# Web Application Pentesting

Vivek Ramachandran

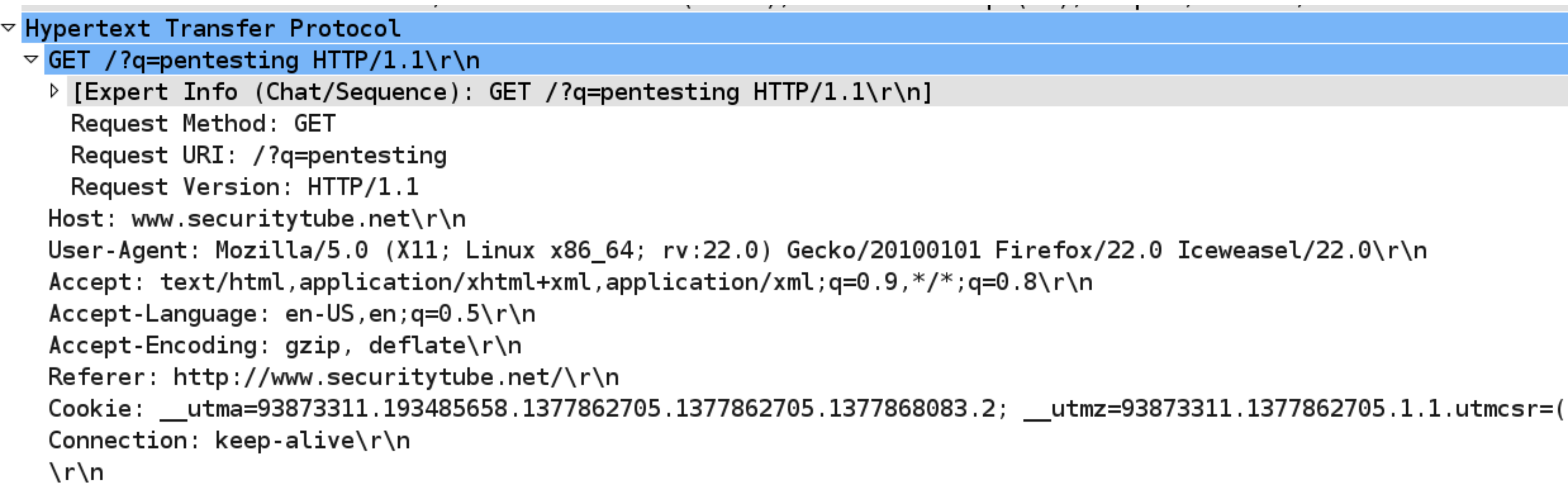
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

