Hack in Paris

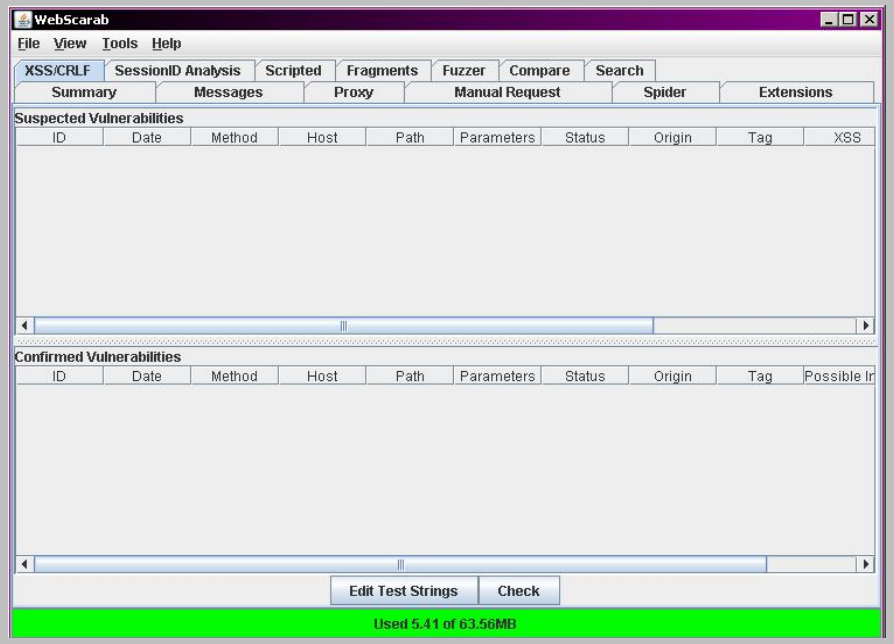
Burp Suite Pro
Real-life tips & tricks

Nicolas Grégoire

Me & Myself

Founder & owner of Agarri

Lot of Web PenTesting



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/

"Web Application Hacker's Handbook" 2nd Edition, Chapter 21

This is NOT "Burp 101"

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 on Burp Pro v1.5.11

Pro vs. Free vs. Zap

To do...

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

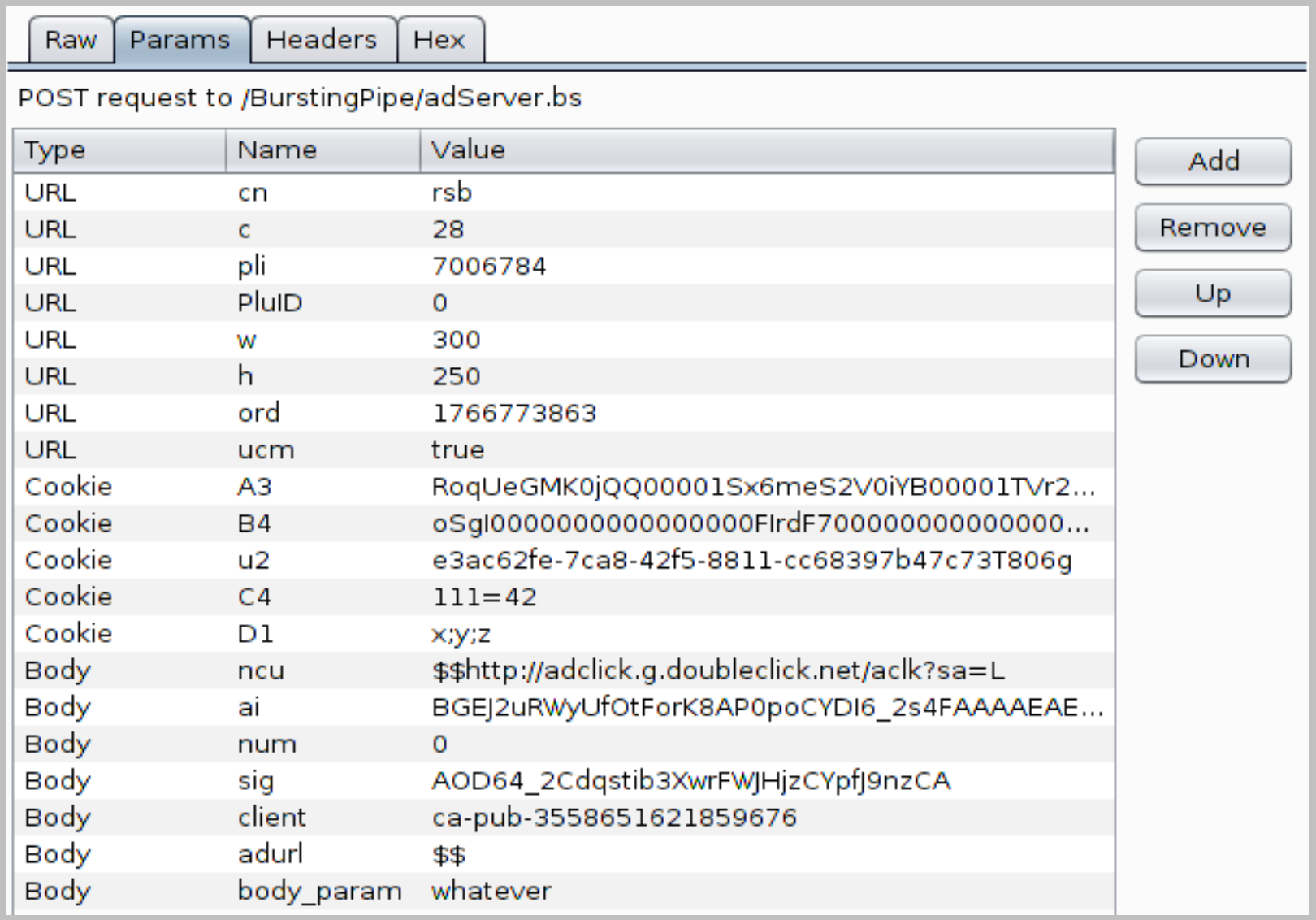
Parameters

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=RoqUeGMK0jQQ00001Sx6meS2V0iYB00001TVr2eUDN03BK00001QWLteG3S0iYB00001TRJ
MeSHH09Fb00001QPXYeFRo0iYB00002PyFeeGMK09ZX00000PaOxeG1B0hEp00000RqzleHyc0
iYB00001Tz+5eSHH0g9Q00001QjVreHXn0goR00000;
B4=oSgI0000000000000000FIrdF700000000000000000G1pwb500000000000000000FNpEGn0
0000000000000000FMqx2A000000000000000000Ger98c000000000000000000Ggr2n1000000000
0000000GgoW7B000000000000000000FIp7vu000000000000000000FKpI6Q000000000000000000F
Kpzp.0000000000000000FH 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=$$http://adclick.g.doubleclick.net/aclk?sa=L&ai=BGEJ2uRWyUfOtForK8AP0p
oCYDI6_2s4FAAAAEAEgADgAWK7i-oJ6YPv58IL4CYIBF2NhLXB1YiOzNTU4NjUxNjIxODU5Njc
2sgEOd3d3LnBsYXlib3kuZGW6AQlnZnBfaW1hZ2XIAQnaATJodHRwOi8vd3d3LnBsYXlib3kuZ
8gGqAMB4AQBoAYf&num=0&sig=AOD64_2Cdqstib3XwrFWJHjzCYpfJ9nzCA&client=ca-pub
-3558651621859676&adurl=$$&body_param=whatever
```

Parameters



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	oSgI0000000000000000FIrdF700000000000000...
Cookie	u2	e3ac62fe-7ca8-42f5-8811-cc68397b47c73T806g
Cookie	C4	111=42
Cookie	D1	x;y;z
Body	ncu	$$http://adclick.g.doubleclick.net/aclk?sa=L
Body	ai	BGEJ2uRWyUfOtForK8AP0poCYDI6_2s4FAAAAEAE...
Body	num	0
Body	sig	AOD64_2Cdqstib3XwrFWJHjzCYpfJ9nzCA
Body	client	ca-pub-3558651621859676
Body	adurl	$$
Body	body_param	whatever

XML

Response

Raw | Headers | Hex | XML

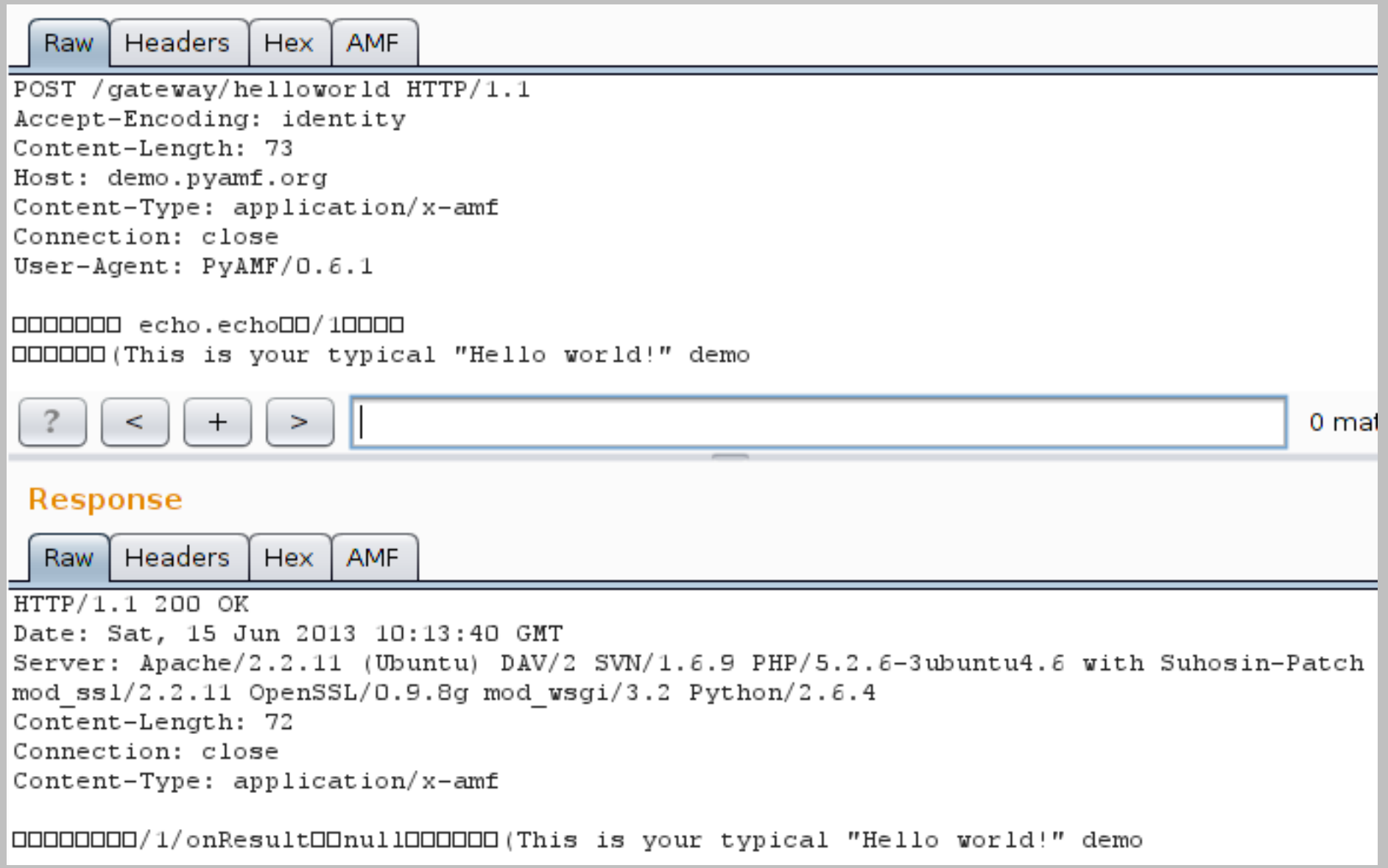

```
<?xml version="1.0" encoding="utf-8"?><infos_diffusions total="4" nb="4"><diffusions
type="now"><diffusion debut="1370624400" utc="1370624400" chaine="france2"
bureau_regional=""><id_plurimedia>83157220</id_plurimedia><id_ftv>1718306</id_ftv><titre><![CDATA
[Mot de passe]]></titre><soustitre/><date_heure><![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]]></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><soustitre/><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><soustitre><![CDATA[Le coup du
lapin]]></soustitre><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

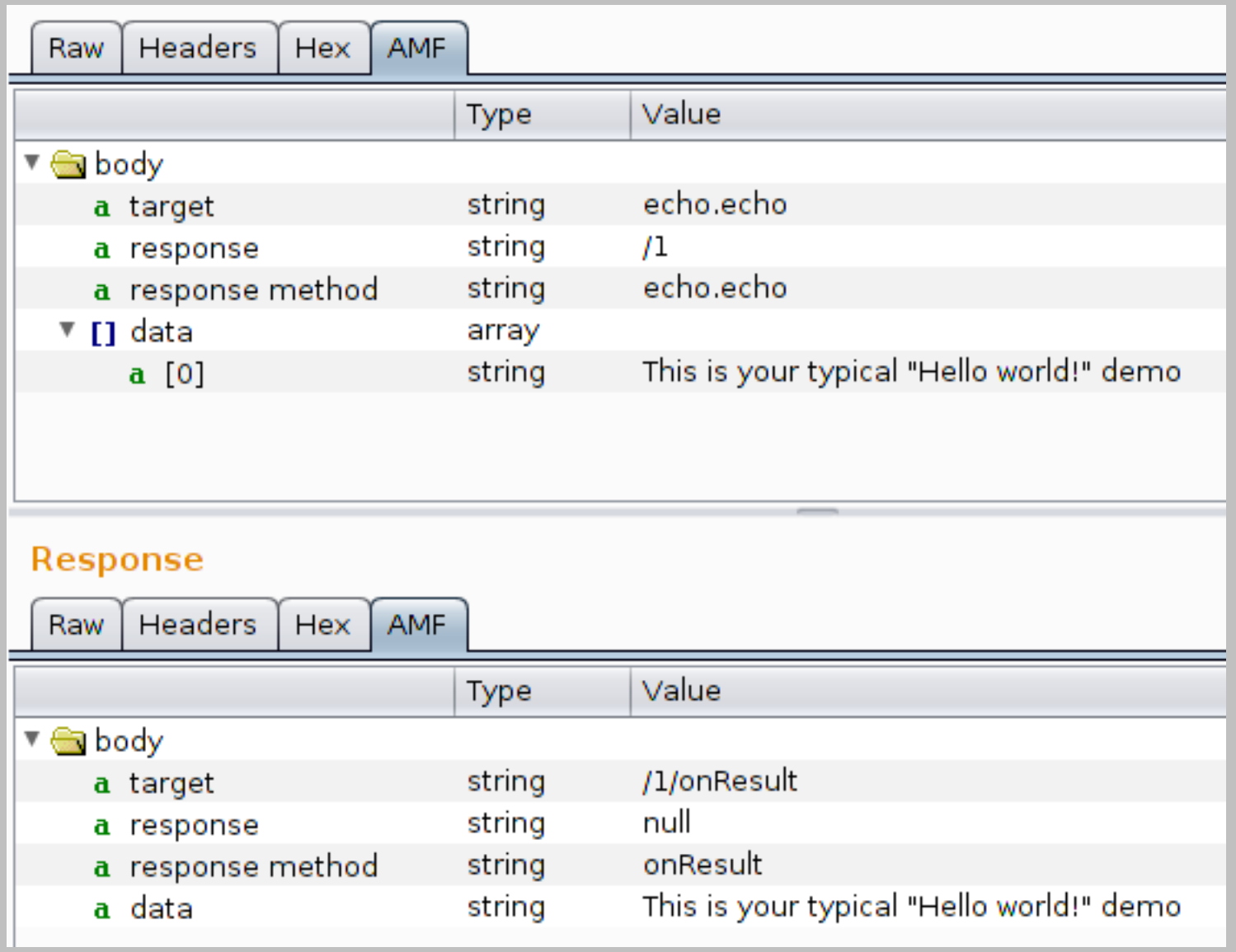
Raw | Headers | Hex | XML

```
<?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
target
string
echo.echo
response
string
/1
response method
string
echo.echo
data
array
[0]
string
This is your typical "Hello world!" demo
Response
Raw
Headers
Hex
AMF
Type
Value
body
target
string
/1/onResult
response
string
null
response method
string
onResult
data
string
This is your typical "Hello world!" demo

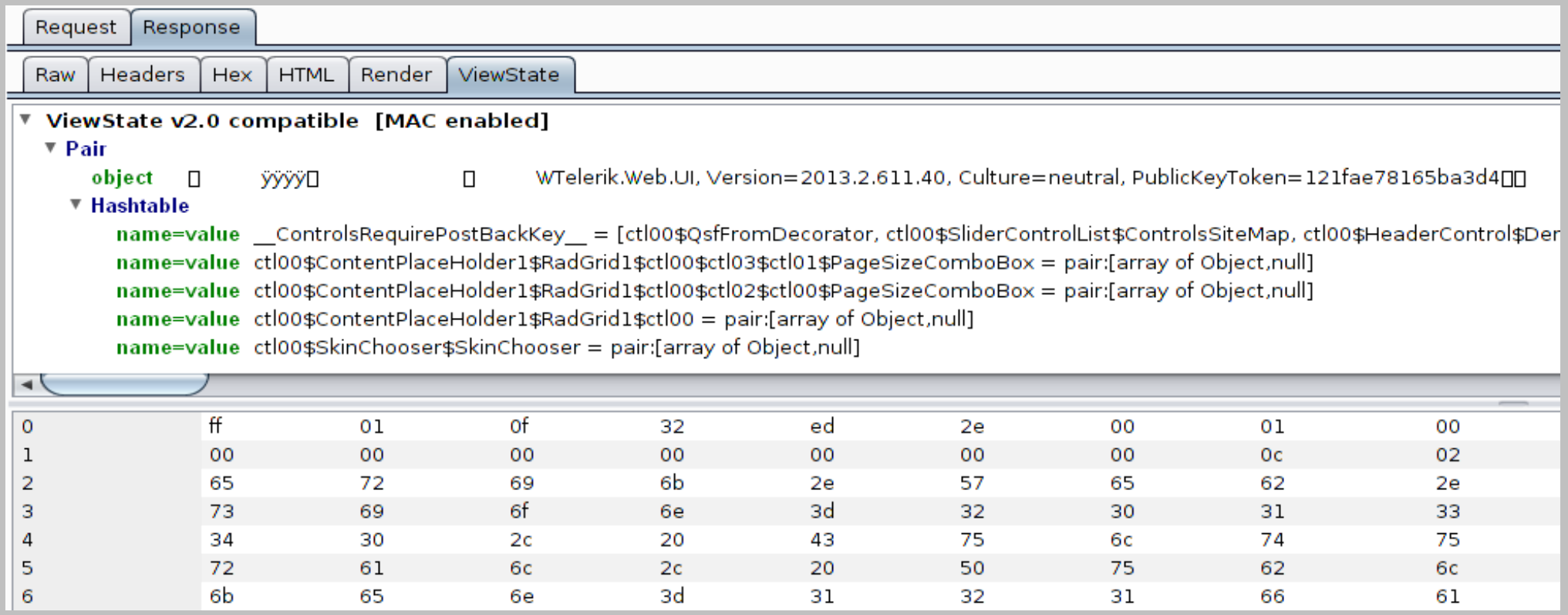
ViewState

Request | Response

Raw | Headers | Hex | HTML | Render | ViewState

