_gwt(){var O='',vb="" for "gwt:onLoadErrorFn",tb="" for "gwt:onPropertyErrorFn",hb=""&gt;&lt;/script&gt;',Y='#',Yb='.cache.html',\$='/',Rb='19CF2CFAEA361BC9322AB6BA0 049A1EC',Sb='1A432AC32F64235633E7D122787AC882',Tb='5002B6412ABD5B4C8F6F8D56590FC449',Ub='55860FE4F948 701465AE6303D5E1503D',Xb=':',nb='::',\$b='&lt;script defer="defer"&gt;wp_cirrus_gwt.onInjectionDone(\'wp_cirrus_gwt\')&lt;/script&gt;',gb='&lt;script id="",qb='',Z='?',Eb='ActiveXObject',sb='Bad handler "',Fb='ChromeTab.ChromeFrame',Zb='DOMContentLoaded',Vb='F797846EE06A281B237C60BF95CD2CA3',Wb='FF0F5B4 5604CEA0EA47B4C76C6F91E3D',ib='SCRIPT',fb='__gwt_marker_wp_cirrus_gwt',jb='base',bb='baseUrl',S='begi n',R='bootstrap',Db='chromeiframe',ab='clear.cache.gif',pb='content',X='end',Lb='gecko',Mb='gecko1_8', T='gwt.codesvr',U='gwt.hosted',V='gwt.hybrid',wb='gwt:onLoadErrorFn',rb='gwt:onPropertyErrorFn',ob= 'gwt:property',Pb='hosted.html?wp_cirrus_gwt',Kb='ie6',Jb='ie8',Ib='ie9',wb='iframe',_='img',xb="java script:''",Ob='loadExternalRefs',Kb='meta',zb='moduleRequested',W='moduleStartup',Hb='msie',lb='name' ='undefined',Nb='unknown',Ab='user.agent',Cb='webkit',P='wp_cirrus_gwt',db='wp_cirrus_gwt.nocache.js' ,nb='wp_cirrus_gwt::';var l=window,m=document,n=1.__gwtStatsEvent?function(a){return 1.__gwtStatsEvent(a):null,o=1.__gwtStatsSessionId?1.__gwtStatsSessionId:null,p,q,r,s=0,t={},u=[],v=[ ],w=[],x=0,y,z;n&amp;&amp;n({moduleName:P,sessionId:o,subSystem:Q,evtGroup:R,millis:(new Date).getTime(),type:S});if(!1.__gwt_stylesLoaded){1.__gwt_stylesLoaded={}}if(!1.__gwt_scriptsLoaded) {1.__gwt_scriptsLoaded={}}function A(){var b=false;try{var c=l.location.search;return (c.indexOf(T)!=-1  c.indexOf(U)!=-1  l.external&amp;&amp;l.external.gwtOnLoad)}&amp;&amp;c.indexOf(V)==-1}catch(a){} A=function(){return b};return b} function B(){if(p&amp;&amp;q){var b=m.getElementById(P);var c=b.contentWindow;if(A()){c.__gwt_getProperty=function(a){return G(a)}}wp_cirrus_gwt=null;c.gwtOnLoad(y,P,s,x);n&amp;&amp;n({moduleName:P,sessionId:o,subSystem:Q,evtGroup:W,m</pre>			

# ***Javascript***

**Both beautifier extensions use  
libs from jsbeautifier.org**

**burp-suite-beautifier-extension  
Uses Rhino to call Javascript from Java**

**<http://code.google.com/p/burp-suite-beautifier-extension/>**



**burp\_jsbeautifier  
Much cleaner, uses the Python library**

**[https://github.com/Meatballs1/burp\\_jsbeautifier](https://github.com/Meatballs1/burp_jsbeautifier)**



# *JavaScript*

Request		Response	
Raw	Headers	Hex	JavaScript
<pre>function wp_cirrus_gwt() {   var O = '',       vb = '" for "gwt:onLoadErrorFn"',       tb = '" for "gwt:onPropertyErrorFn"',       hb = '&gt;&lt;\\script&gt;',       Y = '#',       Yb = '.cache.html',       \$ = '/',       Rb = '19CF2CFAEA361BC9322AB6BA0049A1EC',       Sb = '1A432AC32F64235633E7D122787AC882',       Tb = '5002B6412A8D5B4C8F6F8D56590FC449',       Ub = '55860FE4F948701465AE6303D5E1503D',       Xb = ':',       nb = '::',       \$b = '&lt;script defer="defer"&gt;wp_cirrus_gwt.onInjectionDone(\\wp_cirrus_gwt\\)&lt;\\script&gt;',       gb = '&lt;script id="',       qb = '=',       Z = '?',       Eb = 'ActiveXObject',       sb = 'Bad handler "',       Fb = 'ChromeTab.ChromeFrame',       Zb = 'DOMContentLoaded',       Vb = 'F797846EEO6A281B237C60BF95CD2CA3',       Wb = 'FFOF5B45604CEAOEA47B4C76C6F91E3D',       ib = 'SCRIPT',       fb = '__gwt_marker_wp_cirrus_gwt',       jb = 'base',       bb = 'baseUrl',       S = 'begin',       R = 'bootstrap',       Db = 'chromeiframe',       ab = 'clear.cache.gif',       pb = 'content',       X = 'end',</pre>			

# ***Protobuf***

**“Google Protocol Buffers”**

<https://code.google.com/p/protobuf/>

**Decodes Protobuf messages**

**Allows tampering if a “.proto” file is provided**

<https://github.com/mwielgoszewski/burp-protobuf-decoder>

Raw	Params	Headers	Hex	Protobuf
<pre>name: "Johnny Eat Rockets" id: 3 email: "johnny.rockets@example.com" phone {   number: "555-555-0DAY" }</pre>				

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***GUI navigation***

**Contextual buttons**

**Hotkeys**

**Auto-scroll in Proxy / History**

**Custom payload lists**

**Personalized scans**



# *Contextual buttons*



## Temporary Files Location



These settings let you configure where up.

☒ Use default system temp directory

☐ Use custom location:



**RTFM**



**Restore defaults**



## Spider Scope



☒ Use suite scope [defined in Target tab]

☐ Use custom scope



## Payload Sets

You can define one or more payload sets. T tab. Various payload types are available for

Payload set:

Payload type:

Request to <http://www.google.com:80> [173.194.78.105]

Forward

Drop

Intercept...

Action

[Comment this item](#)



# Hotkeys

Target

Intruder

Repeater

Proxy

Sequencer

Decoder

Spider

Comparer

Extender

Scanner

Options

Alerts

Connections

HTTP

SSL

Sessions

Display

Misc

?

Hotkeys

↺

These settings let you configure hotkeys for common actions. These include item-specific actions such as "Send to Repeater", global actions such as "Switch to Proxy", and in-editor actions such as "Cut" and "Undo".

Action	Hotkey
Send to Repeater	Ctrl+R
Send to Intruder	Ctrl+I
Forward intercepted Proxy message	Ctrl+F
Toggle Proxy interception	Ctrl+T
Issue Repeater request	Ctrl+G
Switch to Target	Ctrl+Shift+T
Switch to Proxy	Ctrl+Shift+P

Edit hotkeys

# ***Hotkeys***

## **Classic:**

**Ctrl+X|C|V for “Cut|Copy|Paste”**

## **Decoding:**

**Ctrl+(Shift)+U|H|B for “URL|HTML|Base64 (de)code”**

## **Navigating to another tab:**

**Ctrl+Shift+T|P|S|I|R for “Switching to ...”**

## **Personal favorite:**

**Ctrl+G for “Issue Repeater request”**

# *History auto-scroll*

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparer

InterceptHistoryOptions

Filter: Showing all items

#	Host	Method	URL	Params
94	http://192.168.2.66	GET	/favicon.ico	<input type="checkbox"/>
93	http://192.168.2.66	GET	/	<input type="checkbox"/>
92	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/`true`	<input type="checkbox"/>
91	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/`false`	<input type="checkbox"/>
90	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/"`false`"	<input type="checkbox"/>
89	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/`true`	<input type="checkbox"/>
88	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/`false`	<input type="checkbox"/>
87	http://192.168.2.66	GET	/AdbeRdr1014_fr_FR.exe/"`true`"	<input type="checkbox"/>

# *Custom payload lists*

**Some payload lists are shipped with Burp  
Configurable from the Intruder menu**

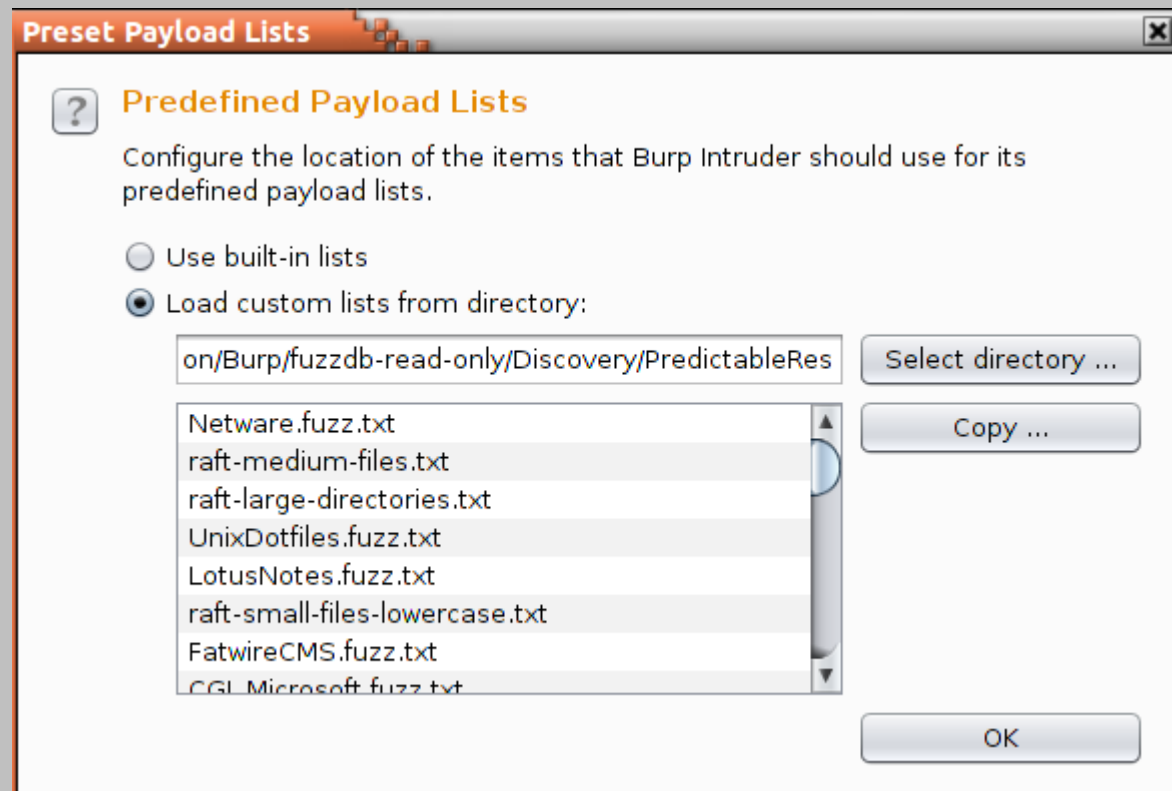
**Magic combo:**

**Burp**

**Nikto**

**DirBuster**

**FuzzDB (+)**



# ***Personalized scans***

**Define your own insertion points in Intruder**  
**Then right-click and select “Actively scan ...”**

Target

Positions

Payloads

Options

?

