UA-Tester

... or why Web-Application Penetration Testers are only getting half the story

UA-Tester

... or why Web-Application Penetration Testers are only getting half the story

... or time to PIMP your tool!

... and you are?

- Chris John Riley (@ChrisJohnRiley)
- Penetration Tester
- Blogger
  - http://blog.c22.cc
- Podcaster
  - Eurotrash Security podcast

UA-Tester

... Fo' Shizzle!

```
 _/    _/  _/_/_/    _/_/_/  _/_/_/  _/_/_/  _/_/_/  _/_/_/  _/_/_/
_/    _/  _/    _/  _/    _/    _/  _/    _/  _/    _/    _/    _/
_/    _/  _/_/_/    _/    _/    _/  _/    _/  _/    _/    _/_/_/
_/    _/  _/        _/    _/    _/  _/    _/  _/    _/    _/    _/
 _/_/_/   _/        _/_/_/  _/_/_/  _/    _/  _/_/_/  _/    _/

                                    _/ User-Agent Tester
                                       _/ ChrisJohnRiley
                                          _/ blog.c22.cc

[*] Running in Verbose mode

[>] Performing initial request and confirming stability
[>] Using User-Agent string Mozilla/5.0

   [ ] URL (ENTERED): http://facebook.com
   [!] URL (FINAL): http://www.facebook.com/
   [!] Response Code: 301 Moved Permanently
   [ ] Cache-Control: private, no-cache, no-store, must-revalidate
   [ ] Expires: Sat, 01 Jan 2000 00:00:00 GMT
   [ ] P3P: CP="DSP LAW"
   [ ] Pragma: no-cache
   [ ] Set-Cookie: datr=1285177164-8491a76ddeaaf38ab75f5d553fb4f803d1d5f537a3c7913b919c5;
                   expires=Fri, 21-Sep-2012 17:39:24 GMT; path=/; domain=.facebook.com
   [ ] Set-Cookie: lsd=pAx2d; path=/; domain=.facebook.com
   [ ] Set-Cookie: reg_fb_gate=http%3A%2F%2Fwww.facebook.com%2F; path=/; domain=.facebook.com
```

What the $%*& is a UA?

... and why do we care!

UA == User-Agent

example:

Mozilla/5.0 (X11; Linux i686; rv:2.0.1) Gecko/20100101 Firefox/4.0.1

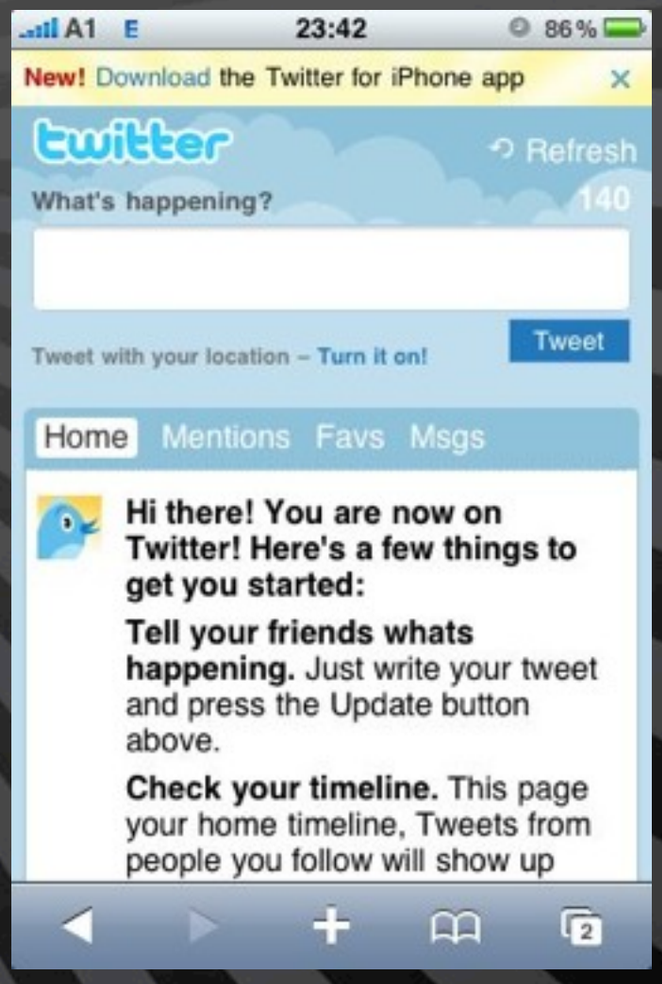
Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.10

