KARADENİZ TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
Bilgisayar Mühendisliği Bölümü
20010-2011 Eğitim-Öğretim Bahar Yarıyılı
Web Programlama Final Sınavı Soruları

- ✓ Soru kâğıdına **adınız**, **soyadınız** ve **numaranız** dışında başka hiçbir şey yazmayınız.
- ✓ Sorular **eşit** puanlıdır. Süre **120** dakikadır.

veritabani.php

```
…
$baglan = mysql_connect('localhost', 'root', '');
if (!$baglan) die('Bağlantı yapılamıyor: ' . mysql_error());
mysql_select_db("Ziyaret", $baglan);
$q = $_REQUEST["q"];
$sql = "SELECT * FROM Ziyaretcidefteri WHERE ziyaretci_id = '".$q."'";
$sonuc = mysql_query($sql);
…
```

veritabani.html

```
…
<form> Kullanıcı ID: <input type = "text" size = "5" onchange = "kullaniciGoster(this.value)" /> </form>
…
```

veritabani.js

```
function kullaniciGoster(str) { //…  } …
```

S.1) Yukarıda verilen kod parçalarından görülebileceği gibi, `ziyaret` veritabanındaki `ziyaretcidefteri` ilişkisinde bir SQL sorgulaması yapılmaktadır. Kullanıcı tarafından ziyaretçinin sıra numarası, `ID`, bir metin kutusuna girilmekte ve bu değer sorgulamaya parametre olarak gönderilmektedir. Buna göre,

a) `kullaniciGoster();` fonksiyonunun tanımlamasında bir `AJAX` nesnesi kullanılarak veritabanına istek gönderilip, elde edilen sonuç yine `AJAX` nesnesi yardımıyla ekrana yazdırılacaktır. İlgili fonksiyonun tanımlamasını `GET` veya `POST` metodunu kullanarak yapınız (`prototype.js` kütüphanesine bağlı olarak tanımlama yapabilirsiniz). Ayrıca `AJAX` yaklaşımı kullanılmasının avantajları neler olabilir? Kısaca açıklayınız.

b) Verilen SQL sorgulama ifadesi bir problem oluşturabilir mi? Başka ifadeyle programda bir kod açığı var mıdır? Eğer varsa kodda ne gibi düzenleme yapılması gerekir? Kısaca açıklayınız.

veritabani.php

```
…
$ad = $_REQUEST['ad']; $il = $_REQUEST['il']; $eposta = $_REQUEST['eposta']; $gorus  = $_REQUEST['gorus'];
$sorgu = "INSERT INTO Ziyaretcidefteri (ad,il,eposta,gorus) VALUES ('$ad', '$il', '$eposta', '$gorus')";
mysql_query($sorgu);
…
```

S.2) Yukarıda verilen kod parçasında parametrelerle gönderilen ziyaretçi bilgileri veritabanına kaydedilmektedir. Buna göre,

a) İlgili programda istenmeyen bir duruma yol açabilecek bir kod açığı olabilir mi? Eğer varsa nasıl giderilebilir? Kısaca açıklayınız.

b) Kullanıcı tarafından girdisi yapılan `il` ve `elektronik posta` verilerine, örneğin sadece Türkiye'deki 81 ilin adlarının girilmesine izin verilmesi gibi bazı kısıtlamalar getirilmesi düşünülse nasıl bir yöntem önerirsiniz? Gerekli gördüğünüz yerlerde program kod parçalarını da yazarak kısaca açıklayınız.

S.3) Bir web tabanlı uygulamada yönetici panelinde oturum (session) işlemlerine niye gereksinim duyulabilir? Oturumu başlatma/kapatma işlemleri yerine, benzer adımları gerçekleştirmek için çerez (cookie) yaklaşımı kullanılması ne gibi sakıncalar ortaya çıkarabilir? Gerekli gördüğünüz yerlerde program kod parçalarını da yazarak kısaca açıklayınız.

S.4) Web sitesi tasarımında sayfaların içerikleri kadar görünümleri de önemlidir. Web sayfasının başlık, menü, içerik gibi bölümlere ayrılması işlemi için HTML çerçeveleri (frames) ve/veya tabloları kullanılabilir. Fakat daha profesyonelce hazırlanmış sitelerde CSS teknolojisi tercih edilmektedir. Nedenini kısaca açıklayınız. Ayrıca CSS teknolojisi kullanılarak bir web sayfası şablonunun (template) nasıl hazırlanabileceğini örnek kod parçalarıyla anlatınız.

```
<html> <head> <script language="javascript">
                    var dur, sayac = 0, im = new Array();
                    for(i=0; i<3; i++) im[i] = new Image, im[i] = i + ".jpg";
                    function baslat() { if(sayac == 2) sayac = 0;
                           else ++sayac;  document.imge.src = im[sayac];
                           dur = setTimeout("baslat()", 360);   }
                    function durdur() { clearTimeout(dur); document.imge.src = im[0];  }
             </script> </head>
       <body> <div>  <img src = "0.jpg" name = "imge" /> <form>
                           <input type = "button" value = "baslat" onclick = "baslat();"/>
                           <input type = "button" value = "durdur" onclick = "durdur();"/> </form>
             </div> </body> </html>
```

S.5) Yukarıda verilen kod parçasıyla yapılan işlevi kısaca açıklayınız. Programı göze çarpmayan (unobtrusive) `javascript` betik dili yaklaşımıyla yeniden düzenleyiniz. Benzer işlevi yerine getirebilecek bir programın PHP betik diliyle gerçekleştirilmesi durumunda avantajların ve dezavantajların neler olabileceğini kısaca açıklayınız.