```
        <input type="hidden" name="ctl00_QsfStyleSheetManager_TSSM" id="ctl00_QsfStyleSheetManager_TSSM" value="" />
        <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
        <input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
        <input type="hidden" name="__LASTFOCUS" id="__LASTFOCUS" value="" />
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPMuOuAAEAAAD/////AQAAAAAAAAAMAgAAAFdUZWxlcmlrLldlYi5VSSwgVmVyc2lvbj0yMDEzLjIuNjExLjQwLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTEyMWZhZTc4MTY1Ym
lZERhdGEHAgIAAAAJAwAAAA8DAAAArRYAAALsvQdgHEmWJSYvbcp7fOr1StfgdKEIgGATJNiQQBDswYjN5pLsHWlHIymrKoHKZVZlXWYWQMztnbz33nvvvffee++997o7nU4n99//P1xmZAFs9s5K2smeIYCq
HhJf+fPdn5y/ft89zvNT3317Bf9Pr/3/E22V66/Wvzk+qc+/8nr7Lv3lxm9++2Ln/zB7Nt181M/8dWLn/q8/MHO83fz/M1qPdm7X3659xMC88LBfPLsVZ1/+yeePTmdEYxXb3/q+OzZ072f+O7J57/PS8H14P
mnz9rqf9yev3w+vf57iv5/PPd+WTxbP1Tv/fZ5U99u6Tx7K5+HxrH9Ns/ufNTi7KZOVimez+5M/u8XP/UvS8uaWyL3+f3/kn6/MUPni+e/WD67Yu7029/h979yZ+ePd1dThf1W8GLxnZxcEC4nh7/xDGN7SfO
+OAtufHF199Z7pXNtn1kx9grrgNz+1PaJufyE9OX/xguvOi+X1+7xc/ePL6J99N936fNvvu2cXO936xeP7dF5eT5avryd4VfUa/FO/4+5+6953VT52Abg/X3754dX72ky9o7N/B3D19enXw3eP5wcmTn3j1be
fXGA+ysvJT+/sPP/p4/UXJ/tX1Obp7LvvdmZEr5ffvV/Ofu9XNL9XzdmzJ7u/D97bacv8J19dE13XL79L/L13uvv7/OCrvS/evP3Bi8+/uvry6dunX1zv7xl+IrzPwHNPgD/9PL44eyK4ngmun1/kJ7sH8lef
mpvvmO+u3r2k/rdwbPj6vjpTz2xcM6fvGukOemT7CeIneg5P3min33x5CfNZO9+4vc6Pt77CcgH4fv7fP7tq+lEGjO5/u5b+oeeb19d6GdPj3/yK/PZVycXxy/eAn/ig+8+mR98u4/zwdmPcPORrj/C9Ue4/i
7Szanfl7Oyt+nuP+Tr18H9uP6i6enP3j+O2frFz99+u75T//E+9mRN6fXX3z3p+Y/9Wa6/8Wb34e+P/3BTz39ie8+X/w+L78WzS9ekT386smTr77T/D6w9cdkc6zt/MmTyefPyC8QX+dD4D/dEfhvvvuTO9PF
w8aH3ms5CuQzxn28fmrxcPrn/q9X+yIX/RB4zh9tffucrYXwNfPgP9XH4T/8c58nn83gP3O9efP7ouv9kF4P9M5NzxE/jNx91e75Qz+I/tlHwT/99rAU53vQKeLD6LTyduHpBHKn/6pN2dXXzydBWPqfkey9E
lXfTbfFC/p6dBv2+y777b+6nf+zvBmIfaEH5ffBi9Zy9J9zaTvYcdPeh9Tvz19Cc+iF9Pv0Is1JFj+Qz02/8g+jOpKX75vZ8OPxXK8ucEn+M9xv8D5Y1g7fzUd39qNVmUOx2dOfmOxjM//tDx7E6WL8quXv3q
iFrtkfzD7RHP/lTK4pp5x17/t2MbNHvw/PyEx8In3ybnz676sD/vX/qu2fXXzD+H2aPKENS/j5vv9PMvvuTod3wPqe+v/th8j7/vS1f9HZyb/aDF+Hcn/Ok5yke3pv+YGZzQcfkY7GPesF9fv5T7/bf/D57pG
7iB/lBO8/lPd3xK7+5OcPd3+fvYvzk735W/GPzlhGAr+H35tRzuOn5vA/v33VLrv9Wb+G2/7U5+TnltN7PxGDK74Ij+XVtydEO4LXw5/9jFdo8+Ls9/m938bgqL9wQHkr93ukXWjbGb9V4DvG+g9t9BR9/F5v
/9UOZ3HxuHsGPp+svOQ8pDvLicO1th8sk2S+UR/OXFZe8Nz+lPUbvdq8vlXOfkKbAO3X73JKPdI41rTz/sD8EX/C/+9oZzXD37q947yn9PXjPPMxmFRPujoY9Cj/1kEH9WrTD/7e6yd6EdpZ36PtLP67CvM5b
se/LkuOTrH2TffUgxKXjyi/UXxT7lNk/XL54eN2enNG/ffrU7XXz1cLL4yV3SSfPJyRVmifRh+dOv937yPumo+qe+u/+Qcv/vKMouX/zg4t2Ln/7J4vd58+Ltiye/z/VPcdzxE+dPjil/vHhRUO5yjhw/bMXx
LZ1+pTm3saKyic27tqgW23sZOI19Kk6Vsdm4hOXczFe9neBc6I+1Hvo1ZMTh19Xh+IdT2ceW3xPHL4DuvOLeExj5+rKzdX7611TrulP/Q3rz6ZNXTwJ9Dz04W4DvFIYb97ff3PvJHZqPS9U5nn7Vtm68Q/rO5F
4rgy795niYnzCjXrO5Jmj7zPoG5of9gXM74rD7+3hS37nd+z8+zpV2/4+ru3NOvT44q3lN7/9FdYDf+Li+esn382++5P3vrqHdbGvLt7ce7JDtm6VL57tQAcKb5t1L/9n4Ff+opefn33yleLZ21dYu3p6dfn7
Av3Z89eXZp1OSfZF1+9/PzValY8oX53CvrsB78P4TD9Nq1H7u3TWhet431O+cni7JOnP1EB+4uX3z62v/P/n72qst/7i4uf+r3nc+bL1+QdfneX1uZekL54tvNT9J21wddPYEt47e079764mC3Kckbrf8iVOr
b/gRouQdann2b4hzyLUA/+p1OHfWzmF7MPp+XZ6e6fkx8910/9+yN4nRFOu+KcN/Jf2Ln97L9njzZmVw/WZBP/wNqc4/ktiF489niK4H1+e4l6e8L9nvufYdiq/sOZ5jHU/r+QNp8+8n8p/a+usA6JXTu5MTS
oZx4P3O///Jb5dYO51PPn9336PbBcFhP/+M1pvPngVOuZwsqO3nOC27P3i+Z9Zi31Fb+p1O1e9zj+ewOfv8/uXs5AnWk+dEoOvKZ3fHw989L568IR+DYvqyBc8QjciuzKozWrPEPPw+35ORzRgHQydau96/oP
S2c+I/8CTX9H4y8uZ9unN2U5GPEf8VGafPyMee3gd5a2n74qXbyP89YZlPZgLrJ9PSTZJfzOvvPz87SfkKzTTva8Onu+9/YRwXpx9m3F5Szy4ntxjXvlBxrh8dfFTWAd+Db45U17054bmUcbJa/MBLb796pL/
6Iz/+RXy7p1yMfkA/3ePwk/6FP6bIWxTIsnRU5jyOiXOLm9X1JMfAoe+mrvIfmWNJeAwTKn8/H57BI6oTPeivDb/am9iwvM6U/85IufeP72/rOfPDm+fr68uPzi+v6+kdmphWtoeUX8MKvIT72QeSd9E9cfsK
4cDppPidZuYKsE+33OAfm+/e5R+tTsNUnLBegOfTc5XQpvAOem9q8BOsL2KqltRUnD69eWh3OzvOuePwE+Q9zGe+zGraNaEv89+ynaczkk/yEwesHOAuEL/TwnO3R8gvSrftRu3L2+TvKzVk5KPNvI357wfZ4
XtsD69gv1g3fv5uPiWd8Pw4GP9Pz8ivn+ztXBD/rmai61uy7xV8mp8knTR9a/lNbOEp2OHywxBPgxfe8hyQXOvrVfDFiA+ha5YsOyuKsOhnONttxv37/N4/ObW9kONysniGvNRbOsVfZZ8/hG1bkGzzGiR9L3
pitWX1I5tvvIk9wO/i9ZHL4yNme7twuaVO5/2caVxfv6Ta9g2GvMzpUnoi3k6OhjT5zIetUH3CAei9U+J/v/pszOaZ/GygG58tzshP9uMkeeW25xeCW2+utK2pBtJ3havfN3tdCv5buRPN7/P7l1i/JCVS/hI
31LPPt7POHMCpyJLj/5A+ePue98ecy/+3CX3pvT/CF2gR3YhTxA/ogu5O/MiQ6/z8OzxXxn9u3jT59fP7w3uzcle27k/z7RZOeS5q2ZnjycEO3WpHfb3+e7q3l+8pD55fnvDf8MdNj1+YL8BPZzf8Dr8MX9av
37OO68CcenpHMsO747k+OgEk66hr6n8ZtfLFigy7+qck92JpnNIeIFX/iYvJdti872e/9hOaR+IZi2jP4ZNdif4j/wXO7U+N3IHYhOOFjZz1GdPpp1ukqk5A9yo9wxOn788znIS6kS59dQZ95PAY7R3hBrz/8
b/Deh3rIeTzEyOvyc5ePf+9Q5yfL579YPrtiw7e8v+BMbq5NL446Zyf+rzcw+ffvpi/+Sm1UdMfPL8++Q1Z/7iL54rXp3S1BL8//e5x+eI+fLPJ6/uU13vX2Hev73+b/B6M96efv3OH/+3ii59sJ1/dKOnP/2
M9/3E+ouT/avnP/1+eb7f56en936fNz/5Oy/e/D7vvnzzBdmN4/Ovf3Kn+bnre3dGsEknQO++W/O+xdXFTxKNWEZ/emeH+pC+Tp48RT4PtvE1OZxyPCTTVw2yt78P3ttpy/wnX11SPL5++d2zey/2Tnd/nx9
z7XuHz5xfoVwYe++X2u7z//qd+7FN/lJ5/MyUe++KLO5r5EPA79R7747/3ipOlGKU4+I3x/in19Og8PXwgNaXxXFz9xj9aCvv2T1z/lZpfgI/f3rHmOrMp38d4L9PXVZK8tJz+9W7z4wWz+4rtf7L746dP7X/
xT95GDOEO4Bf9ZPnV58/IJz2+/u5ua/mZfCr2W39YMvf82c9d37+38ONTanP/ye8tNDn+idPPWdkft6fkF5G/Vl6xbF/8Ps+YSfdo7WLvxTXZYaatZ8+ffHKJacBcHHz+BOvaT569JntHdvEn3/7eu+Sza9w6
ll8++pJ9VOOvE/r4yfHr36fk3DNqjPWOeeHO5/tv37NcU75O+TL/gTyMj8J/3OnPH3y6lXYtnzovt/rrI+9cjQhH9TRBHle77uAXu8OfuLJq1X8u92wL+Ref4oygcc/8ZNrF4/ep9zz2fonv3q7R173J8l/Iv
MX11jkzXon7Q8dfGVx1PIubvvXpOH37O7fvZ5Gf/u995F3kPiLc5vXxyYtVFaO3uofPXVybPTUC78924F+/jsidKF+Gn1brr3+7RmjiEPhp/Pvv3sBz9V7K5+n/n+868oJp6dUo5gr/3J6eLq2avfe/9S/N6P
OrJVz/5yfM9jsUubb799/7iEvEo4TEngwQ7cOnHaRQr6Frjqz3iOfi8+y+vX/B4CZd2cr1r6IO+nvJaMcs1rU18Pn97+oT4++LsCf1t5uH3wrw/fWvhPv3qWuBizr8Yir/2fnL/92F5Jn1z7wnlNGbEy7st6S
ffDM4HrymNdDTJz/xjuLVd8Qvr+5PKZb8fe59YXAh+n1H19TnQ2vq5MM8bH5i8ez6J5Y/uUNxxvrnRkeITv/Zn1dDs/shzX7vFlf5E8vrLJMnorftmvlP7H6x5nYn93+a9fab4Ov8Tf7LDvHAL/p9fu+L95XD
6w8XTw5Wf3E75U3v9fx8tkv+uTVqqOOvv3tyRefzi4+++z/CQAA//8LGAUFHl9fQ29udHJvbHNSZXFlaXJlUG9zdEJhY2tLZXlfXxYOBRZjdGwwMCRRc2ZGcm9tRGVjb3JhdG9yBSdjdGwwMCRTbGlkZXJDb2
vbnRyb2wkU2VhcmNoQm94BRhjdGwwMCRIZWFkZXJDb250cm9sJFByZXYFGGNObDAwJEh1YWRlckNvbnRyb2wkTmV4dAUyY3RsMDAkTGVmdE5hdmlnYXRpb25Db250cm9sJENvbnRyb2xEZW1vc05hdmlnYXRp
2ZTa2luUm9OYXRvcgUjY3RsMDAkQ29udGVudFBsYWNlSG9sZGVyMSRDaGVjaOJveDEFImNObDAwJENvbnRlbnRQbGFjZUhvbGRlcjEkUmFkR3JpZDEFRWNObDAwJENvbnRlbnRQbGFjZUhvbGRlcjEkUmFkR3
EZXNjcmlwdGlvblZpd2VyJFRhYlNOcmlwRGVtb1Jlc291cmNlcwU/Y3RsMDAkQ29kZVZpZXdlciREZXNjcmlwdGlvblZpd2VyJE1lbHRpUGFnZURlbW9SZXNvdXJjZXNDb250ZW50OBSJjdGwwMCRDb2RlVml1
GNObDAwJGNObDAzJGNObDAxJFBhZ2VTaXp1Q29tYm9Cb3gPFCsAAgUCNTAFAjUwZAVFY3RsMDAkQ29udGVudFBsYWN1SG9sZGVyMSRSYWRHcmlkMSRjdGwwMCRjdGwwMiRjdGwwMCRQYWdlU2l6ZUNvbWJvQm
AAxQrAAJkFwQFB18hRFNJQwLYBAUIXyFQQ291bnQCDAULXyFJdGVtQ291bnQCMgUQQ3VycmVudFBhZ2VJbmRleGYWAh4DX3N1FgIeAl9jZmRkBR1jdGwwMCRTa2luQ2hvb3N1ciRTa2luQ2hvb3N1cg8UKwAC
      </div>
```

ViewState



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

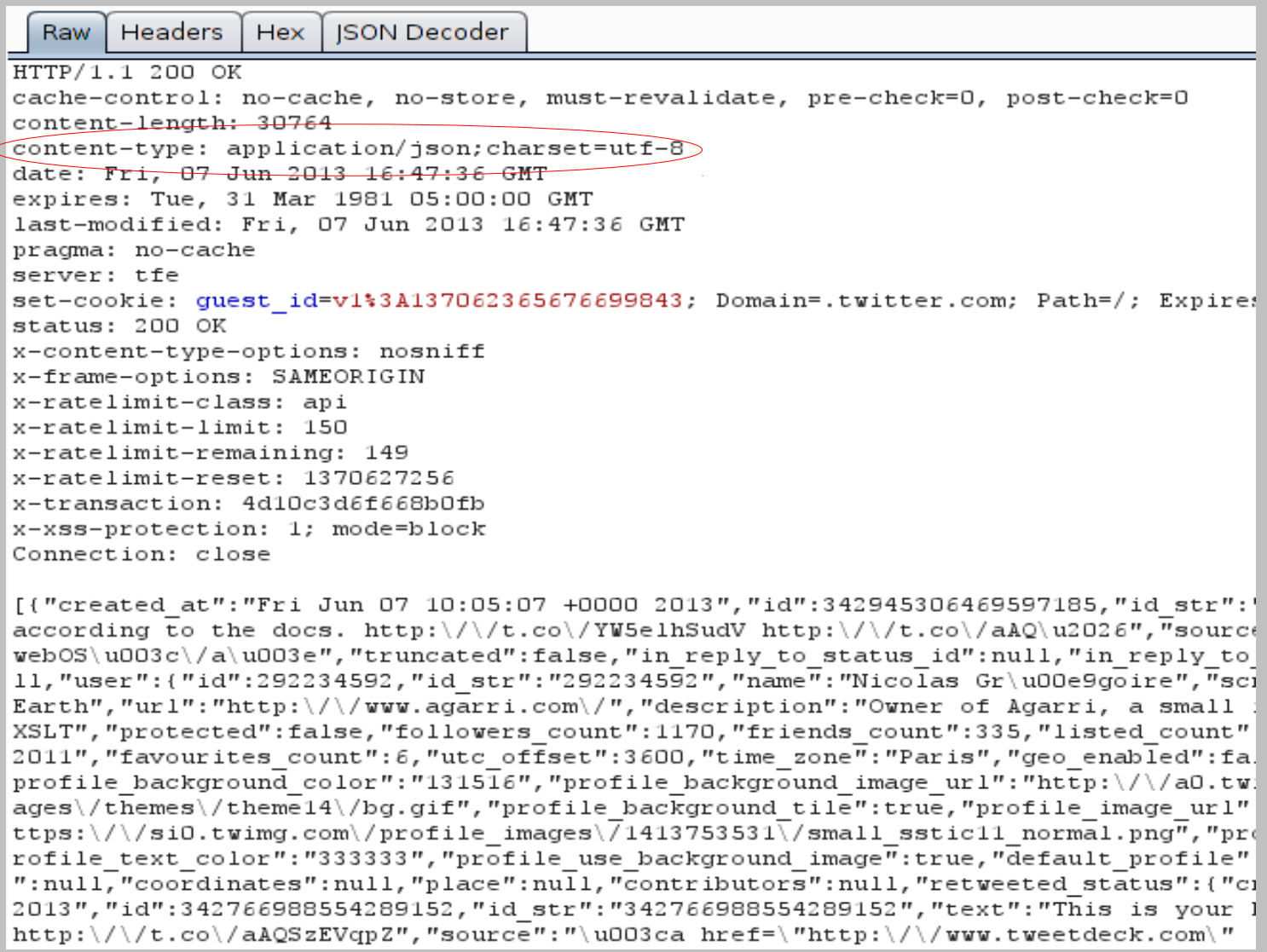
Data visualization

By default

Via extensions

JSON

http://api.twitter.com/1/statuses/user_timeline.json



Raw | Headers | Hex | JSON Decoder

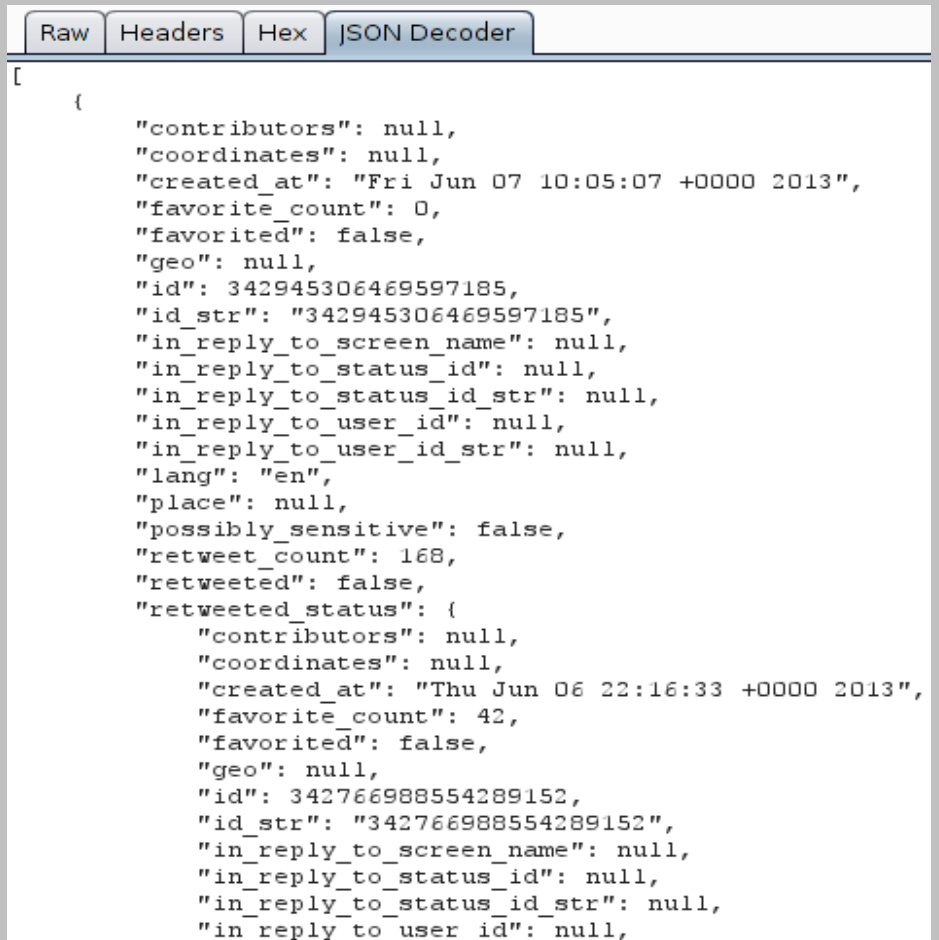
```
HTTP/1.1 200 OK
cache-control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
content-length: 30764
content-type: application/json;charset=utf-8
date: Fri, 07 Jun 2013 16:47:36 GMT
expires: Tue, 31 Mar 1981 05:00:00 GMT
last-modified: Fri, 07 Jun 2013 16:47:36 GMT
pragma: no-cache
server: tfe
set-cookie: guest_id=v1%3A137062365676699843; Domain=.twitter.com; Path=/; Expires
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":"
according to the docs. http:\/\/t.co\/YW5elhSudV http:\/\/t.co\/aAQ\u2026","source
webOS\u003c\/a\u003e","truncated":false,"in_reply_to_status_id":null,"in_reply_to_
ll,"user":{"id":292234592,"id_str":"292234592","name":"Nicolas Gr\u00e9goire","scr
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":fa
profile_background_color":"131516","profile_background_image_url":"http:\/\/a0.tw
ages\/themes\/theme14\/bg.gif","profile_background_tile":true,"profile_image_url"
ttps:\/\/si0.twimg.com\/profile_images\/1413753531\/small_sstic11_normal.png","pr
rofile_text_color":"333333","profile_use_background_image":true,"default_profile"
":null,"coordinates":null,"place":null,"contributors":null,"retweeted_status":{"cr
2013","id":342766988554289152,"id_str":"342766988554289152","text":"This is your
http:\/\/t.co\/aAQSzEVqpZ","source":"\u003ca href=\"http:\/\/www.tweetdeck.com\"
```

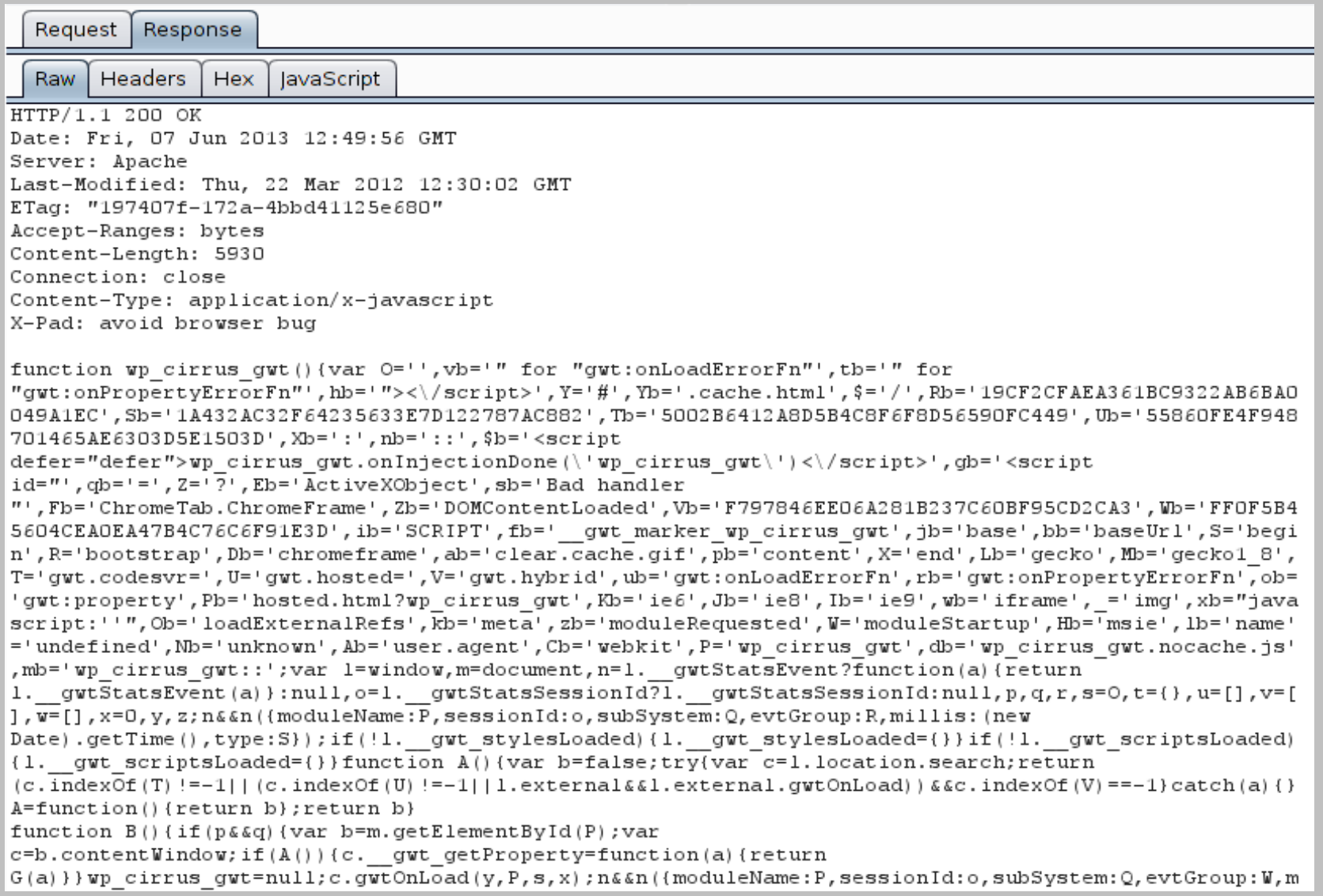
JSON

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

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



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
function wp_cirrus_gwt(){var O='',vb='" for "gwt:onLoadErrorFn"',tb='" for
"gwt:onPropertyErrorFn"',hb='"><\/script>',Y='#',Yb='.cache.html',$='/',Rb='19CF2CFAEA361BC9322AB6BA0
049A1EC',Sb='1A432AC32F64235633E7D122787AC882',Tb='5002B6412A8D5B4C8F6F8D56590FC449',Ub='55860FE4F948
701465AE6303D5E1503D',Xb=':',nb='::',$b='<script
defer="defer">wp_cirrus_gwt.onInjectionDone(\'wp_cirrus_gwt\')<\/script>',gb='<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='chromeframe',ab='clear.cache.gif',pb='content',X='end',Lb='gecko',Mb='gecko1_8',
T='gwt.codesvr=',U='gwt.hosted=',V='gwt.hybrid',ub='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'
,mb='wp_cirrus_gwt::';var l=window,m=document,n=l.__gwtStatsEvent?function(a){return
l.__gwtStatsEvent(a)}:null,o=l.__gwtStatsSessionId?l.__gwtStatsSessionId:null,p,q,r,s=0,t={},u=[],v=[
],w=[],x=0,y,z;n&&n({moduleName:P,sessionId:o,subSystem:Q,evtGroup:R,millis:(new
Date).getTime(),type:S});if(!l.__gwt_stylesLoaded){l.__gwt_stylesLoaded={}}if(!l.__gwt_scriptsLoaded)
{l.__gwt_scriptsLoaded={}}function A(){var b=false;try{var c=l.location.search;return
(c.indexOf(T)!=-1||(c.indexOf(U)!=-1||l.external&&l.external.gwtOnLoad))&&c.indexOf(V)==-1}catch(a){}
A=function(){return b};return b}
function B(){if(p&&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&&n({moduleName:P,sessionId:o,subSystem:Q,evtGroup:W,m

Javascript

Both beautifier extensions use

libs from jsbeautifier.org

burp-suite-beautifier-extension

Uses Rhino to call Javascript from Java

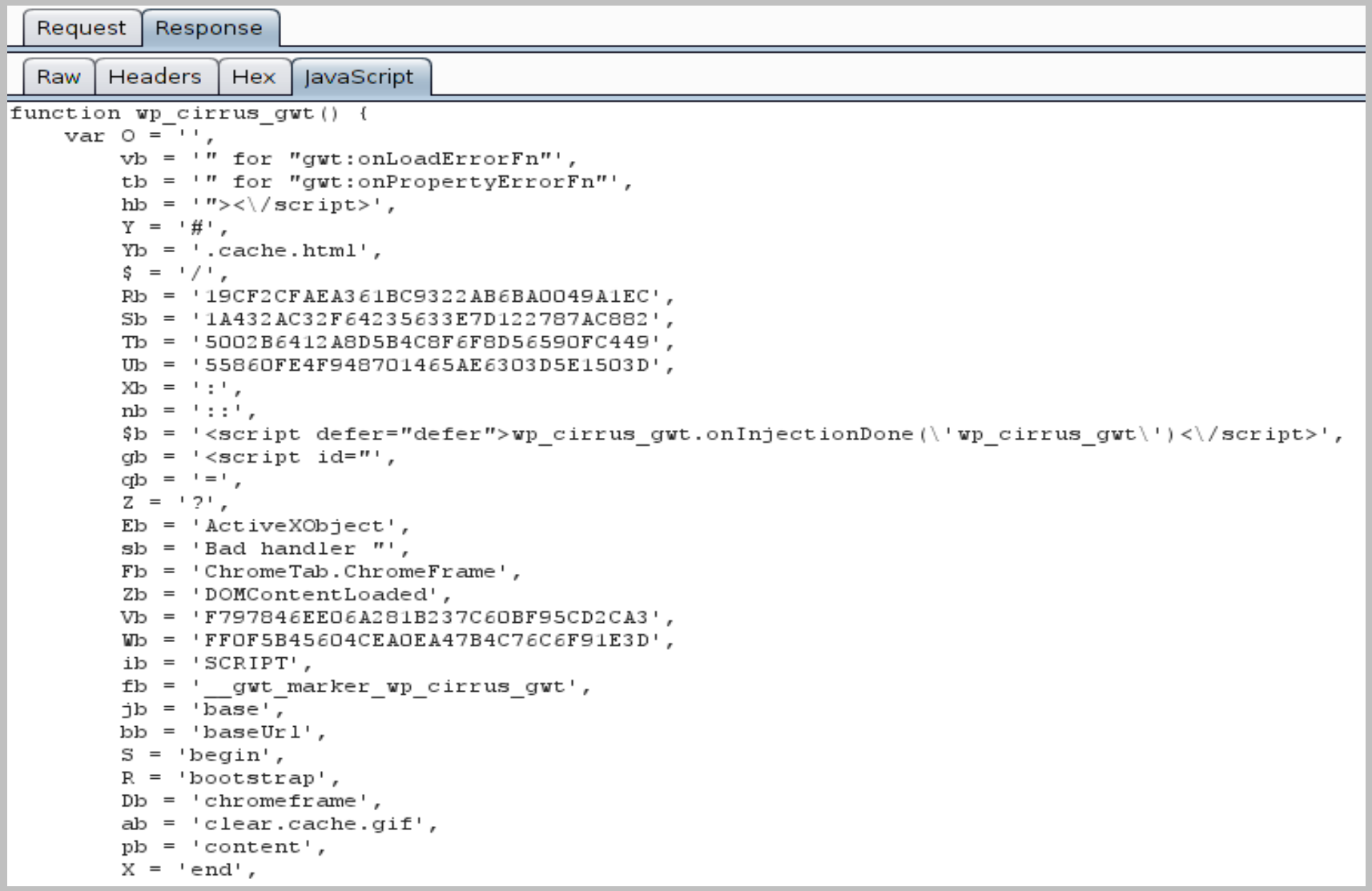
http://code.google.com/p/burp-suite-beautifier-extension/

burp_jsbeautifier

Much cleaner, uses the Python library

https://github.com/Meatballs1/burp_jsbeautifier

Javascript