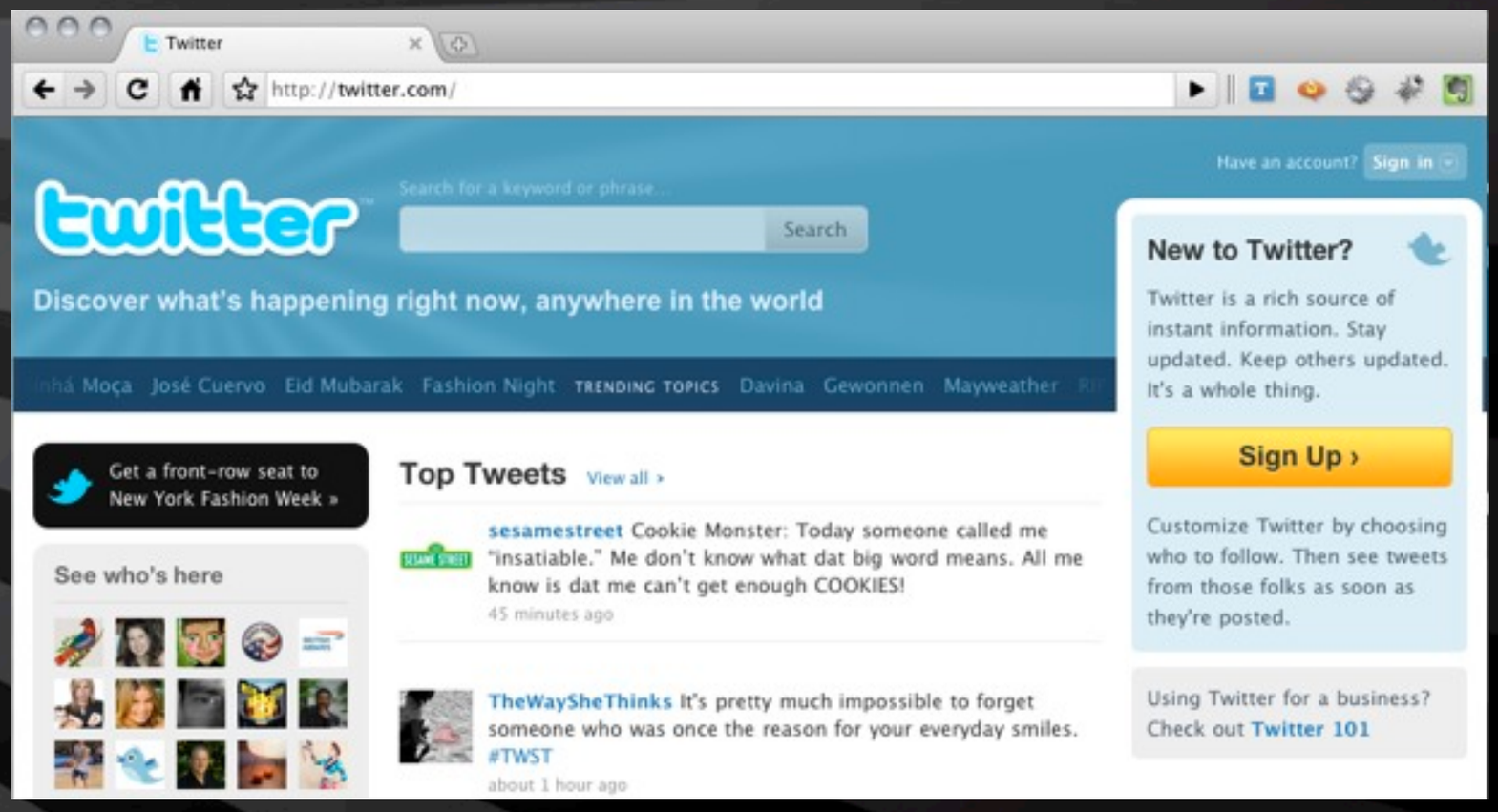
Wget/1.8.1

What the $%*& is a UA?

... and why does that affect us!

Web-Sites don't always respond in the same way!





What the $%*& is a UA?

... right, so what!

So what are these penetration testers testing then?

Std. Desktop Browser

```
HTTP/1.0 200 OK
Server: hi
Status: 200 OK
Content-Type: text/html; charset=utf-8
Pragma: no-cache
X-Revision: DEV
Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Connection: close
Content-Length: 44534
```

What the $%*& is a UA?

... right, so what!

So what are these penetration testers missing then?

Nokia Symbian

```
HTTP/1.1 200 OK
Server: hi
Status: 200 OK
Content-Language: en
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Vary: Accept-Encoding
Connection: close
Content-Length: 7508
```

Std. Desktop Browser

HTTP/1.0 200 OK
Server: hi
Status: 200 OK
Content-Type: text/html; charset=utf-8
Pragma: no-cache
X-Revision: DEV
Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Connection: close
Content-Length: 44534

Nokia Symbian UA

HTTP/1.1 200 OK
Server: hi
Status: 200 OK
Content-Language: en
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Vary: Accept-Encoding
Connection: close
Content-Length: 7508

Std. Desktop Browser

HTTP/1.0 200 OK
Server: hi
Status: 200 OK
Content-Type: text/html; charset=utf-8
Pragma: no-cache
X-Revision: DEV
Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Connection: close
Content-Length: 44534

Nokia Symbian UA

HTTP/1.1 200 OK
Server: hi
Status: 200 OK
Content-Language: en
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Vary: Accept-Encoding
Connection: close
Content-Length: 7508

So what's a UA-Tester?

... and why are we still listening to this guy!

