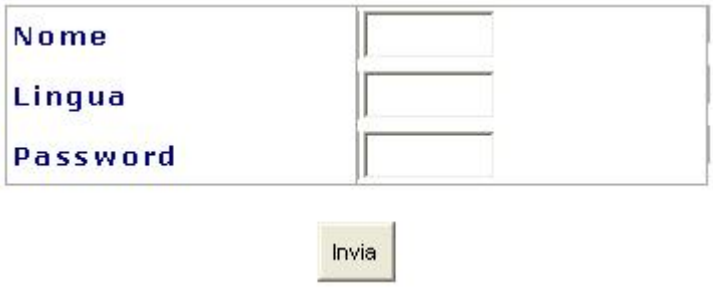
Sicurezza
Protezioni in una pagina Web

HTML è un linguaggio che consente di presentare informazioni in pagine di formato predefinito e accattivante. Quando non si hanno a disposizione informazioni sulle preferenze dell'utente, tali pagine sono uguali per ogni utente. Alternativamente, è possibile far arrivare informazioni dal *client* al *server* secondo schemi prestabiliti, facendo uso della struttura modulo. I moduli, o *form*, consentono di inserire dei controlli che sono già in uso in altri programmi di uso comune (per esempio per l'*Office Automation*): Pulsanti, caselle di testo, caselle combinate, eccetera I dati che possono essere inseriti dall'utente e poi inviati, potranno essere oggetto di elaborazione presso il *server* con programmi presenti allo scopo (e aventi tecnologia differente, per esempio **CGI**, *Common Gateway Interface*, o **ASP**, *Active Server Pages*, eccetera).



Il marcatore fondamentale è senz'altro `<FORM>` che permette di inserire un modulo. Il tag richiederà l'inserimento del corrispondente marcatore di chiusura. Tra i due elementi possono essere inseriti tutti i controlli cui si è già accennato. Nel caso dell'esempio precedente, il codice è riportato a seguire:

```
<FORM NAME="Prima" METHOD="GET" ACTION="http://www.indir.com/pro">
  <LABEL> Nome </LABEL>
    <INPUT NAME="Nome" TYPE="TEXT">
  <LABEL>Lingua</LABEL>
    <INPUT NAME="lingua" TYPE="TEXT">
  <LABEL>Password</LABEL>
    <INPUT NAME="pw" TYPE="PASSWORD">
    <INPUT ID="visitatorep" TYPE=SUBMIT SIZE=3 VALUE="Invia">
</FORM>
```

Un modulo può contenere i vari controlli disponibili, ma non può essere presente un *form* annidato (è possibile tuttavia averne diversi all'interno di una pagina).

Quando viene lanciato un *form*, tutti i suoi campi vengono inviati al *server*. Il tag `<form>` indica al *browser* l'inizio e la fine del *form*. Questo significa che un *form* può agevolmente includere una tabella o un'immagine insieme ai *form field* illustrati in seguito. Per esempio:

```
<html>
  <head>
    <title>Esempio di un form</title>
  </head>
  <body>
    <form>
      <!-- Qui vanno form field e HTML -->
    </form>
  </body>
</html>
```

Diversamente da una tabella, i *form* non sono visibili sulla pagina. Il *form* nel nostro esempio è

inutile. Innanzitutto non contiene *form field*. In secondo luogo, non contiene un ricevente per il *form*. Per fare sì che il *browser* sappia dove inviare il contenuto, dobbiamo aggiungere questi attributi al tag `<form>`:

- **ACTION**: fornisce l'indirizzo e il nome del programma che dovrà elaborare i dati;
- **METHOD**: specifica il metodo con il quale i dati devono essere inviati al *server*;
- **GET**: i dati vengono inviati come parte terminale della URL specificata con *ACTION* (per esempio avendo inserito la riga

  ```
  <FORM NAME="Prima" METHOD="GET" ACTION="http://www.indir.com/pro">
  ```