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type

Attack type:

GET /foo?a=xxxx&id=\$666\$&c=foobar HTTP/1.1  
Host: vulnhost  
Cookie: sessid=azerty123456789

Send to Repeater Ctrl+R

Actively scan defined insertion points

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Managing state***

**Automatic backups**

**Saving & restoring state**



# ***Automatic backups***

**Hacking is immersive**

**You WILL forget to use “Save state”**

**Of course, Murphy's Law applies ;-)**

```
An unexpected error has been detected by Java Runtime Environment:
```

```
EXCEPTION_ACCESS_VIOLATION (0xc0000005) at pc=0x7c918fea, pid=3768, tid=2664
```

```
Java VM: Java HotSpot(TM) Client VM (1.6.0_03-b05 mixed mode)
```

```
Problematic frame:
```



```
C [ntdll.dll+0x18fea]
```

```
An error report file with more information is saved as hs_err_pid3768.log
```

# ***Automatic backups***

Target		Proxy		Spider		Scanner	
Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts

Connections	HTTP	SSL	Sessions	Display	Misc
<div> <b>Automatic Backup</b></div> <div> The automatic backup feature can be used to save a copy of Burp's state periodically in the background, and on exit.</div> <div><input checked="" type="checkbox"/> Automatically backup state every <input type="text" value="30"/> minutes</div> <div>To folder: <input type="text" value="/home/nicob/Confs/2013/HackPra"/> <input type="button" value="Choose folder ..."/></div> <div><input checked="" type="checkbox"/> Include in-scope items only</div> <div><input checked="" type="checkbox"/> Backup on exit</div>					

# ***Save & restore state***

**Complementary to automatic backups**

**Can also be used to**

**Export to your customers**

**Define your own defaults**

**Hotkeys / Automatic backups / Scope**

**Display all items in “Site map” and “Proxy history”**

**Custom payloads lists**

**Extensions options - *buggy***

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Common tasks***

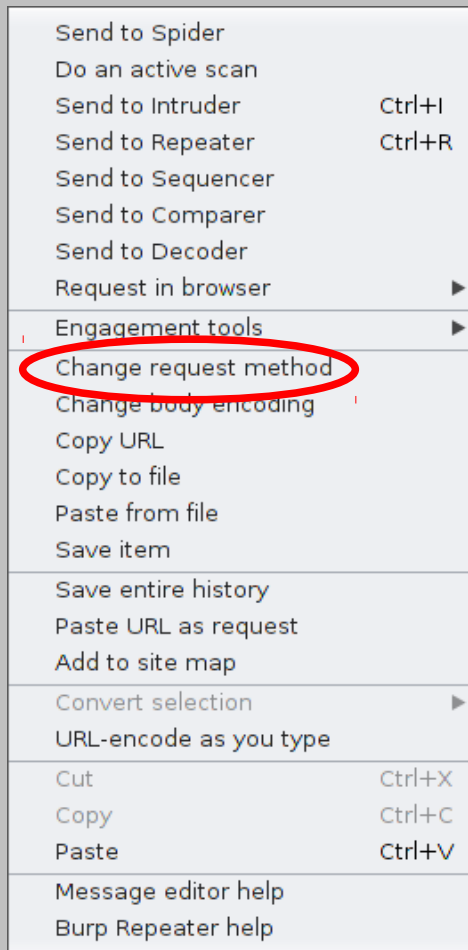
**Switching between GET and POST**

**Non proxy-aware clients**

**Importing & exporting an URL**

# ***GET to POST***

**Classic question: is it also exploitable via POST?**



```
GET /foo?a=xxxx&id=1234 HTTP/1.1
Host: vulnhost
```

```
POST /foo HTTP/1.1
Host: vulnhost
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

a=xxxx&id=1234
```

# ***Non proxy-aware***

**\$ ./skipfish -o 8777 http://127.0.0.1:8777/**

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Proxy Listeners' section is active, displaying a table of listeners. The listener at 127.0.0.1:8777 is selected, and its 'Invisible' checkbox is checked. The 'Edit proxy listener' dialog is open, showing the 'Request handling' tab. The 'Redirect to host' is 192.168.12.106 and the 'Redirect to port' is 80. The 'Support invisible proxying' checkbox is checked and circled in red.

**Proxy Listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8666	<input type="checkbox"/>		Per-host
<input checked="" type="checkbox"/>	127.0.0.1:8777	<input checked="" type="checkbox"/>	192.168.12.106:80	Per-host

**Edit proxy listener**

These settings control whether Burp redirects requests received by this listener.

Redirect to host: 192.168.12.106

Redirect to port: 80

☐ Force use of SSL

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

☒ Support invisible proxying (enable only if needed)

# ***Moving URL in & out***

## **Import**

**“Paste URL as request”**

## **Export**

**“Copy URL”**

**Works only with basic GET requests**

**Not body, no headers, no cookies, ...**

**“curlit” extension**

**Generates a “curl” command**



# ***Moving URL in & out***

```
POST /foo HTTP/1.1
Host: vulnhost
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Cookie: sessid=azerty123456789

a=xxxx&id=1234
```

**<https://github.com/faffi/curlit>**

Details

Output

Errors

☐ Output to system console

☐ Save to file: 

Select file ...

☒ Show in UI:

```
curl -isk -H "Content-Type: application/x-www-form-urlencoded" \
-H "Host: vulnhost" \
-d "a=xxxx&id=1234" \
-X "POST" \
-b "sessid=azerty123456789" \
"http://127.0.0.1:80/foo"
```

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Intruder payloads***

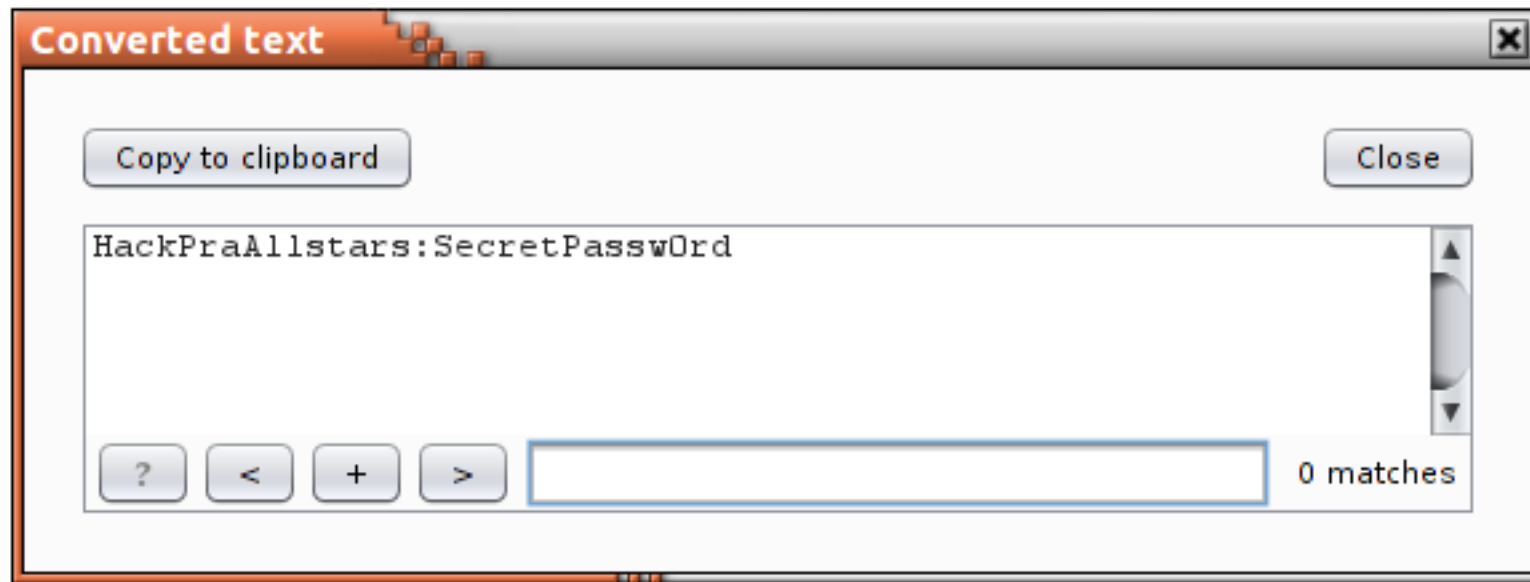
**HTTP Basic Authentication**

**Opaque data**

**Anti-CSRF tokens**

# ***Basic Auth***

```
GET /admin HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic SGFja1ByYUFSbHNOYXJzO1NlY3JldFBhc3N3MHJk
Connection: keep-alive
```



# ***Basic Auth***

## **Algorithm**

**Base64(username + ":" + password)**

## **Advices you may find on blogs**

**Use prefix/suffix**

**Use precompiled lists**

**Use an extension**

# ***Basic Auth***



# ***Basic Auth***

**Use the “Custom Iterator” payload!**

**From the documentation:**

**The custom iterator defines up to 8 different “positions” which are used to generate permutations. Each position is configured with a list of items, and an optional “separator” string, which is inserted between that position and the next.**