UA-Tester

- Python script to test common UA Strings
  - Firefox, IE, Opera, iPad/iPhone, Symbian, Googlebot
  - ...and some not so common ones
    - PS3
    - Apache traceback
    - HTTrack
    - .NASL
- Output differences in response
- Lets penetration testers know where to focus

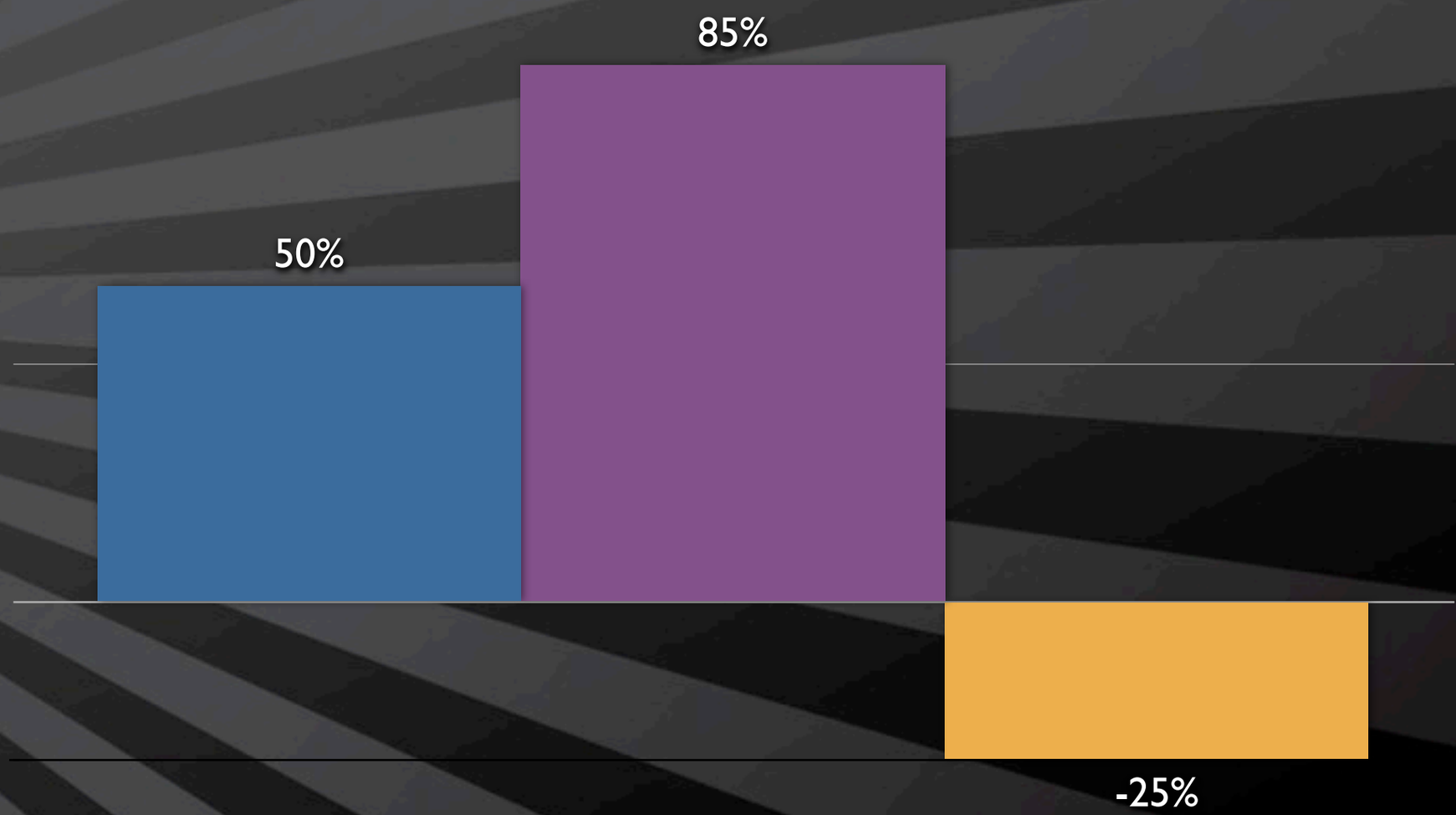
Pimping your pentesters!