```
function wp_cirrus_gwt() {
    var O = '',
        vb = '" for "gwt:onLoadErrorFn"',
        tb = '" for "gwt:onPropertyErrorFn"',
        hb = '"><\/script>',
        Y = '#',
        Yb = '.cache.html',
        $ = '/',
        Rb = '19CF2CFAEA361BC9322AB6BA0049A1EC',
        Sb = '1A432AC32F64235633E7D122787AC882',
        Tb = '5002B6412A8D5B4C8F6F8D56590FC449',
        Ub = '55860FE4F948701465AE6303D5E1503D',
        Xb = ':',
        nb = '::',
        $b = '<script defer="defer">wp_cirrus_gwt.onInjectionDone(\'wp_cirrus_gwt\')<\/script>',
        gb = '<script id="',
        qb = '=',
        Z = '?',
        Eb = 'ActiveXObject',
        sb = 'Bad handler "',
        Fb = 'ChromeTab.ChromeFrame',
        Zb = 'DOMContentLoaded',
        Vb = 'F797846EE06A281B237C60BF95CD2CA3',
        Wb = 'FF0F5B45604CEA0EA47B4C76C6F91E3D',
        ib = 'SCRIPT',
        fb = '__gwt_marker_wp_cirrus_gwt',
        jb = 'base',
        bb = 'baseUrl',
        S = 'begin',
        R = 'bootstrap',
        Db = 'chromeframe',
        ab = 'clear.cache.gif',
        pb = 'content',
        X = 'end',
```

Protobuf

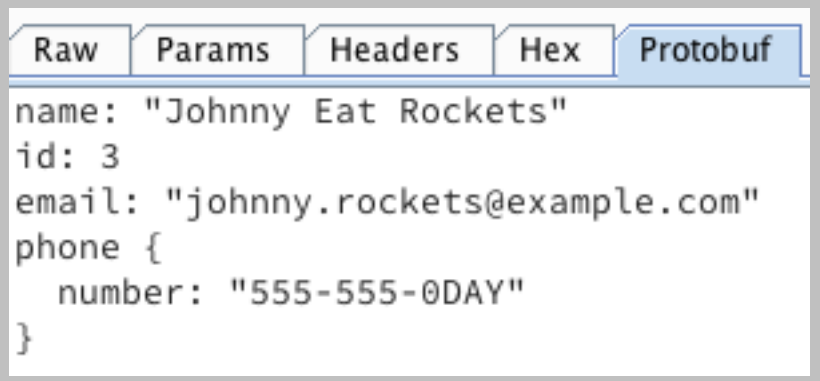
“Google Protocol Buffers”

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

Decode Protobuf messages

Allow tampering if a “.proto” is provided

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



Overview

Data visualization

GUI navigation

Managing state

Common tasks

Intruder payloads

Mobile applications

Extensions

Macros

GUI navigation

Contextual buttons

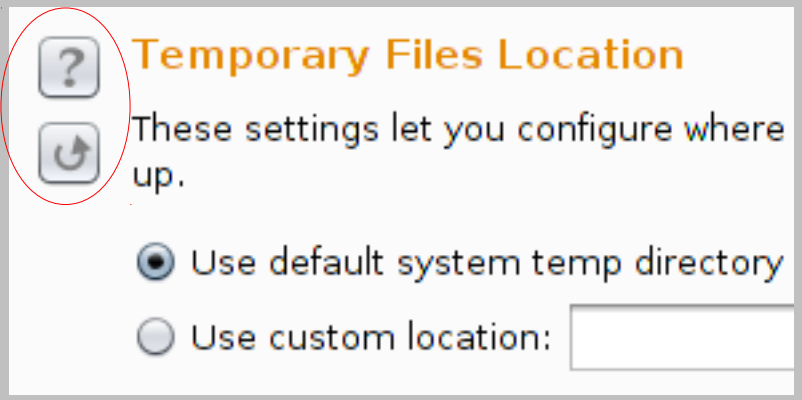
Hotkeys

Auto-scroll in Proxy / History

Custom payload lists

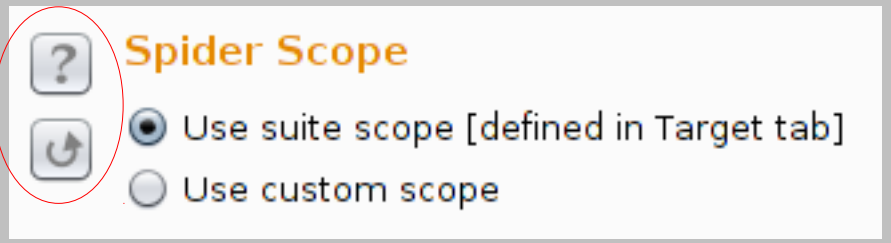
Personalized scans

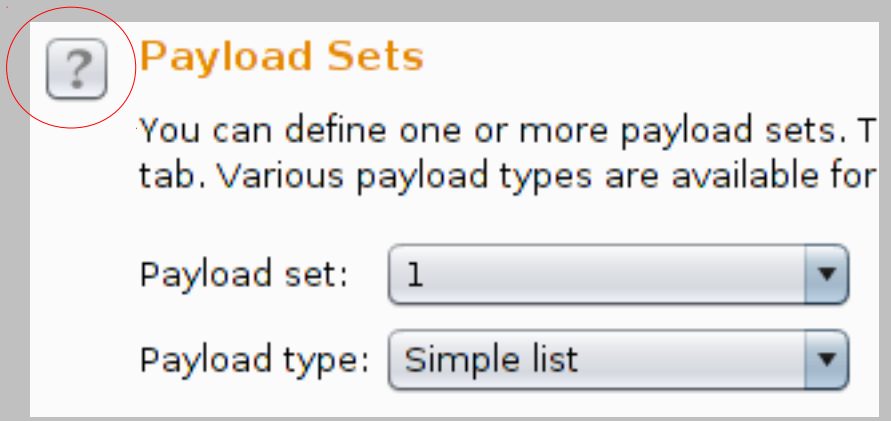
Contextual buttons



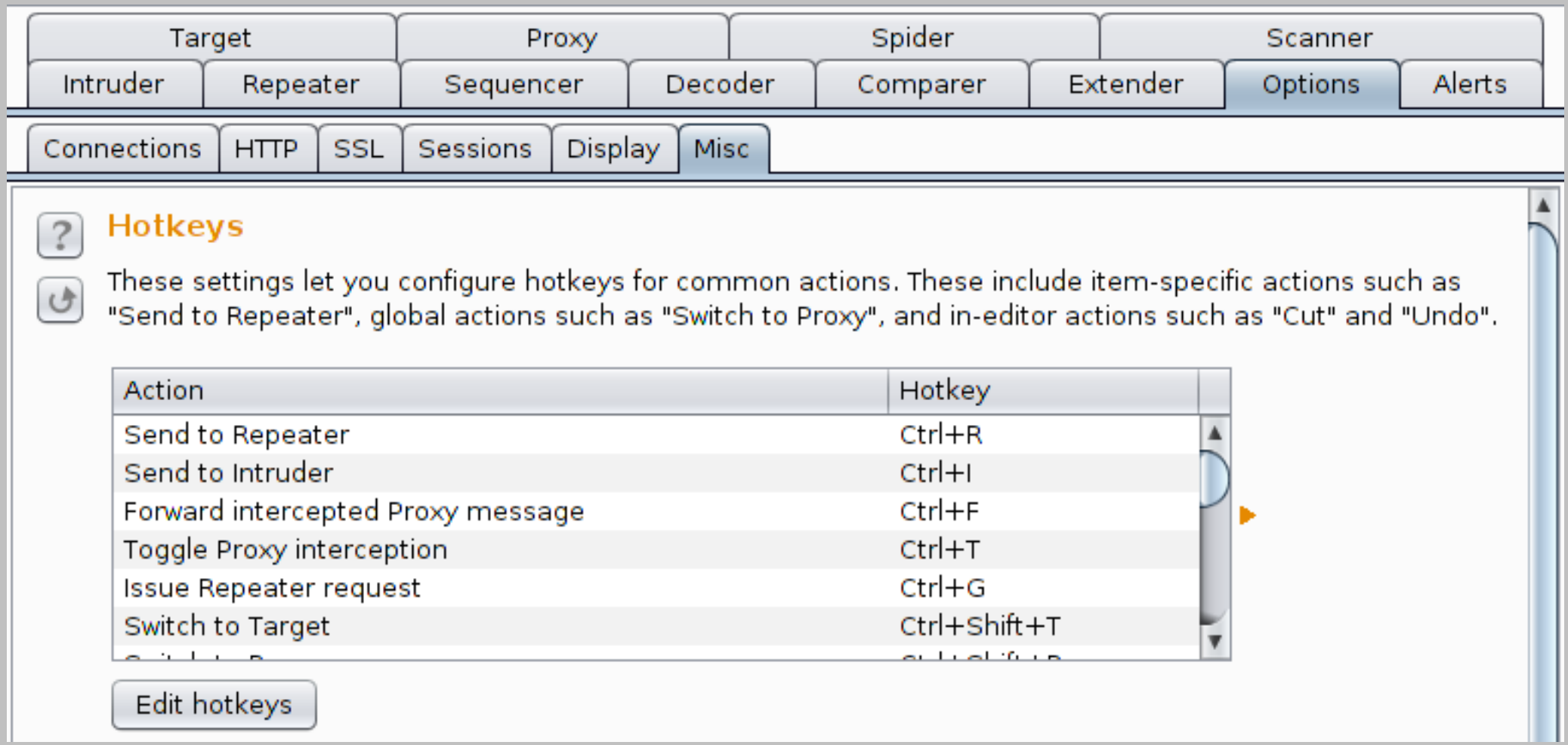
RTFM

Restore defaults





Hotkeys


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
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
Edit hotkeys

Hotkeys

Classic:

Ctrl+X|C|V for “Cut|Copy|Paste”

Decoding:

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

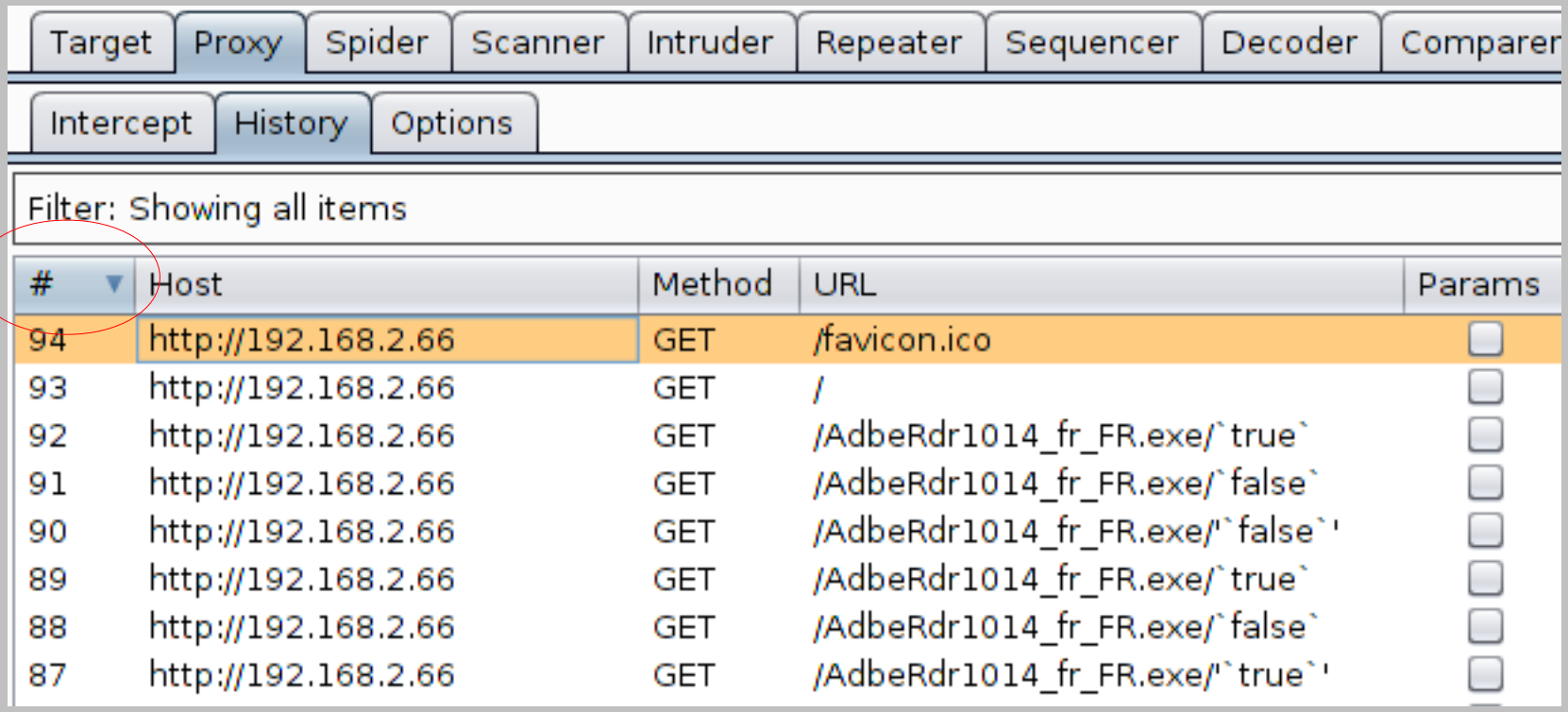
GUI navigation:

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

Personal favorite:

Ctrl+G for "Issue Repeater request"

History auto-scroll



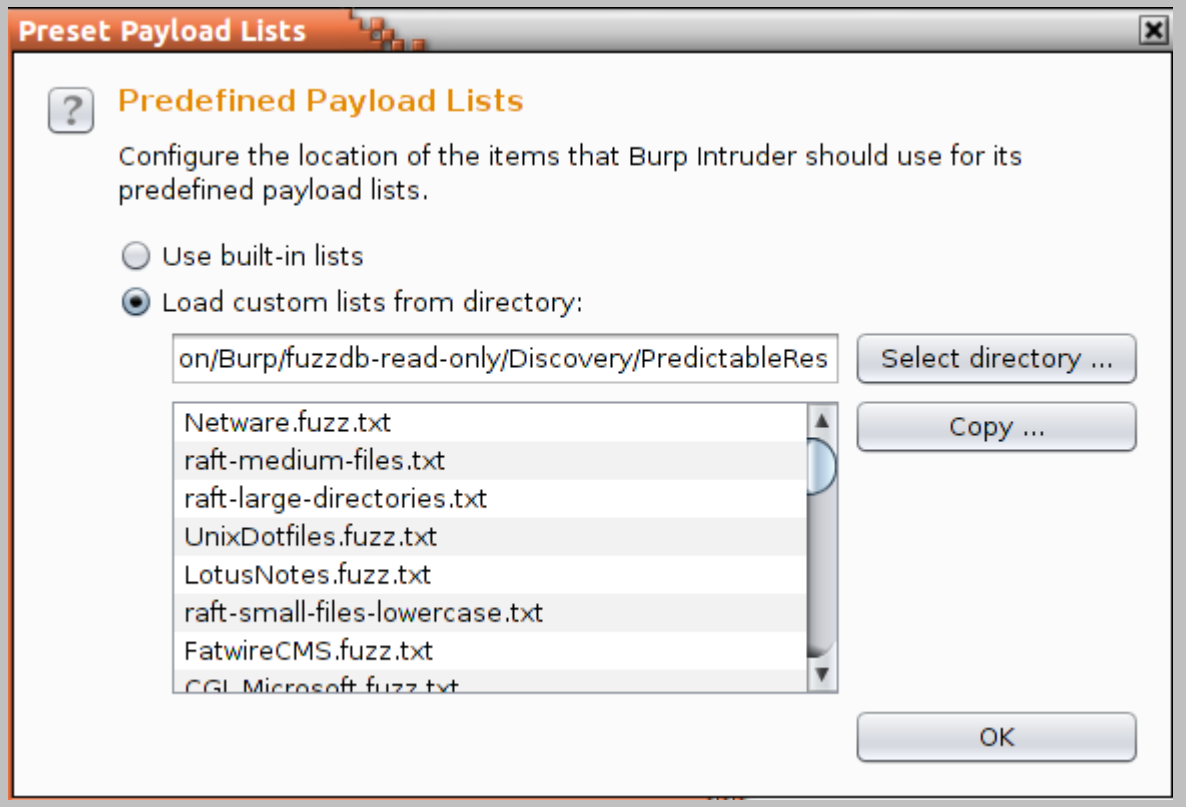
Custom payload lists

Some payload lists are shipped with Burp

Configurable from the Intruder menu

Magic combo:

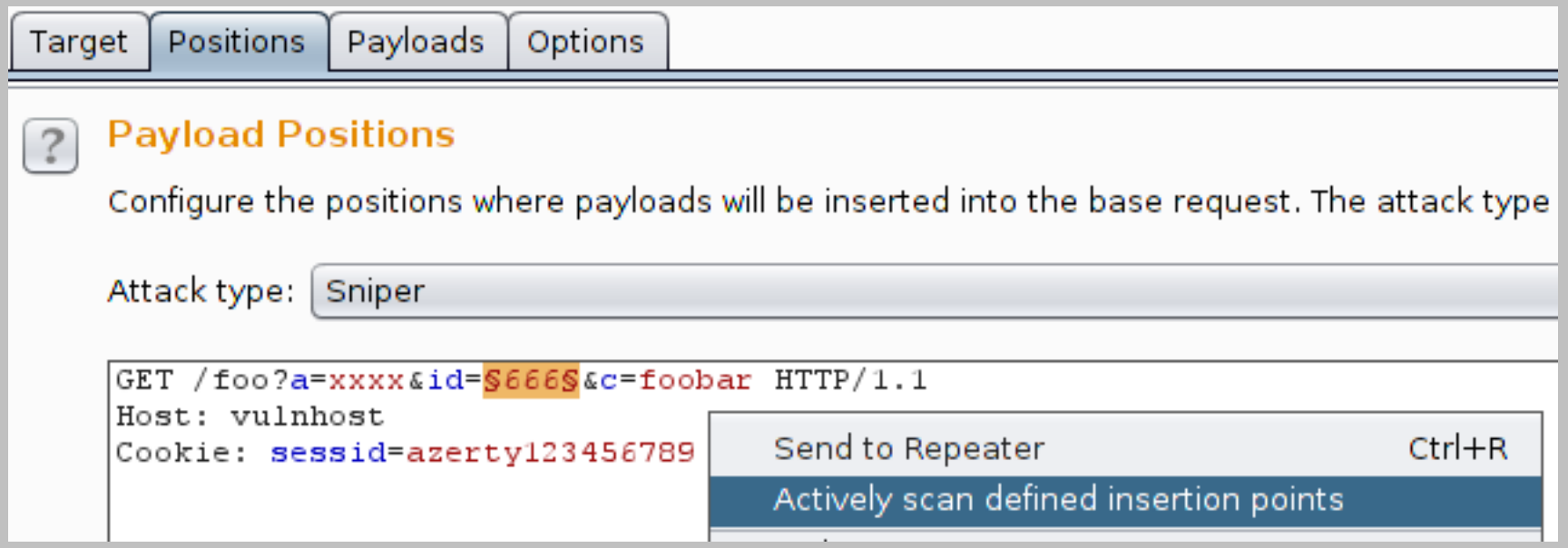
- Nikto
- Burp
- FuzzDB
- DirBuster



Personalized scans

Define your own insertion points in Intruder

Then right-click and select “Actively scan …”



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 ;-)

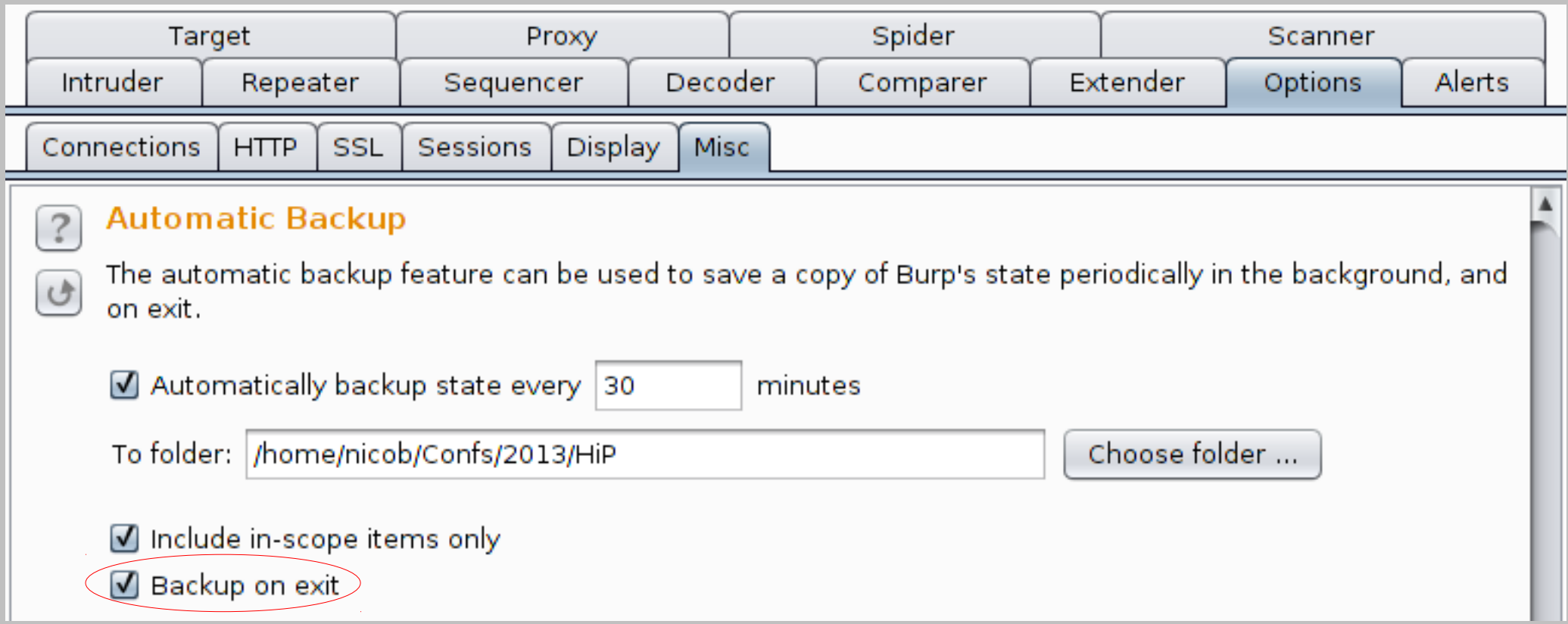
```
An unexpected error has been detected by Java Runtime Environment:

