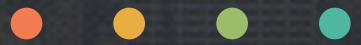

AB16

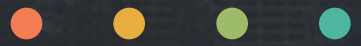
Web App Pentest 101



PRODAFT

Mazlum Ağar

- Prodaft
- Octosec
- info@mazlumagar.com
- @mazlumagar



PRODAFT

Ajanda

1. HTTP / HTTPS
2. OWASP TOP 10

PRODAFT

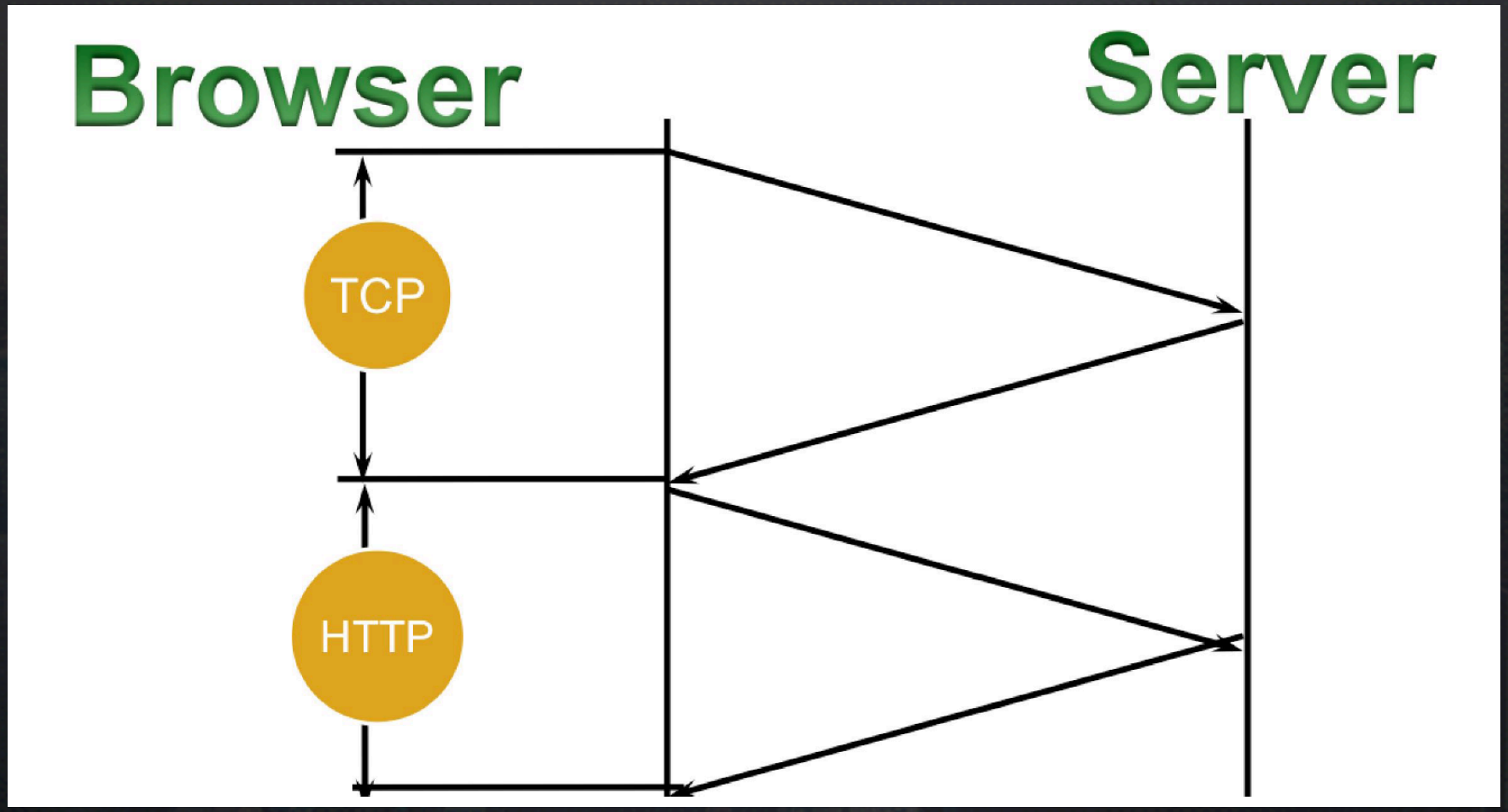
1

HTTP

HTTP Nedir?