# HTTP Methods and Verb Tampering

# HTTP Header

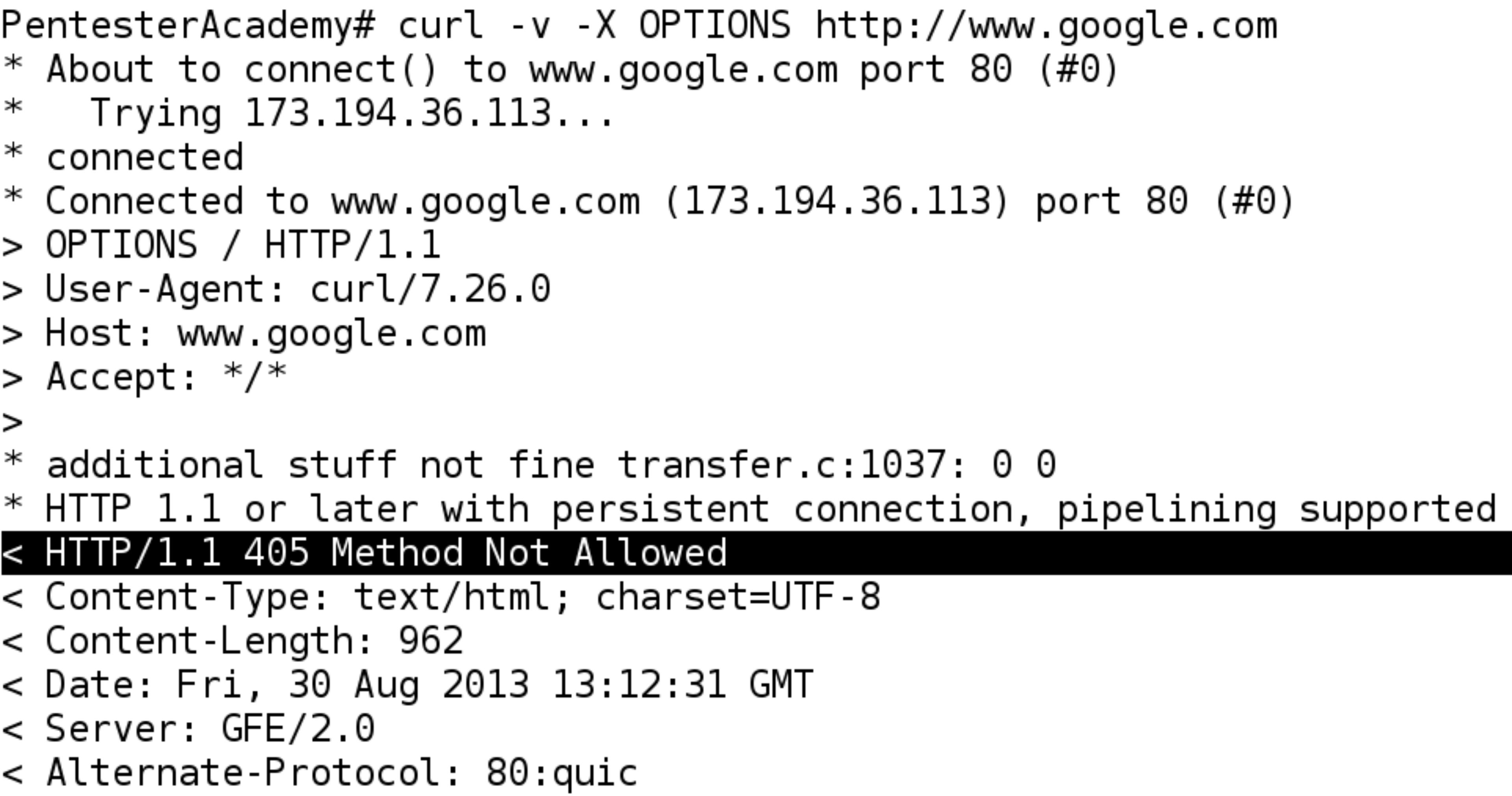


```
▽ Hypertext Transfer Protocol
  ▽ GET /?q=pentesting HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): GET /?q=pentesting HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /?q=pentesting
      Request Version: HTTP/1.1
    Host: www.securitytube.net\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.securitytube.net/\r\n
    Cookie: __utma=93873311.193485658.1377862705.1377862705.1377868083.2; __utmz=93873311.1377862705.1.1.utmcsr=(
    Connection: keep-alive\r\n
    \r\n
```

