TÜBİTAK

Web Uygulamaları Sızma Testi Eğitimi

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Sunum İçeriği

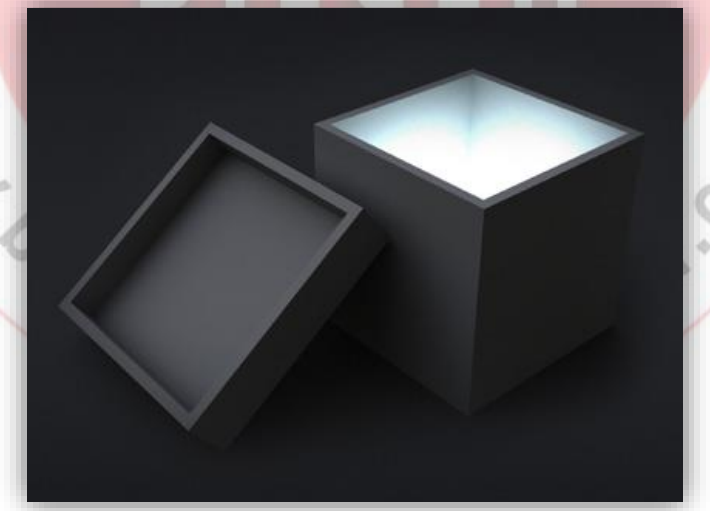
- Giriş
- Web Teknolojileri Standartları
- Bilgi Toplama ve Ayar Yönetimi
- Girdi/Çıktı Alanı Tespiti ve Manipülasyonları
- Kimlik Denetimi
- Yetkilendirme
- Oturum Yönetimi
- İş Mantığı Hataları

Giriş

Giriş

Web Pentest Türleri

- Black Box
- White Box
- Gray Box



Giriş

Tarama Türleri

Manuel

Otomatik

- Ücretsiz Araçlar
- Ticari araçlar

Hibrid

Zaafiyet Tarama Araçları

- Ticari olanlar:
  - Acunetix
  - Netsparker
  - Burp Suite Pro
- Ücretsiz olanlar:
  - ZAP
  - WebScarab

Giriş

Test Süreci(Test Metodolojisi)

Recon. → Mapping → Discovery → Exploit → Reporting

Giriş

Saldırı yüzeyleri

- **Sunucu**
  - Yanlış yapılandırma
  - DOS
- **Uygulama**
  - Login Sistemi
  - Oturum Yönetim Sist.
  - Fonsiyonel Bozukluklar
- **Kullanıcı**
  - Sosyal Mühendislik

Giriş

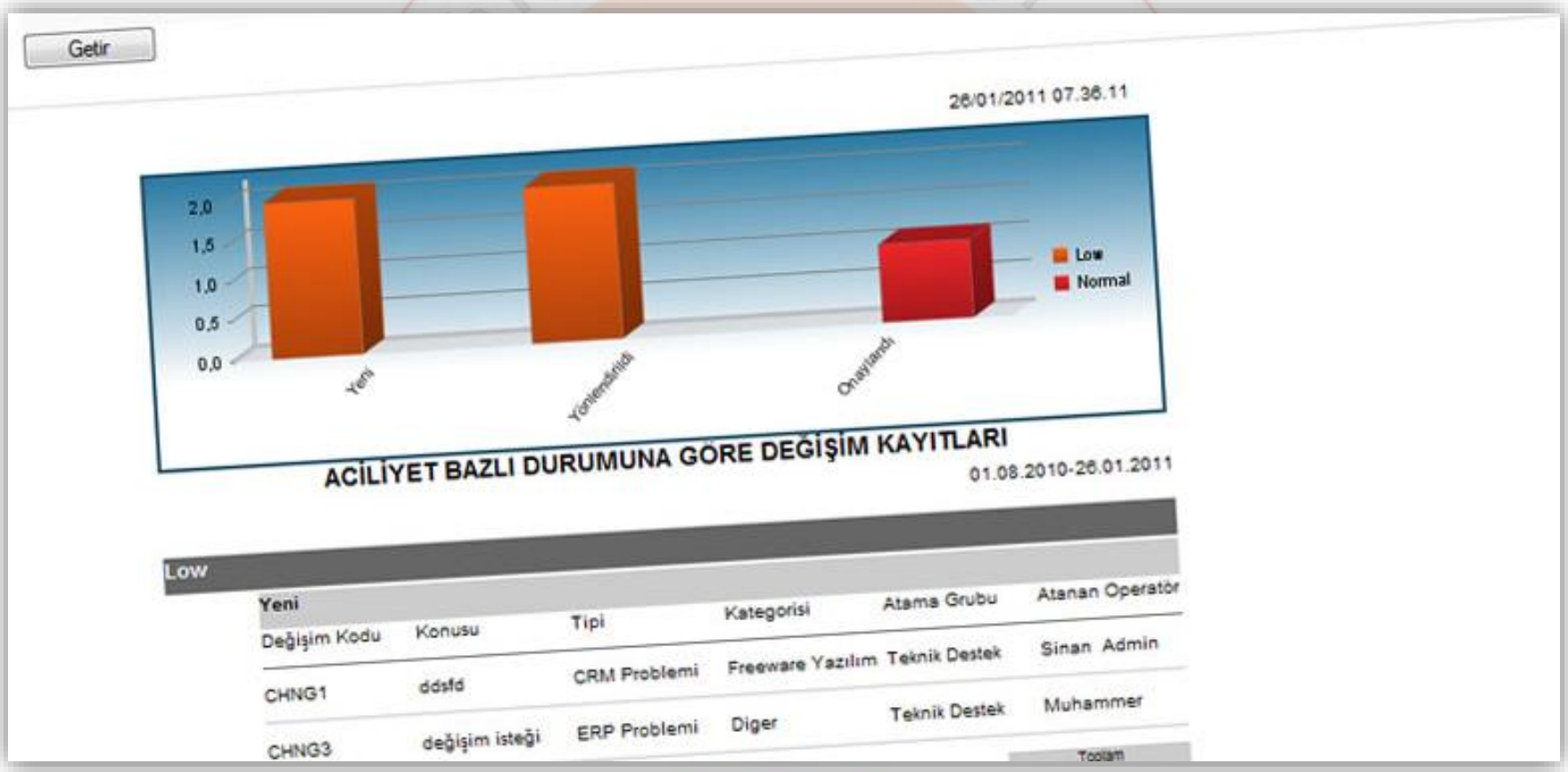
Açıklık Taslakları

- OWASP
- CWE
- SGE Testing Checklist

Giriş

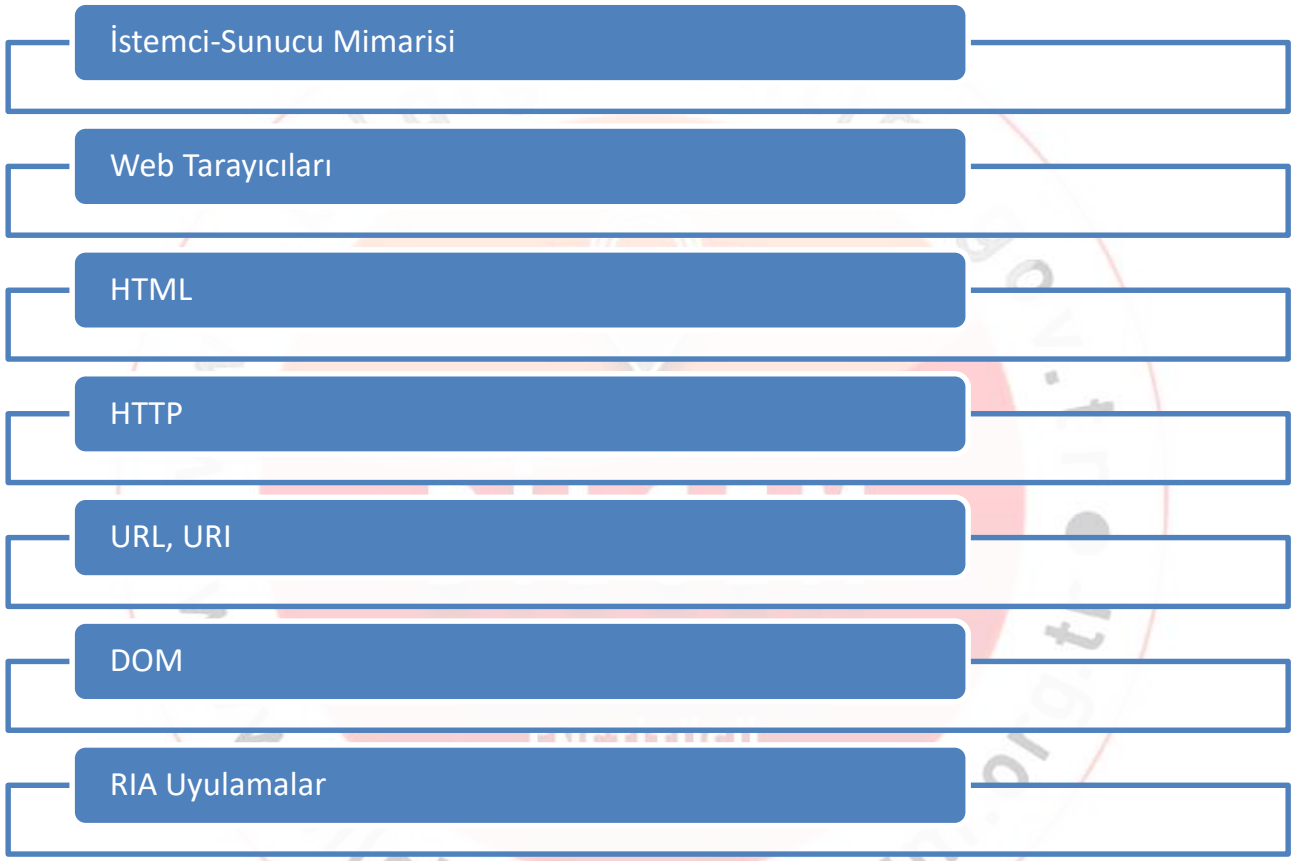
Raporlama

- Bir önceki sunumda hazırlanan taslaklardan raporlama yapılır.