I want stats

... some numbers I made up earlier

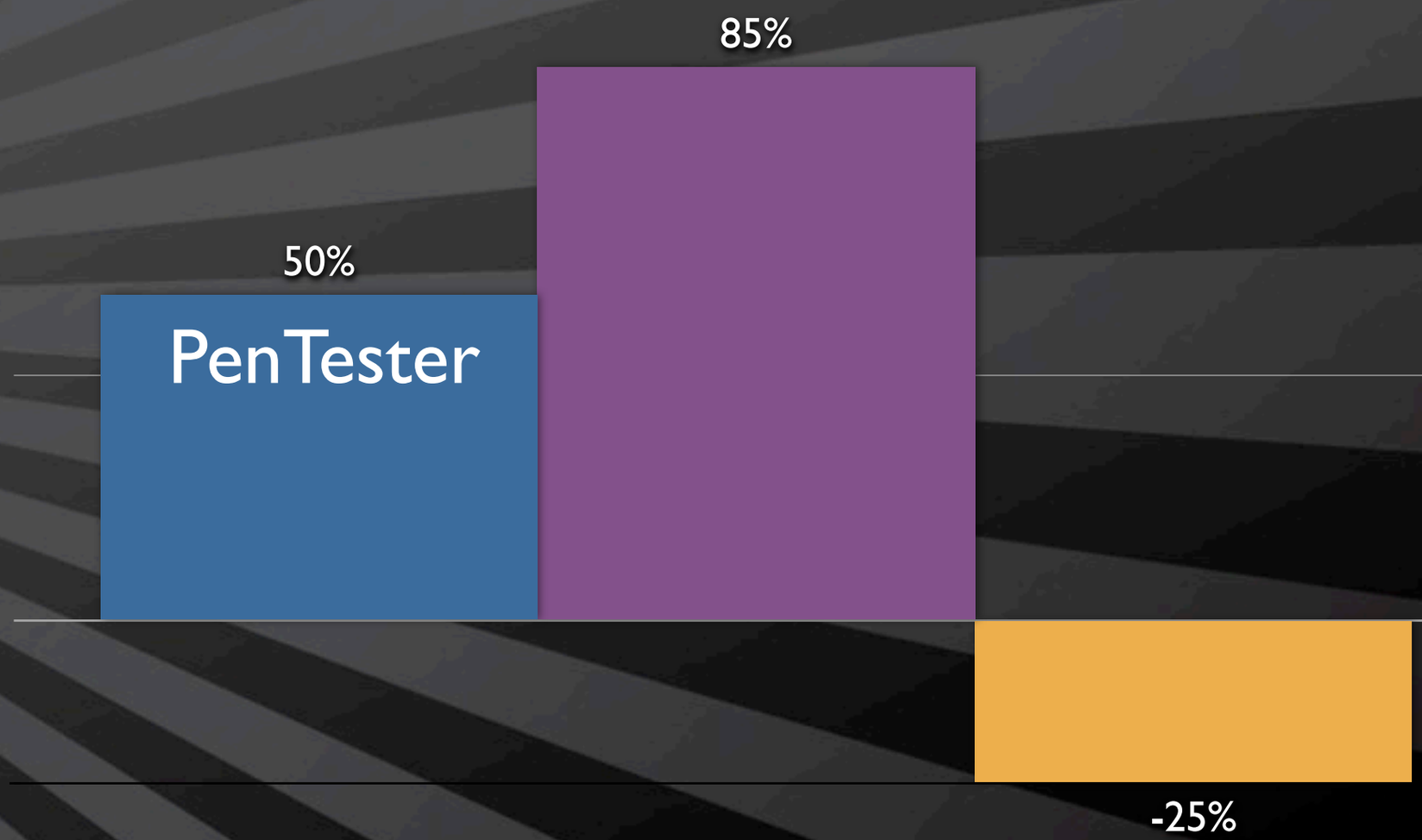
I want stats

... some numbers I made up earlier



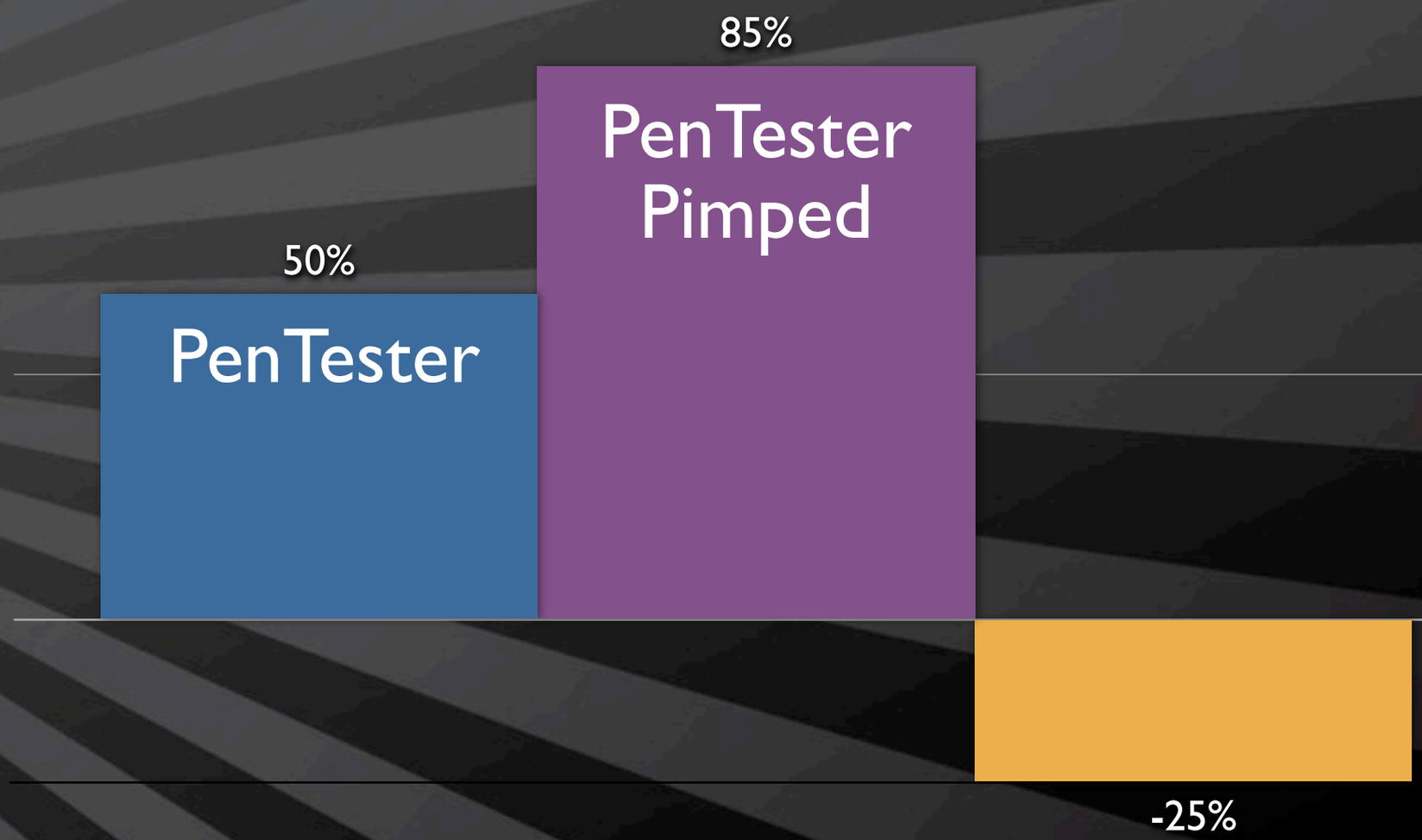
I want stats

