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

The HTTP Protocol

Hypertext Transfer Protocol

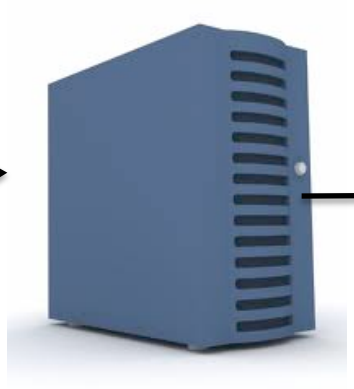
- Client-Server based architecture
- Request-Response model to serve Resources
- Resources are identified by URI / URL
- Versions – HTTP 1.0/1.1
  - 1.1 can reuse connection for multiple URIs

How does it really work?

User

Browser

HTTP



Web Server

Database

Netcat / Curl / Browser

```
PentesterAcademy# curl -v www.securitytube.net

* About to connect() to www.securitytube.net port 80 (#0)
*   Trying 74.125.135.121...
* connected
* Connected to www.securitytube.net (74.125.135.121) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.securitytube.net
> Accept: */*
>
* additional stuff not fine transfer.c:1037: 0 0
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 200 OK
< Content-Type: text/html; charset=utf-8
< Cache-Control: no-cache
< Vary: Accept-Encoding
< Date: Fri, 30 Aug 2013 11:46:11 GMT
< Server: Google Frontend
< Alternate-Protocol: 80:quic,80:quic
< Transfer-Encoding: chunked
```

Wireshark Lab