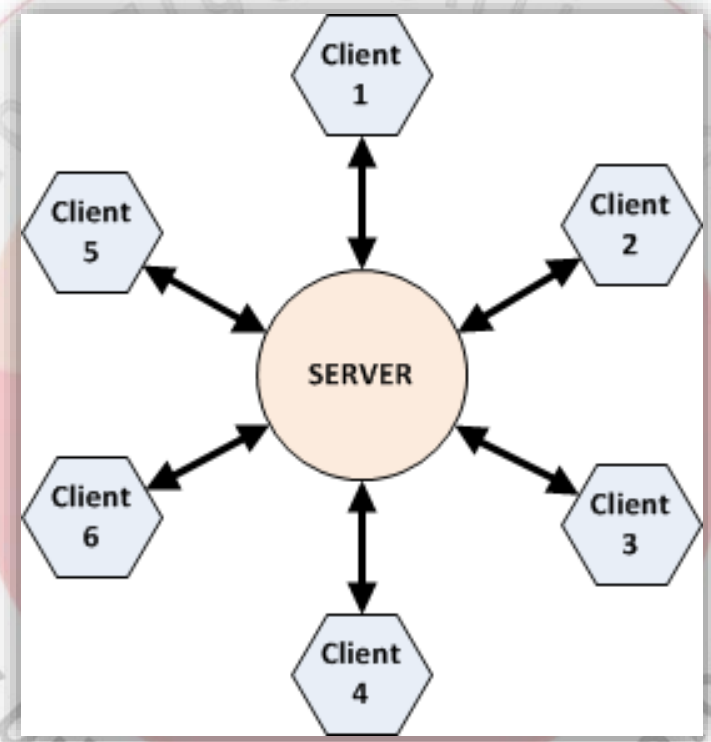


Teknolojiler - Standartlar

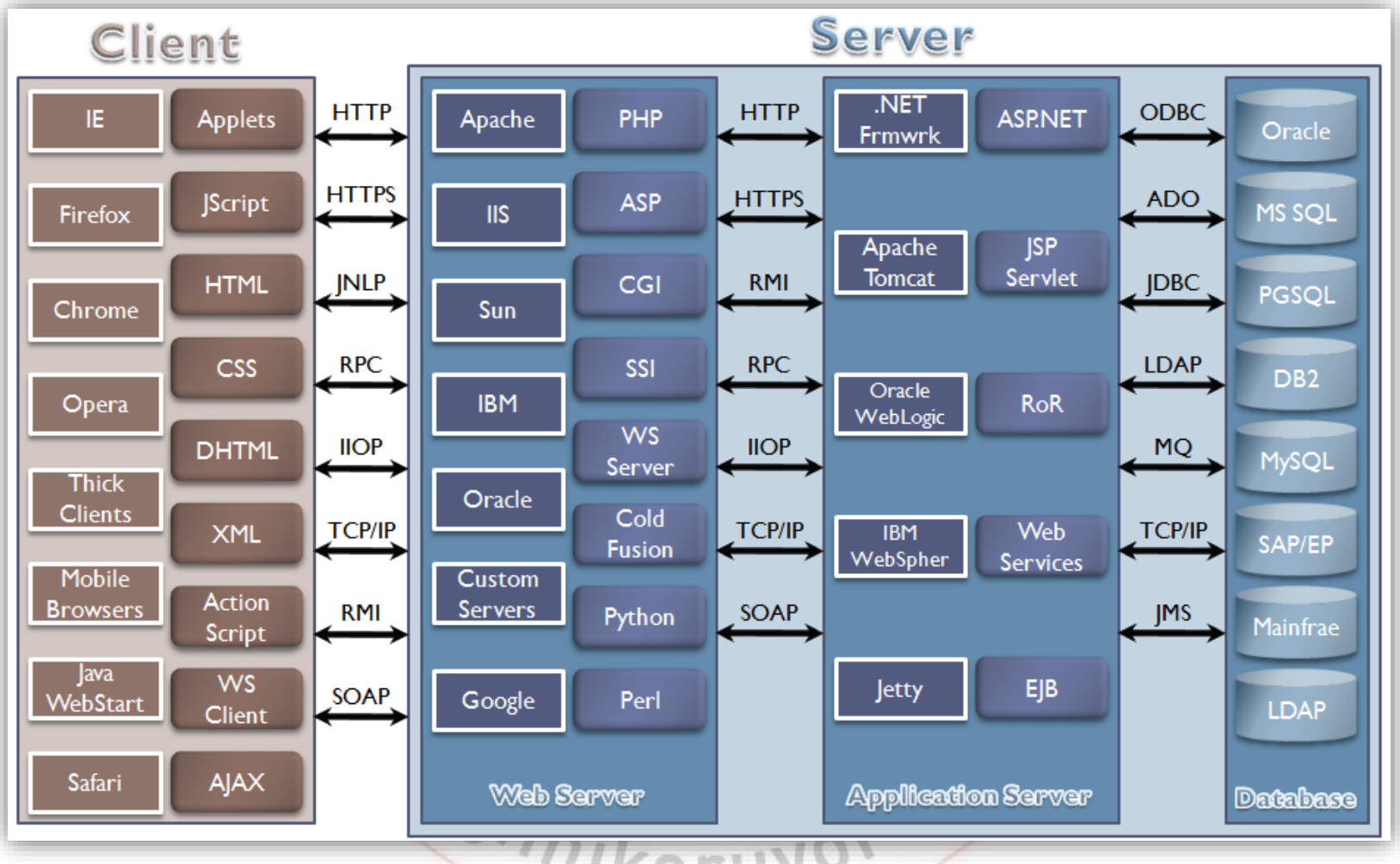
Teknolojiler - Standartlar



İstemci-Sunucu Mimarisi



İstemci – Sunucu Mimarisi



Web tarayıcıları

Chrome	• Firebug
IE	• Debugbar
Firefox	•Firebug •Cookie Manager •HttpFox
Safari	
Opera	
Yandex Browser	

HTML Nedir?

- **H**yper **T**ext **M**arkup **L**anguage
- Bir HTML dökümanına web sayfası denir.
- Bir HTML dökümanı HTML etiketlerinden oluşur.
- Her HTML etiketin bir anlamı vardır.

HTML Dökümanları Nasıl Tarayıcıda Görünür?

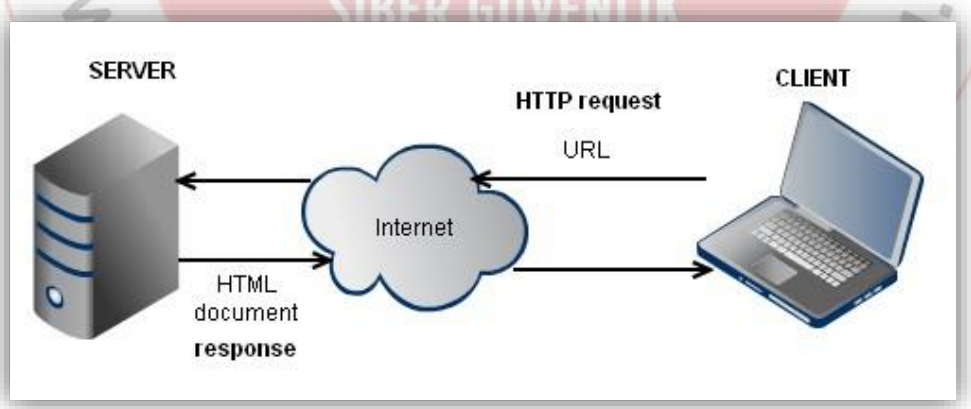
- Tarayıcılar HTML etiketlerini göstermezler. Bu etiketleri yorumlayarak uygun içeriği gösterirler.
- HTML elements, tags, attributes

- ...
- <img>...</img>
- <h1>...</h1>
- ...
- ...
- <head>...</head>
- <title>...</title>

```
<img width="600" height="411" style="margin: 5px; float: left; width: 600px;
height: 411px" title="ulasim.gif" alt="ulasim.gif" src="images/stories
/ulasim.gif">
```

HTML Sayfaları Nasıl Taşınır?

- HTML dökümanları(web sayfaları) HTTP ile İstemci-Sunucu arasında taşınır.
- İstemci bir web sayfasını Sunucudan ister, Sunucu da bu sayfayı istemciye(web taryıcısına) HTML dökümanı olarak gönderir.



HTTP

Nedir?

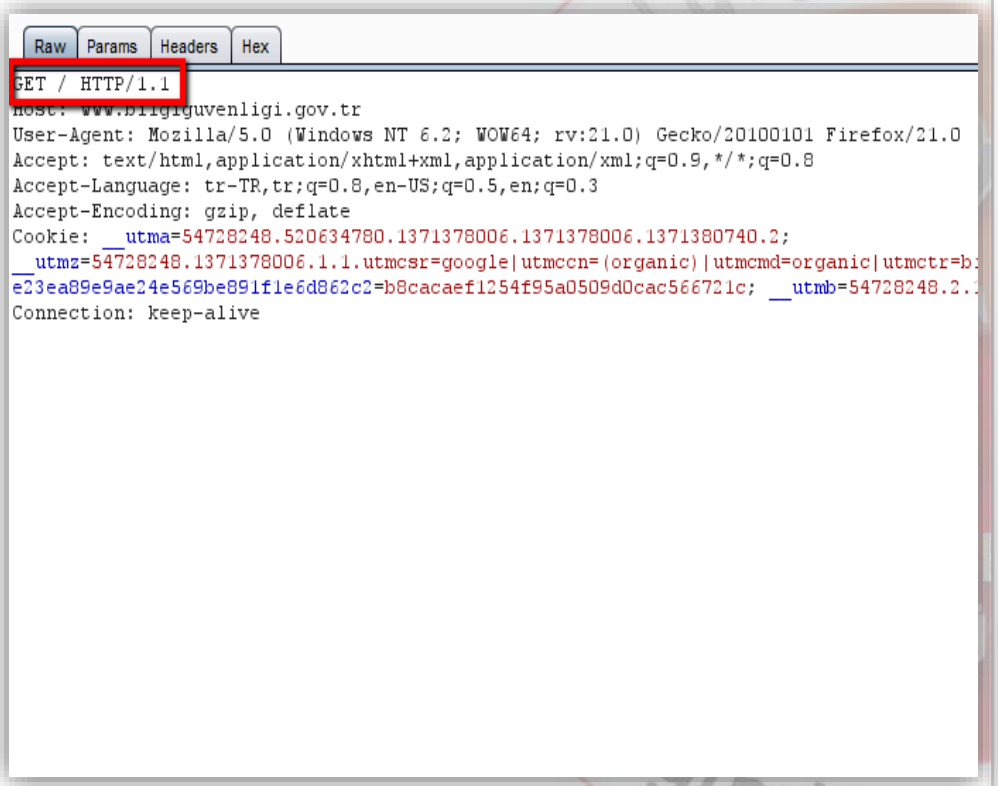
- **H**yper **T**ext **T**ransfer **P**rotocol
- HTTP, Sunucu ve İstemci arasında verilerin taşınmasını sağlayan bir protokoldür.
- Burada veriden kasıt; HTML sayfaları, resimler, videolar gibi sunucu ve istemci arasında taşınabilcek herşeydir.

Request Header	Value
(Request-Line)	GET / HTTP/1.1
Host	www.bilgiguvenligi.gov.tr
User-Agent	Mozilla/5.0 (Windows NT 6.2; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding	gzip, deflate
Cookie	__utma=54728248.520634780.1371378006.1371378006.1371380740.2; __utmz=54
Connection	keep-alive

Response Header	Value
(Status-Line)	HTTP/1.0 200 OK
Date	Sun, 16 Jun 2013 11:06:05 GMT
Server	Apache/2.2.0 (Fedora) mod_perl/2.0.4 Perl/v5.8.8
Set-Cookie	e23ea89e9ae24e569be891f1e6d862c2=b8cacaef1254f95a0509d0cac566721c; path=/
Expires	Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified	Sun, 16 Jun 2013 11:06:05 GMT
Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma	no-cache
Vary	Accept-Encoding
Content-Encoding	gzip
Content-Length	13919
Connection	close
Content-Type	text/html; charset=iso-8859-9

HTTP Başlıkları

- HTTP Başlıkları taleplerde ve cevaplarda dönen mesajların parçalarıdır.
- Bir HTTP talebinin veya cevabının nasıl yorumlanacağını belirlerler.
- IETF tarafından RFC içnde bir standart haline getirilmiştir.



HTTP Metodları

- HTTP metotları sunucu ile istemci arasında iletilen veriler üzerinde işlem yapılmasını sağlar.
- HTTP Metodları
  - GET
  - POST
  - PUT
  - DELETE
  - TRACE
  - OPTIONS
  - PATCH

TÜBİTAK

HTTP İsteği(Request)

- Sunucuya GET metodu ile iletilen bir istek.

```
GET /kilavuz-dokumanlar/index.php HTTP/1.1
Host: www.bilgiguvenligi.gov.tr
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.bilgiguvenligi.gov.tr/
Cookie: __utma=54728248.520634780.1371378006.1371380740.1371385998.3;
__utmz=54728248.1371378006.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=bilgiguvenligi.gov.tr;
e23ea89e9ae24e569be891f1e6d862c2=-; __utmb=54728248.1.10.1371385998; __utmc=54728248
Connection: keep-alive
```

TÜBİTAK

HTTP İsteği(Request) ...