KARADENİZ TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
Bilgisayar Mühendisliği Bölümü
20010-2011 Eğitim-Öğretim Bahar Yarıyılı
Web Programlama Final Sınavı Soruları

1. a) Fonksiyon `get/post` metoduna göre aşağıdaki gibi tanımlanabilir:

```
function kullaniciGoster(str)
{
	var url = "veritabani.php";
	url = url+"?q="+str;
	url = url+"&sid="+Math.random();

	new Ajax.Request(url,
		{
			method:"get",
			onSuccess:durumOgren
		}
	);

}

function kullaniciGoster(str)
{
	var url = "veritabani.php";

	new Ajax.Request(url,
		{
			method:"post",
			parameters:{q:str, sid:Math.random()},
			onSuccess:durumOgren
		}
	);

}

function durumOgren(ajax)
{
	$("metin").innerHTML = ajax.responseText;
}
```

AJAX nesnesiyle web sunucundan dosyalar alınıp getirilebilir. Bu işlem eşzamansız olarak yapılabilir. Alınıp getirilen dosyanın içeriği geçerli web sayfasına DOM kullanılarak aktarılabilir. Sonuçta web sayfası sayfa tekrar yüklenmeden dinamik olarak güncellenmiş olur.

b) SQL sızıntısı olabilir. Örneğin aşağıdaki ifade ile q parametresiyle gönderilen değer sorgulamada hiçbir anlam ifade etmemektedir.

```
//$q = $q.'OR '1'='1
```

Bu durumda kodda aşağıdaki gibi bir düzenleme yapılabilir.

```
$q = mysql_real_escape_string($_REQUEST["q"]);
```

2. a) HTML sızıntısı olabilir. Bu durumda kodda aşağıdaki gibi bir düzenleme yapılabilir.

```
$ad     = htmlspecialchars($_REQUEST['ad']);
$il     = htmlspecialchars($_REQUEST['il']);
$eposta = htmlspecialchars($_REQUEST['eposta']);
$gorus  = htmlspecialchars($_REQUEST['gorus']);
```

b) İl için bir liste kutusundan seçim yaptırılabilir. E-posta girdisi ise düzenli ifadeyle kontrol ettirilebilir:

```
function dogrulaEposta($deger)
{

  return (!preg_match('/^[_a-z0-9-]+(\.[_a-z0-9-]+)*@[a-z0-9-]+(\.[a-z0-9-]+)*(\.[a-z]{2,3})$/', $deger))
? 0 : 1;
}
```

3. Oturum açma/kapama işlemlerine güvenli veri işlemi açısından gereksinim duyulur. Çerez istemcide saklanan bir veridir, oturum verisi ise sunucuda saklanır. Bu yüzden daha güvenlidir. Oturum açma işlemi için aşağıda bazı kod parçaları verilmiştir:

```
$sorgu = "SELECT kullaniciadi, sifre FROM yonetici WHERE kullaniciadi =
'" . mysql_real_escape_string($_POST['kullaniciadi']) . "' AND sifre = (password('" .
mysql_real_escape_string($_POST['sifre']) .
"'));";
$sonuc = mysql_query($sorgu) or die(mysql_error());

if (mysql_num_rows($sonuc) == 1)
{
```

```
        $_SESSION['yon_otur_ac'] = $_POST['kullaniciadi'];
        $_SESSION['yon_sifre'] = $_POST['sifre'];
}
```

4. CSS Teknolojisi kullanılarak tasarlanan web sayfaları daha hızlı yüklenir. Şablon örnekleri için derste verilen kodlara bakınız.

5. Animasyonla ilgili bir uygulama yazılmıştır. Kod aşağıdaki gibi yeniden düzenlenebilir:

ornek.js

```
function $(id) {
        return document.getElementById(id);
}

var dur, sayac = 0, im = new Array();

for(i=0;i<3;i++) im[i] = new Image, im[i] = i + ".jpg";

function baslat() {
        if(sayac == 2) sayac = 0;
        else ++sayac;
        document.imge.src = im[sayac];
        dur = setTimeout("baslat()",360);
}

function durdur(){
        clearTimeout(dur);
        document.imge.src = im[0];
}

window.onload = function() {
        $("1").onclick = baslat;
        $("2").onclick = durdur;

};
```

ornek.html

```
<html>
        <head>
                 <script src="ornek.js" type="text/javascript">
                </script>
        </head>
        <body>
                <div>
                        <img src="0.jpg" name="imge" />
                        <form>
                                <input type="button" value="baslat" id = "1"/>
                                <input type="button" value="durdur" id = "2"/>
                        </form>
                </div>
        </body>
</html>
```

Programın PHP betik dilinde yazılması; güvenlik, internet tarayıcılarıyla uyumluluk ve daha etkin olma açısından tercih edilebilir. Hız açısından ise bir dezavantaj sağlayabilir. Çünkü programı koşarken sunucuyla bağlantı kurulması gerekmektedir.