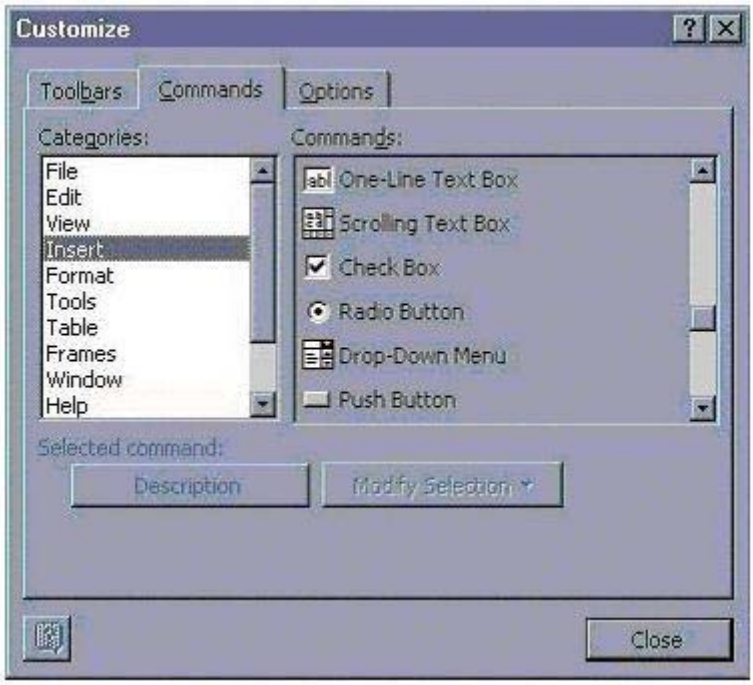
  al *computer* giungerà il messaggio

  http://www.indir.com/pro?visitatore=mario ...

- **POST**: i dati vengono inviati sotto forma di pacchetti al **CGI** (in genere se si hanno molti dati da spedire);
- **ENCTYPE**: specifica il formato con cui i dati vengono trasmessi al *server*. Il valore di *defaul è application/x-www-form-urlencoded*; altri valori ammissibili sono *multipart* e *form-data*;
- **NAME**: serve a identificare un *form* tra quelli presenti in una pagina.

I controlli

Una *form* necessita di controlli che consentano di inviare i dati ad un *server*. *form* e controlli possono essere inseriti agevolmente con un *editor Web* (per esempio *Front Page*), magari rendendo disponibili tali controlli sulle barre.



Da un punto di vista pratico ognuno dei controlli ha un nome, e contiene un valore. E' importante ricordarsene quando tali valori vengono raccolti dal *server* per l'elaborazione. Una stringa tipica generata da una *form* è la seguente:

```
www.sito.it/pagina.html?nomecontrollo1=valore1&nomecontrollo2=valore2
```

dove nomecontrollo è il nome di ognuno dei controlli presenti nella *form*, e valore è il dato presente nel controllo quando viene premuto il tasto di conferma.

Vediamo in dettaglio quali sono i controlli che è possibile inserire in una *form*.

Check box: Le caselle di scelta (check boxes) si adoperano quando si vuole dare al visitatore la possibilità di selezionare una o più opzioni da una serie di alternative. I *check* sono controlli indipendenti (ognuno assume un valore indipendente dagli altri). Se si vuole permettere una sola opzione, bisogna allora usare i bottoni radio. Il controllo ed il codice **HTML** per ciascun *check* è il seguente:

 `<input TYPE="checkbox" NAME="Checkbox1" VALUE="ON">`

l'attributo value assume i due valori on e off.

Radio button: I *radio buttons* (bottoni radio) vengono usati quando si vuole che il visitatore selezioni una - e soltanto una - opzione da una serie di alternative. Se si vogliono permettere più opzioni contemporaneamente, bisogna invece usare i *check boxes*. Il controllo ed il codice **HTML** per ciascun *check* è il seguente:

 `<input TYPE="radio" NAME="radio" VALUE="radiobutton3" CHECKED="true">`

l'attributo *checked* (modificato di solito a *runtime*) è presente soltanto sul controllo selezionato.