- Sunucuya POST metodu ile iletilen bir istek.

```
POST /index.php?option=com_comprofiler&task=login HTTP/1.1
Host: www.bilgiguvenligi.gov.tr
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.bilgiguvenligi.gov.tr/
Cookie: __utma=54728248.520634780.1371378006.1371380740.1371385998.3;
__utmz=54728248.1371378006.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=bilgiguvenligi.gov.tr;
e23ea89e9ae24e569be891f1e6d862c2=07ec1e8735f54413e93834c35b91984d;
__utmb=54728248.4.10.1371385998;
__utmc=54728248
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 183

username=KULLANICI&passwd=S%DDFRE&op2=login&lang=turkish&force_session=1&
return=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2F&message=0&
jc7d3114441a56b7268c2c494b8da1f10=1&Submit=Giri%FE
```

HTTP Cevabı(Response)

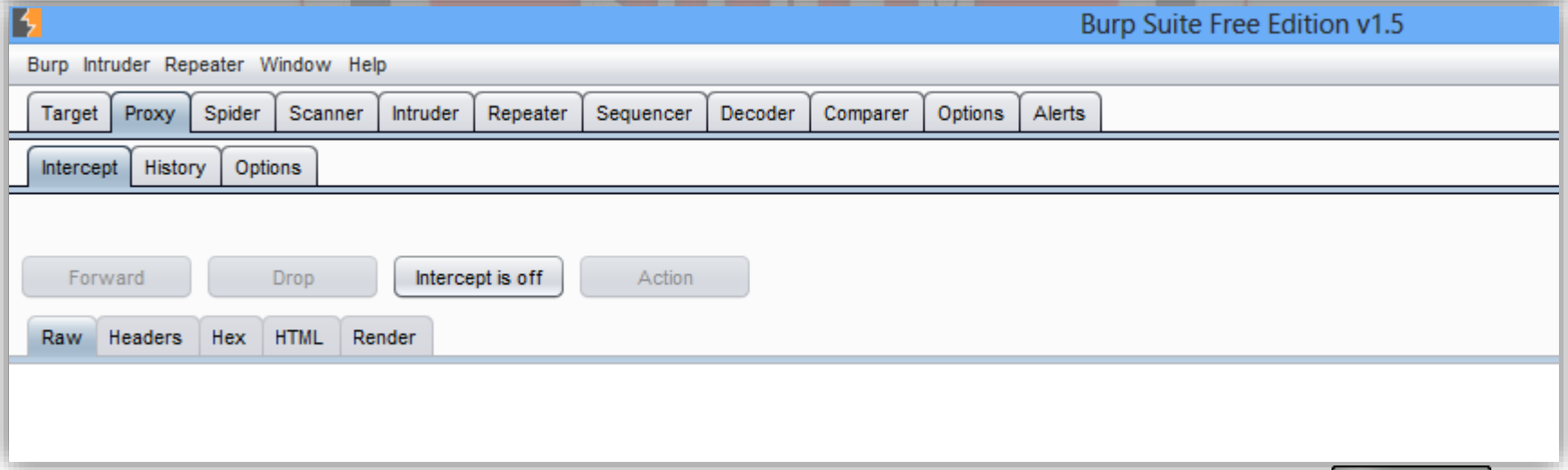
- Sunucudan gelen bir cevap ve içindeki HTML etiketleri.

```
HTTP/1.0 200 OK
Date: Sun, 16 Jun 2013 13:06:48 GMT
Server: Apache/2.2.0 (Fedora) mod_perl/2.0.4 Perl/v5.8.8
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Sun, 16 Jun 2013 13:06:48 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 76691
Connection: close
Content-Type: text/html; charset=iso-8859-9

<?xml version="1.0" encoding="iso-8859-9"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional/
<html xmlns="http://www.w3.org/1999/xhtml">
<head>

<title>Anasayfa - Ulusal Bilgi Güvenliği Kapısı</title>
<meta name="description" content="Ulusal Bilgi Güvenliği Kapısı" />
<meta name="keywords" content="Ulusal Bilgi Güvenliği Kapısı, bilgi, güvenlik, TUBİTAK, UEKAE" />
<meta name="robots" content="index, follow" />
<base href="https://www.bilgiguvenligi.gov.tr/" />
        <link rel="shortcut icon" href="https://www.bilgiguvenligi.gov.tr/images/favicon.ico" />
        <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-9" />
<link href="https://www.bilgiguvenligi.gov.tr/templates/ubgp_template/css/template_css.css"

rel="stylesheet" type="text/css" />
<link rel="shortcut icon" href="https://www.bilgiguvenligi.gov.tr/images/favicon.ico" />
<link rel="alternate" type="application/rss+xml" href="http://www.bilgiguvenligi.gov.tr/index.php?opt

<script language=javascript>
  var min = 10;
  var max = 50;
```

TÜBİTAK

HTTP Bağlantılarında Araya Girme

- Web uygulamaları çalışırken sunucu ve istemci arasında HTTP ile sağlanan bağlantının arasına girilebilir.
- Bu iş için Local Proxy programları yada tarayıcı eklentileri kullanılılır.
- Bu eğitimde Burp Suite Free uygulaması kullanılacak.



SSL/TSL

Nedir?

- SSL ve TSL sunucu ve istemci arasında HTTP üzerinde aktarılan verilerin şifrelenerek iletilmesini sağlayan bir protokoldür.
- Web uygulamalarında güvenli bağlantı için yaygın olarak SSL / TLS kullanılır.
- Bir HTTP bağlantısının güvenliği SSL ile sağlanınca artık bağlantı **HTTPS** olarak adlandırılacaktır.
- Test süreci içinde detaylı değinilecektir.

URL

Nedir?

- **U**niform **R**esource **L**ocator
- Genel anlamda internet ortamında, dar anlamda ise sunucuda olan bir kaynağın konumunu belirten ve karakterlerden oluşan ifadedir.
- Web uygulamaları için adresleme standartıdır.

URI-UDI

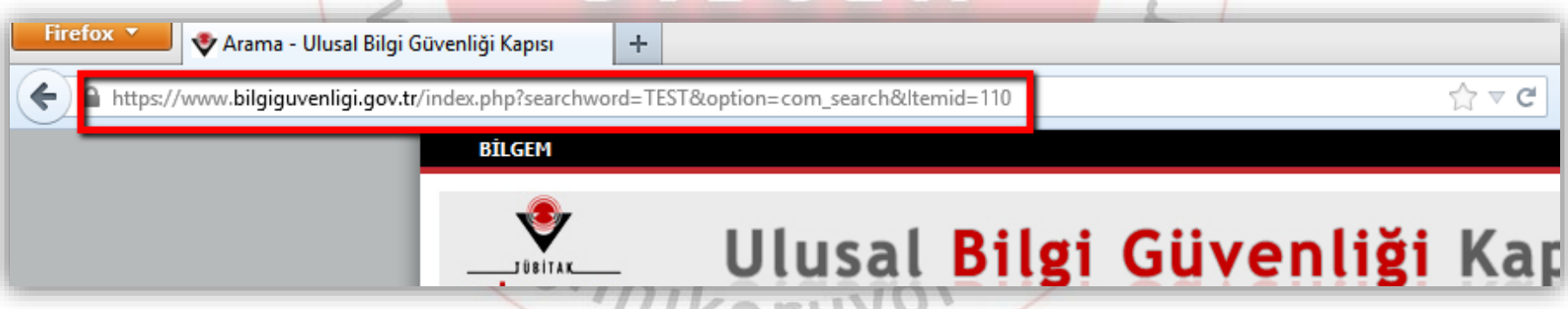
- **U**niform **R**esource **I**dentifier
- **U**niversal **D**ocument **I**dentifier
- Her ikisi de URL için temel oluşturmuş isimlendirmelerdir.

URL

scheme://host:port/path?parameter=value#fragment

http://www.bilguvenlig.gov.tr:80/arama.aspx?kelime=TEST#bookmark=2

scheme	http, https, telnet, ftp…
host:port	mail.google.com:80, www.turkiye.gov.tr
path	/, /index.html, /home/default.aspx
?parameter=value	?param1=val1&param2=val2…
#fragment	#anchor



Nerdeyiz?

- *Giriş*
- *Web Teknolojileri Standartları*
- Bilgi Toplama ve Ayar Yönetimi
- Girdi/Çıktı Alanı Tespiti ve Manipülasyonları
- Kimlik Denetimi
- Yetkilendirme
- Oturum Yönetimi
- İş mantığı Hataları

TÜBİTAK

TEST SÜRECİ

Test Süreci

Bilgi Toplama ve Ayar Yönetimi

TÜBİTAK

HTTP BAŞLIKLARINI İNCELEME

- Server ve Teknoloji Bilgisi
- Oturum Bilgisi
- Url Bilgisi
- HTTP Metod Bilgisi

PORT VE SERVİS BİLGİSİ

SSL/TSL BİLGİSİ

- Versiyonları
- Algoritmaları

UYGULAMA DİZİN YAPISI

YÖNETİCİ ARAYÜZÜ ERİŞİMİ

MİNİMUM BİLGİ PRENSİBİ AYKIRI DURUMLAR

- Yardım ve Hata Sayfaları
- Unutuluş HTML Açıklama Satırları
- E-mail ve Kullanıcı Toplama

YEDEKLENMİŞ VE UNUTULMUŞ DOSYALAR

BİLİNEN AÇIKLIKLAR

- Google Hacking
- ExploitDB

TÜBİTAK

HTTP Başlıkları İnceleme

- Request başlığı

```
GET /dvwa/index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/dvwa/login.php
Cookie: security=high; PHPSESSID=dpfe4vtedoinidskp2nl7mmni0
Connection: keep-alive
```

```
POST /dvwa/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/dvwa/login.php
Cookie: security=high; PHPSESSID=dpfe4vtedoinidskp2nl7mmni0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=admin&password=password&Login=Login
```

HTTP Başlıkları İnceleme

- Response başlığı.

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
X-Powered-By: PHP/5.4.7
Set-Cookie: PHPSESSID=95uf9s4n12a85abo56f6m86n50; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Set-Cookie: security=high
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Bilgi Toplama ve Ayar Yönetimi

HTTP Başlıkları İnceleme

- Nikto ile yapılan bir tarama.

```
samurai@webtest-VirtualBox:~$ nikto -host http://www.[redacted].com
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:
+ Target Port:        80
+ Start Time:         2013-06-18 15:12:14
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-aspnet-version header: 2.0.50727
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Server banner has changed from Microsoft-IIS/7.5 to Microsoft-HTTPAPI/2.0, this may suggest a WAF or load balancer is in place
```

Bilgi Toplama ve Ayar Yönetimi

SSL Denetimi

- SSL'in ve TSL'in versiyonları düşük olmamalı.
- SSL de en az versiyon 3.0, TSL de ise en az versiyon 1.0 olmalı.
- SSL ve TSL algoritalrı güçlü olmalı.
- Bu sertifikalar geçerli otoritelerden alınmalı.

HTTPS Denetimi

- Uygulama hassas veri iletiyorsa bağlantı güvenliğinin sağlanması gerekir.
- Kullanıcı giriş bilgileri, bankacılık bilgileri vb önemlibilgiler HTTPS gibi doğru yapılandırılmış güvenli bağlantılarla iletilmelidir.