 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



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

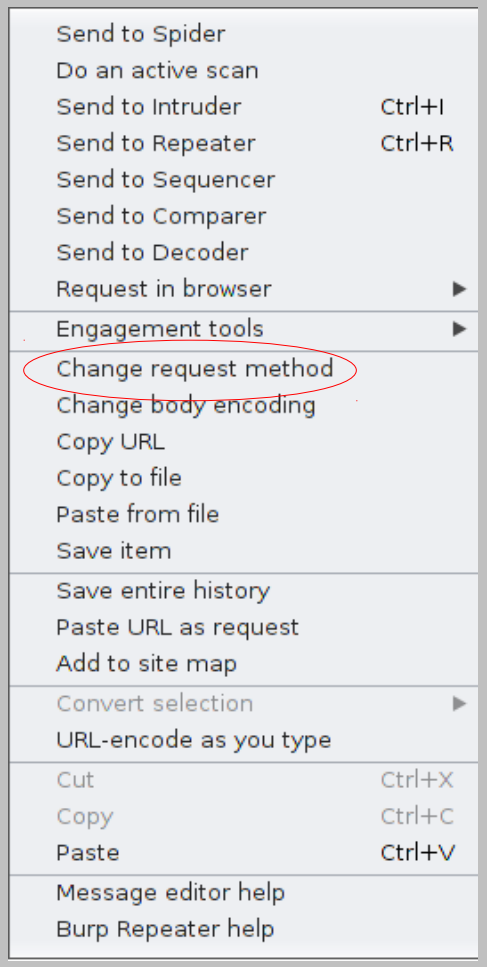
Switching between GET and POST

Non proxy-aware clients

Importing & exporting an URL

GET to POST

Classic question: is it also exploitable via POST?



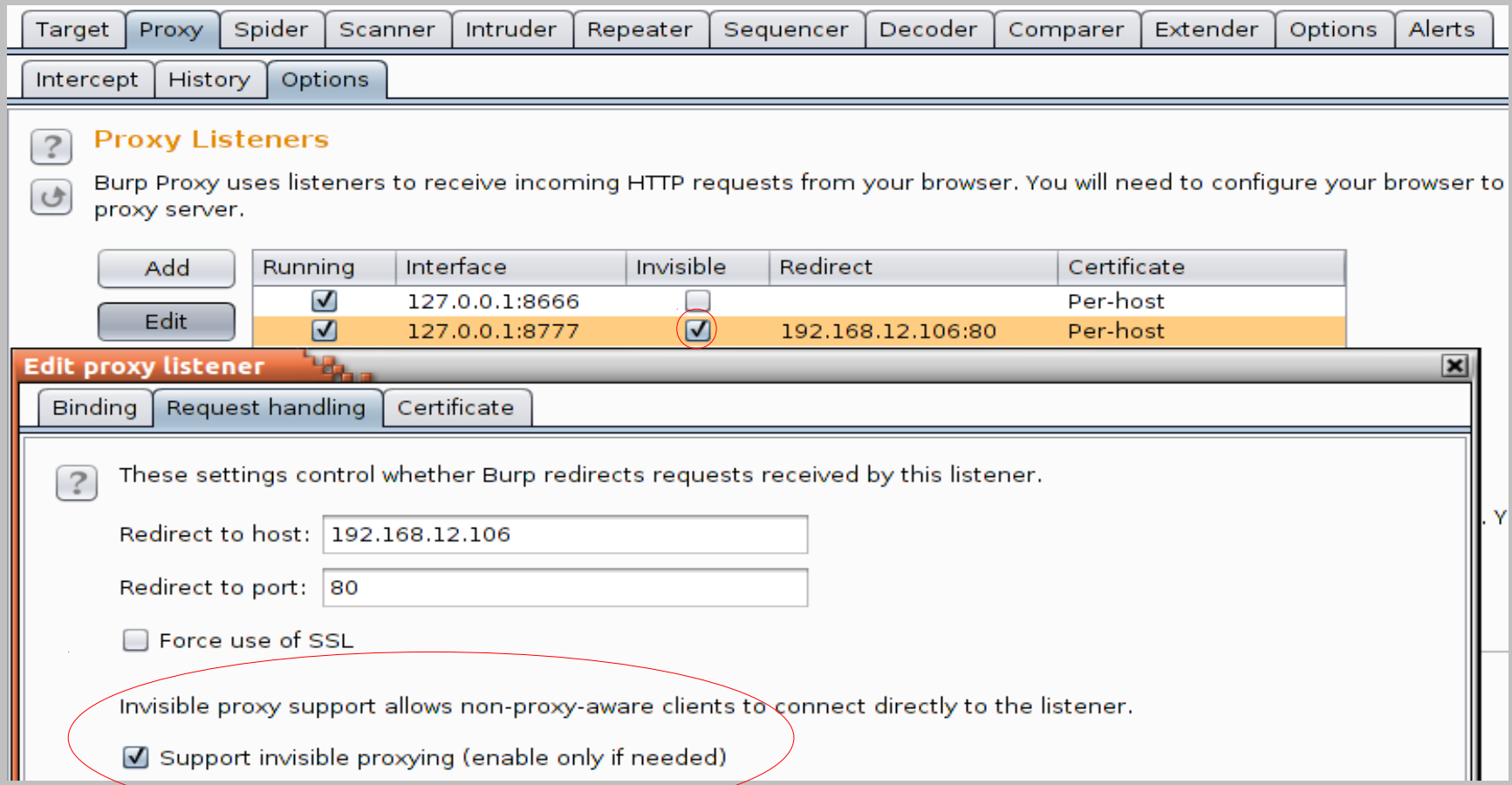

```
GET /foo?a=xxxx&id=1234 HTTP/1.1
Host: vulnhost
```

```
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/



Moving URL in & out

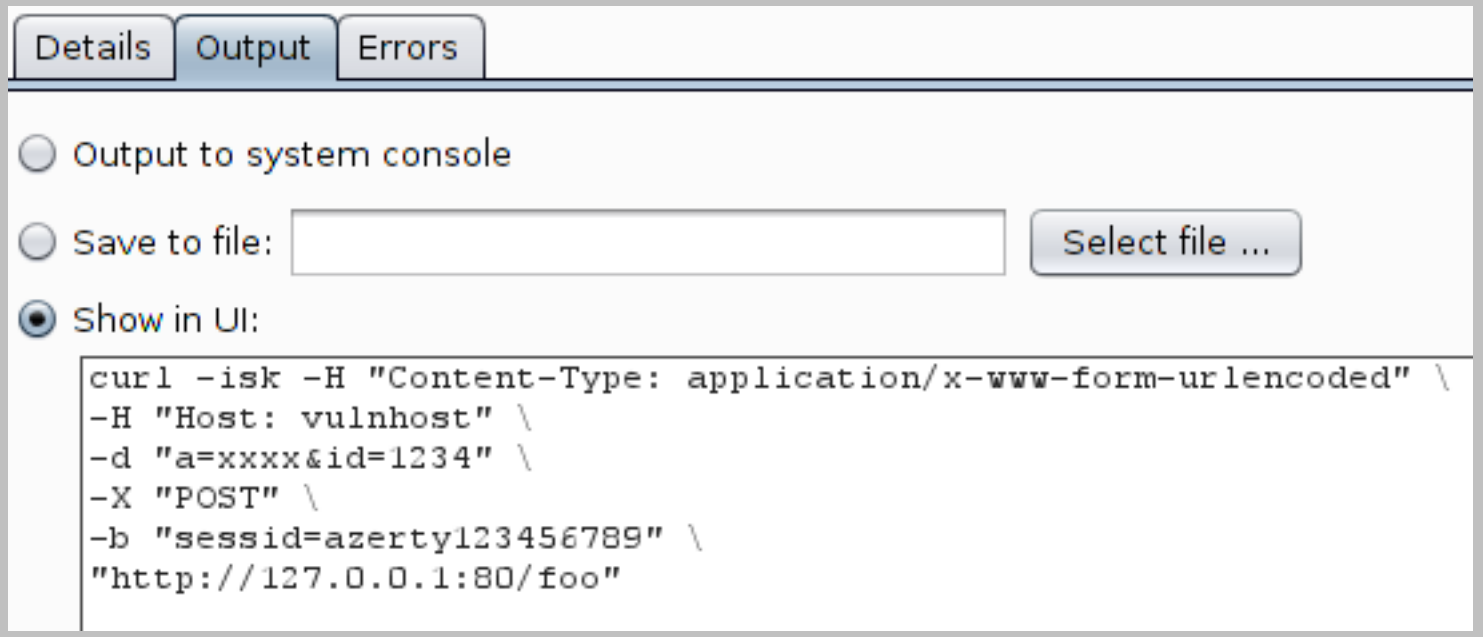
- Import
  - “Paste URL as request”
- Export
  - “Copy URL”
    - Works only with basic GET requests
    - Not body, no headers, no cookies, ...
  - “curlit” extension
    - Generates a “curl” command

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



Overview

Data visualization

GUI navigation

Managing state

Common tasks

Intruder payloads

Mobile applications

Extensions

Macros

Intruder payloads

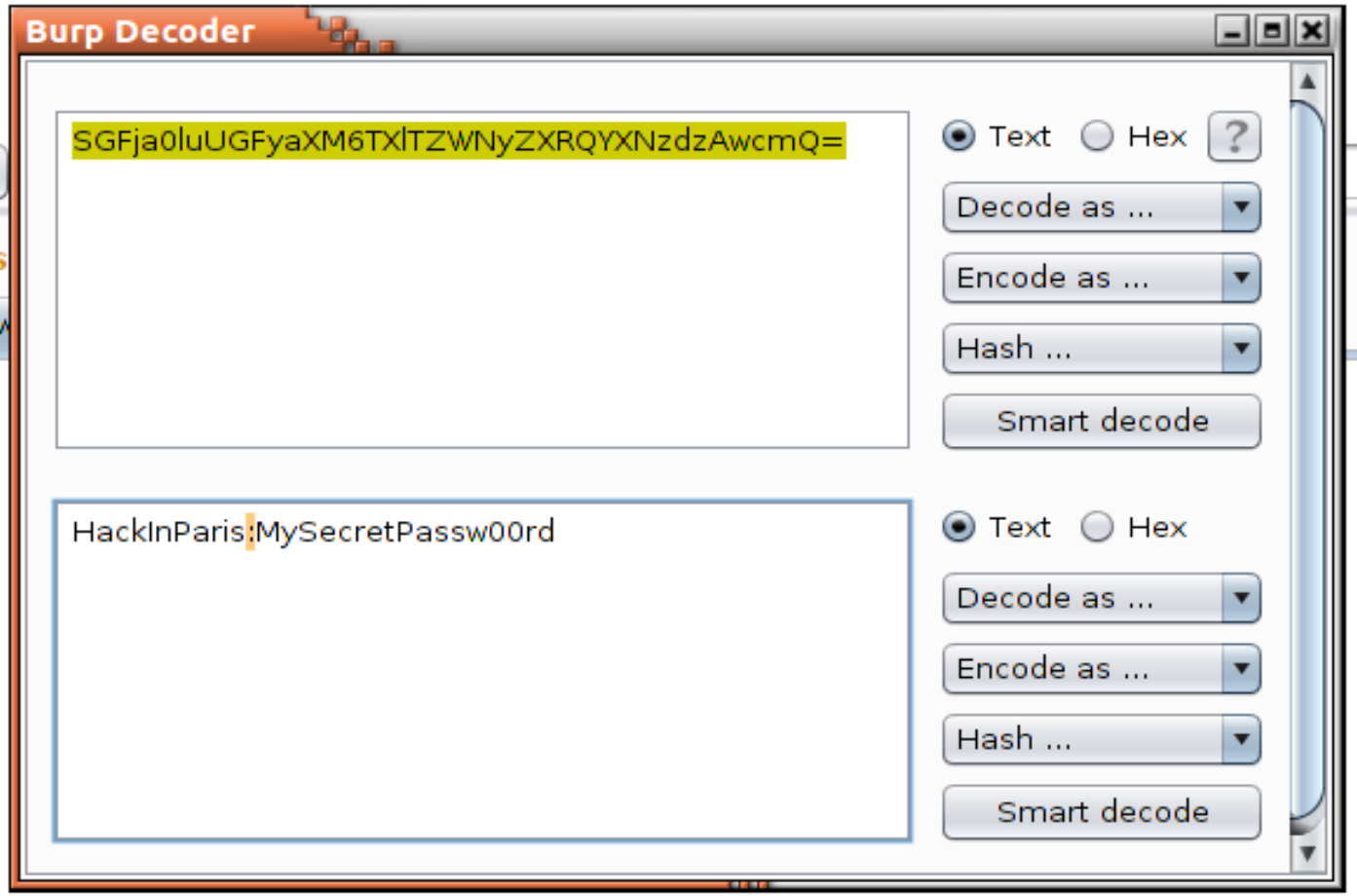
HTTP Basic Authentication

Opaque data

Anti-CSRF tokens

Basic Auth