**That's exactly what we want!**

# ***Basic Auth***

## **Howto**

**Payload type : Custom Iterator**

**Position #1: list of usernames + separator “:”**

**Position #2: list of passwords**

**Payload processing: Base64-encode**

**Payload encoding: None**



# ***Basic Auth***

## **Another approach**

**Payload type : Custom Iterator**

**Position #1: list of usernames**

**Position #2: string “:”**

**Position #3: list of passwords**

**Position #4: common suffixes**

**Payload processing: Base64-encode**

**Payload encoding: None**

# *Basic Auth*

RequestResponse

RawHeadersHex

GET /admin/ HTTP/1.1  
Host: 127.0.0.1  
Accept: \*/\*  
Accept-Language: en  
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)  
Authorization: Basic YWRtaW46cDRzc3cwMHJkMjAxMA==  
Connection: close

Converted text

Copy to clipboardClose

admin:p4ssw00rd2010

?<+>

0 matches

# ***Intruder payloads***

**HTTP Basic Authentication**

**Opaque data**

**Anti-CSRF tokens**

# *Opaque data*

## Request

Raw Params Headers Hex

```
GET /profile.php?auth=a04211e6384ab9801b24db2b5e4246bc11105cd9518b549cc9fb765783bd4450 HTTP/1.1
Host: 127.0.0.1
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

?

<

+

>

Type a search term

## Response

Raw Headers Hex HTML Render

```
<html>
  <head>
    <title>Your profile</title>
  </head>
  <body>Welcome in the 'Payroll' application
    <br/>
    Your privileges: UID=100, GID=100</body>
</html>
```

# ***Opaque data***

**No cookie + long GET token + authenticated access?**

**Is the token**

**An anti-cache mechanism: **safe****

**A session ID: **unsafe** (logs, referrer)**

**Authentication data provided by the client**

**Verified server-side: **safe****

**Not verified server-side: **unsafe****

**From the documentation:**

**Character frobber: It cycles through the base string one character at a time, incrementing the ASCII code of that character by one.**

# *Opaque data*

## ? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: unknown  
Payload type:  Request count: unknown

## ? Payload Options [Character frobber]

This payload type operates on a string input and modifies the value of each character position in turn. It is useful to quickly test which parts of a long string have an effect on the application's processing.

Operate on: ☒ Base value of payload position

☐ Specific string:

# Opaque data

12	a04211e6384bb9801b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroml	100	100
13	a04211e6384ac9801b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payrol	100	100
14	a04211e6384ab:801b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payrolp	100	100
15	a04211e6384ab9901b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	100	100
16	a04211e6384ab9811b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	100	100
17	a04211e6384ab9802b24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	000	100
18	a04211e6384ab9801c24db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	600	100
19	a04211e6384ab9801b34db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	1 0	100
20	a04211e6384ab9801b25db...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	110	100

Request Response

Raw Headers Hex HTML Render

```
<html>
  <head>
    <title>Your profile</title>
  </head>
  <body>Welcome in the 'Payroll' application
    <br/>
    Your privileges: UID=600, GID=100</body>
</html>
```

# ***Opaque data***

**It looks like unverified encrypted data (XOR or ECB)**

**We know which part of the string impacts the UID**

**Let's try to modify it at the bit level**



# *Opaque data*

## Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way assigned to payload positions - see help for full details.

Attack type:

```
GET /profile.php?auth=a04211e6384ab98$01b24db2b$5e4246bc11105cd9518b549cc9fb765783bd4450
HTTP/1.1
Host: 127.0.0.1
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

# *Opaque data*

Payload set: 1

Payload count: unknown

Payload type: Bit flipper

Request count: unknown

## Payload Options [Bit flipper]

This payload type operates on an input and modifies the value of each bit position in turn. It can sometimes be used to meaningfully modify the decrypted values of CBC-encrypted data, and potentially interfere with application logic.

Operate on:

☒ Base value of payload position

☐ Specific string:

Format of original data: ☐ Literal value

☒ Encoded as ASCII hex

Select bits to flip:

☒ 1 (LSB) ☒ 3 ☒ 5 ☒ 7  
☒ 2 ☒ 4 ☒ 6 ☒ 8 (MSB)

# *Opaque data*

10	01b04db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	100
11	01b64db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	1p0
12	01ba4db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	1°0
13	01a24db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	411	Payroll	000
14	01924db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	300
15	01f24db2b	200	<input type="checkbox"/>	<input type="checkbox"/>	361	Payroll	500

Request Response

Raw Headers Hex HTML Render

```
<html>
  <head>
    <title>Your profile</title>
  </head>
  <body>Welcome in the 'Payroll' application
    <br/>
    Your privileges: UID=000 GID=100
    Well done. But you need UID=000 and GID=000!
    <br/>
  </body>
</html>
```

# ***Intruder payloads***

**HTTP Basic Authentication**

**Opaque data**

**Anti-CSRF tokens**

# Anti CSRF tokens

Raw Params Headers Hex

POST request to /csrf.php

Type	Name	Value
Cookie	PHPSESSID	rvtfcsgn18677t68aa0frr8c54
Body	token	a_long_value
Body	value	1

Body encoding: application/x-www-form-urlencoded

Response

Raw Headers Hex HTML Render

```
<html>
  <head>
    <title>CSRF protected form</title>
  </head>
  <body>[ALERT] Anti-CSRF token is *NOT* valid.
    <br/>
    <hr/>
    Value is lower than 50:
    <br/>
    <form action="" method="post">Value:
      <input type="text" name="value" value=""/>
      <br/>
      <input type="hidden" name="token" value="9ca26d363d179c5fc5ed91d991c0ee73"/>
      <br/>
      <input type="submit"/>
    </form>
```

# Anti CSRF tokens

RawParamsHeadersHex

POST request to /csrf.php

Type	Name	Value
Cookie	PHPSESSID	rvtfcsgh18877t68aa0fn8c54
Body	token	9ca26d363d179c5fc5ed91d991c0ee73
Body	value	1

Body encoding: application/x-www-form-urlencoded

## Response

RawHeadersHexHTMLRender

```
<html>
  <head>
    <title>CSRF protected form</title>
  </head>
  <body>Anti-CSRF token is valid.
    <br/>
    Please try another value!
    <br/>
    <hr/>
    Value is lower than 50:
    <br/>
    <form action="" method="post">Value:
      <input type="text" name="value" value=""/>
      <br/>
      <input type="hidden" name="token" value="222221fcafdebc124ad0befb89d9a777"/>
      <br/>
    </form>
  </body>
</html>
```

# Anti CSRF tokens

Raw Params Headers Hex

POST request to /csrf.php

Type	Name	Value
Cookie	PHPSESSID	rvtfcsgr18677t68aa0fr8e54
Body	token	222221fcdfdebc124ad0befb89d9a777
Body	value	2

Body encoding: application/x-www-form-urlencoded

## Response

Raw Headers Hex HTML Render

```
<html>
  <head>
    <title>CSRF protected form</title>
  </head>
  <body>Anti-CSRF token is valid.
    <br/>
    Please try another value!
    <br/>
    <hr/>
    Value is lower than 50:
    <br/>
    <form action="" method="post">Value:
      <input type="text" name="value" value=""/>
      <br/>
      <input type="hidden" name="token" value="b43aab68562b3dc731581fa518da6226"/>
    <br/>
```

# ***Anti CSRF tokens***

**Recursive Grep to the rescue!**

**From the documentation**

**This payload type lets you extract each payload from the response to the previous request in the attack.**

**The text that was extracted from the previous response in the attack is used as the payload for the current request.**



# ***Anti CSRF tokens***

**Attack type: Pitchfork**

**Payload #1:**

**Location: Parameter “token”**

**Type: Recursive Grep**

**Initial value: A valid token**

**Regexp: name="token" value="[\*?]" /><br/>**

**Payload #2:**

**Location: Parameter “value”**

**Type: Numbers from 0 to 50**

# ***Anti CSRF tokens***

## **Caveats**

**Only applies if the result page includes a valid token**

**You must use only one thread (idem if macro-based)**

**Twice faster than its macro-based counterpart 🤖**

# Anti CSRF tokens

Request	Payload1	Payload2	Status	Length	Please try another val...	Anti-CSRF token is *NOT*...	"token" value=
27	a575edd7b8e689dede2c65e200eaed43	26	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c9275dff1f27e058b8d43a97ce1...
28	c9275dff1f27e058b8d43a97ce12945e	27	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	7ba26334ecae3b899475782a1...
29	7ba26334ecae3b899475782a1e5f162a	28	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	df0894ca4f5d6647b57299dfef5...
30	df0894ca4f5d6647b57299dfef5bdf7	29	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6487a328e657fd8e4950c45a2d...
31	6487a328e657fd8e4950c45a2def3430	30	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	d39a05b2fa22fcc69df6d6bc380...
32	d39a05b2fa22fcc69df6d6bc38004f52	31	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	866ec10ca898fdc441573e6c71...
33	866ec10ca898fdc441573e6c71aa5a1b	32	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	d9087cace61e7e3c905fb5c80f3..
34	d9087cace61e7e3c905fb5c80f36f725	33	200	738	<input type="checkbox"/>	<input type="checkbox"/>	23b4d2beeaddc95ad993f2fac8...
35	23b4d2beeaddc95ad993f2fac841081b	34	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c50399865813e9b08a79139e3f...
36	c50399865813e9b08a79139e3f282f55	35	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2a6a8b9b802daeeaae42068ca9...
37	2a6a8b9b802daeeaae42068ca98d6baec	36	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	edb824d8101d1feb4f7cf2b888f...
38	edb824d8101d1feb4f7cf2b888f357f4	37	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	22a2ff0e37a22ab507b997dff41...
39	22a2ff0e37a22ab507b997dff4107458	38	200	723	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0eddf967f12e140d01e81d8e8b...