Bilgi Toplama ve Ayar Yönetimi

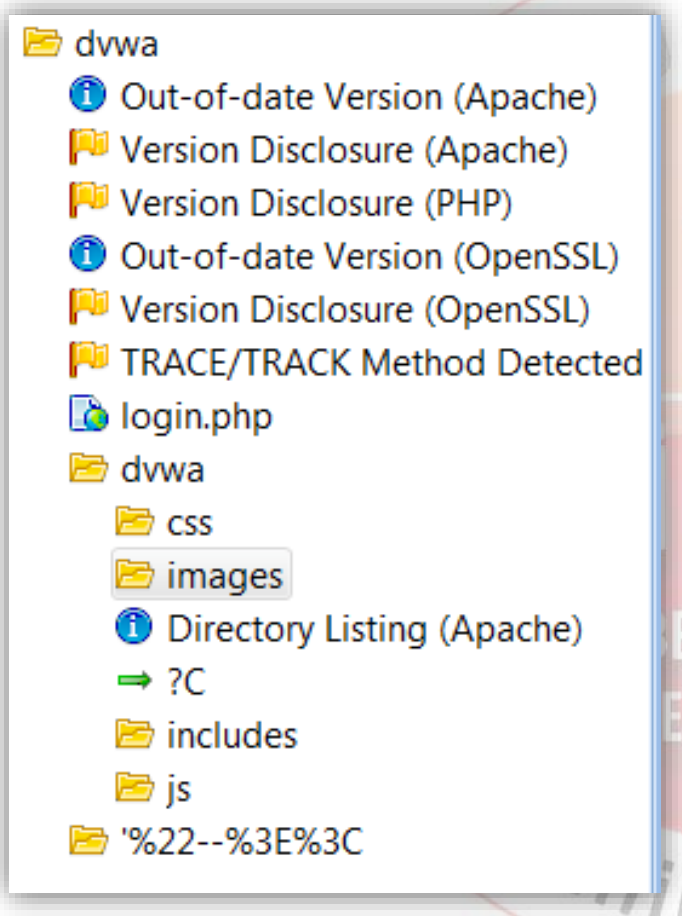
```
root@bt:~# sslscan 193.140.74.7:443
                    _
 ___ ___| |___ ___ __ _ _ __
/ __/ __| / __|/ __/ _` | '_ \
\__ \__ \ \__ \ (_| (_| | | | |
|___/___/_|___/\___\__,_|_| |_|

                Version 1.8.2
        http://www.titania.co.uk
     Copyright Ian Ventura-Whiting 2009

Testing SSL server 193.140.74.7 on port 443

  Supported Server Cipher(s):
    Rejected  SSLv2  168 bits  DES-CBC3-MD5
    Rejected  SSLv2  56 bits   DES-CBC-MD5
    Rejected  SSLv2  40 bits   EXP-RC2-CBC-MD5
    Rejected  SSLv2  128 bits  RC2-CBC-MD5
    Rejected  SSLv2  40 bits   EXP-RC4-MD5
    Rejected  SSLv2  128 bits  RC4-MD5
    Rejected  SSLv3  256 bits  ADH-AES256-SHA
    Accepted  SSLv3  256 bits  DHE-RSA-AES256-SHA
    Rejected  SSLv3  256 bits  DHE-DSS-AES256-SHA
    Accepted  SSLv3  256 bits  AES256-SHA
    Rejected  SSLv3  128 bits  ADH-AES128-SHA
    Accepted  SSLv3  128 bits  DHE-RSA-AES128-SHA
    Rejected  SSLv3  128 bits  DHE-DSS-AES128-SHA
    Accepted  SSLv3  128 bits  AES128-SHA
    Rejected  SSLv3  168 bits  ADH-DES-CBC3-SHA
    Rejected  SSLv3  56 bits   ADH-DES-CBC-SHA
```

SSL Kontrolü

- Sslscan

```
  Prefered Server Cipher(s):
    SSLv3  256 bits  DHE-RSA-AES256-SHA
    TLSv1  256 bits  DHE-RSA-AES256-SHA

  SSL Certificate:
    Version: 2
    Serial Number: 108636830896463
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /C=TR/L=Gebze - Kocaeli/O=T\xC3\xBCrkiye Bilimsel ve Teknolojik Ara\xC5\x9Ft\xC4\xB
xC3\xBCs\xC3\xBC - UEKAE/OU=Kamu Sertifikasyon Merkezi/CN=Cihaz Sertifikas\xC4\xB1 Hizmet Sa\xC
    Not valid before: Jan 20 14:30:26 2012 GMT
    Not valid after: Jan 19 14:30:26 2015 GMT
    Subject: /C=TR/ST=Kocaeli/L=Kocaeli/O=TUBITAK BILGEM-UEKAE/OU=BSG/CN=*.bilgiguvenligi.gov.t
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
      Modulus (2048 bit):
          00:b6:77:3e:a2:b0:0d:41:08:fb:84:db:40:5b:b7:
          b0:da:b3:1e:ce:66:85:28:0b:92:6c:a5:89:66:18:
          fd:d7:da:09:73:44:ea:d3:67:1f:df:7a:9d:7a:78:
          e8:6e:64:3e:54:43:37:01:fa:9d:85:08:e7:ae:fb:
          1c:e3:8e:54:40:95:36:4f:28:24:7f:65:a7:a0:2a:
          ab:72:cf:50:29:a0:55:c3:7c:bd:03:19:11:03:4c:
          a6:7d:a2:96:2d:c8:d2:c9:36:52:26:b2:75:ba:af:
          0e:31:80:0f:f7:05:e5:52:9c:71:d3:62:cc:86:b5:
          cd:e7:4a:ee:e4:54:e8:18:b2:37:87:ce:cd:f1:b4:
```

Bilgi Toplama ve Ayar Yönetimi



Uygulama Dizin Yapısı

- Uygulamanın dizin yapısının çıkarılması gerekir.
- Böylece hassas verilerin saklanabileceği dizinler bulunur.
- Yönetici arayüzüne erişilir.
- Daha odaklı manipülasyonlar yapılır.
- Dizin yapısı otomatize araçlar sayesinde çıkartılır.
  - Netsparker
  - Accunetix
  - Burp …

Bilgi Toplama ve Ayar Yönetimi

TÜBİTAK

- Yönetici Arayüzüne Erişim
- Yedeklenmiş veya Unutulmuş Dosyalar
- Servis ve Port Bilgileri

Minimum Bilgi Prensibi

Bilgi ?

- HTTP Başlıkları
- Hata sayfaları ve hata kodları
- Unutulmuş açıklama satırları
- Kullanıcı uyarı mesajları
- E-posta adresleri
- Sosyal ağlar
- Arama motorları
- …

Bilgi Toplama ve Ayar Yönetimi

Bilinen Açıklıklar

- Güvenlikçiler veya hackerlar tarafından bazı teknolojilerde veya uygulamalarda tespit edilmiş açıklıklar internette yayınlanmış olabilir.
- Uygulama sunucusunun, teknolojisinin ve diğer eklentilerinin bilinmesi burada işe yarar.

Google Hacking

- Google ve diğer arama motorlarının ileri arama teknikleri kullanılarak hassas veriler, kullanıcı bilgileri, açık yönetici arayüzleri gibi önemli bulgular elde edilebilir.
- GİAT(Google İleri Arama Teknikleri-Google Advanced Search Techniques)

TÜBİTAK

Google Hacking

- Google Hacking, Google'ın ileri arama teknikleri ve diğer servisleri kullanılarak yapılan bilgi toplama ve açıklık bulma işlemidir.
- Google Hacking Database(GHDB), google kullanılarak uygulamalarda ve teknolojilerde tespit edilmiş açıklıkların depolandığı veritabanıdır.
- Google' da hedef uygulama veya teknoloji için böyle bir arama yapmak meşakkatli olacağından, bu aramaları yapan ve veritabanındaki açıklıkları deneyen otomatize araçlar kullanılır.
  - Google Hacking Toolbar
  - SearchDiggty
  - Founstone GHDB
  - …

TÜBİTAK

Google Hacking

- İleri Arama Teknikleri
  - intext
  - allintext
  - intitle
  - allintittle
  - link
  - cache
  - site
  - related
  - info
  - inurl
  - allinurl
  - author
  - id
  - inanchor
  - location
  - movie
  - filetype
  - phonebook
  - insubject

GİRDİ-ÇIKTI DENETİMİ

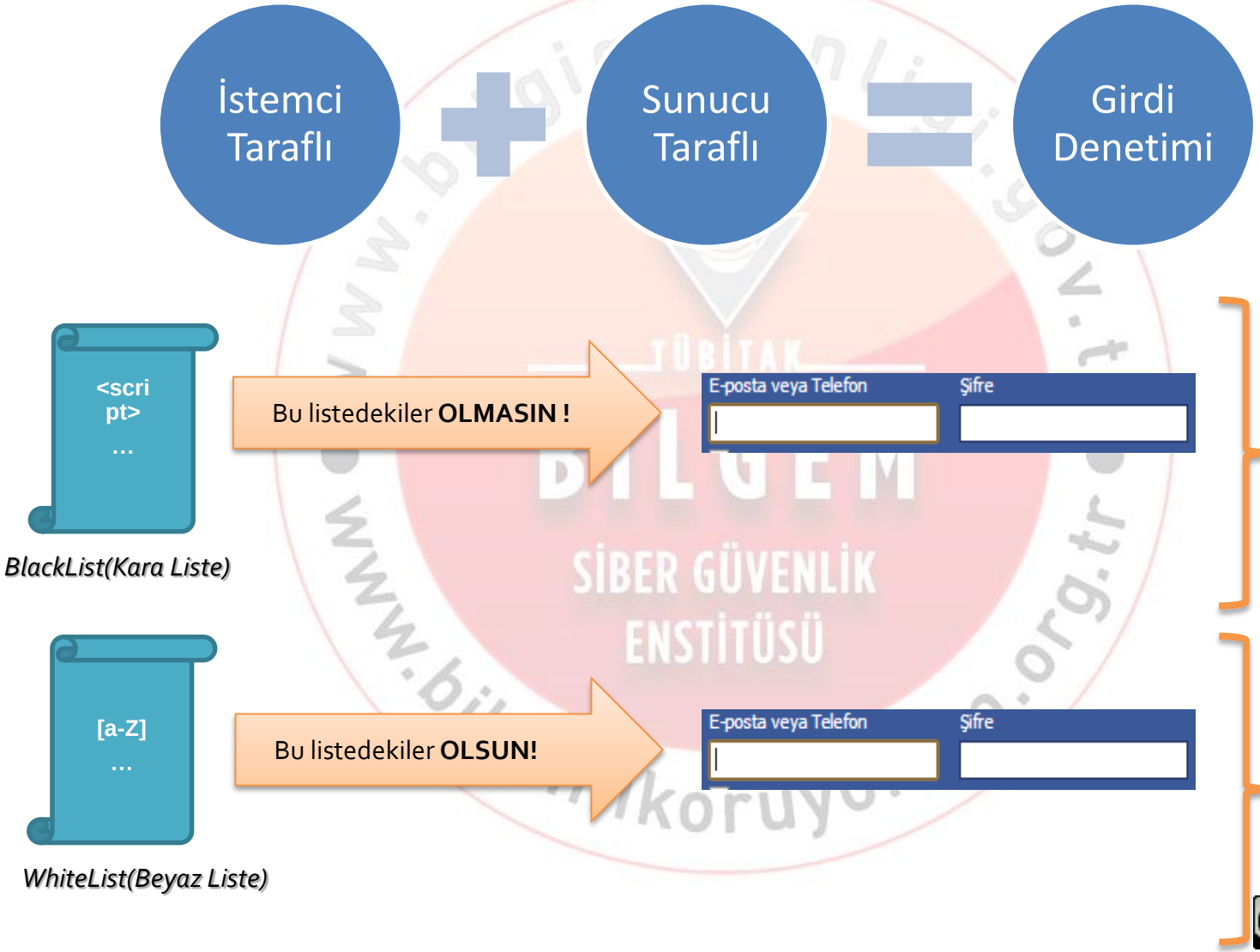
Girdi-Çıktı Denetimi

TÜBİTAK

Girdi ve Çıktı Alanlarının Belirlenmesi

- Web uygulamlarında genelde karşılaşılan problem; veri ile zararlı kodun birbirine karışmasıdır.
- Yeterli denetimlerin yapılmadığı bir uygulamada girdi alanları hackerlar tarafından kötü niyetle kullanılabilir.
- Testlerde yeterli denetim olduğunu anlayabilmek için girdi alanlarının tespiti gerekir.
- Girdi alanlarını sadece birşeyler yazacağımız text kutuları olarak görmek hatalıdır. HTTP bağlantılarında sunucu ve istemci arasında taşınan veya taşınmayan herşeyi girdi alanı olarak görmemiz gerekir.

Girdi - Çıktı Denetimi



Girdi-Çıktı Denetimi

Çıktı Denetimi

- Web uygulamalarında, sadece girdi alanları değil çıktı alanları da problem oluşturabilirler.
- Bazı durumlarda uygulama koduna karıştırılan zararlı kodlar çıktı olarak istemciye gönderilebilir. Böyle bir durumda istemci dolaylı olarak bu zafiyetten etkilenir.