- Hyper Text Transfer Protocol
- Uygulama Katmanı
- Web'e erişmek için kullanılan transfer protokolü
- Mesaj temelli kullanım
  - Kullanıcı mesajı, request
  - Server mesajı, response

HTTP



HTTP Request

Request Line + Headers + Empty Line

```
GET / HTTP/1.1
Host: mazlumagar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:44.0) Gecko/20100101 Firefox/44.0
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: __cfduid=daf73cc584fd58f01d61c5c1198503e201439029020; wp-settings-1=post_dfw%3Doff
%26editor%3Dhtml%26posts_list_mode%3Dlist%26libraryContent%3Dbrowse%26imgsize%3Dfull
%26mfold%3Do; wp-settings-time-1=1439772067;
__utma=150681770.407965547.1442435644.1451521381.1452729708.4;
__utmz=150681770.1442435644.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
DNT: 1
Connection: keep-alive
```

Request Line = Method + Resource Location + HTTP Version

HTTP Response

Response Line + Headers + Empty Line + Body

```
HTTP / 1.1 200 OK
Date: Sat, 30 Jan 2016 21:38:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Server: cloudflare-nginx
CF-RAY: 26d05397a1a02792-FRA
Content-Length: 107994

<!DOCTYPE html>
<html class="no-js" itemscope="itemscope" itemtype="http://schema.org/WebPage" lang="tr-TR”>
<head>
…
```

Response Line = HTTP Version + Response Code

POST Metodu

- POST metodu yazma işlemi için kullanılır.
- Önemli değişkenler URL yerine HTTP body içerisinde taşınmalıdır.

HTTP Metodları

- GET
  - Kaynakları almak için kullanılır.
- POST
  - İşlem yapmak için kullanılır.
- HEAD
  - Get ile aynı sadece header döner.
- TRACE
  - Sunucuyu kontrol amaçlı kullanılır.
- OPTIONS
  - Hangi metodları izin verdiğini öğrenmek için kullanılır.
- PUT
  - Kaynak yükleme işlemi için kullanılır.
- DELETE
  - Kaynak silme işlemi için kullanılır.