Submit button:Quando un visitatore clicca su un tasto d'invio, il *form* viene mandato all'indirizzo specificato nell'attributo action del tag <form>. Il controllo ed il codice **HTML** è il seguente:

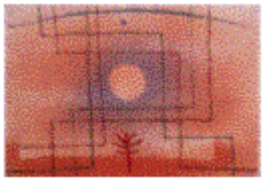
`<input TYPE="submit" ACTION="..." METHOD="post" NAME="submit">`

Il testo invia è un testo di *default* stabilito dal *browser*. E' possibile modificarlo mediante l'attributo *value*.

Reset button: quando un visitatore clicca su un bottone di *reset*, i controlli sono resettati ai valori di *default*.

`<input TYPE="reset" VALUE="Reset" NAME="resetbutton">`

Image button: i bottoni di immagine hanno lo stesso effetto dei bottoni di invio, tranne che per la possibilità di essere personalizzati graficamente. Quando un visitatore clicca su un bottone di immagine il *form* viene mandato all'indirizzo specificato nell'attributo *action* del tag `<form>` .

 `<input TYPE="image" SRC="immagine.gif" NAME="image">`

Text field: I *text fields* sono aree di una riga sola che permettono all'utente di inserire testo. L'opzione *size* definisce la larghezza del *field* e quindi la quantità dei caratteri visibili che il *field* riesce a contenere. *Maxlength* invece la lunghezza massima del *field* e la quantità di caratteri che possono entrare nel *field*.

```
<input TYPE="TEXT" SIZE="10" NAME="shorttext">
```

La variante TYPE="password" sostituisce i caratteri digitati con asterischi, permettendo così l'inserimento di *password*. Tale controllo però non cifra il testo, che quindi viene inviato in chiaro al *server*.

Hidden field: I *field* nascosti (hidden fields) sono simili a *field* di testo, con una differenza importantissima: il *field* nascosto non è mostrato sulla pagina. Di conseguenza il visitatore non può scriverci nulla sopra; lo scopo di questo tipo di *field* è dunque di introdurre informazioni non accessibili al visitatore. Il codice è il seguente:

```
<input TYPE="HIDDEN" NAME="nascosto">
```

Select: I *drop-down* menu sono probabilmente gli oggetti più flessibili da aggiungere ai *form*. Il menù a discesa ha lo stesso scopo dei bottoni radio (una selezione soltanto) o dei check boxes (dove sono permesse selezioni multiple).

voce1 voce2

```
<select size="1" name="D1">
<option value="valore1">voce1</option>
<option selected="true" value="valore2">voce2</option>
</select>
```

I vari *option* definiscono le voci, e *SELECTED* indica la voce selezionata.

Cookies

Un *cookie* (biscottino) è un piccolo frammento di informazione che un *server Web* può immagazzinare temporaneamente in un *browser Web*. Ciò risulta utile per permettere al *browser* di ricordare alcune informazioni specifiche che il *server Web* può recuperare successivamente.

È questa la definizione di *cookie* data da *Netscape*. Si tratta di un meccanismo di connessione server side attraverso il quale il *server Web* può immagazzinare informazioni sulla connessione con il *client*; in altre parole, il *server* su cui risiede la pagina ***Internet*** visualizzata ha la possibilità di memorizzare alcune informazioni sia sul *server* che sul *client*, per utilizzarle in modi diversi; per esempio è possibile personalizzare le pagine in modo diverso in funzione delle preferenze, oppure fornire in video il numero di accessi di un determinato utente alla pagina corrente. In pratica attraverso l'uso dei *cookie* si può memorizzare lo stato della connessione (altrimenti non previsto dal protocollo HTTP), in modo da consentire al *server* di agire in funzione di esso. Tuttavia, quello dei *cookie* può essere uno strumento utilizzato per carpire indebitamente informazioni all'utente, trasgredendo alle norme sulla *privacy*.