Encoding/Decoding

- Çıktı alanlarında zararlı kodların çalışmasını engellemek amacıyla uygulanması gereken bir yöntemdir.
  - HTML Encode
  - URL Encode
  - JS Encode

Girdi-Çıktı Denetimi

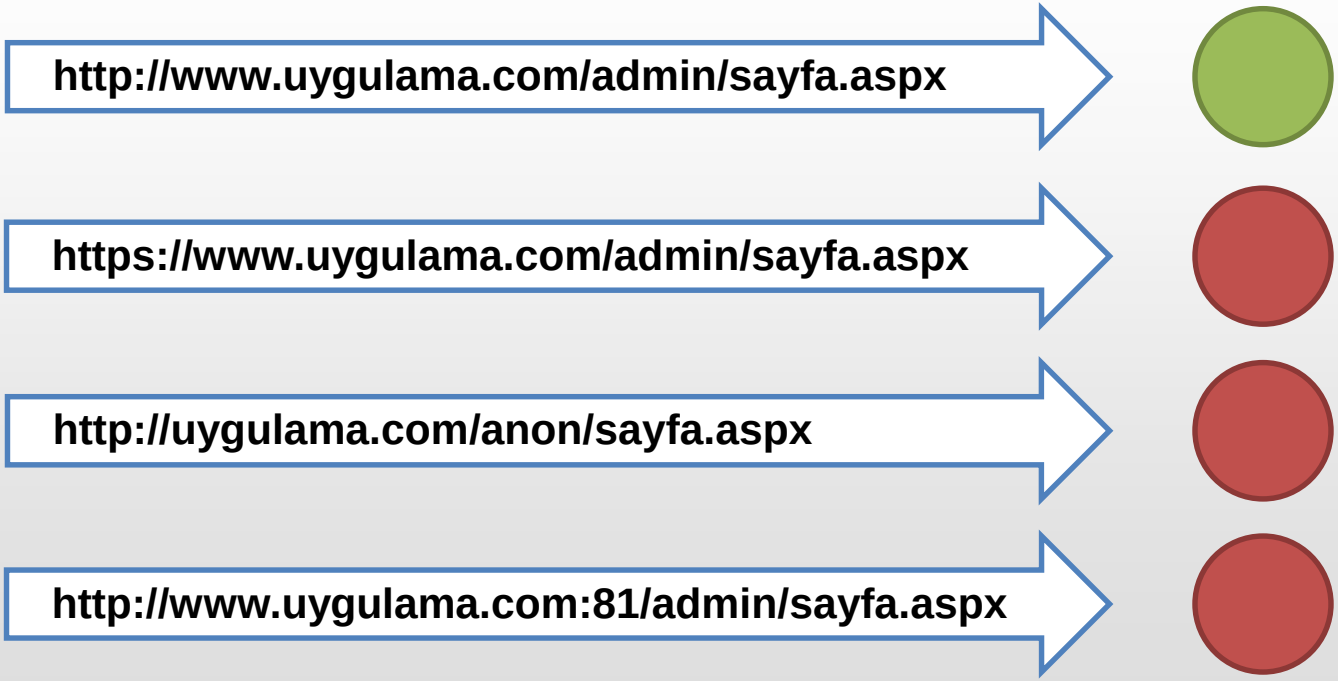
SOP(Same Origin Policy)

- Aynı Kaynak Politikası
- SOP, bir web uygulamasını, sayfasını oluşturan kaynakların veya uygulamanın kendisinin, başka uygulamalar tarafından kullanım kurallarını belirleyen bir standarttır.
- SOP, bu kontrolü sağlamak için;

Girdi-Çıktı Denetimi

SOP Kuralları

http://www.uygulama.com:80/anon/zararli.js



Girdi-Çıktı Denetimi

JavaScript

- Başlangıçta statik HTML sayfalarını görsel anlamda zenginleştirmek için kullanıldı.
- İlerleyen zamanlarda Sunucu ve İstemci arasındaki veri trafiğini azaltmak için kullanıldı.
- Günümüzde ise artık masaüstü programlarda bile kullanılacak kadar dinamik bir yapı kazandı.
- Bu durum; kullanıcı bilgisayarlarında, web tarayıcılarında, web uygulamalarında veya sayfalarında JavaScript kodlarının izinsiz kullanılmasının da önünü açmış oldu.

Girdi-Çıktı Denetimi

JavaScript Sayfa İçinde Nasıl Kullanılır?

Dışarıdan dosya ile

```
...
<script type="text/javascript" src="js_code.js"/>
...
<script type="text/javascript">
    alert("Sayfa yükleniyor.");
</script>
...
<p onclick="alert('Tıkladın!');">Tıkla!</p>
...
```

Sayfa içi

Olay işleyici

Girdi-Çıktı Denetimi

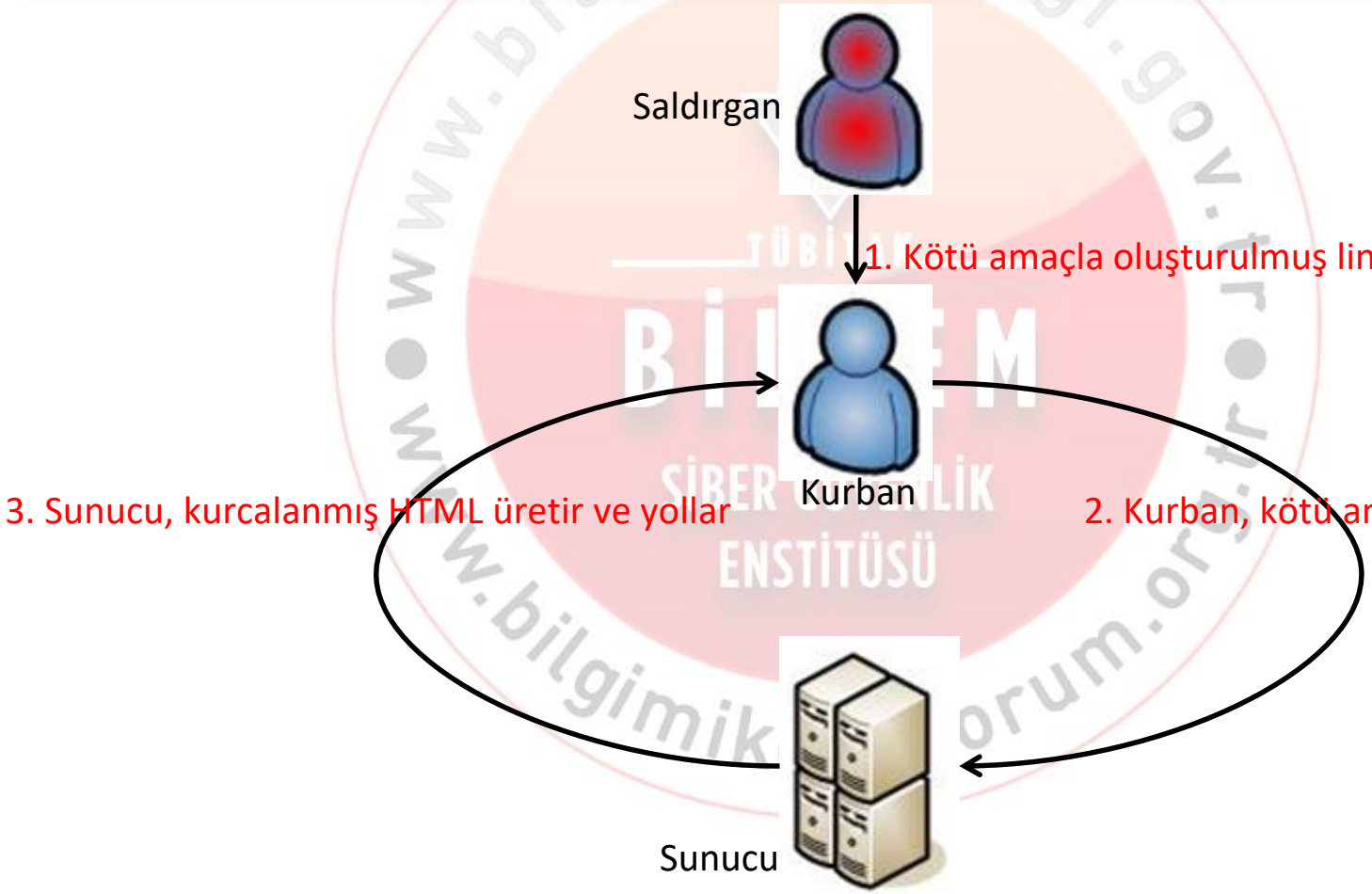
XSS(CSS-Cross Site Scripting)

- Web uygulamasını barındıran sunucuda veya istemcide Javascript gibi dillerin kodlarının izinsiz çalıştırılmasıdır.

