Esame di **Progettazione di servizi web e reti di calcolatori (01NBE)**
Corso di Laurea in Ing. dell'Organizzazione d'Impresa

Prova scritta di teoria (18/7/2013)

> NOTA
> Le tracce delle soluzioni fornite in questo testo sono da considerarsi solo come un aiuto per comprendere i principali punti da toccare nel risolvere gli esercizi proposti ma non sono né esaustive né presentate in forma adeguata per l'elaborato da consegnarsi in sede d'esame.
> In particolare per molti esercizi le soluzione è volutamente schematica e ci si attende che il candidato spieghi adeguatamente i singoli punti, per dimostrare reale comprensione dell'argomento invece che semplice capacità mnemonica di ricordare i punti elencati nelle slide (o in queste tracce di soluzione).

Esercizio 1 ***(punti: 6)***
Spiegare che cosa è un *cookie* HTTP, quali suoi parametri un server può impostare quando lo trasmette al client e quale ragionamento un client svolge per decidere quali cookie trasmettere ad un server.

Traccia di una possibile risposta
Cookie = dati inviati all'interno di una risposta HTTP dal server al client (tipicamente per memorizzare preferenze dell'utente o informazioni di stato all'interno di una sessione o tra sessioni diverse), rimandati dal client al server; stessi dati rimandati dal client all'interno delle richieste HTTP successive.
Parametri impostabili: chiave=valore, path e/o dominio delle URI richieste, data di scadenza, trasmissione solo su canali sicuri.
I cookie presenti sul client sono selezionati in base alla loro corrispondenza con la URI richiesta (path e dominio) purché non siano scaduti e si usi https se è richiesto un canale sicuro.

Esercizio 2 ***(punti: 4)***
Illustrare la funzionalità di un MSA e MTA all'interno di un sistema di posta elettronica.
Volendo autenticare gli utenti (ad esempio per permettere solo agli utenti registrati di spedire posta) su quale dei due elementi sarebbe meglio effettuare l'autenticazione? Giustificare la propria risposta.

Traccia di una possibile risposta
MSA = Mail Submission Agent, server che riceve mail dai MUA e la introduce nella catena degli MTA.
MTA = Mail Transfer Agent, server che partecipa alla trasmissione della posta effettuando l'operazione di store-and-forward (riceve posta da un MSA o MTA e la ritrasmette ad un MTA o MS).
L'autenticazione degli utenti ha senso solo su MSA perché sono gli unici server a dialogare direttamente col MUA e quindi con l'utente (es. per richiedergli username e password).

Esercizio 3 ***(punti: 6)***
Dato il seguente spezzone di file CSS, identificare e spiegando le tecniche errate o sconsigliate che sono state usate e suggerendo le opportune correzioni.

```
body {
   font-family: "Times New Roman", Serif, Garamond;  font-size: 12px;
   background: black;  color: rgb(10,10,10);
}

*.rosso { color: red; }

h1 {
  font-family: "Times New Roman", Serif, Garamond;
  font-size: 120%;  font-weight: bold;
}
```

Traccia di una possibile risposta

- *Garamond ignorato perché preceduto da font generico (mettere Serif in ultima posizione);*
- *mai font-size in PX (usare PT per la stampa, percentuali o proporzioni per il video);*
- *colore grigio scuro su sfondo nero è praticamente illeggibile (usare colore con maggior contrasto);*
- `rosso` *non è una classe logica (usare un nome logico, ad esempio* `avviso`*);*
- *font-family su H1 duplica inutilmente quella del body (eliminare questa dichiarazione in H1).*

Esercizio 4 ***(punti: 5)***
Un server web concorrente è installato su un computer dotato di 4 CPU a 1 GHz, 8 GB di RAM, scheda di rete a 10 Mbps e disco (non frammentato) da 1 TB, 10 ms e 10 MB/s. Sapendo che il server è collegato ad Internet tramite una linea ADSL da 2 Mbps, calcolare il tempo necessario a fornire risposta a due client che effettuano la loro richiesta simultanemente, tenendo conto dei seguenti parametri: per attivare un processo occorrono 20 ms, il server inizialmente è scarico (ossia non ha client collegati) e nessun altro client si collega oltre ai due in discussione, la dimensione di una richiesta è 8 kB e di una risposta è 2 MB e per fornire ciascuna risposta il server deve svolgere 2 milioni di istruzioni e leggere 5 file diversi ciascuno da 1 MB.