Request Response

Raw Headers Hex HTML Render

```
<html>
<head>
  <title>CSRF protected form</title>
</head>
<body>Anti-CSRF token is valid.
<br/>
Bingo [5ec9bdbaf9d1a07680769551b057e0b8]
<br/>
<hr/>
Value is lower than 50:
<br/>
<form action="" method="post">Value:
  <input type="text" name="value" value=""/>
  <br/>
  <input type="hidden" name="token" value="23b4d2beeaddc95ad993f2fac841081b"/>
  <br/>
```

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Mobile applications***

**Traffic redirection**

**Burp CA certificate**

**Missing developers tools**

# ***Redirect to Burp***

**Your target is running on a rooted Android smartphone**

**You want to use your usual tool and workflow**

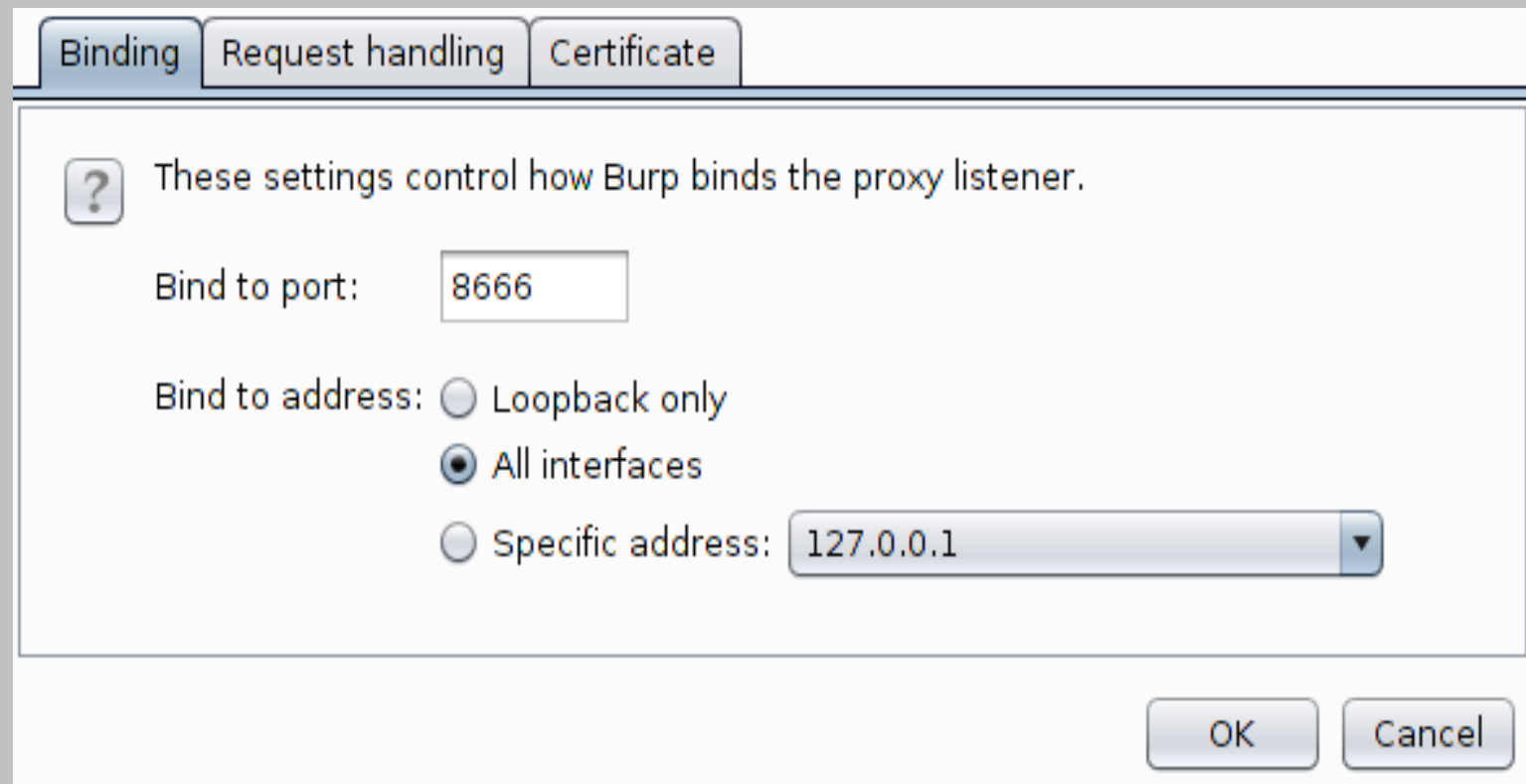
**Burp listens elsewhere, on an external interface**

**ProxyDroid redirects to the Burp instance**

**App-specific or global proxying**

**Option “DNS Proxy” should be checked**

# ***Redirect to Burp***



The image shows the 'Binding' tab of the Burp Suite configuration window. It has three tabs: 'Binding', 'Request handling', and 'Certificate'. The 'Binding' tab is active. Below the tabs, there is a help icon (a question mark in a square) followed by the text: 'These settings control how Burp binds the proxy listener.' Below this, there are three settings: 'Bind to port:' with a text box containing '8666'; 'Bind to address:' with three radio button options: 'Loopback only', 'All interfaces' (which is selected), and 'Specific address:'. The 'Specific address' option has a text box containing '127.0.0.1' and a dropdown arrow. At the bottom right, there are 'OK' and 'Cancel' buttons.

Binding Request handling Certificate

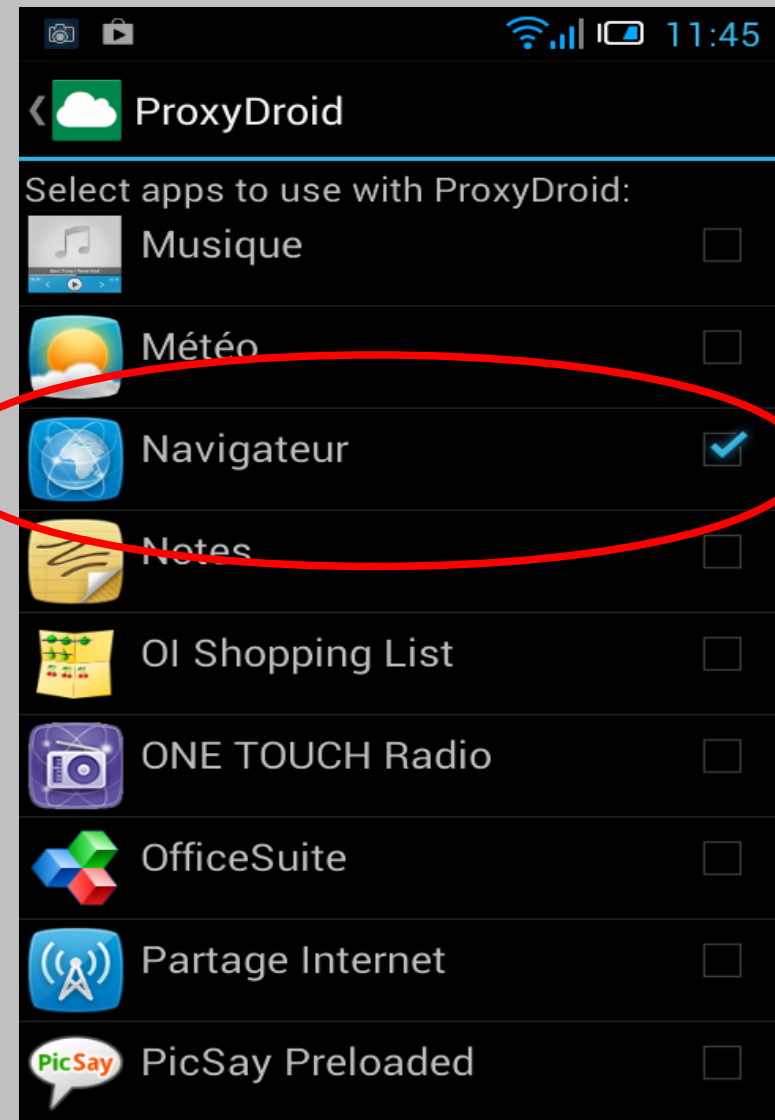
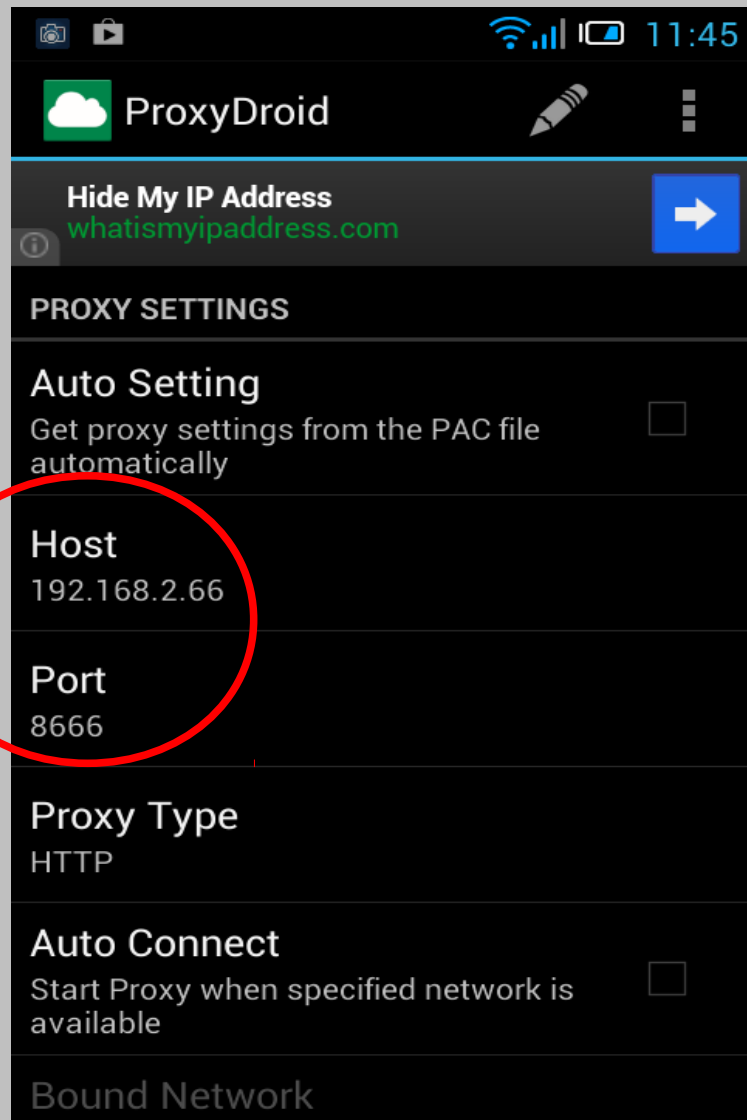
? These settings control how Burp binds the proxy listener.