```
GET /admin/ HTTP/1.1
Host: 127.0.0.1
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Authorization: Basic SGFjaOluUGFyaXM6TXlTZWNyZXRQYXNzdzAwcmQ=
Connection: close
```



Basic Auth

Algorithm

Base64(username + “:” + password)

Blogs

My Sys Admin Cookbook: Use prefix/suffix

SecurityNinja: Use prefix/suffix

SecureState: Use prefix/suffix or precompiled lists

SANS: Use prefix/suffix or precompiled lists

Smeege Sec: Use an extension or precompiled lists

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!

Only the “ePsiLoN's Information Security Blog” was right

Basic Auth

http://blog.securestate.com/burp-suite-series-efficient-use-of-payload-options-when-attacking-http-basic-authentication/

http://carnal0wnage.attackresearch.com/2009/08/using-burp-intruder-to-brute-force.html

http://www.smeegesec.com/2012/02/attacking-basic-authentication-with.html

http://sysadmincookbook.blogspot.fr/2013/01/test.html

http://www.securityninja.co.uk/hacking/burp-suite-tutorial-the-intruder-tool/

http://www.sans.org/reading_room/whitepapers/testing/fuzzing-approach-credentials-discovery-burp-intruder_33214

http://www.dailysecurity.net/2013/03/22/http-basic-authentication-dictionary-and-brute-force-attacks-with-burp-suite/

http://portswigger.net/burp/help/intruder_payloads_types.html#customiterator

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 ":"

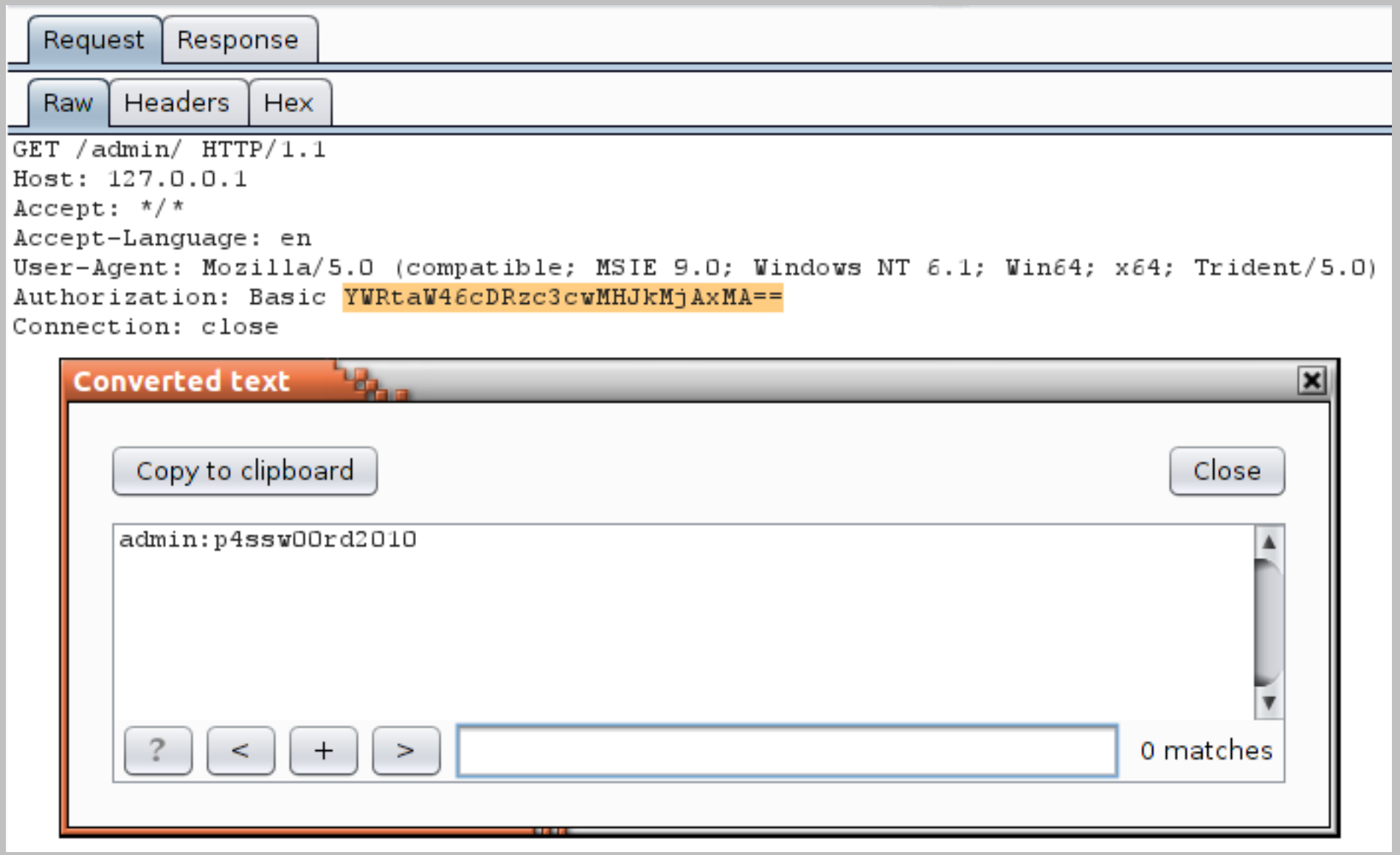
Position #3: list of passwords

Position #4: common suffixes

Payload processing: Base64-encode

Payload encoding: None

Basic Auth


Request
Response
Raw
Headers
Hex
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 clipboard
Close
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 token + authenticated access?

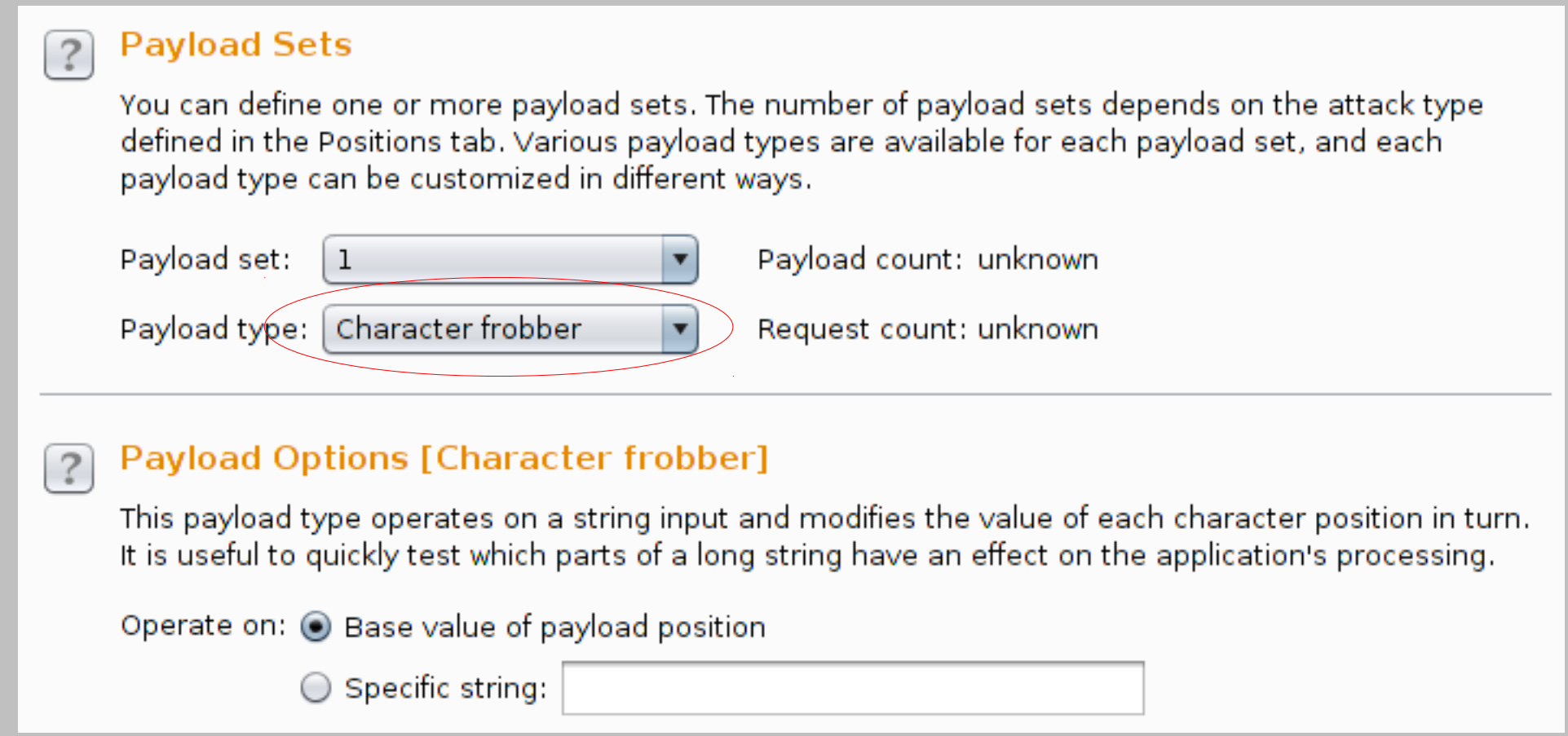
Is the token

- An anti-cache mechanism: OK
- A session ID: not safe (logs, referrer)
- Authentication data provided by the client
  - Checked server-side: OK
  - Not checked server-side: not safe

From the documentation:

> 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: 1
Payload count: unknown
Payload type: Character frobber
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			361	Payroml	100	100
13	a04211e6384ac9801b24db...	200			361	Payrol□	100	100
14	a04211e6384ab:801b24db...	200			361	PayrolÞ	100	100
15	a04211e6384ab9901b24db...	200			361	Payroll	100	100
16	a04211e6384ab9811b24db...	200			361	Payroll	100	100
17	a04211e6384ab9802b24db...	200			361	Payroll	□00	100
18	a04211e6384ab9801c24db...	200			361	Payroll	600	100
19	a04211e6384ab9801b34db...	200			361	Payroll	1 0	100
20	a04211e6384ab9801b25db...	200			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

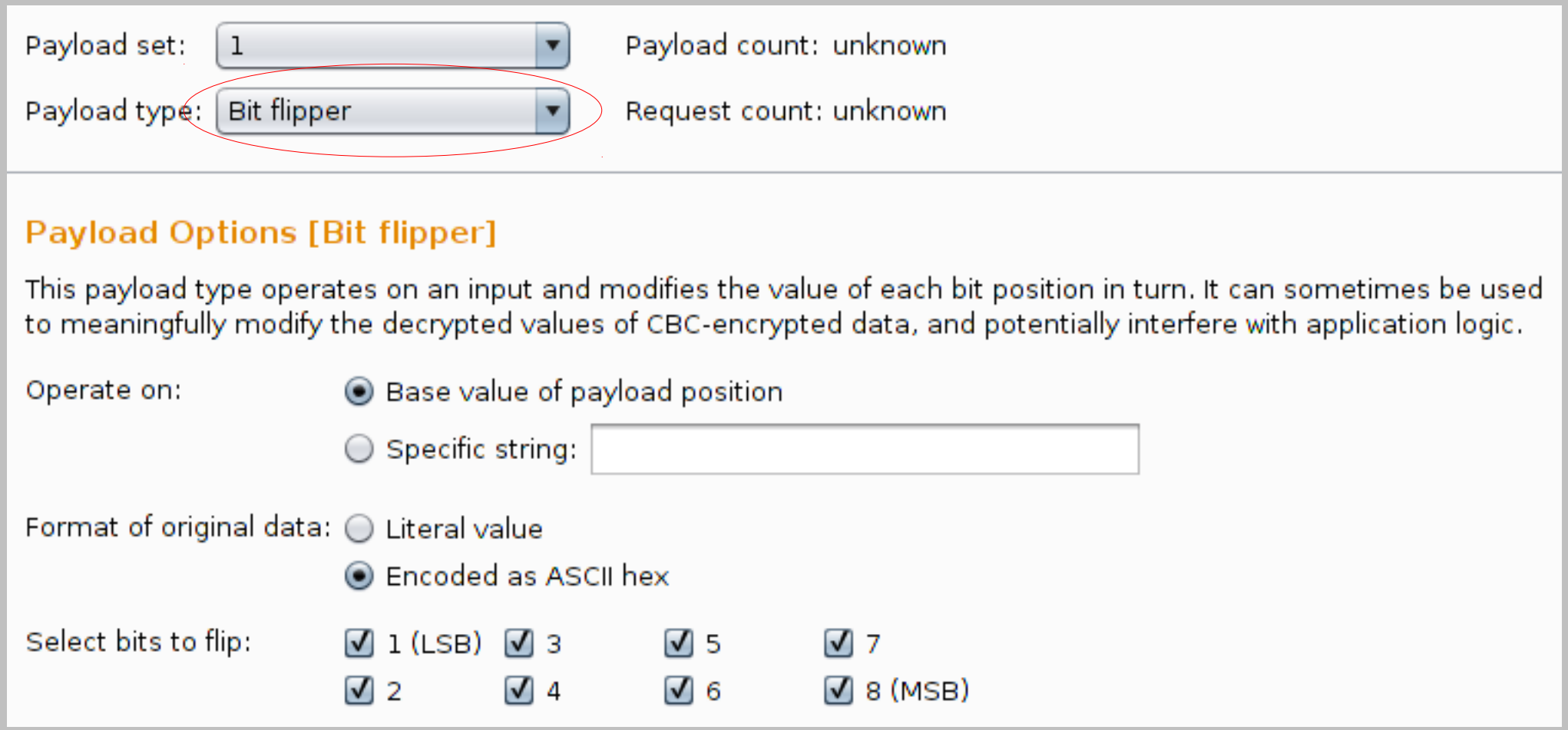
Payload Positions

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

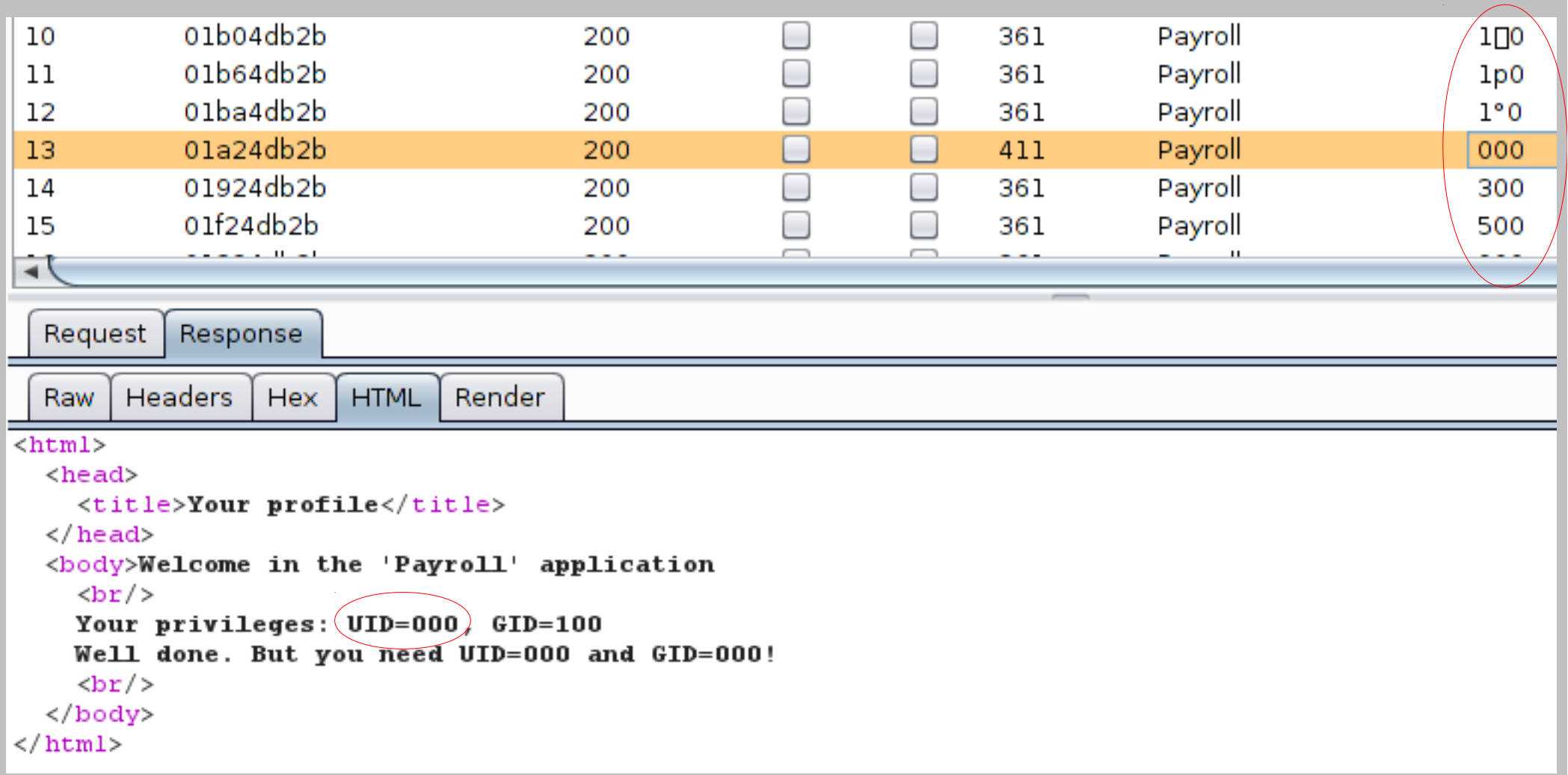
Attack type: Sniper

```
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)
2
3
4
5
6
7
8 (MSB)

Opaque data



10	01b04db2b	200	☐	☐	361	Payroll	1□0
11	01b64db2b	200	☐	☐	361	Payroll	1p0
12	01ba4db2b	200	☐	☐	361	Payroll	1°0
13	01a24db2b	200	☐	☐	411	Payroll	000
14	01924db2b	200	☐	☐	361	Payroll	300
15	01f24db2b	200	☐	☐	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>
```

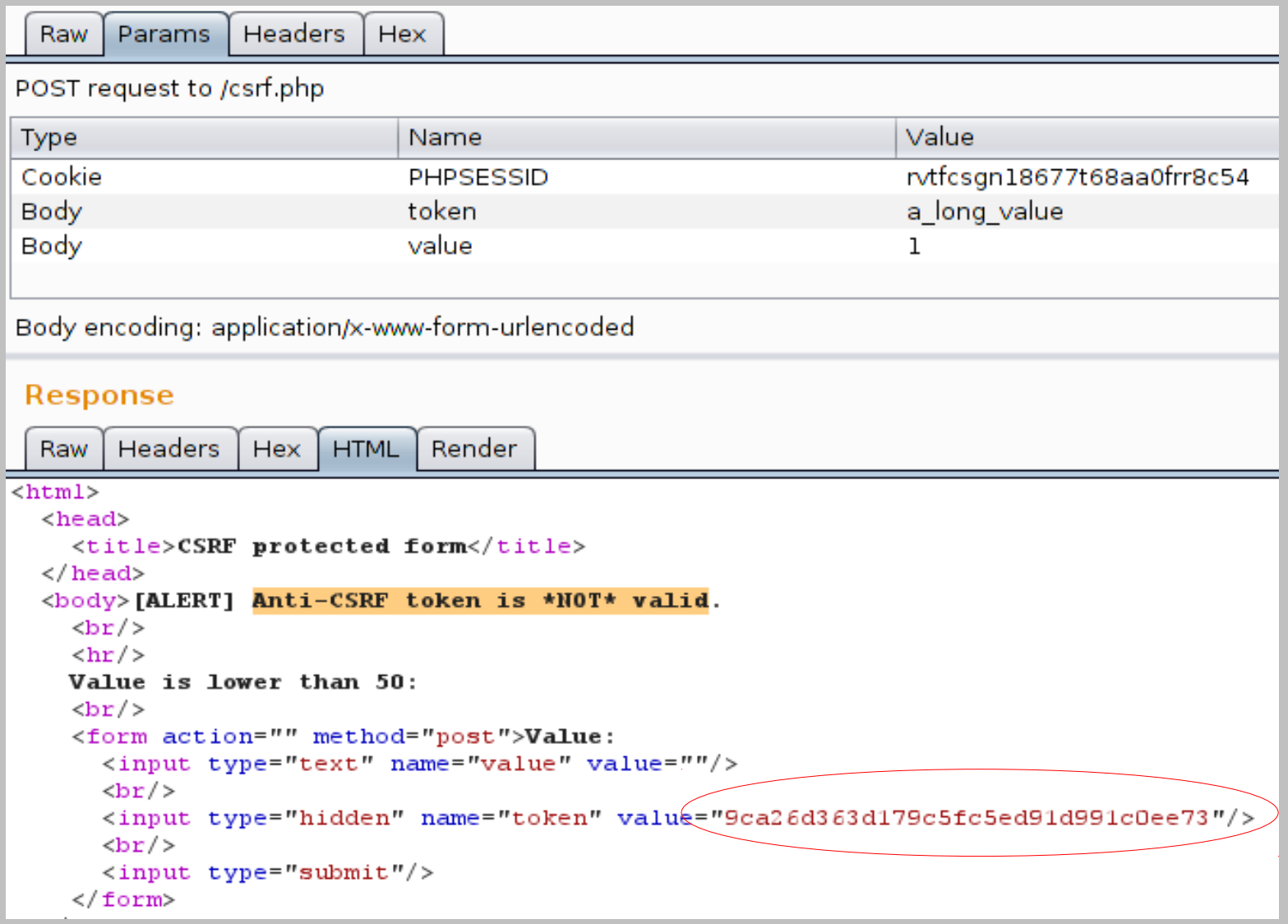
Intruder payloads

HTTP Basic Authentication

Opaque data

Anti-CSRF tokens

Anti CSRF tokens



Anti CSRF tokens

Raw | Params | Headers | Hex

POST request to /csrf.php

Type	Name	Value
Cookie	PHPSESSID	rvtfcsgn18677t68aa0frr8c54
Body	token	9ca26d363d179c5fc5ed91d991c0ee73
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>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/>
```