... some numbers I made up earlier



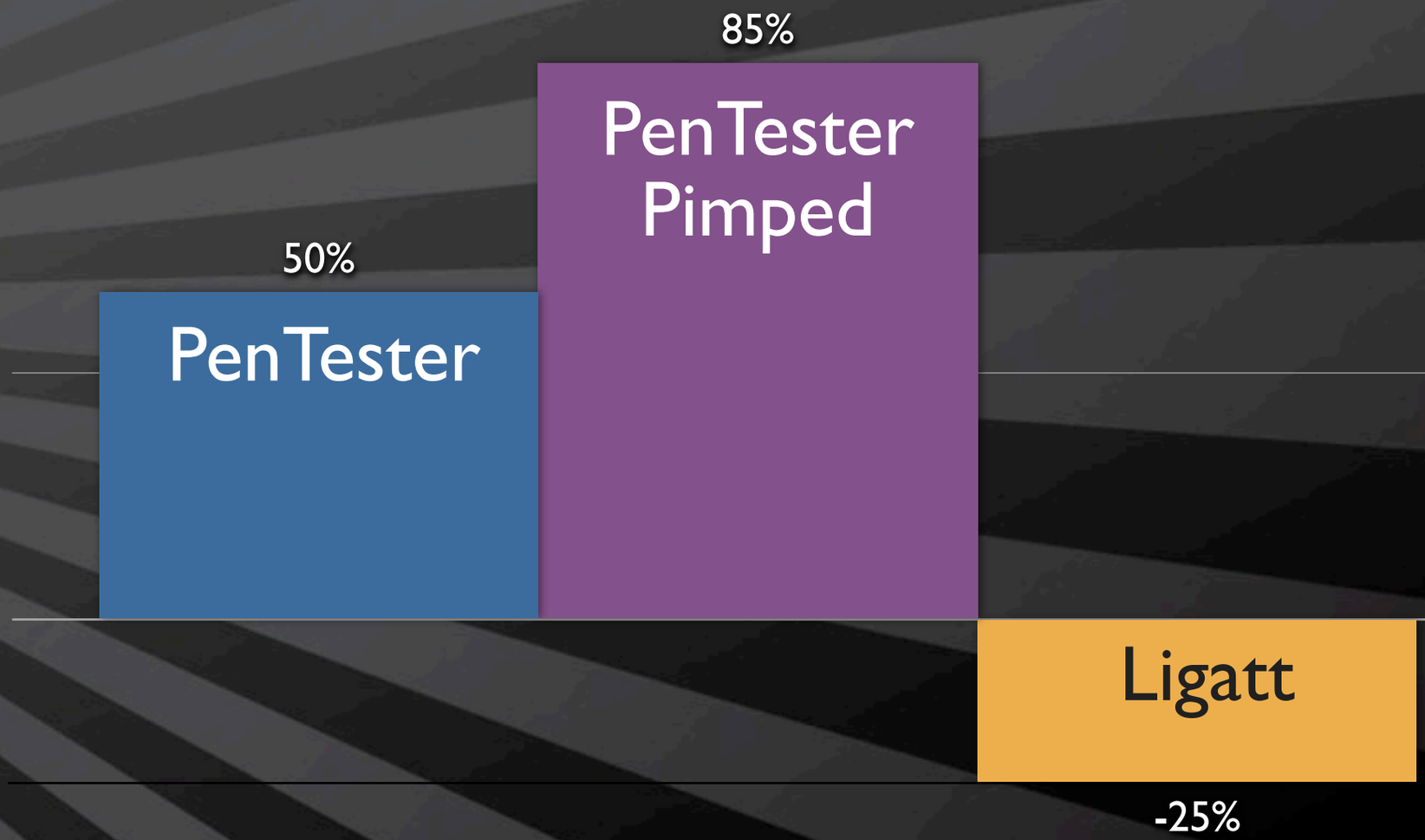
I want stats

... some numbers I made up earlier



I want stats

... some numbers I made up earlier



Ok, so what I'm tired!