Bind to port: 8666

Bind to address: ☐ Loopback only  
☒ All interfaces  
☐ Specific address: 127.0.0.1 ▼

OK Cancel

# *Redirect to Burp*

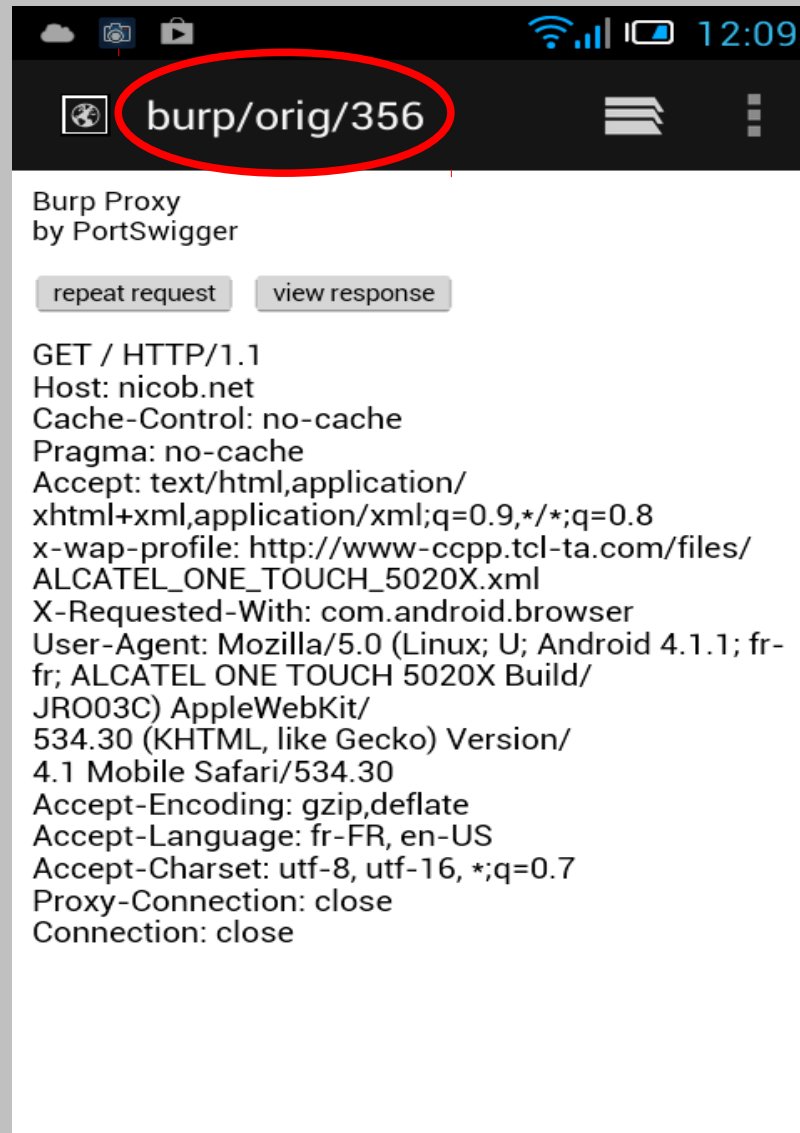




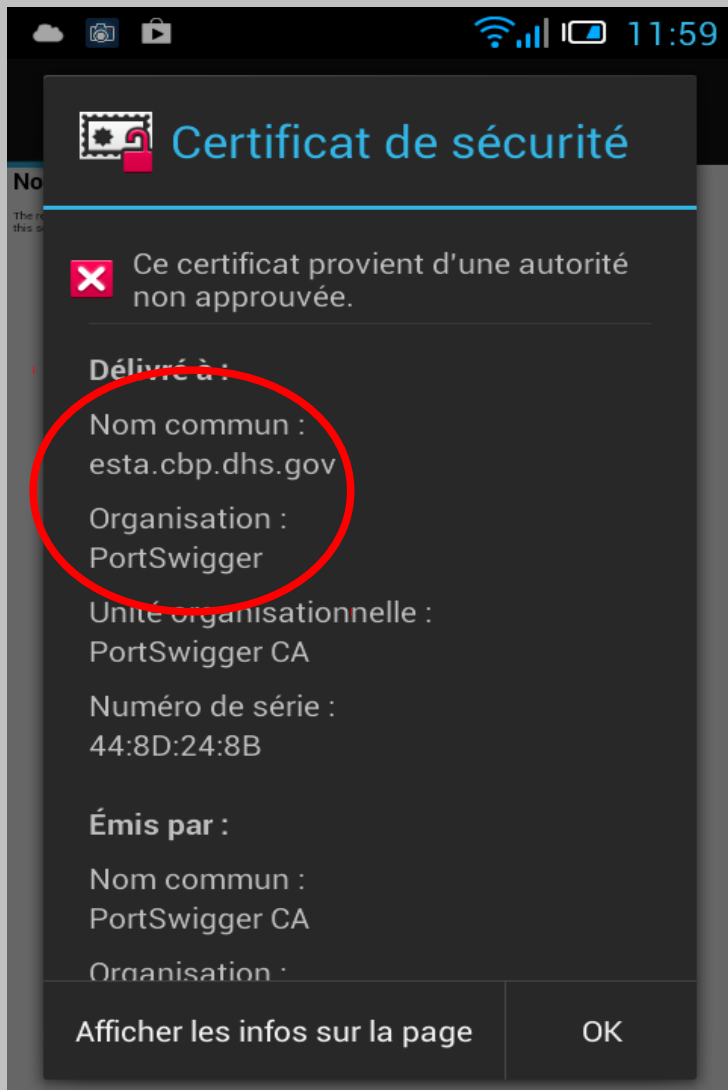
# ***Redirect to Burp***

Request	Response
<div>Raw Headers Hex</div> <pre>GET / HTTP/1.1 Host: nicob.net Cache-Control: no-cache Pragma: no-cache Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 x-wap-profile: http://www-ccpp.tcl-ta.com/files/ALCATEL_ONE_TOUCH_5020X.xml X-Requested-With: com.android.browser User-Agent: Mozilla/5.0 (Linux; U; Android 4.1.1; fr-fr; ALCATEL ONE TOUCH 5020X Build/JRO03C) Accept-Encoding: gzip,deflate Accept-Language: fr-FR, en-US Accept-Charset: utf-8, utf-16, *;q=0.7 Proxy-Connection: close Connection: close</pre>	

# ***Redirect to Burp***



# Burp CA



# ***Burp CA***

## **Fetch your Burp CA certificate**

**GUI: Proxy / Options / Proxy Listeners / CA Certificate / Export in DER**

**Proxied browser: <http://burp/cert>**

## **Rename from DER to CRT**

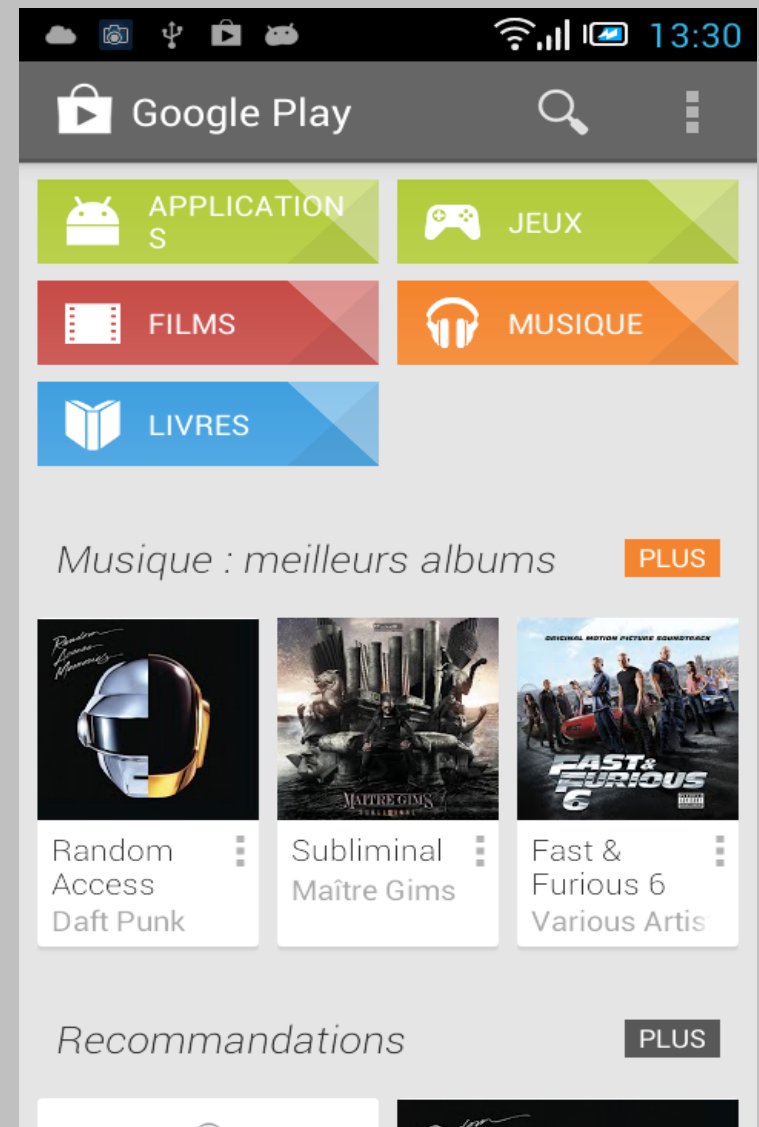
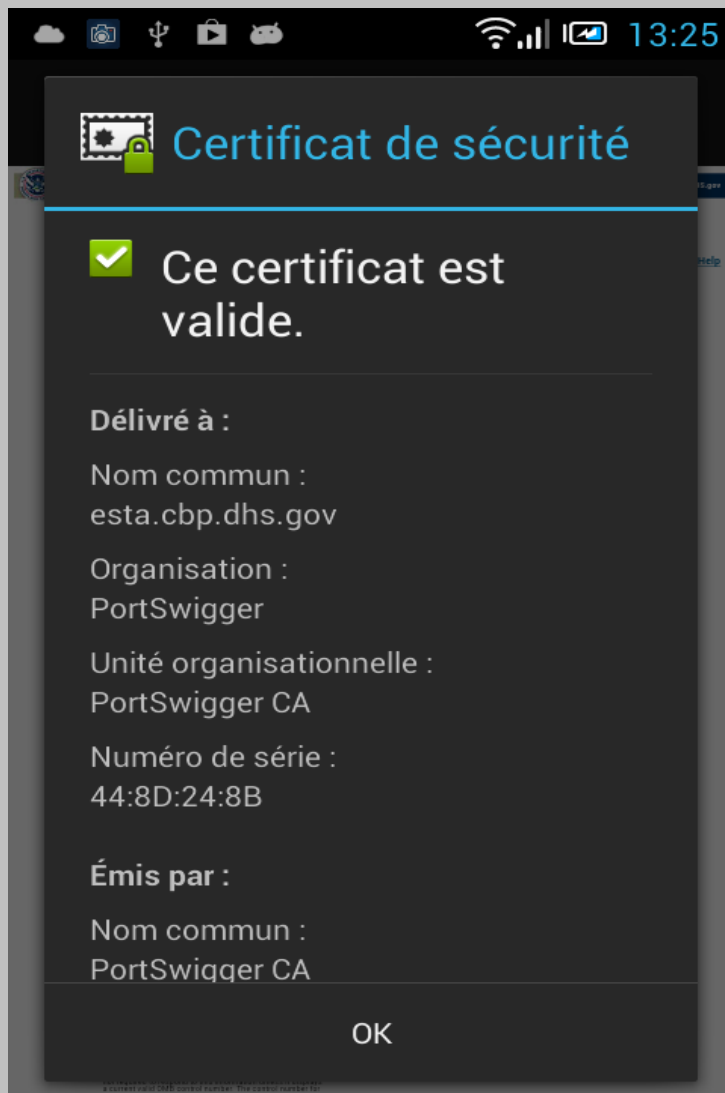
**No need for OpenSSL** 