# HTTP Request Methods

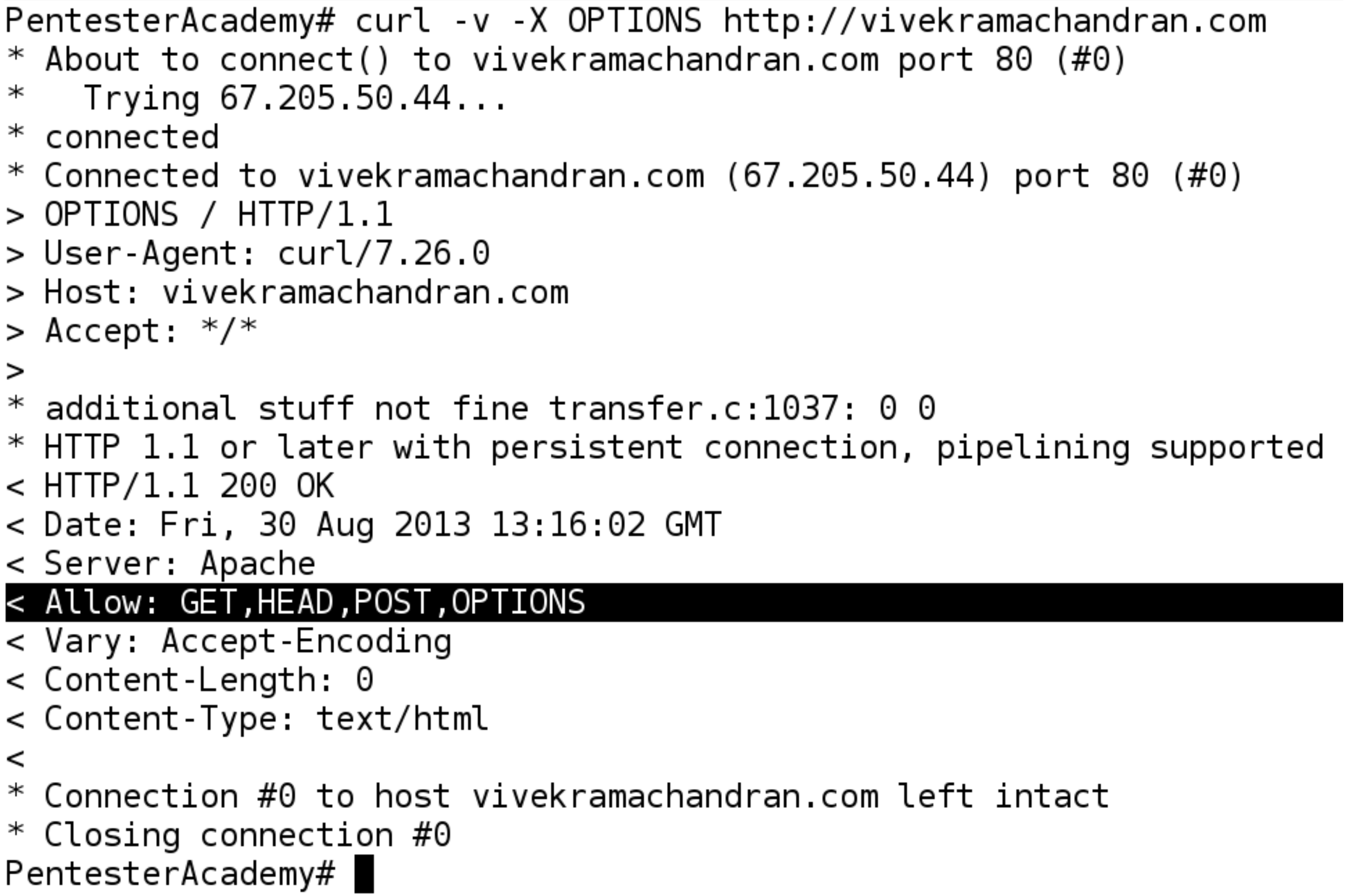
- GET
  - Parameters in URL
- POST
  - Form submissions, data in message body
- OPTIONS
  - List of methods supported for URL
- HEAD
  - Response for GET but no message body
- TRACE
  - Echo client request back for diagnostics
- PUT
  - Store in URI
- DELETE
  - Delete resource
- …

# OPTIONS – Might not be allowed!



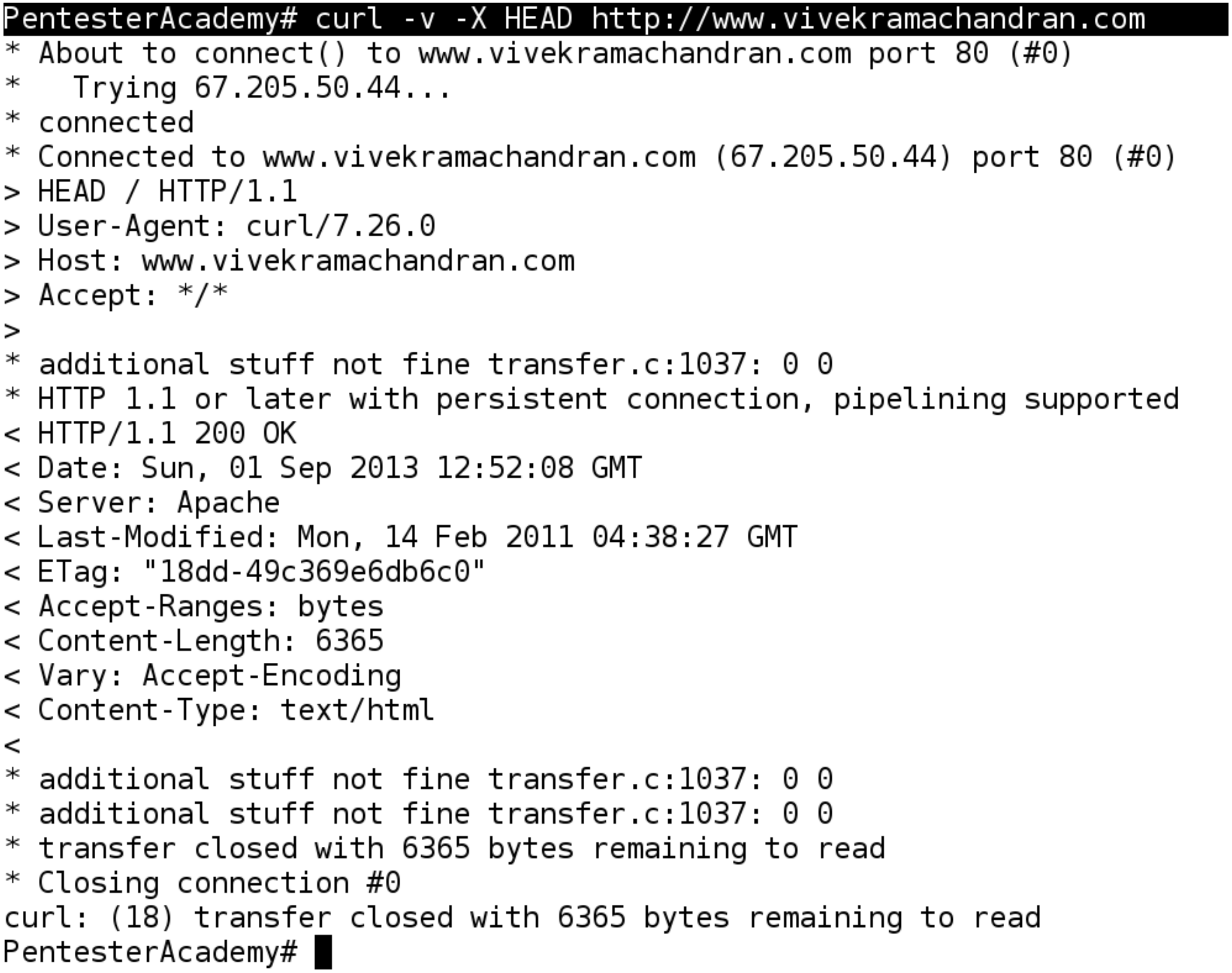
```
PentesterAcademy# curl -v -X OPTIONS http://www.google.com
* About to connect() to www.google.com port 80 (#0)
*   Trying 173.194.36.113...
* connected
* Connected to www.google.com (173.194.36.113) port 80 (#0)
> OPTIONS / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.google.com
> Accept: */*
>
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 405 Method Not Allowed
< Content-Type: text/html; charset=UTF-8
< Content-Length: 962
< Date: Fri, 30 Aug 2013 13:12:31 GMT
< Server: GFE/2.0
< Alternate-Protocol: 80:quic
```