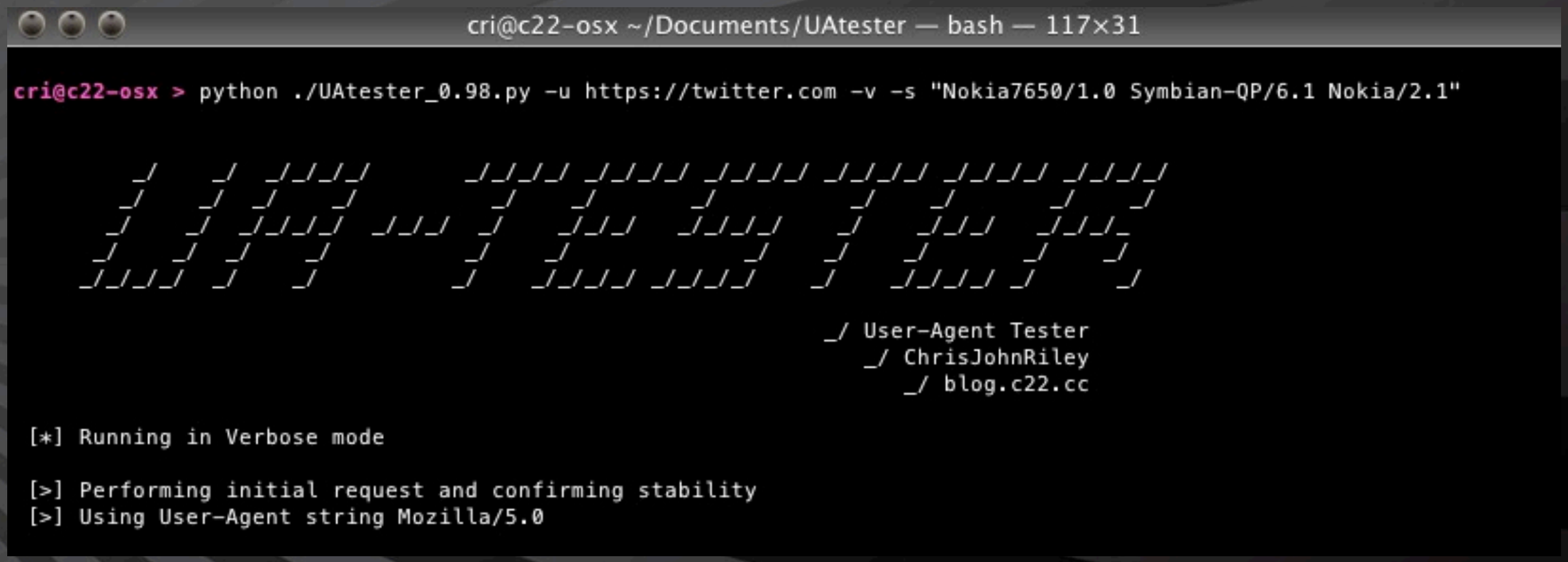
... and why is this guy wearing a purple pimp suit!

UA-Tester

- Takes the challenge out of seeing the differences
- Lets you test what you want and when you want#
- It's free... so stop complaining
  - Beer optional!

Ok, so what I'm tired!

... and why is this guy wearing a purple pimp suit!



Test String:

python ./UAtester_0.98.py -u https://twitter.com -v -s "Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1"

cri@c22-osx ~/Documents/UAtester — bash — 117×31

```
[>] Using User-Agent string Mozilla/5.0

   [ ] URL (ENTERED): https://twitter.com
   [ ] Response Code: 200 OK
   [ ] Date: Thu, 23 Sep 2010 10:54:05 GMT
   [ ] Server: hi
   [ ] Status: 200 OK
   [ ] X-Transaction: 1285239245-21739-8722
   [ ] ETag: "e94c038ee10b36df308bd44988afef44"
   [ ] Last-Modified: Thu, 23 Sep 2010 10:54:05 GMT
   [ ] X-Runtime: 0.00406
   [ ] Content-Type: text/html; charset=utf-8
   [ ] Content-Length: 44818
   [ ] Pragma: no-cache
   [ ] X-Revision: DEV
   [ ] Expires: Tue, 31 Mar 1981 05:00:00 GMT
   [ ] Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
   [ ] Set-Cookie: k=188.20.117.70.1285239245385067; path=/; expires=Thu, 30-Sep-10 10:54:05 GMT;
                   domain=.twitter.com
   [ ] Set-Cookie: guest_id=1285239245387871 97; path=/; expires=Sat, 23 Oct 2010 10:54:05 GMT
   [ ] Set-Cookie: auth_token=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [ ] Set-Cookie: _twitter_sess=BAh7CDoHaWQiJWUwYWU4Yjc5YjdlYTBiZTQwMGRmZmM5MWMyNzI0NGVjIgpm%250Ab
                   GFzaElDOidBY3Rpb25Db250cm9sbGVyOjpGbGFzaDo6Rmxhc2hIYXNoewAG%250AOgpAdXNlZHsAOg9jcmVhdGV
                   kX2F0bCsITIo6PisB--5e6a3412a54cc69469c713785b41f5373dc49586; domain=.twitter.com;
                   path=/
   [ ] X-XSS-Protection: 1; mode=block
   [ ] X-Frame-Options: SAMEORIGIN
   [ ] Vary: Accept-Encoding
   [ ] Connection: close
   [ ] Data (MD5): e94c038ee10b36df308bd44988afef44
```

Ok, so what I'm tired!