La memorizzazione dei *cookie* avviene in modi e in cartelle diverse in funzione del *browser*: *Netscape* crea un unico *file* denominato cookies.txt memorizzato nella cartella relativa al nome dell'utente e posta all'interno di `Programmi\Netscape\Users`. *Explorer* invece registra separatamente ogni *cookie*. La cartella di memorizzazione si chiama proprio ***Cookie*** e si trova all'interno della *directory Windows*. Quando vengono impostati diversi utenti, verranno create automaticamente cartelle diverse atte a contenere i *cookie*.

Di seguito viene visualizzato il contenuto del *cookie* **sandro@www.sun[1].txt** sun_visitor_uid

```
313333531383237325e30
www.sun.com/0
3578172800
29305075
2662236192
29296023
```

Effetti dei cookie

Attraverso i *cookie* vengono memorizzate informazioni sul *browser* in modo che a una successiva connessione allo medesimo sito il *server* possa leggere lo stato della stessa. Viene scritto un numero identificativo che consente di riconoscere l'utente e, insieme a questo, altre informazioni di servizio o utili al *server*: per esempio, si utilizza spesso una data di scadenza del *cookie*, oppure si può memorizzare la data della connessione o il numero di collegamenti effettuati. I *cookie* possono essere quindi utilizzati per diversi scopi; di seguito viene fornito un elenco di possibili appicazioni:

- salvataggio di informazioni generiche sulla connessione (identificativo utente, data di connessione, data di scadenza, numero di connessioni, eccetera);
- salvataggio dello stato della navigazione (esempio pagine visitate) per permettere una migliore fruizione del sito;
- memorizzazione di informazioni utili per il commercio elettronico (per esempio quando si vuole riempire un carrello elettronico della spesa le informazioni parziali possono essere memorizzate nei *cookie*);
- salvataggio di informazioni utili a fini statistici;
- salvataggio di informazioni utili per applicazioni ludiche.

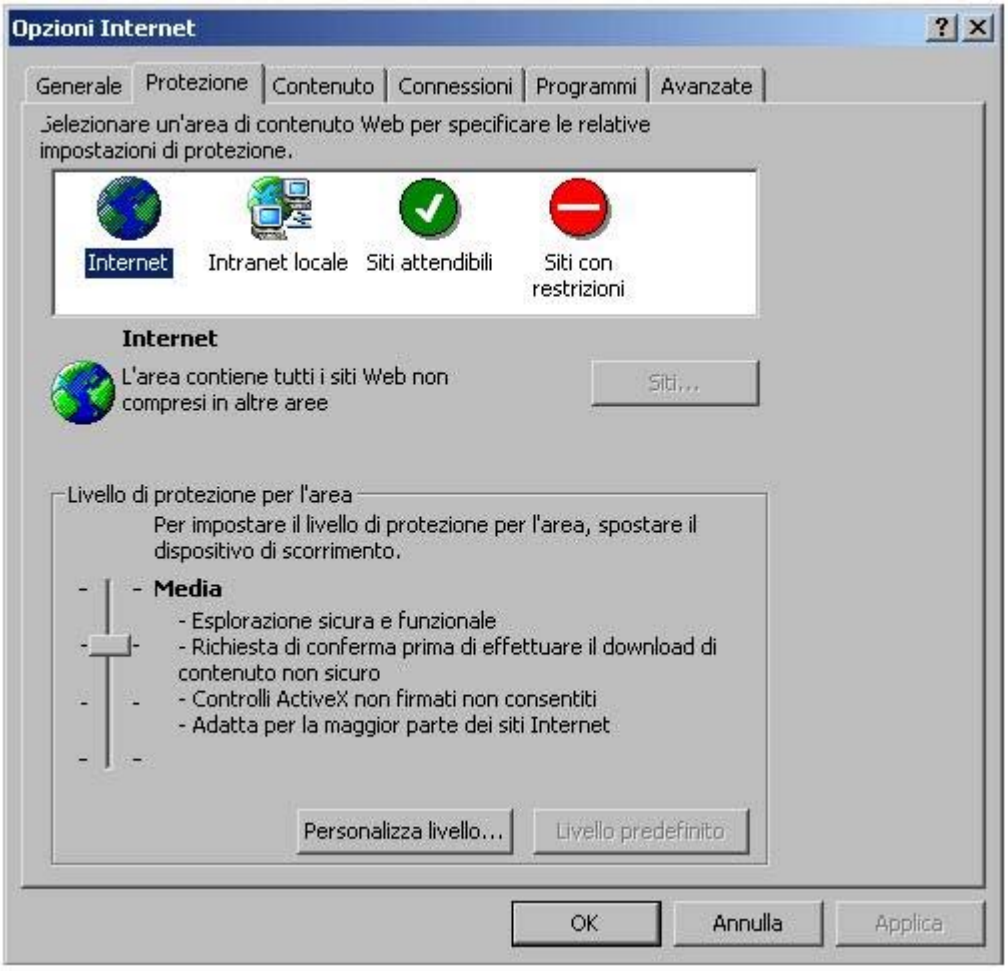
Tuttavia la maggior parte dei *cookie* permangono nella macchina *client* solo durante la connessione, al termine della quale vengono distrutti. I *cookie*, in ogni caso, non interagiscono con altri *file* presenti sul *client* o con il sistema operativo. Sopravvalutando le capacità di questi oggetti, li si ritengono erroneamente capaci di carpire *password*, numero di carte di credito o altre informazioni sul *software* installato sul nostro *computer*. Attraverso i *cookie* vengono memorizzati in un *database* i siti visitati durante la navigazione, costruendo un profilo dell'utente riguardante i sui interessi; con un sistema legato ai *cookie* viene selezionata la pubblicità da mostrare durante la navigazione, pubblicità che risponderà selezionata in base ai gusti individuati dell'utente (per esempio il sito