Anti CSRF tokens

Raw | Params | Headers | Hex

POST request to /csrf.php

Type	Name	Value
Cookie	PHPSESSID	rvtfcsgn18677t68aa0frr8c54
Body	token	222221fcafdebc124ad0befb89d9a777
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="(.*?)"/>

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	☑	☐	c9275dff1f27e058b8d43a97ce1...
28	c9275dff1f27e058b8d43a97ce12945e	27	200	723	☑	☐	7ba26334ecae3b899475782a1...
29	7ba26334ecae3b899475782a1e5f162a	28	200	723	☑	☐	df0894ca4f5d6647b57299dfef5...
30	df0894ca4f5d6647b57299dfef5bdfe7	29	200	723	☑	☐	6487a328e657fd8e4950c45a2d...
31	6487a328e657fd8e4950c45a2def3430	30	200	723	☑	☐	d39a05b2fa22fcc69df6d6bc380...
32	d39a05b2fa22fcc69df6d6bc38004f52	31	200	723	☑	☐	866ec10ca898fdc441573e6c71...
33	866ec10ca898fdc441573e6c71aa5a1b	32	200	723	☑	☐	d9087cace61e7e3c905fb5c80f3..
34	d9087cace61e7e3c905fb5c80f36f725	33	200	738	☐	☐	23b4d2beeaddc95ad993f2fac8...
35	23b4d2beeaddc95ad993f2fac841081b	34	200	723	☑	☐	c50399865813e9b08a79139e3f...
36	c50399865813e9b08a79139e3f282f55	35	200	723	☑	☐	2a6a8b9b802daeaae42068ca9...
37	2a6a8b9b802daeaae42068ca98d6baec	36	200	723	☑	☐	edb824d8101d1feb4f7cf2b888f...
38	edb824d8101d1feb4f7cf2b888f357f4	37	200	723	☑	☐	22a2ff0e37a22ab507b997dff41...
39	22a2ff0e37a22ab507b997dff4107458	38	200	723	☑	☐	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/>
```

Anti CSRF tokens

DEMOS?

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

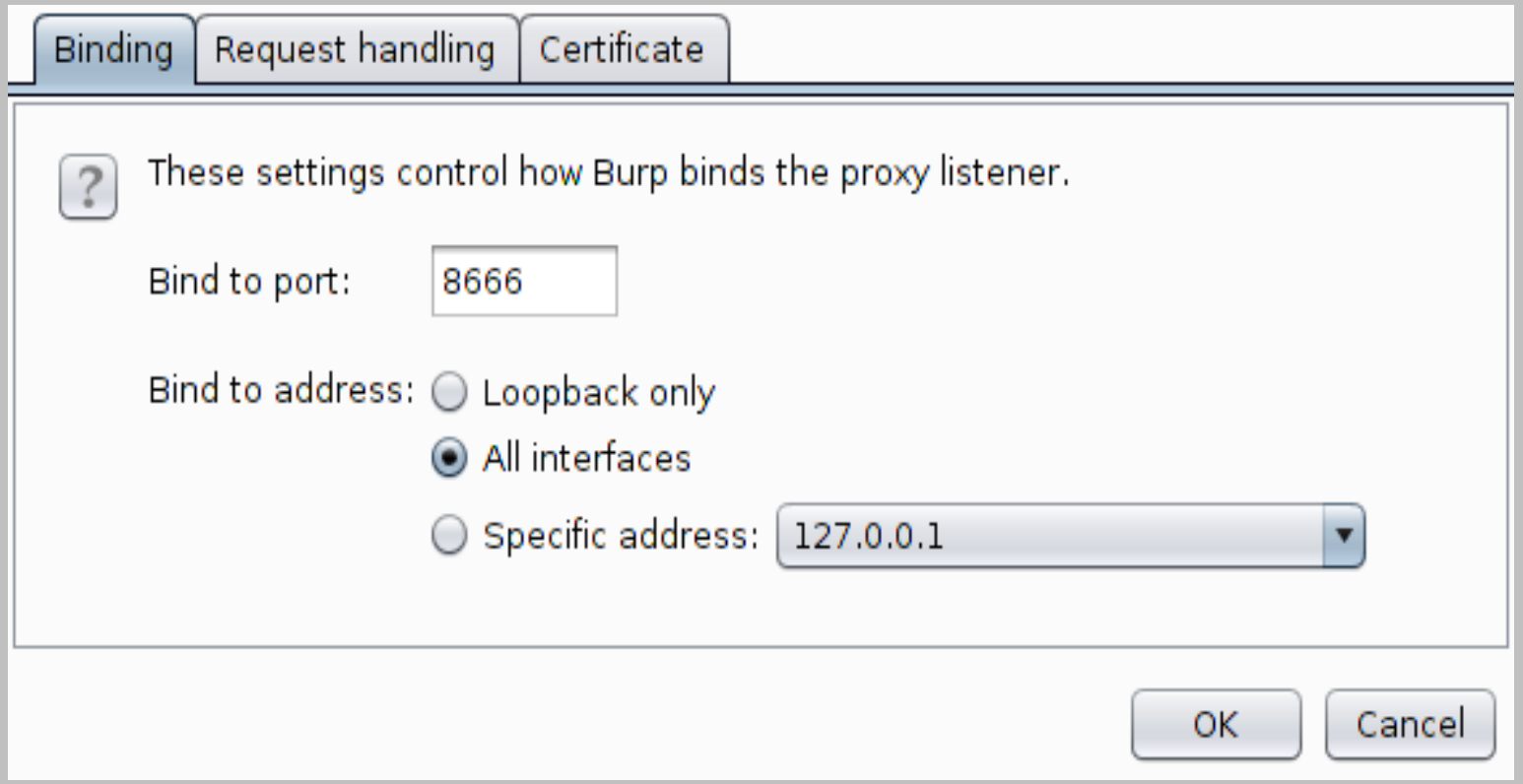
You want to use your usual tool and workflow

Burp listens elsewhere, on an external interface

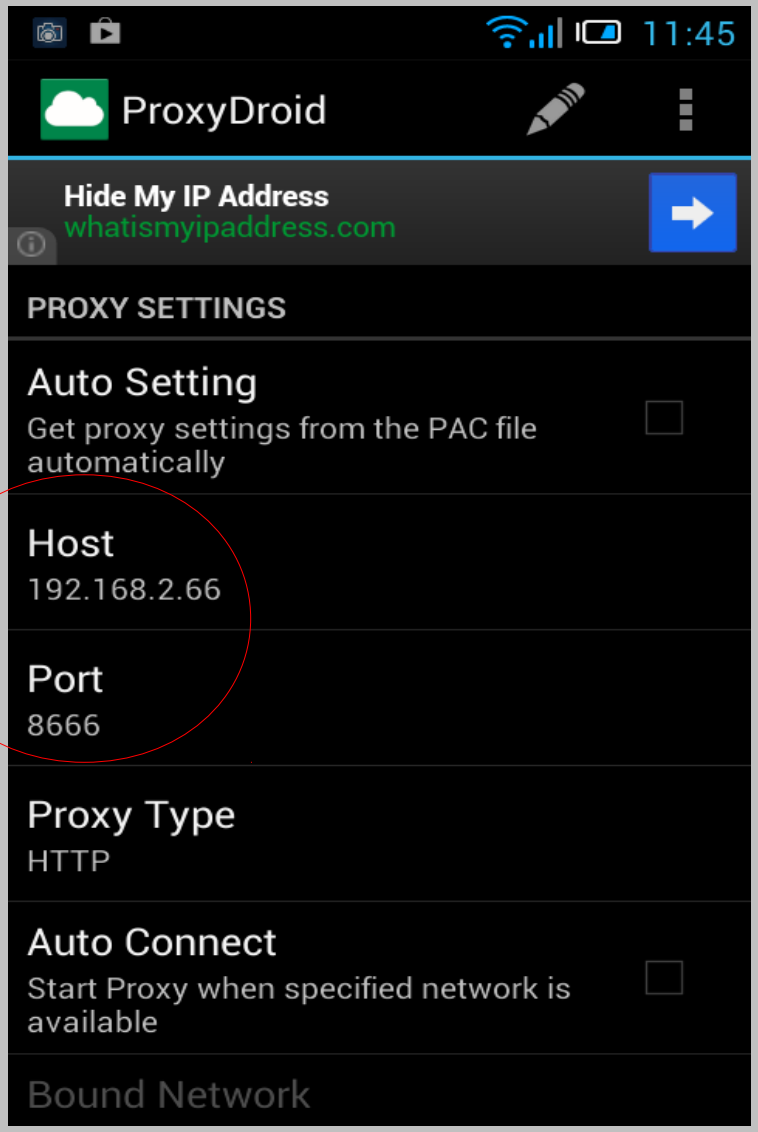
ProxyDroid redirects to the Burp instance

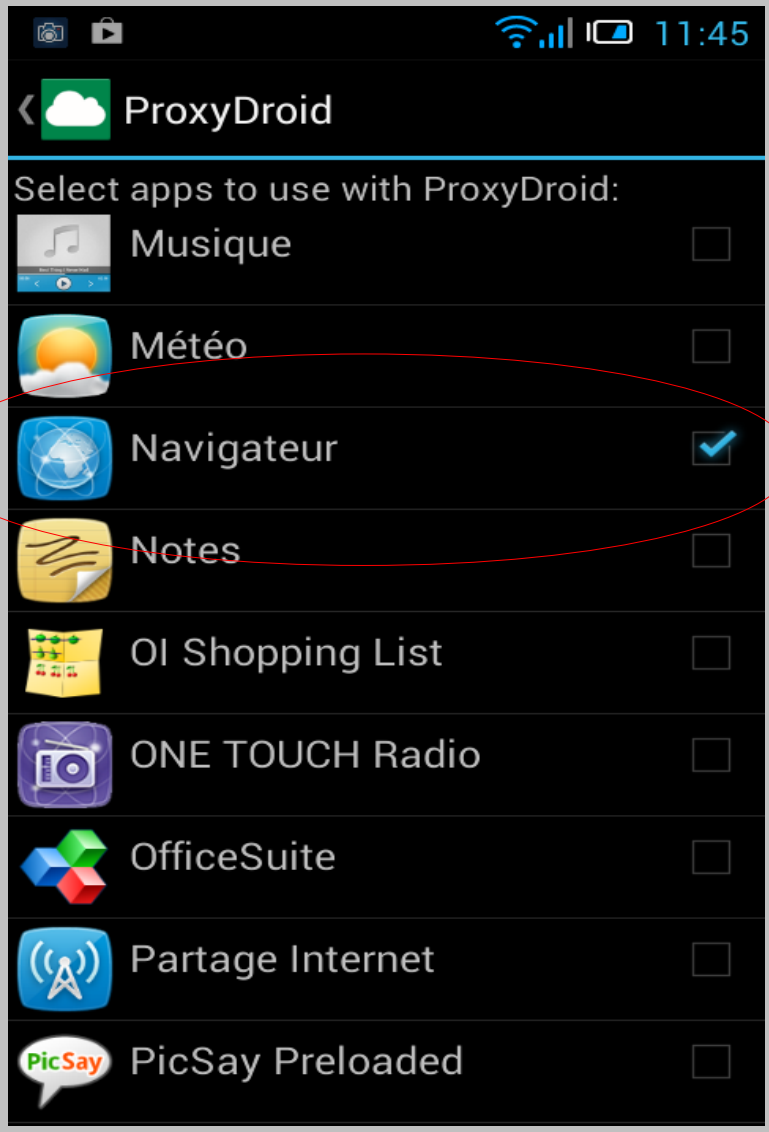
- App-specific or global proxying
- Option “DNS Proxy” should be checked

Redirect to Burp



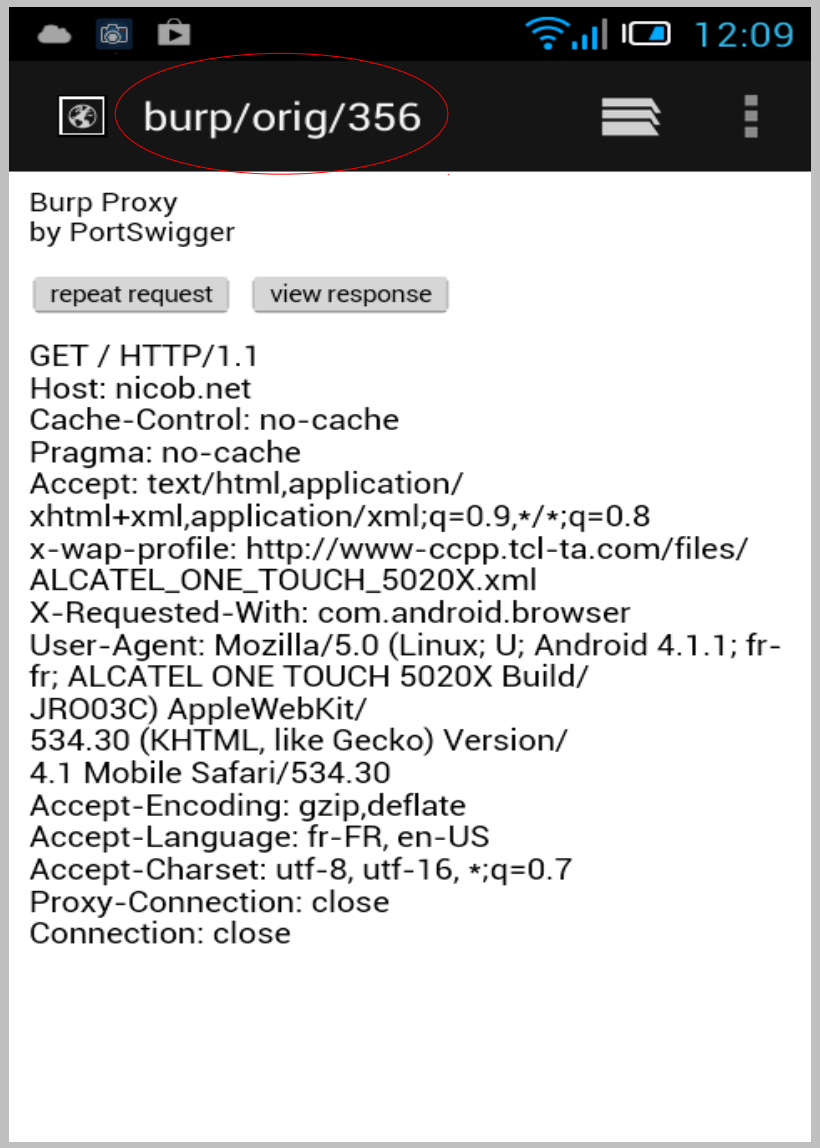
Redirect to Burp



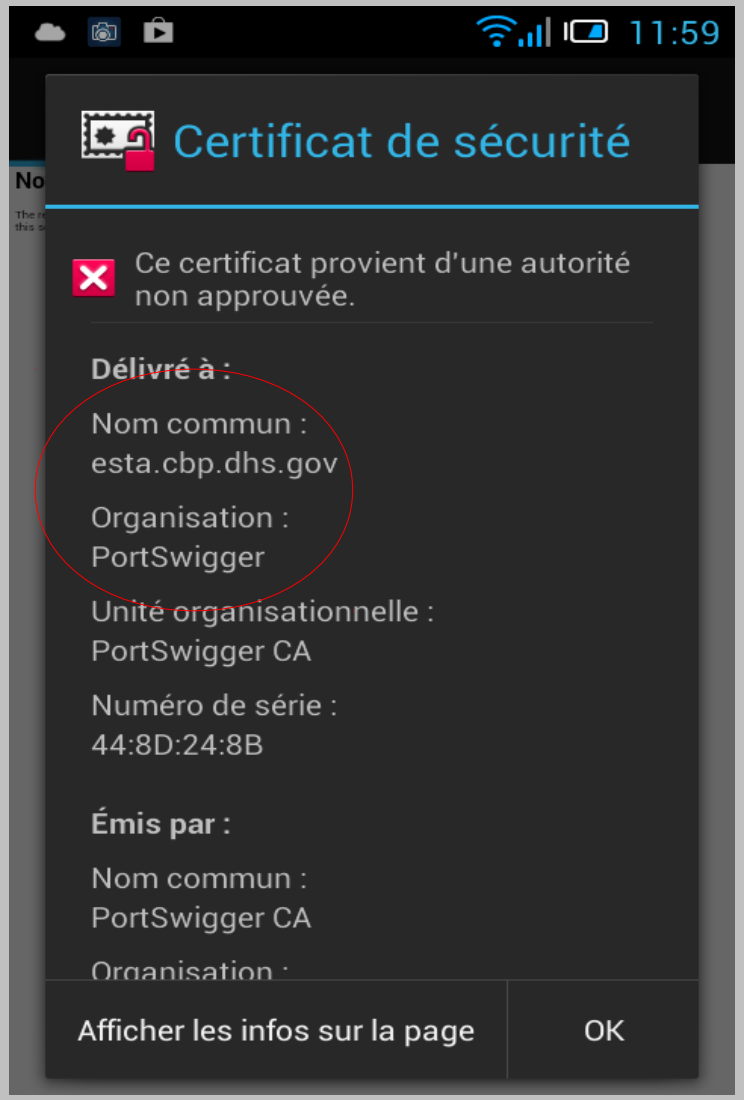


Redirect to Burp

Redirect to Burp



Burp CA


11:59
Certificat de sécurité
Ce certificat provient d'une autorité non approuvée.
Délivré à :
Nom commun :
esta.cbp.dhs.gov
Organisation :
PortSwigger
Unité organisationnelle :
PortSwigger CA
Numéro de série :
44:8D:24:8B
Émis par :
Nom commun :
PortSwigger CA
Afficher les infos sur la page
OK


11:58
Play Store
Aucune connexion
Réessayer

Burp CA

Fetch your Burp CA certificate

- GUI: Proxy / Options / Proxy Listeners / CA Certificate / Export in DER