## **Depending on the Android version:**

**Touch the file in any “File Explorer” application**

**Parameters / Security / Install from SD**

# Burp CA



# Burp CA

## First request when opening Google Play

570	https://173.194.38.169	GET	/fdfe/toc?shh=zen2III1nK1Sx2swLcCn16w
<div>RequestResponse</div>			
<div>RawParamsHeadersHex</div>			
Name	Value		
GET	/fdfe/toc?shh=zen2III1nK1Sx2swLcCn16w HTTP/1.1		
X-DFE-Device-Config-Token	1370992447587		
Accept-Language	fr-FR		
X-DFE-MCCMNC	20815		
Authorization	GoogleLogin auth=DQAAAJIAAAAYmaUUTyi39KXHeqsurm07ZjNSGkWgT0rorH6-mWs7ysOSWhXD...		
X-DFE-Unsupported-Experiments	nocache:dfc:dc:1,nocache:dfc:uc:FR,buyer_currency,buyer_currency_in_app,checkin.set_asset_p...		
X-DFE-Device-Id	39b3e219f8da8b09		
X-DFE-Client-Id	am-android-alcatel		
X-DFE-Logging-Id	112729f7e426557		
User-Agent	Android-Finsky/4.1.10 (api=3,versionCode=80210010,sdk=16,device=Megane_GSM,hardware=...		
X-DFE-SmallestScreenWidthDp	320		
X-DFE-Filter-Level	3		
Host	android.clients.google.com		
Connection	Keep-Alive		

# ***Developers tools***

**Mobile browsers miss some common features**

**Like no built-in developers tools**

**I don't care, except when looking for XSS**

# ***Developers tools***

**Let's include Firebug Lite in every response**  
**“startOpened=true” is your friend**



## **Firebug Lite: doing the Firebug way, anywhere.**

- ✓ Compatible with all major browsers: IE6+, Firefox, Opera, Safari and Chrome
- ✓ Same look and feel as Firebug
- ✓ Inspect HTML and modify style in real-time
- ✓ Powerful console logging functions
- ✓ Rich representation of DOM elements
- ✓ Extend Firebug Lite and add features to make it even more powerful

[Tour >>](#)



# *Developers tools*

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

### ? Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Type	Match	Replace
<input checked="" type="checkbox"/>	Response body	</head>	<script type='text/javascript' src='https://getfirebug.com/releases/lite/1.4/firebug-lite.js#startOpened=true'> ...

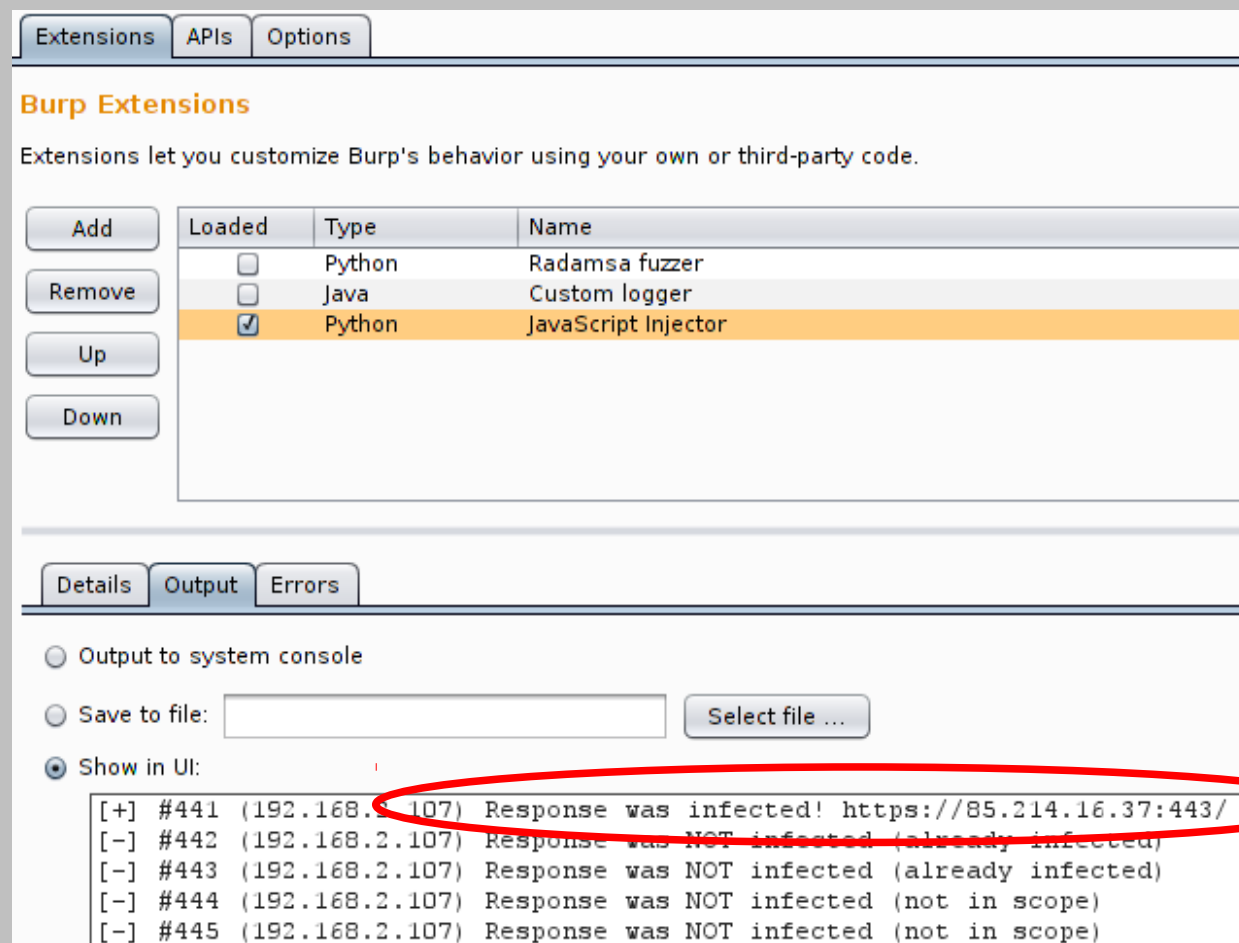
Add Edit Remove Up Down

**This seems to be a good idea**

**But Firebug itself contains the “</head>” string**



# *Developers tools*



The screenshot shows the Burp Suite interface with the 'Extensions' tab selected. Under 'Burp Extensions', there is a table of installed extensions. The 'JavaScript Injector' extension is checked and highlighted. Below the table, the 'Output' tab is selected, showing a log of network activity. A red circle highlights the first log entry, which indicates a successful infection of a response.

**Extensions** | APIs | Options

### Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

**Add** **Remove** **Up** **Down**

Loaded	Type	Name
<input type="checkbox"/>	Python	Radamsa fuzzer
<input type="checkbox"/>	Java	Custom logger
<input checked="" type="checkbox"/>	Python	JavaScript Injector