DoubleClick spesso si occupa della selezione dei *banner* pubblicitari da mostrare).

E' possibile definire le impostazioni del *browser* in modo da impedire l'uso dei *cookie*; tuttavia alcuni siti non funzionano regolarmente qualora vengano attivate tali misure di protezione. Il sistema di comunicazione dei *cookie* tra *client* e *server* prevede che quest'ultimo possa richiedere al *browser* le informazioni eventualmente presenti, creandole se non ci sono o modificandole se è il caso. Il *server* comunque viene a conoscenza delle generalità dell'utente (ad esempio nome o indirizzo di posta elettronica) solo attraverso una comunicazione diretta (e volontaria) degli stessi, non avendo la possibilità di prelevarli autonomamente dal disco rigido.

Impostazioni di protezione

I *browser* sono tipicamente configurati per consentire la creazione di *cookie*; l'utente tuttavia può stabilire che venga visualizzato un messaggio prima che il sito collochi il *cookie* sul disco rigido, in modo che l'utente possa decidere di acconsentire o meno all'operazione. In alternativa è possibile configurare i *browser* in modo da impedire l'accettazione di qualsiasi *cookie*. Di seguito si fa riferimento alle procedure atte all'impostazione delle protezioni su *Internet Explorer* 5.



Selezionando la voce Strumenti `--> Opzioni Internet -->` Personalizza livello è possibile definire diverse modalità per la gestione dei *cookie*. A proposito della gestione dei *cookie*, è possibile prevedere un diverso modo di procedere tra i *cookie* temporanei e quelli memorizzati nel disco rigido; in ogni ipotesi è possibile scegliere tra tre diverse soluzioni:

- si desidera accettare un *cookie* da un sito ***Internet*** senza ricevere alcun messaggio di avviso (Attiva).
- Prima di accettare un *cookie* da un sito ***Internet*** si desidera ricevere un messaggio di avviso,

(Conferma).

- Ai siti *Web* non è consentito inviare *cookie* al *computer* in uso, né leggere quelli salvati sul disco rigido(Disattiva). Tuttavia alcuni siti sono visualizzabili in modo ottimale solo se è possibile gestire i *cookie*.

È importante segnalare che ogni volta che che viene inviata una richiesta al *server*, essa include l'indirizzo *IP* del mittente, il *browser* e il sistema operativo utilizzato, a prescindere dall'utilizzo o meno di un *cookie*, che non è quindi da ritenersi responsabile della diffusione di tali dati di riferimento.