HTTP/HTTPS

1. Малко история на протокола HTTP

   - Измислен от CERN (какво е CERN)
   - Измислен за пренос на хипертекст
     Какво е хипертекст, какво е markup language (HTML)

   - HTTPS - HTTP over TLS, съвсем просто и ясно, почти прозрачно за самия протокол

2. Принцип на работа на протокола

   - URL, URI
     http_URL = "http:" "//" host [":" port] [abs_path ["?" query]]
   - Клиента подава заявка, сървъра отговаря - кратко и ясно

3. Самият протокол

   - header-и в самия протокол - при подаване на завка и при отговор
     При отговор
       Content*
         type
         encoding
         language
         length
         range
       Location
       Allow - еквивалент на accept
     При заявка
       Accept*
       Authorization
       Cache-Control
       Host
       User-Agent
       If-Modified-Since
       Referer
       Via

   - Типове заявки
     GET - изтегля документ
     HEAD - изтегля само header-ите за документ
     POST - изпраща информация на сървъра
     CONNECT - да направи връзка до друг host, използва се за proxy сървъри
     OPTIONS - показва възможностите на даден сървър/ресурс (позволени типове заявки и т.н.)
     TRACE - действа като loopback, и ни показва какво точно получава отсрещния web сървър, може да се използва за откриване на proxy сървъри.
     PUT, DELETE - почти не се използват

4. Сървъри

   - Отдавна е практика сървърите да не работят като root

   - Apache
     Най-разпространения сървър за момента, сравнително бърз и много удобен. Има сравнително бедна история със security проблеми, и само няколко сериозни такива.
   - IIS
     Убийствена история за security проблеми, има няколко worm-а, базирани на него.
   - Netscape Enterprise
     Един от първите комерсиални web сървъри, идващ от идеята на netscape да печелят от сървъри, а не от browser.
   - Zeus
   - Zope
   - thttpd
     Малък, бърз и сигурен сървър за статични данни. С малко security проблеми.

5. Security проблеми

- Повечето проблеми са проблеми на browser-ите

- HTTP authentication, и време за изтичане на credentials
  - Няма 'logout'
  - При basic auth паролата се предава в cleartext
- proxies и възможностите, които те дават.
- Вариант да гледаме в чужди директории чрез symlinks
  - Опции FollowSymlinks, SymlinksIfOwnerMatch
- directory traversal при някои сървъри
  - Дългата история на IIS
- http://user:pass@www.blah.com/ - криене на хост
  - История на стандарта, и на решенията на проблема при IE и Mozilla
- DoS