- Proxied browser: http://burp/cert

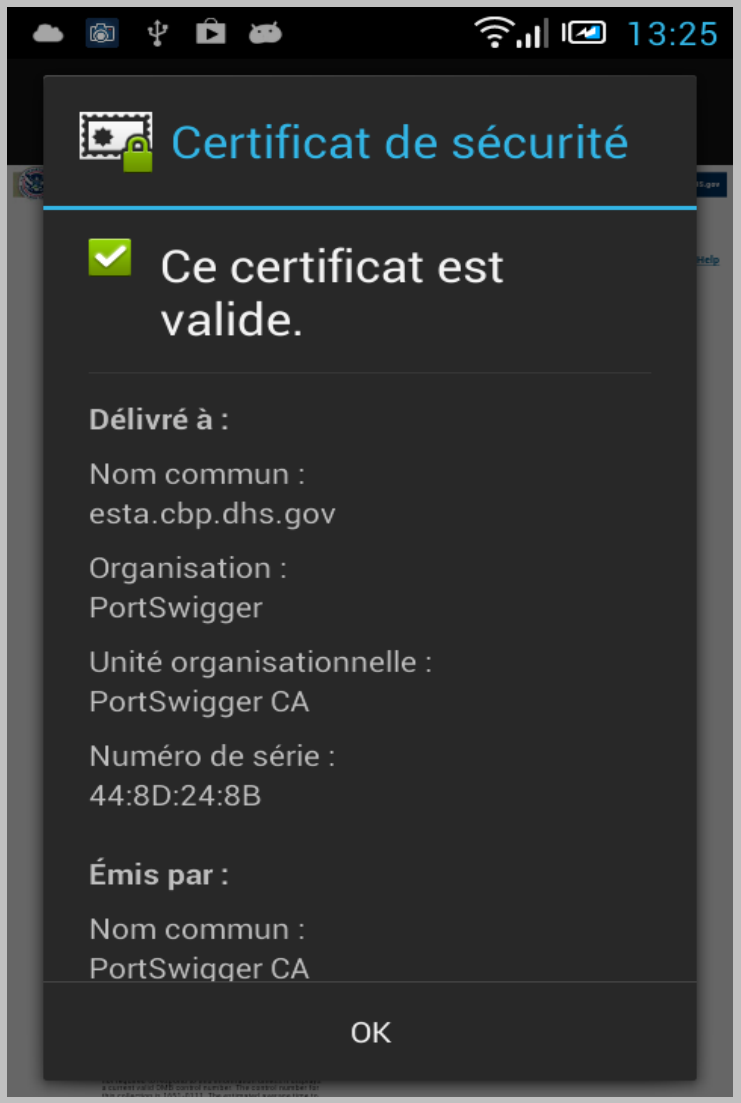
Rename from DER to CRT

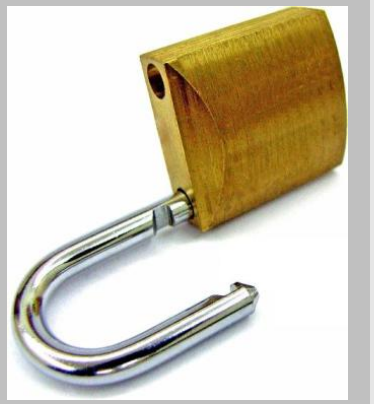
- No need for OpenSSL 

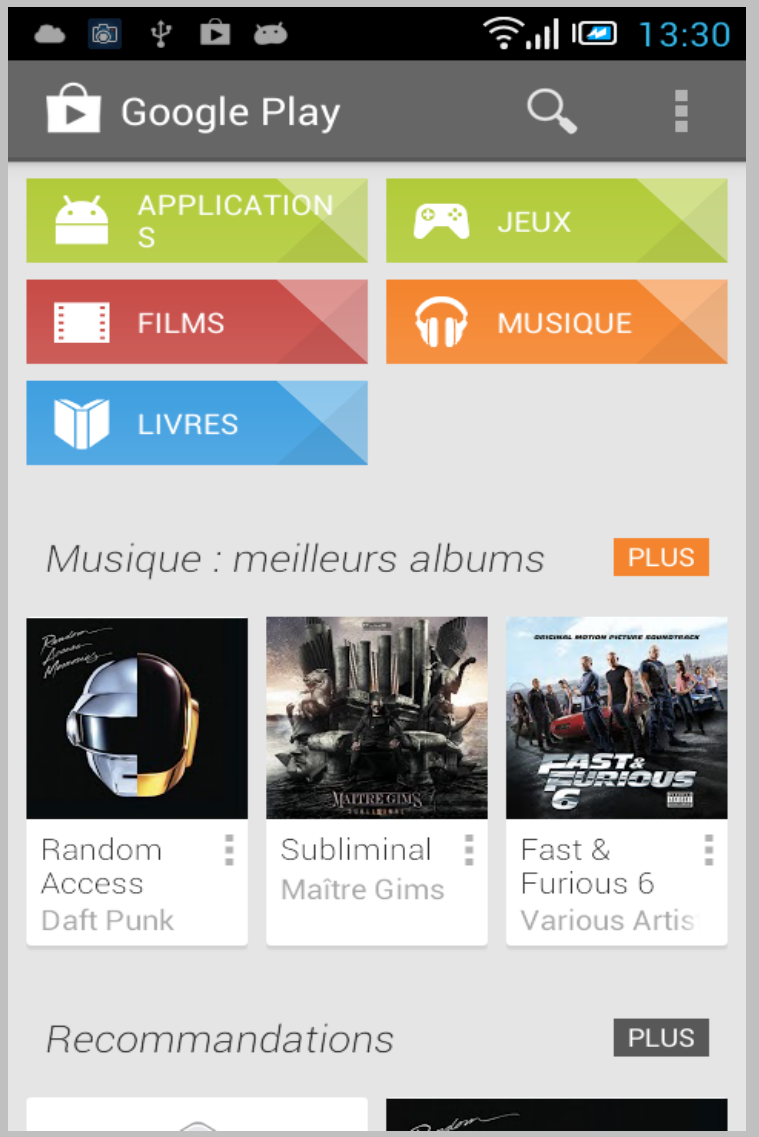
Depending on the Android version:

- Touch the file in any “File Explorer” application
- Parameters / Security / Install from SD

Burp CA

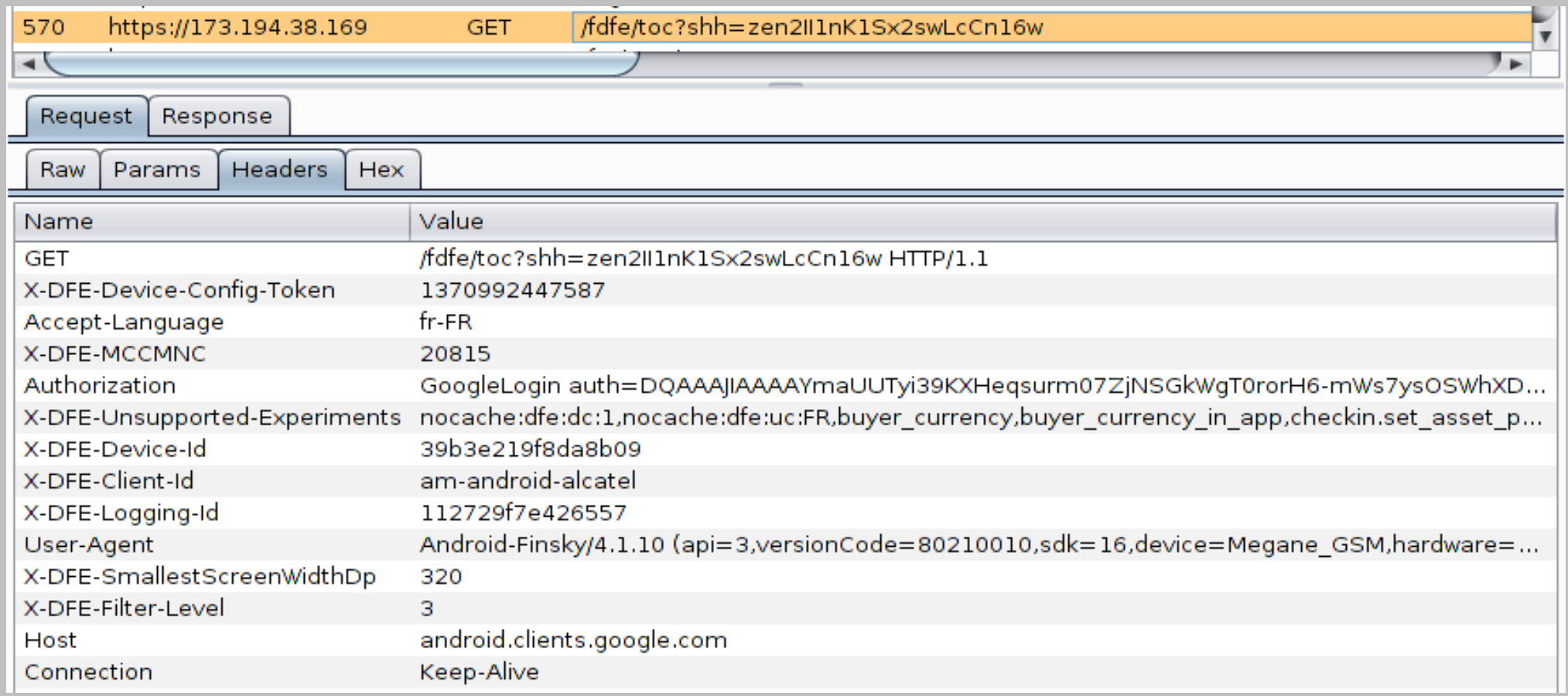

13:25
Certificat de sécurité
Ce certificat est valide.
Délivré à :
Nom commun :
esta.cbp.dhs.gov
Organisation :
PortSwigger
Unité organisationnelle :
PortSwigger CA
Numéro de série :
44:8D:24:8B
Émis par :
Nom commun :
PortSwigger CA
OK




13:30
Google Play
APPLICATIONS
JEUX
FILMS
MUSIQUE
LIVRES
Musique : meilleurs albums
PLUS
Random Access
Daft Punk
Subliminal
Maître Gims
Fast & Furious 6
Various Artis
Recommandations
PLUS

Burp CA

First request when opening Google Play



570	https://173.194.38.169	GET	/fdfe/toc?shh=zen2II1nK1Sx2swLcCn16w

Request | Response

Raw | Params | Headers | Hex

Name	Value
GET	/fdfe/toc?shh=zen2II1nK1Sx2swLcCn16w 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:dfe:dc:1,nocache:dfe: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

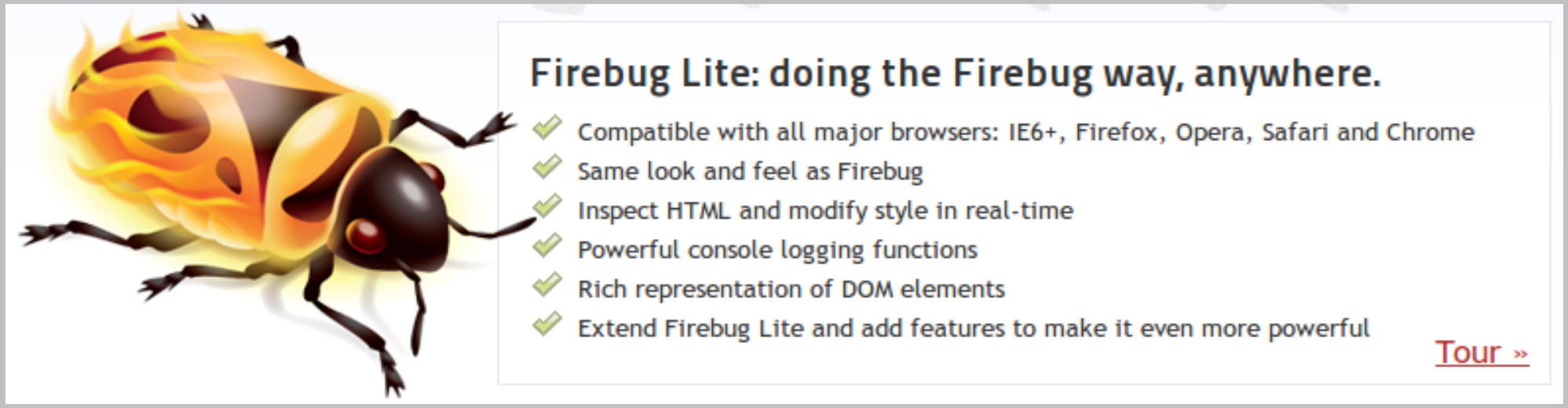
Like no built-in developers tools

I don't care, except when looking for XSS

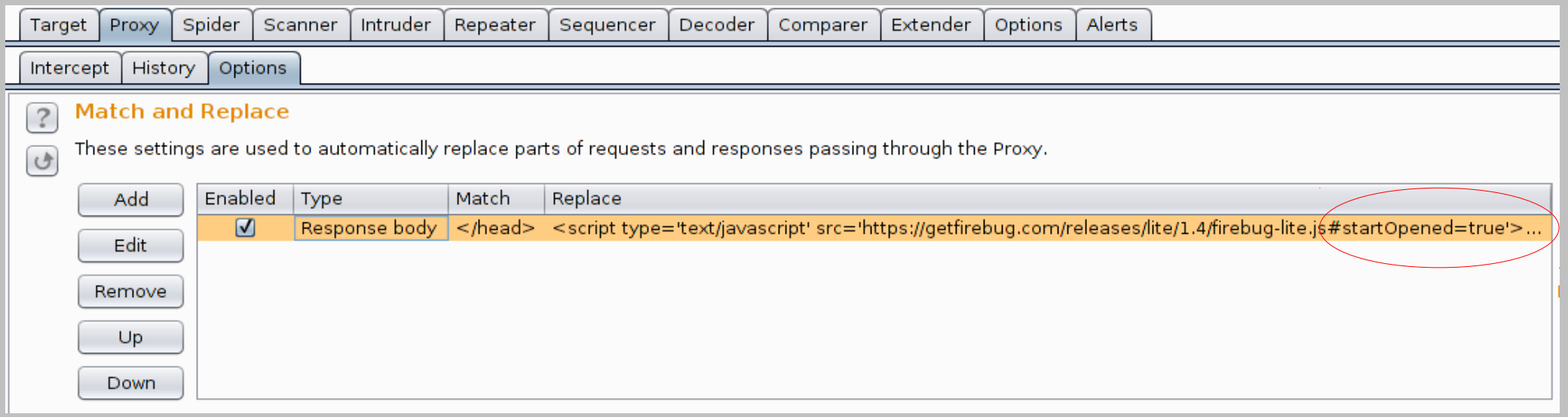
Developers tools

Let's include Firebug Lite in every response

“startOpened=true” is your friend



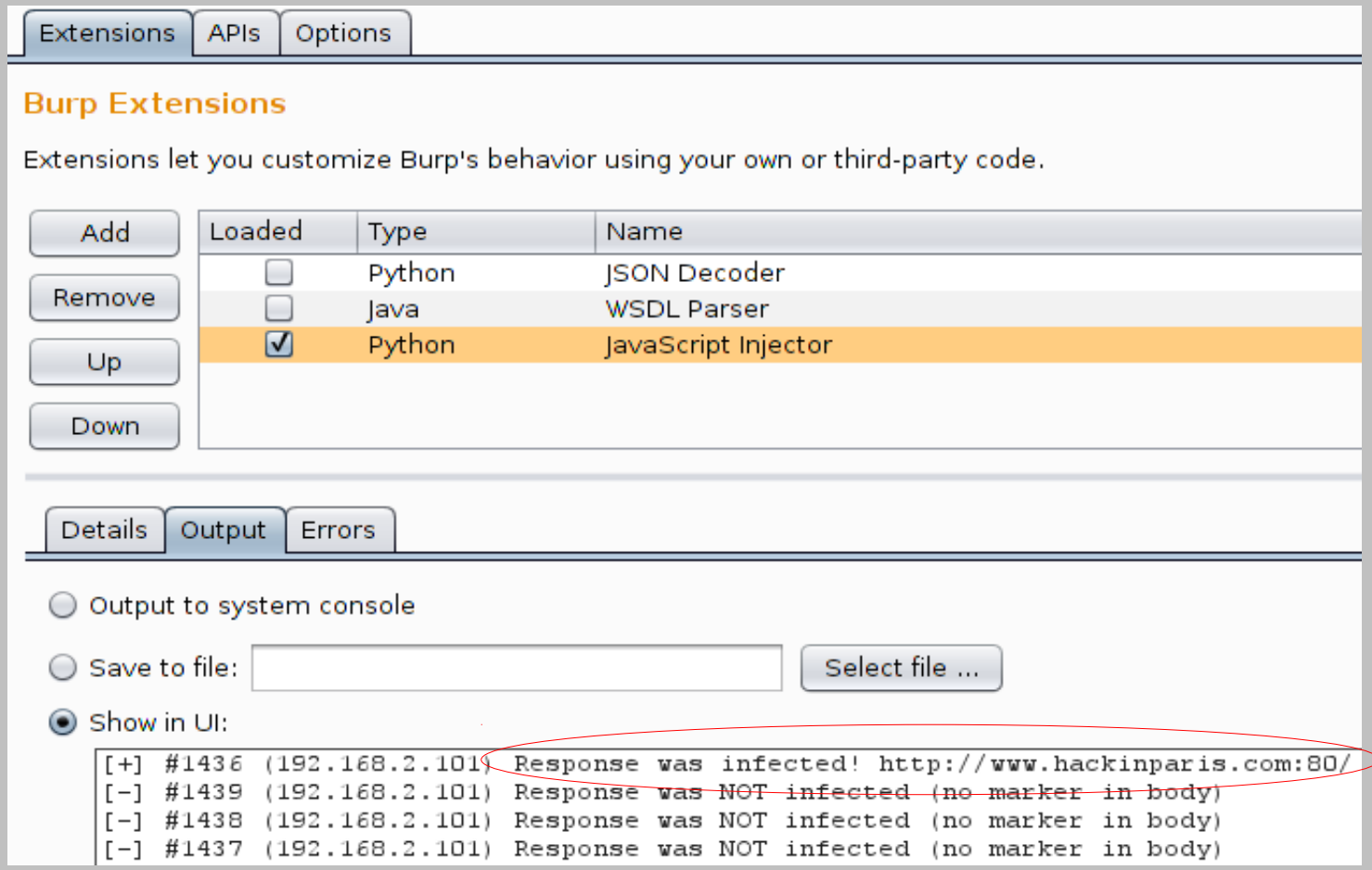
Developers tools



This seems to be a good idea

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

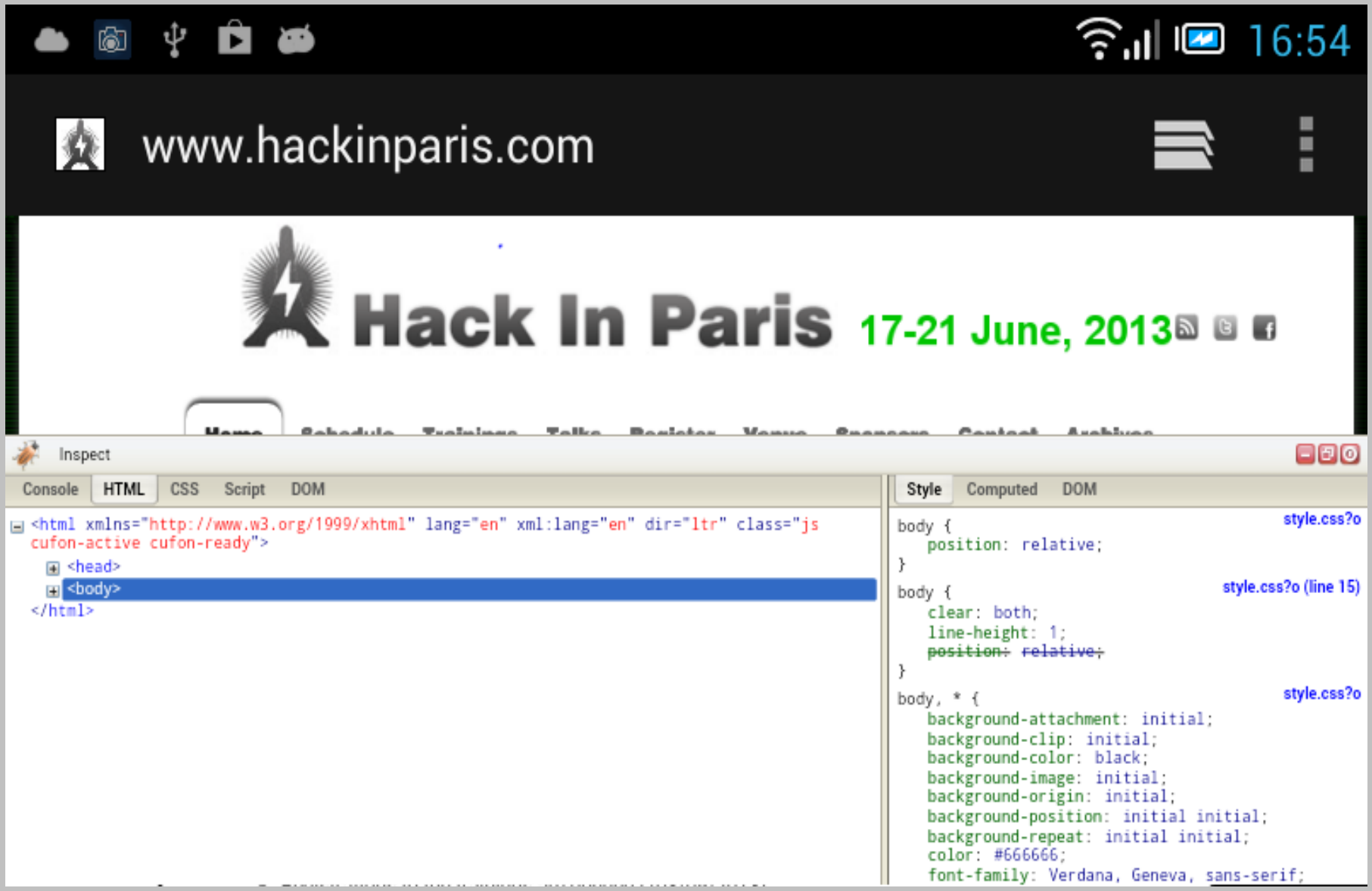
Developers tools



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

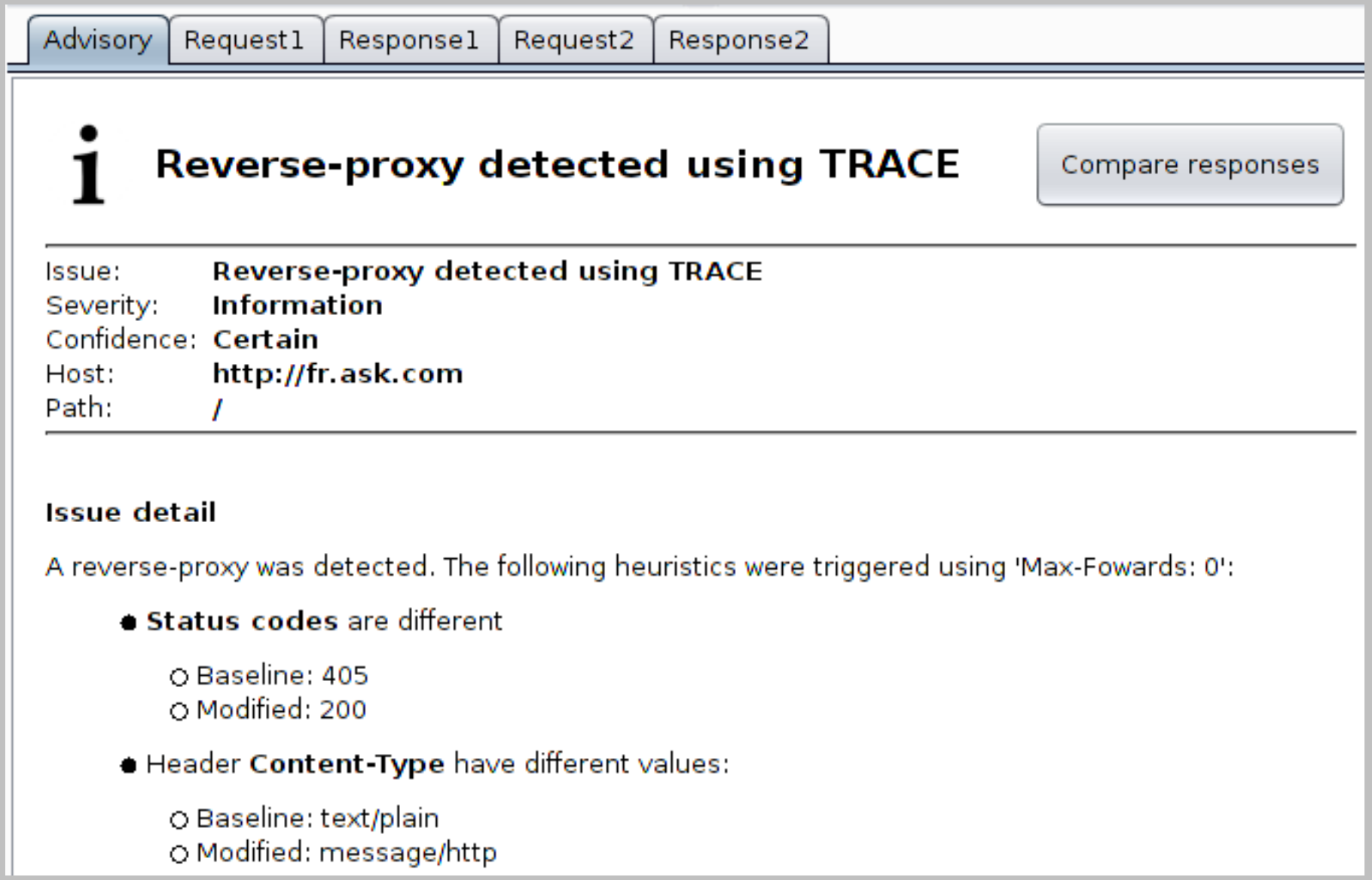
Blog (+ samples)

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
- **Misc**
  - Custom Logger, Burp Notes, Proxy Color, Referrer Checker
- **My own**
  - JavaScript Injector, HTTP Traceroute, DomXssRegexp

Detect reverse-proxies



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

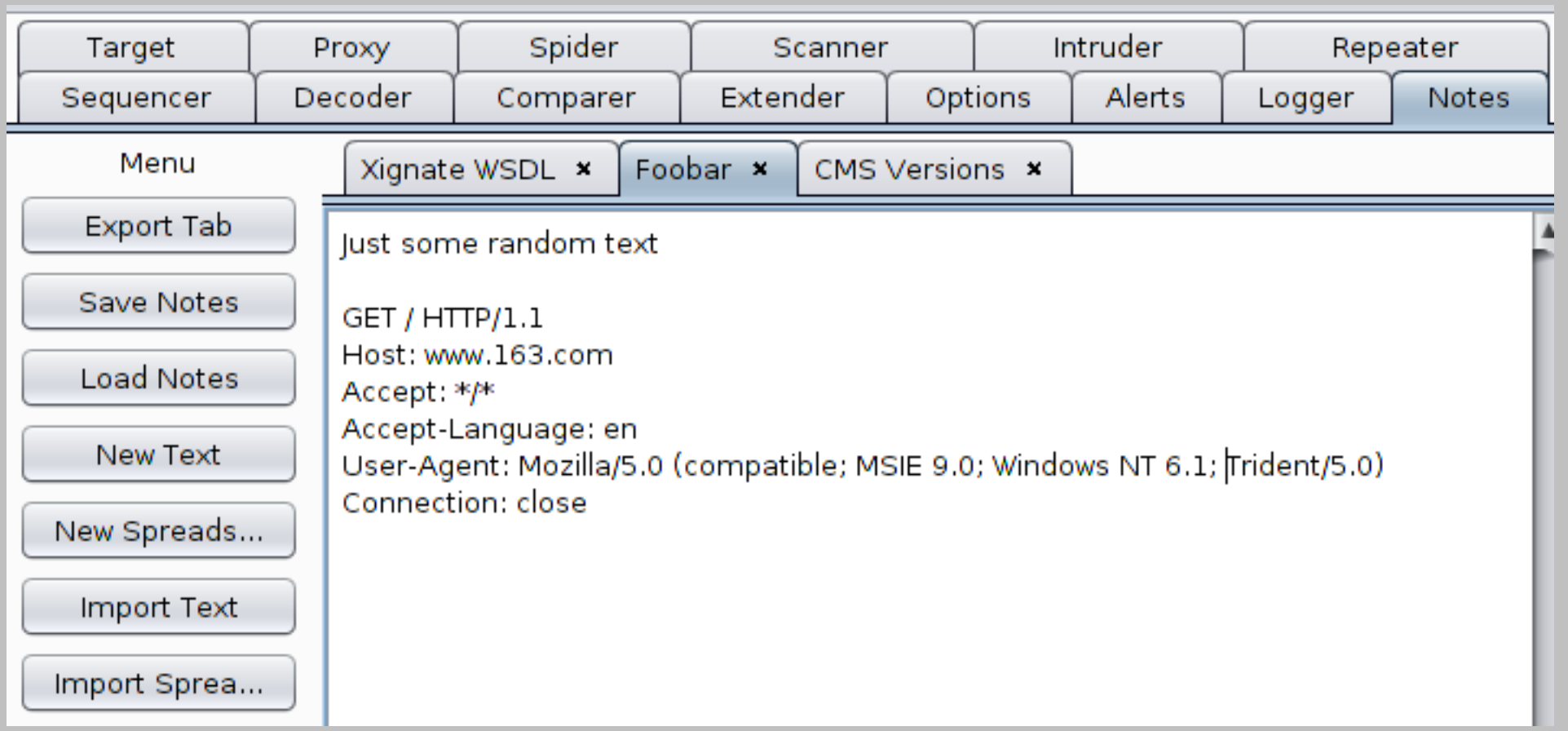
Request

Raw | Params | Headers | Hex | XML

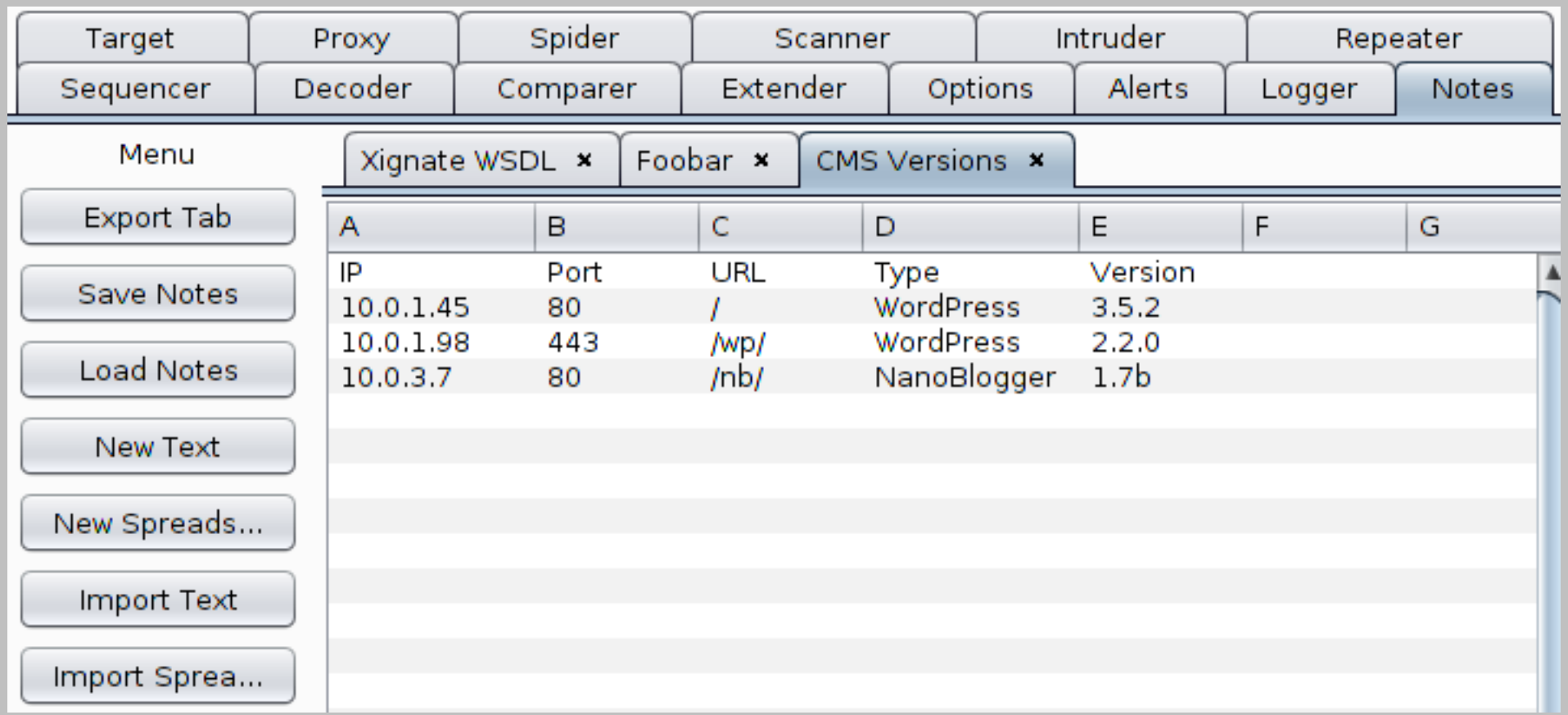
```
POST /onca/soap?Service=AWSECommerceService HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: http://soap.amazon.com/BrowseNodeLookup
Host: webservices.amazon.fr
Content-Length: 1199