Traccia di una possibile risposta
Per servire un client vanno svolte nell'ordine le seguenti operazioni:
1. attivazione figlio:

$$T_A = 20\,\text{ms}$$

2. lettura della richiesta:

$$T_R = \frac{8 \cdot 1024 \cdot 8\,\text{bit}}{2 \cdot 1024 \cdot 1024\,\text{bps}} = 64/1024\,\text{s} = 62\,\text{ms}$$

3a. lettura dati dal disco:

$$T_D = 5 \cdot 10\,\text{ms} + \frac{5\,\text{MB}}{10\,\text{MB/s}} = 0.550\,\text{s}$$

3b. . . . ed esecuzione istruzioni:

$$T_C = \frac{2 \cdot 10^6 \text{istruzioni}}{1 \cdot 10^9 \text{ips}} = 2\,\text{ms}$$

4. invio della risposta:

$$T_W = \frac{2 \cdot 1024 \cdot 1024 \cdot 8\,\text{bit}}{2 \cdot 1024 \cdot 1024\,\text{bps}} = 8\,\text{s}$$

Essendoci quattro CPU l'esecuzione delle istruzioni avverrà in parallelo (ossia T_A e T_C), mentre tutte le altre operazioni usano una risorsa condivisa e quindi saranno gestite in time sharing (es. letture alternate da disco) e comporteranno un raddoppio del tempo relativo.
Tempo per servire entrambi i client:

$$T_2 \approx T_A + 2 \cdot T_R + T_C + 2 \cdot T_D + 2 \cdot T_W = 20 + 124 + 2 + 1100 + 16000 = 17\,246\,\text{ms}$$

Esercizio 5 ***(punti: 5)***
Illustrare quali informazioni vengono inviate a livello di protocollo HTTP (versione 1.1) dal browser al server quando un utente, dopo aver visualizzato la pagina web contenente il form qui sotto riportato, inserisce come prodotto "televisore a colori" e come quantità "2" e preme OK.
Discutere anche i pregi e difetti di questo metodo per la trasmissione di dati tramite form.

```
<form name="login" action="http://a.b.com/acquista.asp" method="get">
   <input type="hidden" name="account" value="U101">
   prodotto? <input type="text" name="prod"> <br>
   quantit&agrave;? <input type="text" name="qty"> <br>
   <input type="submit" value="OK">
</form>
```

Traccia di una possibile risposta
Dati trasmessi con OK:

```
GET /acquista.asp?account=101&prod=televisore+a+colori&qty=2 HTTP/1.1
Host: a.b.com
Content-Length:  0
```

Pregi: permette di fare cache della risposta e bookmarking, entrambe con gli specifici valori dei parametri.
Difetti: limita la quantità di dati che può essere trasmessa (in questo caso non è un problema) e mostra i valori dei parametri sia nella barra degli indirizzi (si noti la visualizzazione anche del parametro nascosto) sia nel log del server HTTP.

Esercizio 6 ***(punti: 6)***
Spiegare che cosa è un attacco *SQL injection* e quali tecniche si possono adottare per prevenirlo.

Traccia di una possibile risposta
Tramite un'operazione di input (es. dati di un form) un utente malevolo trasmette dati che – usati dal server per creare una query SQL in forma di stringa – fanno svolgere al server un'operazione SQL diversa da quella prevista. Ad esempio . . .
Per prevenire l'attacco: controllare tutti gli input forniti dall'utente verificando che non contengano caratteri illegali (es. apice singolo), o meglio controllando che contengano solo caratteri legali; meglio ancora strutturare tutte le operazioni su DB in modo che siano eseguite tramite query parametrizzate *perché in questo modo l'input fornito dall'utente non può alterare la struttura della query SQL.*