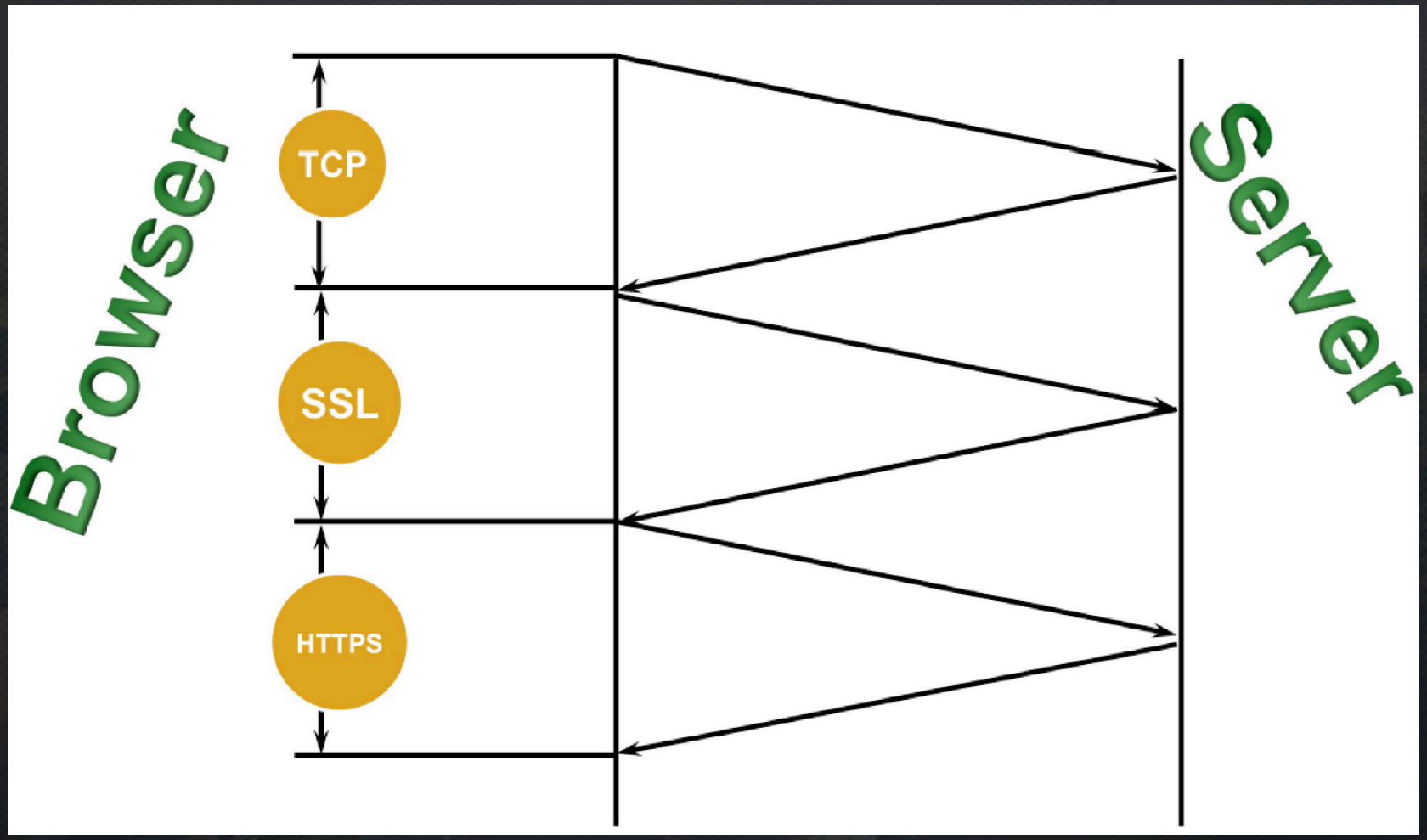
HTTP Güvenlik Problemleri

- Privacy (Gizlilik)
  Tüm veriler clear text (düz metin) olarak gittiği için herkes okuyabilir.
- Integrity (Bütünlük)
  Birisi içeriği değiştirebilir.
- Authentication (Doğrulama)
  Kiminle konuşulduğu kesin değil.