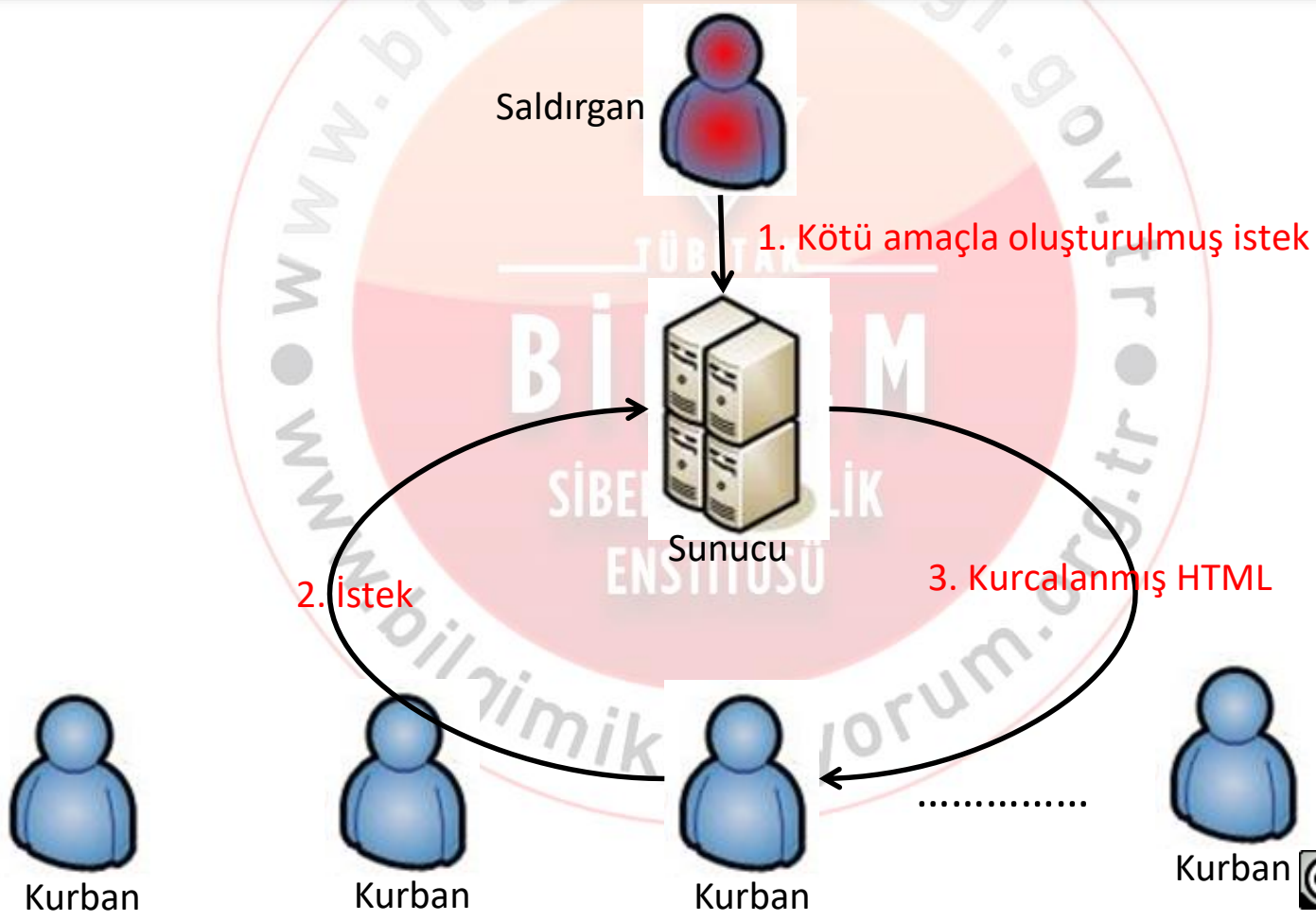
XSS Türleri

- Reflected(Yansıtılan) XSS
- Stored(Persistent-Depolanmış) XSS
- DOM XSS

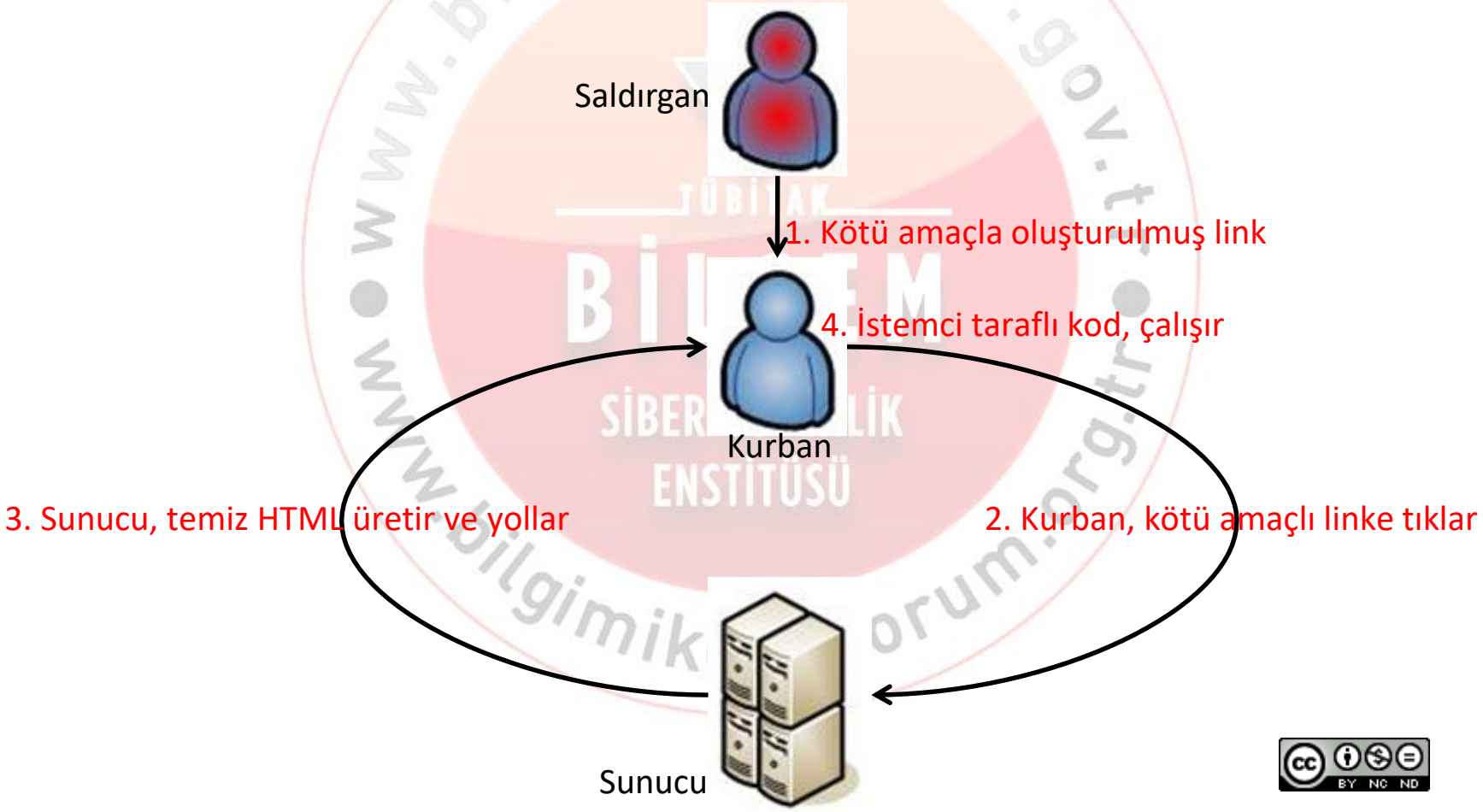
Reflected XSS



Stored XSS



DOM XSS


Saldırgan
1. Kötü amaçla oluşturulmuş link
4. İstemci taraflı kod, çalışır
Kurban
3. Sunucu, temiz HTML üretir ve yollar
2. Kurban, kötü amaçlı linke tıklar
Sunucu

Girdi-Çıktı Denetimi

SQL(Structured Query Language)

- Veritabanı üzerinde işlem yapılmasını sağlayan bir veri işleme dilidir.
- ANSI tarafından standart haline getirilmiştir.
- Daha sonra bazı firmalarca kendilerine has verisyonları çıkartılmıştır.
  - MSSQL(Transact-SQL)
  - MySQL
  - Oracle(Procedural Language- SQL)
  - …
- Temel SQL komutları
  - SELECT
  - UPDATE
  - DELETE
  - INSERT

Girdi-Çıktı Denetimi

SQL Injection(SQL Enjeksiyonu)

- Uygulamadan alınan parametrelerin doğrudan veritabanı sunucusuna gönderilmesi sonucu veritabanı üzerinde izinsiz sorgular çalıştırılabilir.
- Uygulama seviyesinde yeterli girdi denetimi yapılmadığında veya Veritabanı sunucusunda gelen sorguların denetimi yapılmadığında SQL-i gerçekleştirilebilir.

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

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

TÜBİTAK

SQL Injection

Dinamik bir SQL sorgusu

```
$sQuery = 'SELECT * FROM users WHERE id=' + $id;
```

Normal bir değişken değeri

```
$sQuery = 'SELECT * FROM users WHERE id=100';
```

Anormal bir değişken değeri: SQL Enjeksiyonu

```
$sQuery = 'SELECT * FROM users WHERE id=100 OR 1=1';
```

Girdi-Çıktı Denetimi

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

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

Ürün Detayı
Laptop
(Orijinal Yanıt)

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

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

Hata Sayfası

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

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

Ürün Detayı
Laptop
(Orijinal Yanıt – **5 sn gecikmeli**)

Parametrize Sorgular

```
string commandText = "SELECT * FROM Customers "+ "WHERE
Country=@CountryName";
SqlCommand cmd = new SqlCommand(commandText, conn);
cmd.Parameters.Add("@CountryName",countryName);
```

```
string sql = string.Format("SELECT TOP {0} * FROM
Products", numResults);
```

KİMLİK DOĞRULAMA

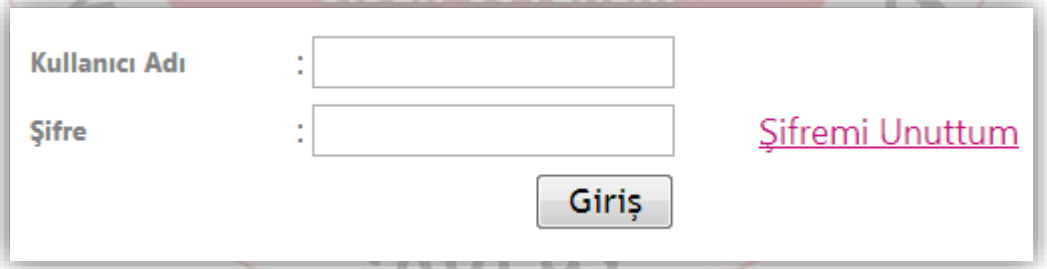
Kimlik Doğrulama

- Kullanılan kimlik doğrulama türü
- Şifre politikası
- Giriş-Çıkış işlevi
- Kimlik doğrulamanın atlatılabilmesi
- Brute Force(Kaba Kuvvet Saldırısı)
- Dictionary Atack(Sözlük Saldırısı)
- CAPTCHA Kullanımı

Kimlik Doğrulama

Kimlik Doğrulama

- Bir uygulamada Sunucunun kaynaklarını doğru kişiye açtığını bilmesi, istemcinin de doğru kaynaktan veri aldığını bilmesi için sunucu ile istemci arasında kimlik doğrulama yapılabilir.
- Yetersiz kimlik doğrulama işlemi kullanıcı sahteciliği, hassas verilere 3. kişilerin ulaşması gibi sonuçlar ortaya çıkartır.



Kimlik Doğrulama

Basic	• Base64 Kodlama Kullanır. • Logout Fonksiyonu yoktur.
Digest	• Parol sunucu tafrafında açık tutulur. • Proxy ve güvenlik duvarları ile uyumlu değildir.
Integrated	• Sadece Windows sunucu ve sistemlerinde çalışır. • Parola sunucu tarafında açık tutulmaz • NTLM veya Kerberos • Proxy ve güvenlik duvarlarıyla uyumlu değildir.
Certificate Based	• İki taraflı kimlik doğrulama mimkündür. • Geçerli sertifikaya ihtiyaç vardır. • Sertifikanın korunması gerekir.
Form Based	• Proxy ve güvenlik duvarlarıyla uyumludur. • Çok kullanıcılı uygulamalarda tercih edilir.

Kimlik Denetimi

Şifre Politikaları

- Kurum Kullanıcı adı ve parola politikası öğrenilmeli.
- Uygulama teknolojilerinin ön tanımlı kullanıcı adları ve parolaları denenmeli.
- Yanlış yapılandırılmış HTTP başlıkları incelenmeli.
- Web sayfalarındaki gizli alanlara bakılmalı.

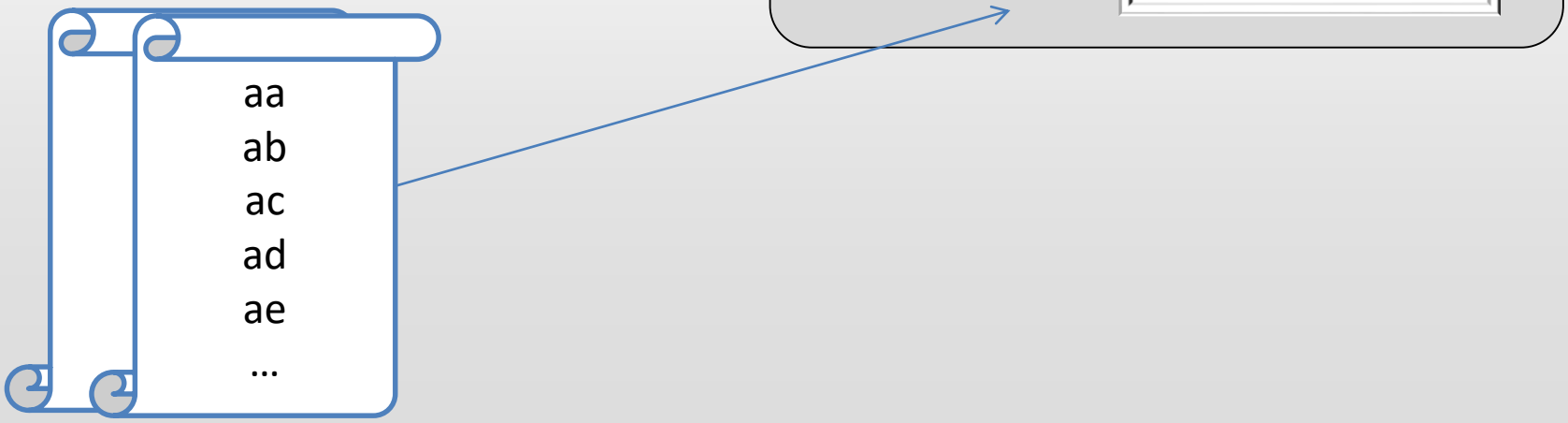
Giriş-Çıkış İşlevi

- Uygulamanın giriş-çıkış işlevlerinin çalışması incelenmeli.
- Uygulama tarayıcıda Cache'e izin verip vermediğine bakılmalı.