<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


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Logger
Notes
Menu
Export Tab
Save Notes
Load Notes
New Text
New Spreads...
Import Text
Import Sprea...
Xignate WSDL
Foobar
CMS Versions
Just some random text
GET / HTTP/1.1
Host: www.163.com
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Connection: close

Takes notes


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Logger
Notes
Menu
Export Tab
Save Notes
Load Notes
New Text
New Spreads...
Import Text
Import Sprea...
Xignate WSDL
Foobar
CMS Versions
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

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

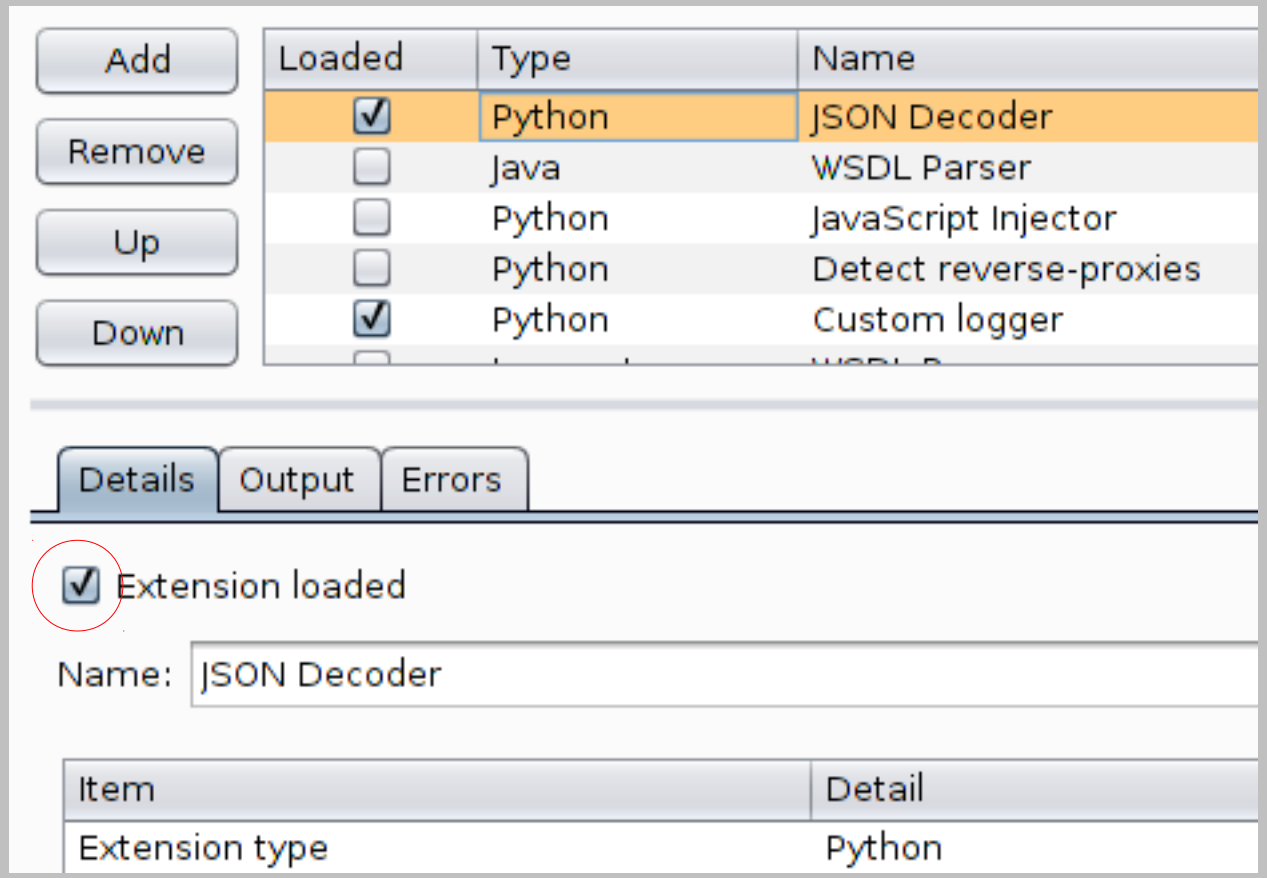
```
ApplyMarkers(
    IHttpRequestResponse httpRequestResponse,
    java.util.List<int[]> requestMarkers,
    java.util.List<int[]> responseMarkers)
```

Python code

```
markers = []
for n in non_overloapping:
    markers.append(array.array('i', [offset + n[0], offset + n[1]]))
marked_message = self._callbacks.applyMarkers(message, None, markers)
```

Quick reload

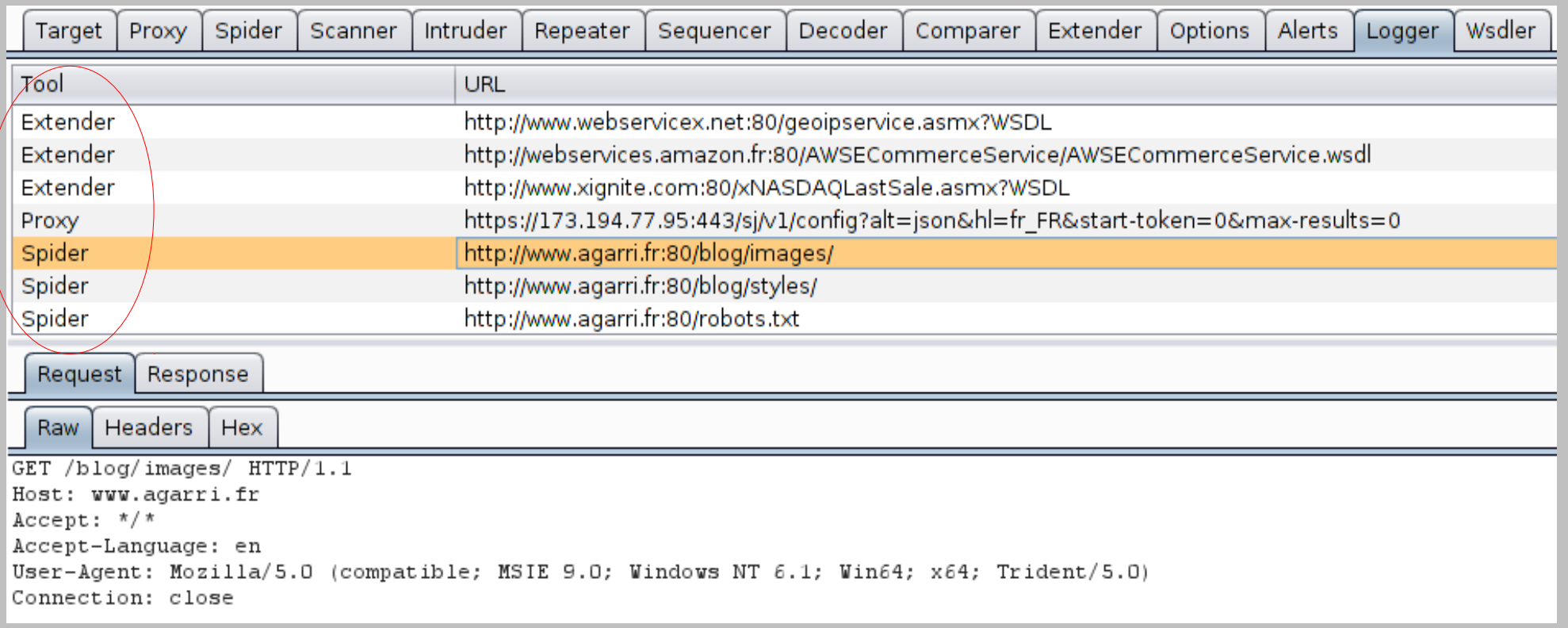
Use Ctrl-Click to quickly reload an extension



Debugging

Custom Logger captures everything

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



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

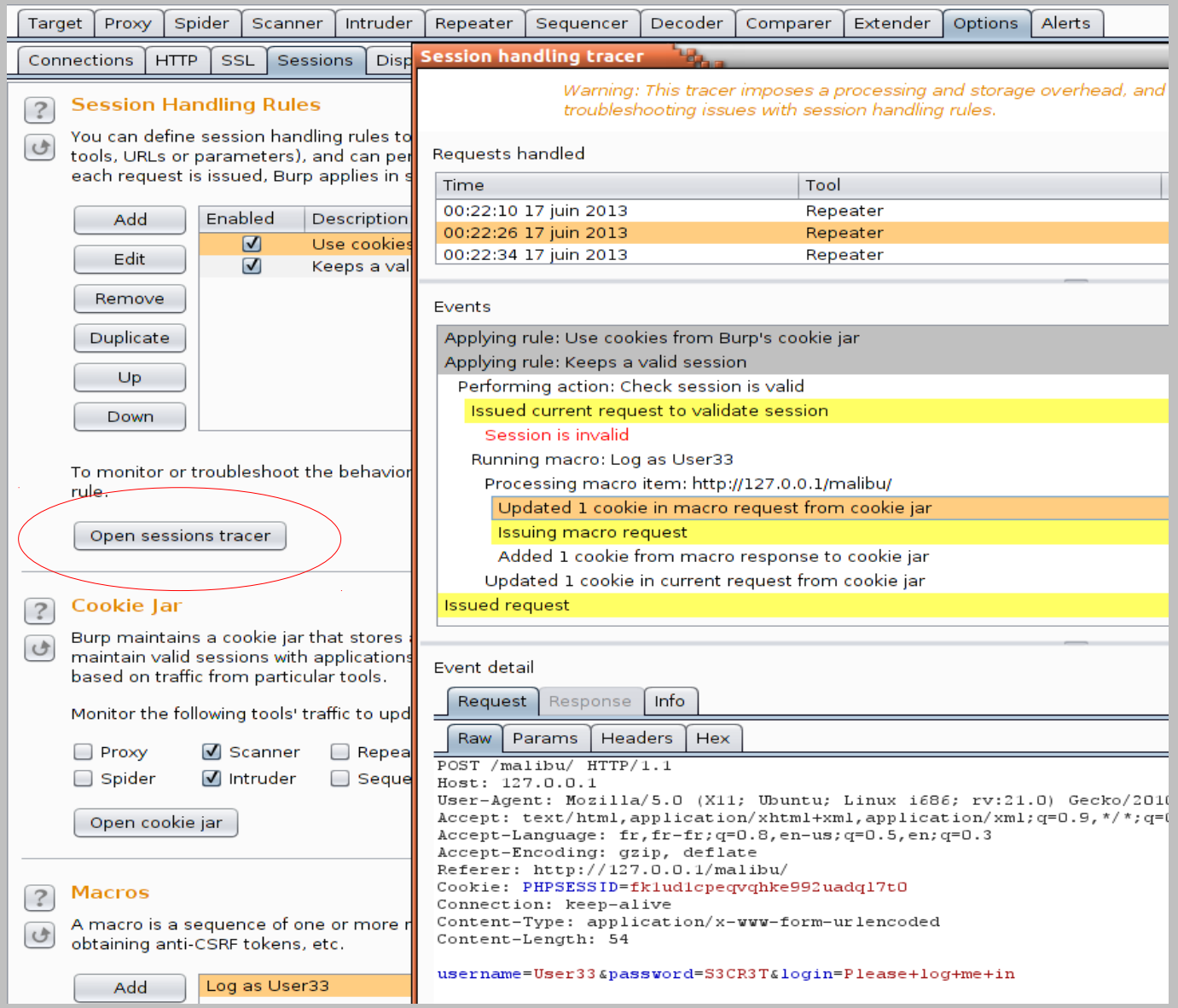
/index.php

- 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


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Connections
HTTP
SSL
Sessions
Session handling tracer
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
Add
Edit
Remove
Duplicate
Up
Down
Enabled
Description
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 r
obtaining anti-CSRF tokens, etc.
Add
Log as User33
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/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
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=fkludlcpeqvqhke992uadql7t0
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