# OPTIONS – might work for some!



```
PentesterAcademy# curl -v -X OPTIONS http://vivekramachandran.com
* About to connect() to vivekramachandran.com port 80 (#0)
*   Trying 67.205.50.44...
* connected
* Connected to vivekramachandran.com (67.205.50.44) port 80 (#0)
> OPTIONS / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: vivekramachandran.com
> Accept: */*
>
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 200 OK
< Date: Fri, 30 Aug 2013 13:16:02 GMT
< Server: Apache
< Allow: GET,HEAD,POST,OPTIONS
< Vary: Accept-Encoding
< Content-Length: 0
< Content-Type: text/html
<
* Connection #0 to host vivekramachandran.com left intact
* Closing connection #0
PentesterAcademy# 
```

# GET vs HEAD



```
PentesterAcademy# curl -v -X HEAD http://www.vivekramachandran.com
* About to connect() to www.vivekramachandran.com port 80 (#0)
*   Trying 67.205.50.44...
* connected
* Connected to www.vivekramachandran.com (67.205.50.44) port 80 (#0)
> HEAD / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.vivekramachandran.com
> Accept: */*
>
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 200 OK
< Date: Sun, 01 Sep 2013 12:52:08 GMT
< Server: Apache
< Last-Modified: Mon, 14 Feb 2011 04:38:27 GMT
< ETag: "18dd-49c369e6db6c0"
< Accept-Ranges: bytes
< Content-Length: 6365
< Vary: Accept-Encoding
< Content-Type: text/html
<
* additional stuff not fine transfer.c:1037: 0 0
* additional stuff not fine transfer.c:1037: 0 0
* transfer closed with 6365 bytes remaining to read
* Closing connection #0
curl: (18) transfer closed with 6365 bytes remaining to read
PentesterAcademy# 
```

# HEAD - Security Risks

- Authentication Bypass
  - Auth only applied for GET, POST and not HEAD
  - http://www.fishnetsecurity.com/6labs/blog/jboss-jmx-console-authentication-bypass
- HTTP Verb Tampering
  - Aspect Security
  - http://jeremiahgrossman.blogspot.in/2008/06/what-you-need-to-know-about-http-verb.html

# Exercise

- Find appropriate Nmap NSE scripts which test for HTTP Verb tampering
- Find appropriate Metasploit module for the same
- Do a demo
- Post on SecurityTube.net as a video if you like ☺