Kimlik Doğrulama

Brute Force Saldırsı(Kaba Kuvvet Saldırısı)

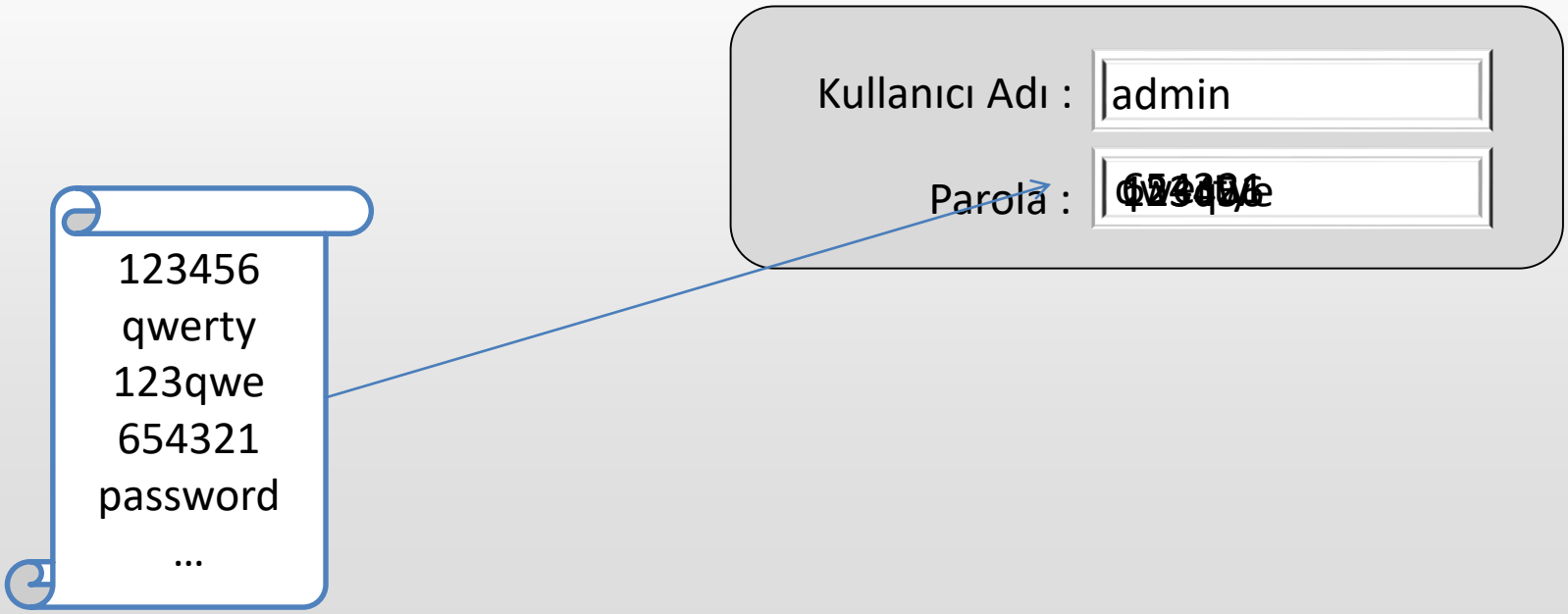
- Başlangıç karakteri
- Bitiş karakteri
- Karakter uzunluğu
- Karakter çeşitliliği



Kimlik Doğrulama

Dictionary Atack(Sözlük saldırısı)

- Daha önce oluşturulmuş bir listedeki tüm sözcüklerin denenmesi ile yapılır.



Kimlik Doğrulama

CAPTCHA Kullanımı

- **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part
- Kullanıcı girişi bulunan uygulamalarda CAPTCHA, kaba kuvvet ve sözlük saldırılarını engelleyebilir.
- CAPTCHA ile ilgili sorunlar;
  - Zayıf algoritmalar
  - Dar örnek uzay
  - Zayıf resimler
  - CAPTCHA tekrarlama

YETKİLENDİRME

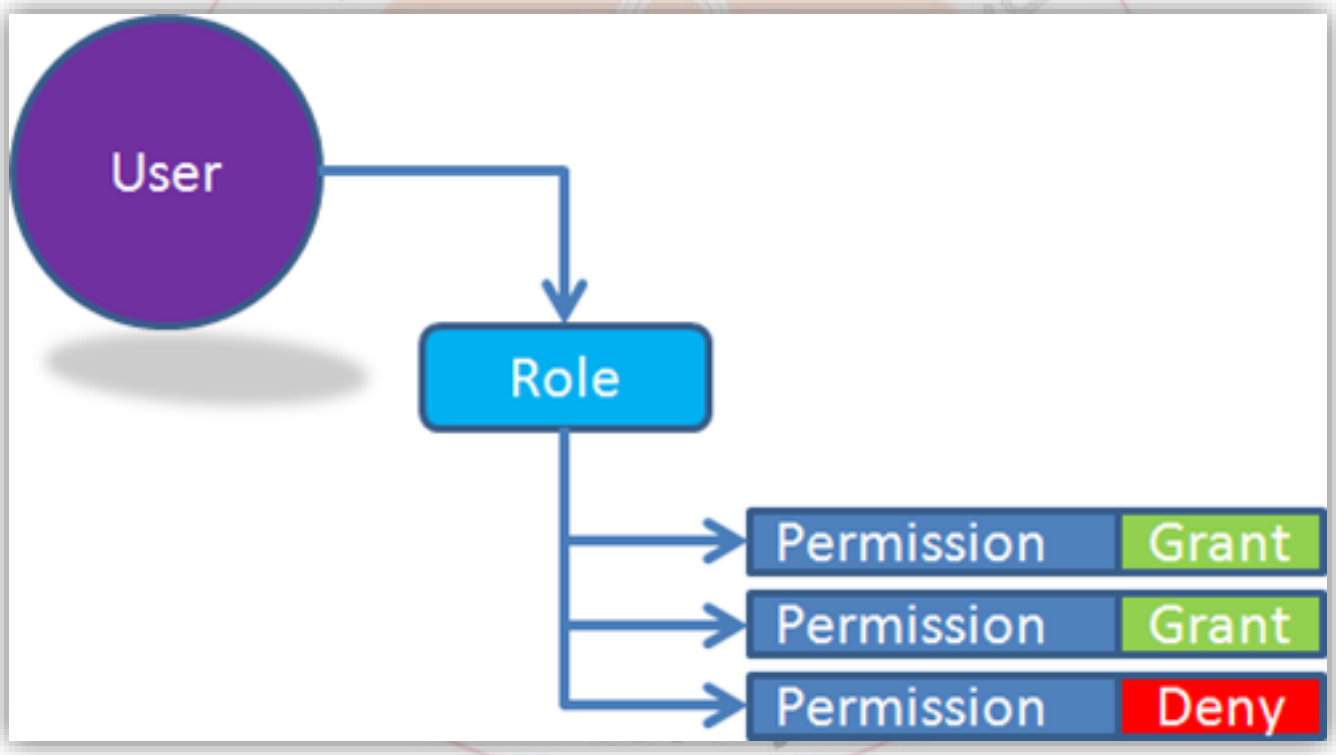
Yetkilendirme

- Yetkilendirme Çeşitleri
- Yetki Artırımı
- Yetki Dışı İşlem
- Dizin Gezinimi

Yetkilendirme

Yetkilendirme

- Kimliği doğrulanmış kullanıcıların uygulama üzerinde farklı hakları olabilir.

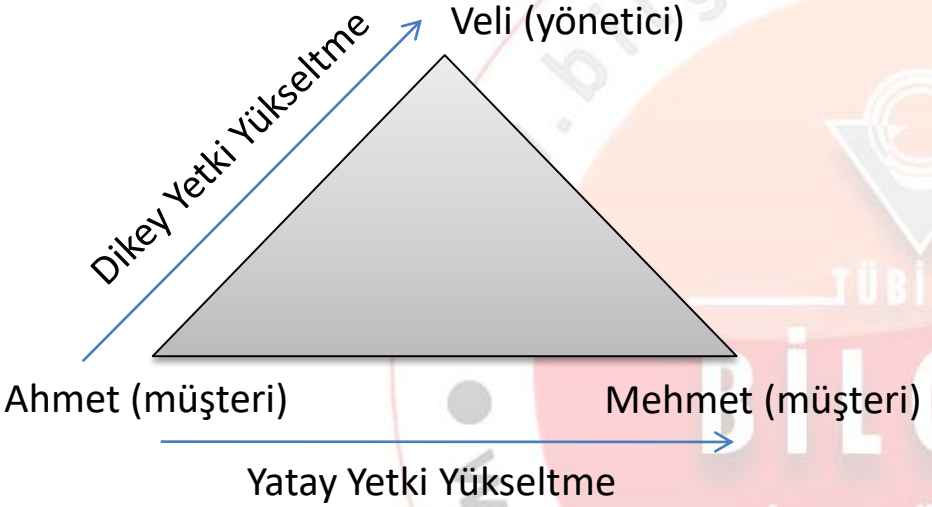


Yetkilendirme

Yetkilendirme Çeşitleri

- IP ve Sunucu ismi Tabanlı
- URL Tabanlı
- Uygulama Tabanlı
- Rol Tabanlı
- Kaynak Tabanlı
- İzin Tabanlı
- Hibrit

Yetkilendirme



Yetki Artırımı

- Kullanıcının kendi yetkisi dışına çıkması ve başka haklar elde etmesidir.
  - Dikey yetki artırımı
  - Yatay yetki artırımı

Yetkilendirme

Yatay ve Dikey Yetki Yükseltme

- Yatay Yetki Yükseltme

```
http://www.orneksite/makale/MakaleGoster.aspx?MakaleId=1003
```

- Dikey Yetki Yükseltme

```
<form method="POST">
action="http://site.com/mailing_list.pl">
    ...
    <input type="hidden" name="login_name" value="aUser">
    <input type="hidden" name="list"
value="FREQUENT_FLYER">
    ...
    <input type="hidden" name="list_admin" value="F">
    ...
</form>
```

Yetkilendirme

Yetki Dışı İşlem

- Uygulamanın bazı fonksiyonları çalıştırması için kullanıcıdan alınan parametreleri yetki kontrolüne tabi tutmadan işleme alması durumudur.

http://www.sirket.com.tr?action=**update**&id=1

http://www.sirket.com.tr?action=**delete**&id=1

Yetkilendirme

Path/Directory Traversal(Dizin Gezinimi)

- Dizin Gezinimi ile uygulamanın web sunucusu üzerinde çağırdığı kaynağın yolu değiştirilerek erişimi yasak olan başka kaynapın çağırılmasıdır.

Açıklık Barındıran Kod

```
<?php //vulnerable.php
$template='sayfa.php';
if (is_set($_COOKIE['TEMPLATE'])) $template=$_COOKIE['TEMPLATE'];
include ("/home/templates/".$template);
?>
```

Talep

```
GET /vulnerable.php HTTP/1.1
Cookie:TEMPLATE=../../../../../../../etc/passwd
```

Yanıt

```
HTTP/1.1 200 OK
Content-Type:text-html

foot:fi3sED95ibqR6:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp:
```

OTURUM YÖNETİMİ

Oturum Yönetimi

- İstemci taraflı kontroller
- Sunucu taraflı kontroller
- Oturum başlatma ve sonlandırma
- Oturum Sabitleme (Session Fixation)
- Siteler arası istek sahteciliği (CSRF)