... and why is this guy wearing a purple pimp suit!

cri@c22-osx ~/Documents/UAtester — bash — 117×31

```
[1] First Pass
[2] Second Pass
[3] Third Pass

[>] URL appears stable. Beginning test

[>] Using SINGLE User-Agent String specified in commandline
[!] Verbose mode activated for SINGLE mode testing


[>] Output: [+] Added Headers, [-] Removed Headers, [!] Altered Headers, [ ] No Change


[>] User-Agent String : Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1
```

Checks URL/Site for stability - 3 checks, 2 second delay
(i.e. the same response headers are returned)

Ok, so what I'm tired!

... and why is this guy wearing a purple pimp suit!

cri@c22-osx ~/Documents/UAtester — bash — 117×31

```
[1] First Pass
[2] Second Pass
[3] Third Pass

[>] URL appears stable. Beginning test

[>] Using SINGLE User-Agent String specified in commandline
[!] Verbose mode activated for SINGLE mode testing

[>] Output: [+] Added Headers, [-] Removed Headers, [!] Altered Headers, [ ] No Change

[>] User-Agent String : Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1
```

Checks URL/Site for stability - 3 checks, 2 second delay
(i.e. the same response headers are returned)

cri@c22-osx ~/Documents/UAtester — bash — 115×46

```
[>] User-Agent String : Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1


   [!] URL (FINAL): https://twitter.com
   [!] Response Code: 200 OK
   [!] Date: Thu, 23 Sep 2010 10:54:27 GMT
   [ ] Server: hi
   [ ] Status: 200 OK
   [!] X-Transaction: 1285239267-67502-21785
   [!] ETag: "f5354386b9878837ab6e1db15ff7ae68"
   [!] Last-Modified: Thu, 23 Sep 2010 10:54:27 GMT
   [!] X-Runtime: 0.00936
   [ ] Content-Type: text/html; charset=utf-8
   [!] Content-Length: 544
   [ ] Pragma: no-cache
   [ ] X-Revision: DEV
   [ ] Expires: Tue, 31 Mar 1981 05:00:00 GMT
   [ ] Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
   [ ] X-XSS-Protection: 1; mode=block
   [ ] X-Frame-Options: SAMEORIGIN
   [ ] Vary: Accept-Encoding
   [ ] Connection: close
   [ ] Set-Cookie: k=188.20.117.70.1285239267978919; path=/; expires=Thu, 30-Sep-10 10:54:27 GMT;
                   domain=.twitter.com
   [ ] Set-Cookie: guest_id=1285239267982677795; path=/; expires=Sat, 23 Oct 2010 10:54:27 GMT
   [ ] Set-Cookie: auth_token=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: ui=m; path=/
   [+] Set-Cookie: admobuu=e52a5f1485015b33505e0a5d189d144d; domain=.m.twitter.com; path=/;
                   expires=Tue, 19 Jan 2038 03:14:07 GMT
   [+] Set-Cookie: param_q=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_page=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_status=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_in_reply_to_status_id=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_in_reply_to=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_source=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_user=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: param_id=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [+] Set-Cookie: dispatch_action=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
   [ ] Set-Cookie: _twitter_sess=BAh7CToVaW5fbmV3X3VzZXJfZmxvdzA6B2lkIiU5MDIyMGMxZDExZjIzYjVj%250AM
                   zc5MDg4MTc0M2UyY2NiMSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6%250ARmxhc2g6OkZsYXNoSGFzaHs
                   ABjoKQHVzZWR7ADoPY3JlYXRlZF9hdGwrCJDi%250AOj4rAQ%253D%253D--2c2b54fd15deca2092752c75a74
                   f5b3be563730c; domain=.twitter.com; path=/


[>] That's all folks... Fo' Shizzle!
```

```
[!] URL (FINAL): https://twitter.com
[!] Response Code: 200 OK
[!] Date: Thu, 23 Sep 2010 10:54:27 GMT
[ ] Server: hi
[ ] Status: 200 OK
[!] X-Transaction: 1285239267-67502-21785
[!] ETag: "f5354386b9878837ab6e1db15ff7ae68"
[!] Last-Modified: Thu, 23 Sep 2010 10:54:27 GMT
[!] X-Runtime: 0.00936
[ ] Content-Type: text/html; charset=utf-8
[!] Content-Length: 544
[ ] Pragma: no-cache
[ ] X-Revision: DEV
[ ] Expires: Tue, 31 Mar 1981 05:00:00 GMT
[ ] Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
[ ] X-XSS-Protection: 1; mode=block
[ ] X-Frame-Options: SAMEORIGIN
[ ] Vary: Accept-Encoding
[ ] Connection: close
[ ] Set-Cookie: k=188.20.117.70.1285239267978919; path=/; expires=Thu, 30-Sep-10 10:
                domain=.twitter.com
[ ] Set-Cookie: guest_id=12852392679826779 5; path=/; expires=Sat, 23 Oct 2010 10:54:
[ ] Set-Cookie: auth_token=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: ui=m; path=/
[+] Set-Cookie: admobuu=e52a5f1485015b33505e0a5d189d144d; domain=.m.twitter.com; pat
                expires=Tue, 19 Jan 2038 03:14:07 GMT