**Details** | **Output** | **Errors**

☐ Output to system console

☐ Save to file:  **Select file ...**

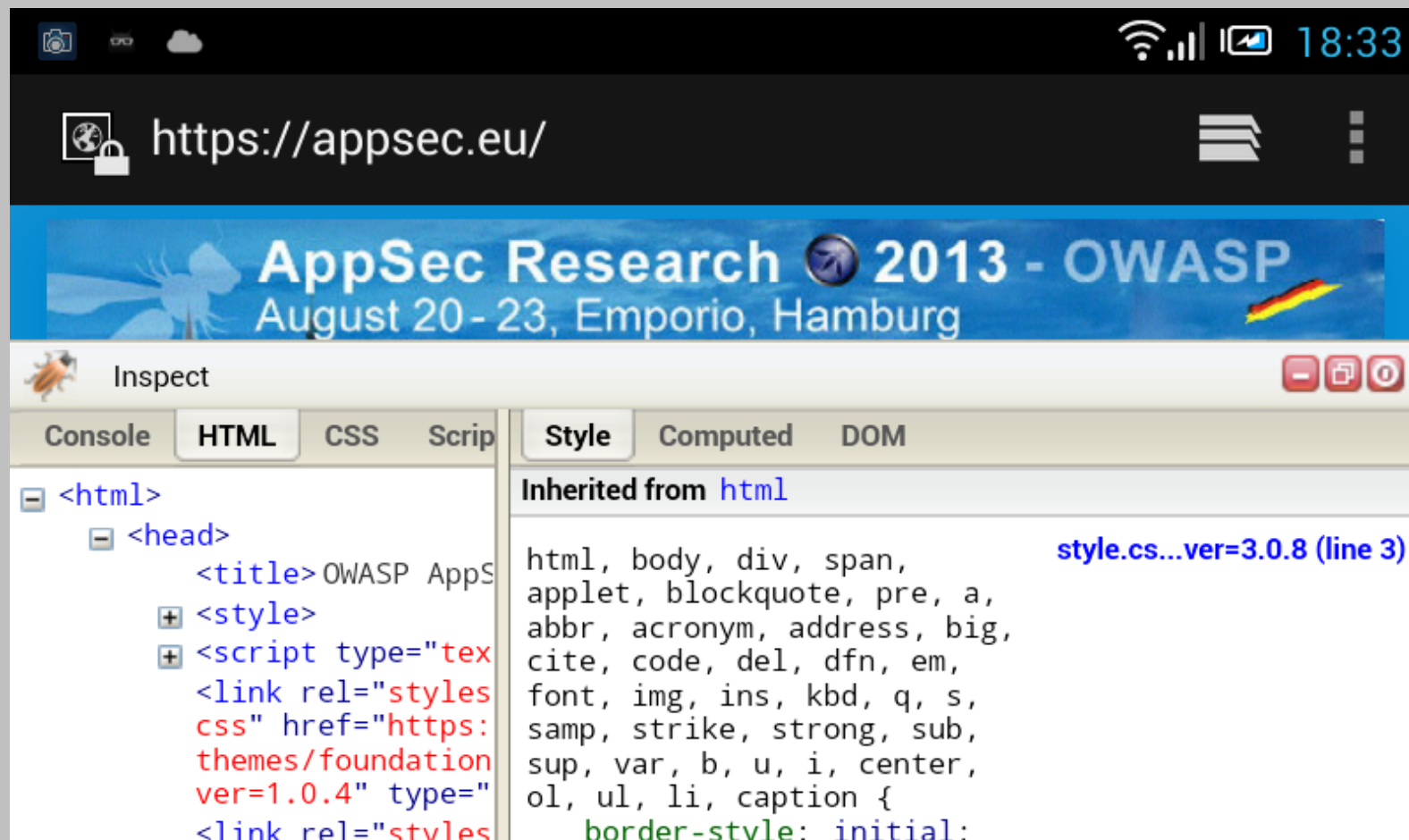
☒ Show in UI:

```
[+] #441 (192.168.2.107) Response was infected! https://85.214.16.37:443/
[-] #442 (192.168.2.107) Response was NOT infected (already infected)
[-] #443 (192.168.2.107) Response was NOT infected (already infected)
[-] #444 (192.168.2.107) Response was NOT infected (not in scope)
[-] #445 (192.168.2.107) Response was NOT infected (not in scope)
```

<http://www.agarri.fr/docs/JavaScriptInjector.py>

**Also works with BeEF and autpwn during a MITM!** 🤖

# *Developers tools*



# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Extensions***

**As an user**

**As a developer**

# ***Resources***

## **Repositories**

**<http://www.burpextensions.com/Extensions/>**

**<https://github.com/Meatballs1/burp-extensions>**

## **Online documentation**

**<http://portswigger.net/burp/help/extender.html>**

**<http://www.burpextensions.com/category/tutorials/>**

## **Forum**

**<http://forum.portswigger.net/board/2/burp-extensions>**

## **Blog (+ samples)**

**<http://blog.portswigger.net/search/label/burp%20extender>**

# ***May be useful***

## **Format specific**

**JSON, JS, Protobuf, AMF, Serialized Java, WSDL, WCF**

## **External tools**

**Google hacks, nmap, sqlmap, w3af, curl, Radamsa**

## **Misc**


**Custom Logger, Proxy Color, Burp CSJ, Site Map Importer**

## **My own**

**JavaScript Injector, HTTP Traceroute, DomXssRegex**

# ***Detect reverse-proxies***

Advisory	Request1	Response1	Request2	Response2
----------	----------	-----------	----------	-----------

 **Reverse-proxy detected using TRACE** [Compare responses](#)

---

Issue: **Reverse-proxy detected using TRACE**  
Severity: **Information**  
Confidence: **Certain**  
Host: **http://fr.ask.com**  
Path: **/**

---

### Issue detail

A reverse-proxy was detected. The following heuristics were triggered using 'Max-Fowards: 0':

- **Status codes** are different
  - Baseline: 405
  - Modified: 200
- Header **Content-Type** have different values:
  - Baseline: text/plain
  - Modified: message/http



# *Generate from WSDL*

Binding	Operation	Port
AWSECommerceServiceBinding	ItemSearch	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	ItemLookup	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	BrowseNodeLookup	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	SimilarityLookup	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	CartGet	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	CartCreate	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService
AWSECommerceServiceBinding	CartAdd	https://webservices.amazon.fr/onca/soap?Service=AWSECommerceService

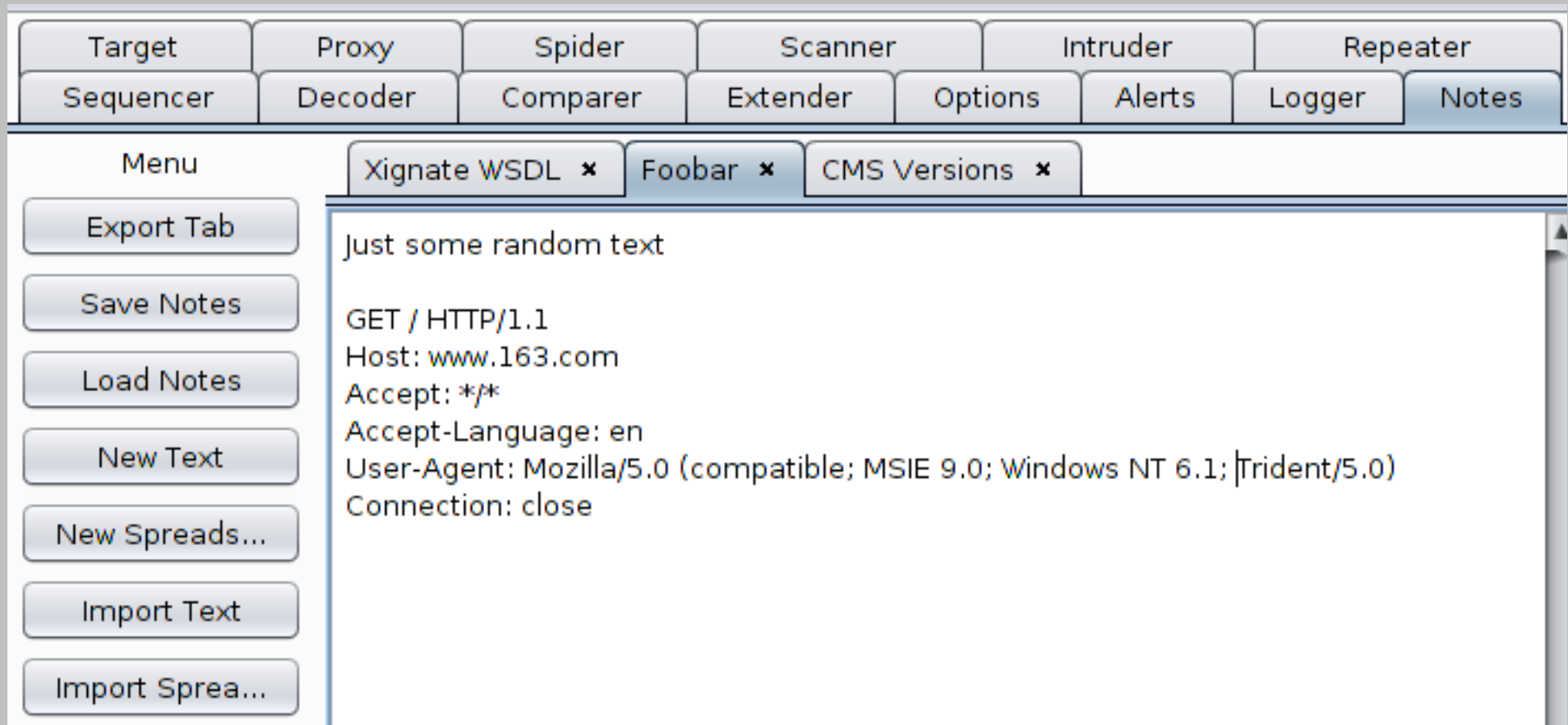
Request

Raw Params Headers Hex XML

```
POST /onca/soap?Service=AWSECommerceService HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: http://soap.amazon.com/BrowseNodeLookup
Host: webservices.amazon.fr
Content-Length: 1199
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://webservices.amazon.com/AWSECommerceService/2011-08-01">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:BrowseNodeLookup>
      <!--type: string-->
      <ns:MarketplaceDomain>gero et</ns:MarketplaceDomain>
      <!--type: string-->
      <ns:AWSAccessKeyId>sonoras imperio</ns:AWSAccessKeyId>
      <!--type: string-->
      <ns:AssociateTag>quae divum incedo</ns:AssociateTag>
      <!--type: string-->
      <ns:Validate>verrantque per auras</ns:Validate>
      <!--type: string-->
      <ns:XMLEscaping>per auras</ns:XMLEscaping>
```

# *Take notes*



***Take notes***

Target

Sequencer

Proxy

Decoder

Spider

Comparer

Scanner

Extender

Intruder

Options

Repeater

Alerts

Logger

Notes

Menu

Xignate WSDL x

Foobar x

CMS Versions x

Export Tab

Save Notes

Load Notes

New Text

New Spreads...

Import Text

Import Sprea...