Oturum Yönetimi

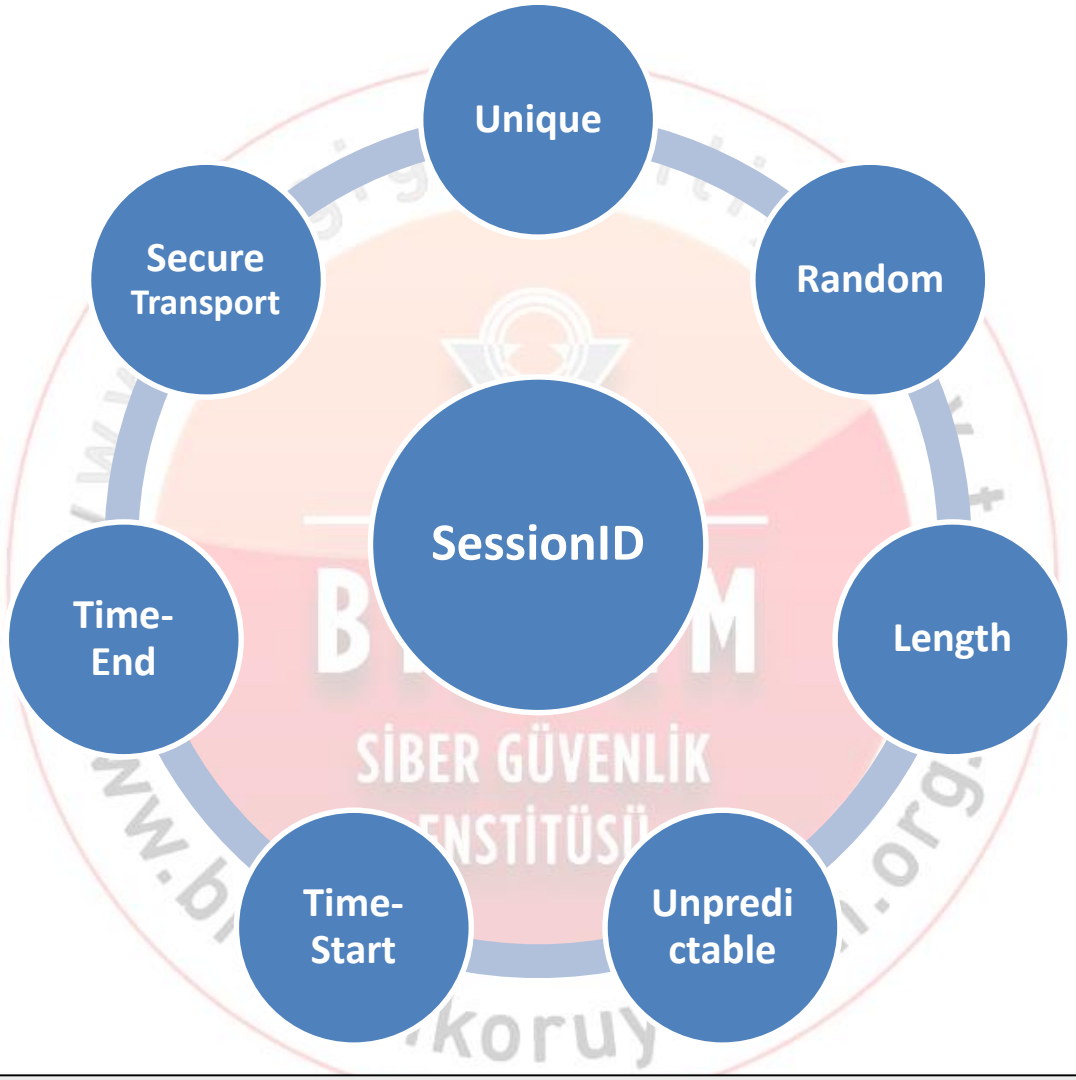
Oturum Yönetimi

- Web uygulamaları HTTP üzerinden haberleşirler. Fakat HTTP, istemcinin kimlik bilgisini doğruladıktan sonra istemcinin durum bilgisini(oturum bilgisini) tutmaz. Yani bir kullanıcıdan gelen iki isteğin aynı kullanıcıdan geldiğini anlayamaz.
- Bu nedenle istemcinin durum bilgisinin kontrol edilmesi için her istemciye özel bir değer sunucu veya geliştirici tarafından üretilir.(Session ID)

Oturum Yönetim Türleri

- URL taşınan oturum bilgisi
- Form gizli alanlarında taşınan outurum bilgisi
- Çerezlerde taşınan oturum bilgisi(en yaygın olanı)

Oturum Yönetimi



ASP.NET_SessionId=5gura4554gaayp55gca4qp45;

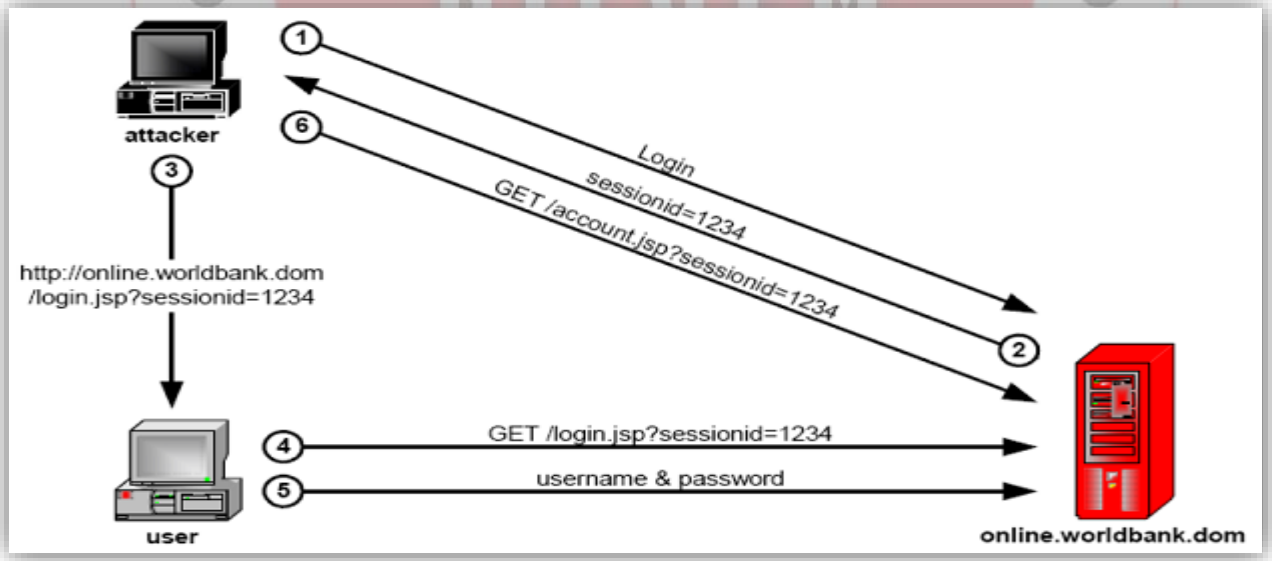
Oturum Yönetimi

1. Gizli alanlar
2. HTTP Başlıkları
3. URL bilgisi
4. Çerezlerin içeriği
5. SessionID özellikleri

Oturum Yönetimi

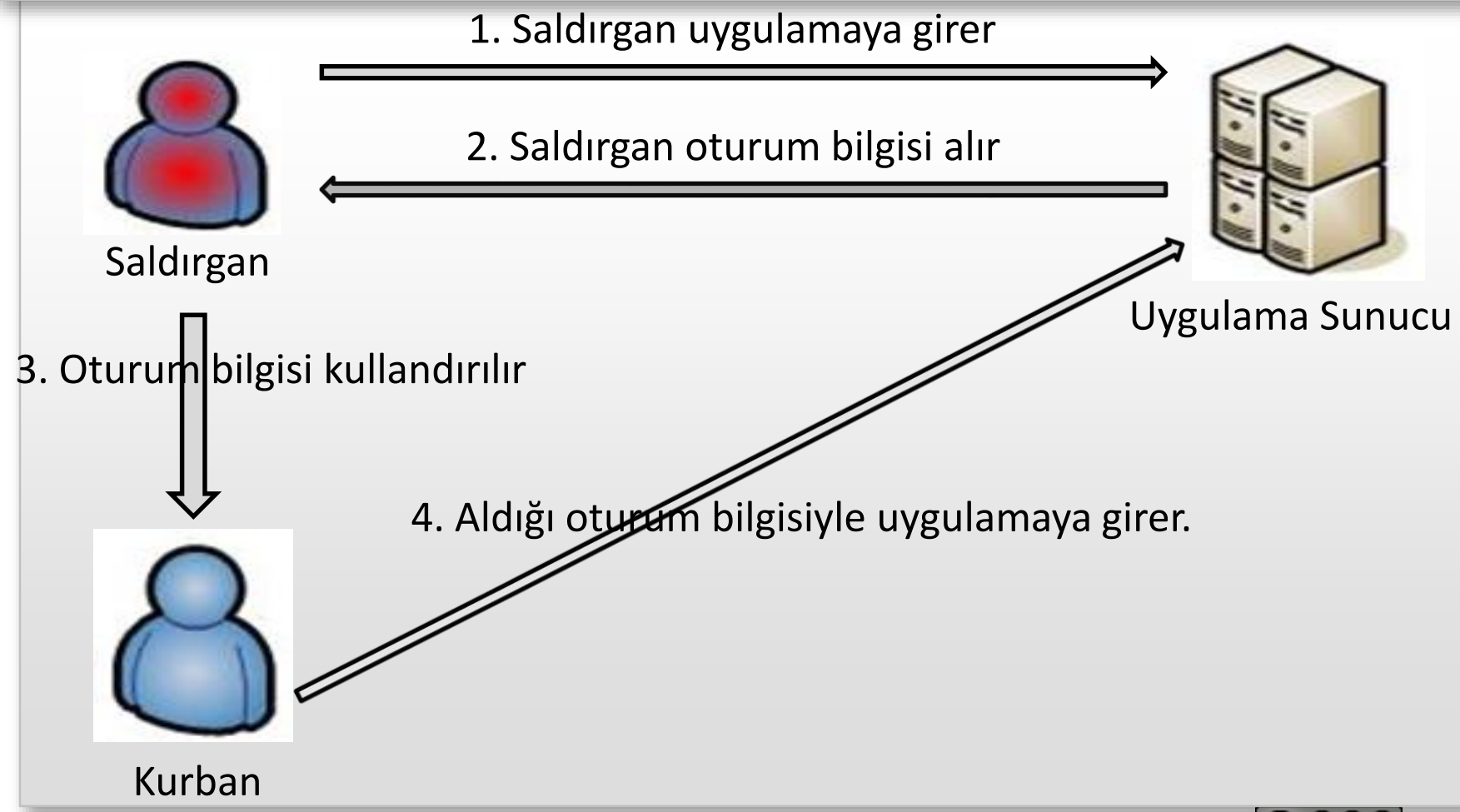
Oturum Sabitleme(Session Fixation)

- Uygulama, kullanıcı giriş yaptıktıktan sonra oturum bilgisini değiştirmediği durumlarda bu saldırı ortaya çıkmaktadır.
- Uygulamanın saldırgana verdiği oturum bilgisiyle, saldırgan kullanıcıyı uygulamaya girmeye zorlayabilir.



Oturum Yönetimi

Oturum Sabitleme



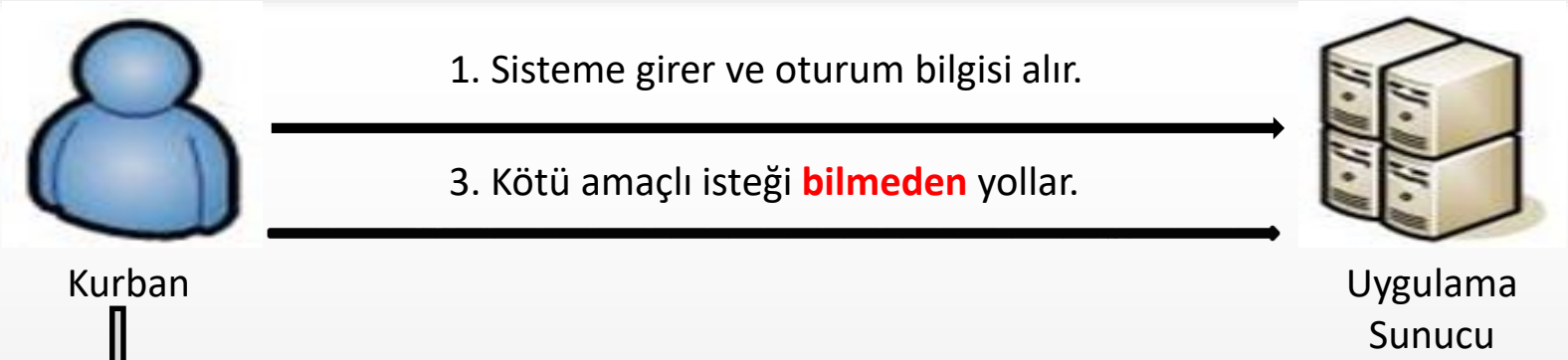
Oturum Yönetimi

Siteler arası istek sahteciliği(CSRF)

- Cross Site Request Forgery
- Kullanıcının giriş yaptığı bir uygulamada kullanıcının izni olmaksızın, kullanıcının oturum bilgisiyle zararlı isteklerde bulunma saldırısıdır.
- Burada kullanıcıdan giden isteklere dönen cevaplar saldırgan tarafından okunamaz. Cevabın önemsenmediği durumlarda bu saldırı kullanılabilir.

Oturum Yönetimi

CSRF …




```
<html>
   ...
  <img src="www.shopping.com/admin?cmd=deleteAll"
height=0 width=0>
   ...
</html>
```

Teşekkürler