[+] Set-Cookie: param_q=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_page=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_status=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_in_reply_to_status_id=; path=/; expires=Thu, 01 Jan 1970 00:00
[+] Set-Cookie: param_in_reply_to=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
```

```
[ ] Pragma: no-cache
[ ] X-Revision: DEV
[ ] Expires: Tue, 31 Mar 1981 05:00:00 GMT
[ ] Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0
[ ] X-XSS-Protection: 1; mode=block
[ ] X-Frame-Options: SAMEORIGIN
[ ] Vary: Accept-Encoding
[ ] Connection: close
[ ] Set-Cookie: k=188.20.117.70.1285239267978919; path=/; expires=Thu, 30-Sep-10 10:
                domain=.twitter.com
[ ] Set-Cookie: guest_id=12852392679826779 5; path=/; expires=Sat, 23 Oct 2010 10:54:
[ ] Set-Cookie: auth_token=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: ui=m; path=/
[+] Set-Cookie: admobuu=e52a5f1485015b33505e0a5d189d144d; domain=.m.twitter.com; pat
                expires=Tue, 19 Jan 2038 03:14:07 GMT
[+] Set-Cookie: param_q=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_page=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_status=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_in_reply_to_status_id=; path=/; expires=Thu, 01 Jan 1970 00:0
[+] Set-Cookie: param_in_reply_to=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_source=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_user=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: param_id=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[+] Set-Cookie: dispatch_action=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT
[ ] Set-Cookie: _twitter_sess=BAh7CToVaW5fbmV3X3VzZXJfZmxvdzA6B2lkIiU5MDIyMGMxZDExZj
                zc5MDg4MTc0M2UyY2NiMSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6%250ARmxh
                ABjoKQHVzZWR7ADoPY3JlYXRlZF9hdGwrCJDi%250AOj4rAQ%253D%253D--2c2b54fc
                f5b3be563730c; domain=.twitter.com; path=/


>] That's all folks... Fo' Shizzle!
```

```
[>] User-Agent String : Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1


   [!] URL (FINAL): https://wordpress.com
   [!] Response Code: 200 OK
   [ ] Server: nginx
   [!] Date: Fri, 24 Sep 2010 11:51:32 GMT
   [ ] Content-Type: text/html; charset=UTF-8
   [ ] Transfer-Encoding: chunked
   [ ] Connection: close
   [ ] X-hacker: If you're reading this, you should visit automattic.com/jobs and apply to join the
                 fun, mention this header.
   [+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16b8100c; expires=Fri, 01-Jan-2038 00:00:00 GMT;
   [ ] X-Pingback: http://wordpress.com/xmlrpc.php
   [ ] Link: <http://wp.me/1>; rel=shortlink
   [+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16b8100c; expires=Fri, 01-Jan-2038 00:00:00 GMT;
                 path=/; domain=.wordpress.com
   [-] Last-Modified: Fri, 24 Sep 2010 11:50:54 +0000
   [-] Cache-Control: max-age=2, must-revalidate
   [-] Vary: Cookie
   [-] X-nananana: Batcache


[>] That's all folks... Fo' Shizzle!
```

```
[>] User-Agent String : Nokia7650/1.0 Symbian-QP/6.1 Nokia/2.1


   [!] URL (FINAL): https://wordpress.com
   [!] Response Code: 200 OK
   [ ] Server: nginx
   [!] Date: Fri, 24 Sep 2010 11:51:32 GMT
   [ ] Content-Type: text/html; charset=UTF-8
   [ ] Transfer-Encoding: chunked
   [ ] Connection: close
   [ ] X-hacker: If you're reading this, you should visit autom
                 fun, mention this header.
   [+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16b8100c; ex
   [ ] X-Pingback: http://wordpress.com/xmlrpc.php
   [ ] Link: <http://wp.me/1>; rel=shortlink
   [+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16b8100c; ex
                 path=/; domain=.wordpress.com
   [-] Last-Modified: Fri, 24 Sep 2010 11:50:54 +0000
   [-] Cache-Control: max-age=2, must-revalidate
   [-] Vary: Cookie
   [-] X-nananana: Batcache
```

```
[!] URL (FINAL): https://wordpress.com
[!] Response Code: 200 OK
[ ] Server: nginx
[!] Date: Fri, 24 Sep 2010 11:51:32 GMT
[ ] Content-Type: text/html; charset=UTF-8
[ ] Transfer-Encoding: chunked
[ ] Connection: close
[ ] X-hacker: If you're reading this, you should v
                  fun, mention this header.
[+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16
[ ] X-Pingback: http://wordpress.com/xmlrpc.php
[ ] Link: <http://wp.me/1>; rel=shortlink
[+] Set-Cookie: admobuu=eb502cecc44108ec4d95e3ab16
                  path=/; domain=.wordpress.com
[-] Last-Modified: Fri, 24 Sep 2010 11:50:54 +0000
[-] Cache-Control: max-age=2, must-revalidate
[-] Vary: Cookie
[-] X-nananana: Batcache
```

Where to get it

http://blog.c22.cc/toolsscripts/

QUESTIONS?

COMMENTS?

DEATH THREATS?

Where to get it

http://blog.c22.cc/toolsscripts/