A	B	C	D	E	F	G
IP	Port	URL	Type	Version		
10.0.1.45	80	/	WordPress	3.5.2		
10.0.1.98	443	/wp/	WordPress	2.2.0		
10.0.3.7	80	/nb/	NanoBlogger	1.7b		

# Augment reality

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Logger Logger Crawljax JUnit (beta)

### Generic Settings

Browser Firefox

Instances 1

Proxy Type

☒ Use System Proxy Settings

☐ Use Manual Proxy localhost 8080

### Configured Browsers

Remote http://server:port/

Chrome Path to chromedriver.exe Choose File

IE Path to IEDriverServer.exe Choose File

PhantomJS Path to phantomjs.exe Choose File

### Advanced Options

☒ Use Burp CookieJar

☒ Click Once

☒ Insert Random Input On Forms

☐ Crawl Hidden Anchors

☐ Crawl Frames

Wait After Reload URL 500 Add

Wait After Event 500 Remove

Maximum Depth 2

Maximum States 0

Max Runtime (mins) 60

Exclusion

- exit
- signout
- signoff
- logoff
- logout

### Crawl Elements

☒ A ☐ INPUT ☐ XHR ☐ SELF

☒ BUTTON ☐ OPTION ☐ REFRESH

☐ TD ☐ IMG ☐ META

☐ SPAN ☐ LINK ☐ RELATIVE

☐ DIV ☐ P ☐ NON

☐ FORM ☐ SELECT ☐ RADIO

☐ TR ☐ OL ☐ LI

### Plugins

☒ No Plugins

☐ Overview Plugin

Choose folder

# ***As a developer***

**Choose your language**

**Quick reload**

**Debugging**

# ***Language***

## **Java**

**Provides the best integration with Burp internals**

## **Python**

**My personal choice**

**But Python != Jython**

## **Ruby**

**Same drawbacks than Python**

# ***Python vs. Java API***

## **Java API**

### **ApplyMarkers(**

**IHttpRequestResponse httpRequestResponse,**

**java.util.List<int[]> requestMarkers,**

**java.util.List<int[]> responseMarkers)**

## **Python code**

**markers = []**

**for n in non\_overlapping:**

**markers.append(array.array('i', [offset + n[0], offset + n[1]]))**

**marked\_message = self.\_callbacks.applyMarkers(message, None, markers)**

# ***Quick reload***

**Use Ctrl-Click to quickly reload an extension**

The screenshot shows a web application interface for managing extensions. On the left, there are four buttons: 'Add', 'Remove', 'Up', and 'Down'. To the right of these buttons is a table with three columns: 'Loaded', 'Type', and 'Name'. The 'JSON Decoder' extension is highlighted in orange and has a checked checkbox in the 'Loaded' column. Below the table, there are three tabs: 'Details', 'Output', and 'Errors'. The 'Details' tab is selected. In the 'Details' section, there is a checked checkbox labeled 'Extension loaded', which is circled in red. Below this, there is a text input field labeled 'Name:' containing the text 'JSON Decoder'. At the bottom, there is a table with two columns: 'Item' and 'Detail'. The 'Item' column contains the text 'Extension type' and the 'Detail' column contains the text 'Python'.

Loaded	Type	Name
<input checked="" type="checkbox"/>	Python	JSON Decoder
<input type="checkbox"/>	Java	WSDL Parser
<input type="checkbox"/>	Python	JavaScript Injector
<input type="checkbox"/>	Python	Detect reverse-proxies
<input checked="" type="checkbox"/>	Python	Custom logger

Details Output Errors

☒ Extension loaded

Name:

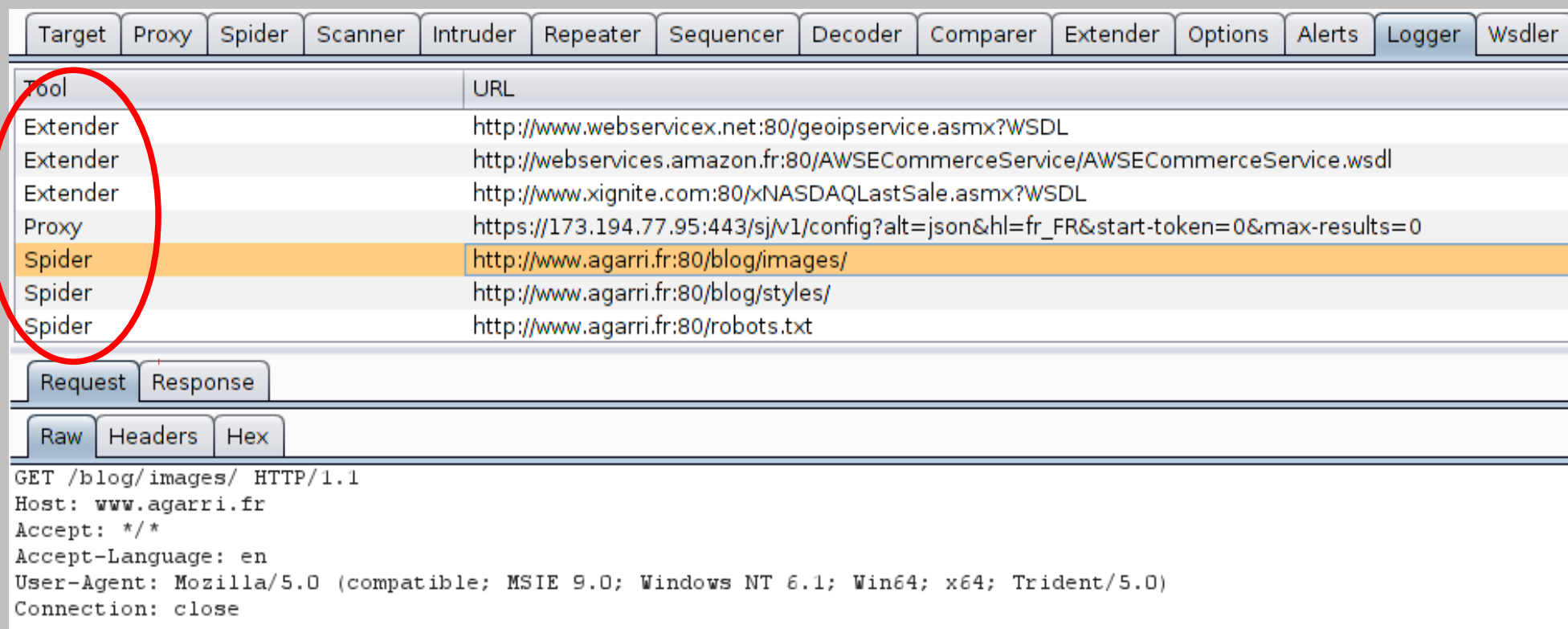
Item	Detail
Extension type	Python



# *Debugging*

## Custom Logger captures everything

<http://blog.portswigger.net/2012/12/sample-burp-suite-extension-custom.html>



The screenshot shows the Burp Suite interface with the 'Tools' tab selected. A red circle highlights the 'Spider' tool in the list. The 'Request' tab is selected in the bottom panel, showing an HTTP GET request to `/blog/images/` on `www.agarri.fr`.

Tool	URL
Extender	<code>http://www.webservices.net:80/geoip/service.asmx?WSDL</code>
Extender	<code>http://webservises.amazon.fr:80/AWSECommerceService/AWSECommerceService.wsdl</code>
Extender	<code>http://www.xignite.com:80/xNASDAQLastSale.asmx?WSDL</code>
Proxy	<code>https://173.194.77.95:443/sj/v1/config?alt=json&amp;hl=fr_FR&amp;start-token=0&amp;max-results=0</code>
Spider	<code>http://www.agarri.fr:80/blog/images/</code>
Spider	<code>http://www.agarri.fr:80/blog/styles/</code>
Spider	<code>http://www.agarri.fr:80/robots.txt</code>

Request Response

Raw Headers Hex

```
GET /blog/images/ HTTP/1.1
Host: www.agarri.fr
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

# ***Target & Goal***

**Target application requires authentication**

**Sessions are very short-lived**

**You want to work “as usual”**

**Manual tools: Repeater, ...**

**Automated tools: Intruder, Scanner, ...**

# ***App details***

## **/index.php**

**Display (GET) & process (POST) the login form**

**username=User33&password=S3CR3T**

## **/logged.php**

**Display session info**

**Display & process the target form**

**Target value is between 1 and 100**

**Session lasts for 15 seconds**

# Debugging

The screenshot displays the Burp Suite interface with the 'Session handling tracer' tab selected. The left sidebar contains three sections: 'Session Handling Rules', 'Cookie Jar', and 'Macros'. The 'Session Handling Rules' section has a red circle around the 'Open sessions tracer' button. The 'Cookie Jar' section has an 'Open cookie jar' button. The 'Macros' section has a 'Log as User33' button. The main panel shows the 'Session handling tracer' window with a warning message, a table of requests handled, a list of events, and an event detail view.

**Session Handling Rules**

You can define session handling rules to tools, URLs or parameters), and can per each request is issued, Burp applies in s

Buttons: Add, Edit, Remove, Duplicate, Up, Down

Enabled: ☒ Use cookies, ☒ Keeps a val

To monitor or troubleshoot the behavior rule

**Open sessions tracer**

**Cookie Jar**

Burp maintains a cookie jar that stores maintain valid sessions with applications based on traffic from particular tools.

Monitor the following tools' traffic to upd

☐ Proxy ☒ Scanner ☐ Repea  
☐ Spider ☒ Intruder ☐ Seque

**Open cookie jar**

**Macros**

A macro is a sequence of one or more obtaining anti-CSRF tokens, etc.

**Add** **Log as User33**

**Session handling tracer**

Warning: This tracer imposes a processing and storage overhead, and troubleshooting issues with session handling rules.

Requests handled

Time	Tool
00:22:10 17 juin 2013	Repeater
00:22:26 17 juin 2013	Repeater
00:22:34 17 juin 2013	Repeater

Events

Applying rule: Use cookies from Burp's cookie jar  
Applying rule: Keeps a valid session  
Performing action: Check session is valid  
Issued current request to validate session  
Session is invalid  
Running macro: Log as User33  
Processing macro item: http://127.0.0.1/malibu/  
Updated 1 cookie in macro request from cookie jar  
Issuing macro request  
Added 1 cookie from macro response to cookie jar  
Updated 1 cookie in current request from cookie jar  
Issued request

Event detail

Request Response Info

Raw Params Headers Hex

POST /malibu/ HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:21.0) Gecko/2010  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://127.0.0.1/malibu/  
Cookie: PHPSESSID=fkiudlcpeqvqhke992uadql7t0  
Connection: keep-alive  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 54

username=User33&password=S3CR3T&login=Please+log+me+in

***Macros***

**DEMO!**

# ***Overview***

**Data visualization**

**GUI navigation**

**Managing state**

**Common tasks**

**Intruder payloads**

**Mobile applications**

**Extensions**

**Macros**

***That's all, folks!***

**Thanks for your attention**  
**Any questions?**

**@Agarri\_FR**

**nicolas.gregoire@agarri.fr**