HTTPS

- SSL
- Arp poising

HTTPS



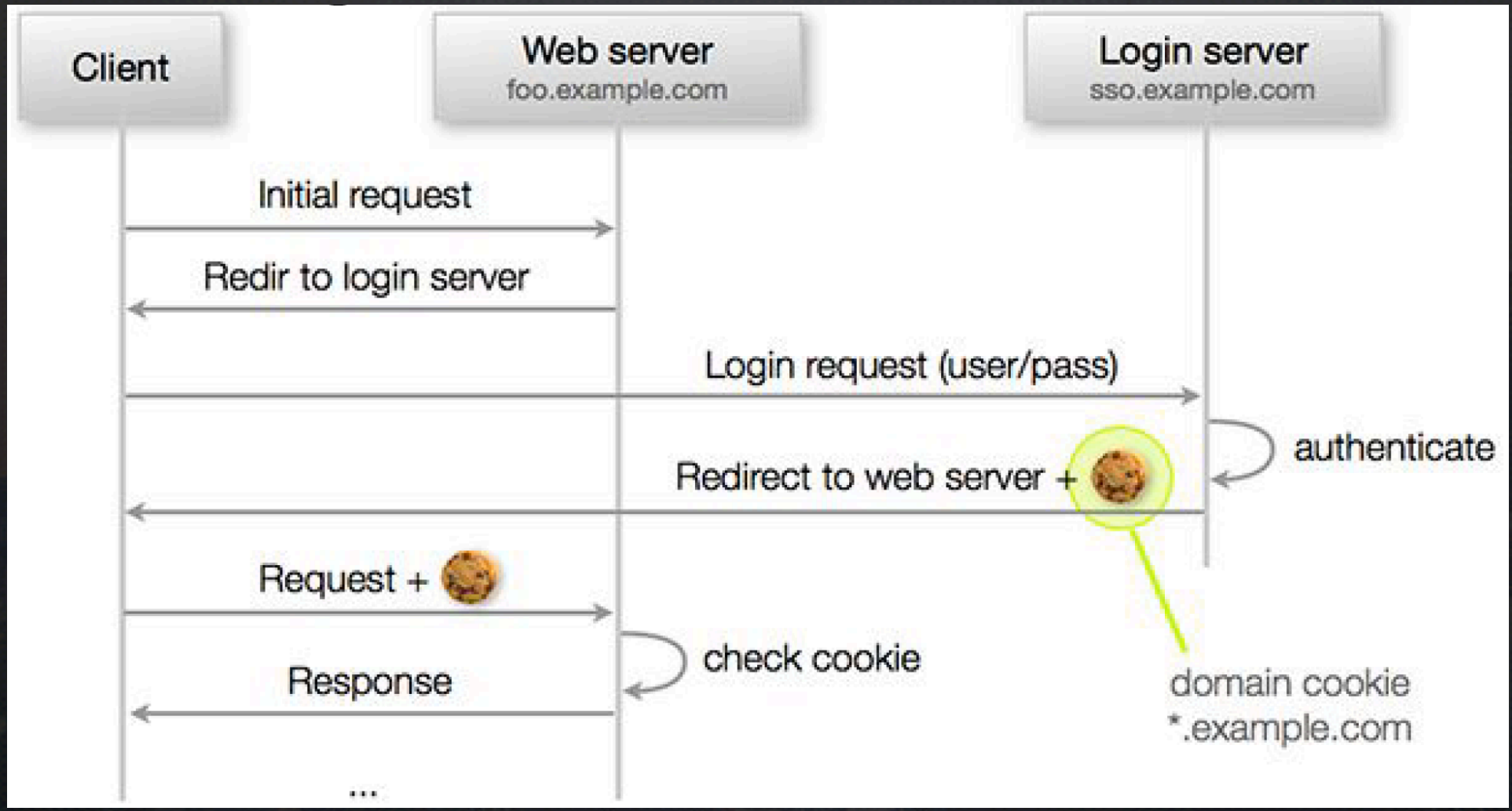
Encode Yöntemleri

- URL Encode
- Html Encoding
- Base64 Encoding

Cookie

Server bizi tanımalı. Peki nasıl?

Login Mekanizması



2

OWASP TOP 10

PRODAFT

OWASP

- Open Web Application Security Project
- Güvensiz yazılımların oluşturduğu problemlerle mücadele etmek için kurulmuş bir topluluk.
- Hiç bir kuruluşa bağlı değildir.

OWASP TOP 10

1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

SQL Injection

SQL

SQL (Structured Query Language) veritabanlarında data çekme, silme ve değiştirme gibi işlemler için kullanılan basit yapılı bir dildir.

SELECT * FROM kullanicilar

SQL Injection

Kullanıcıdan alınan inputlar ile oluşturulan dinamik SQL sorgularının değiştirilmesidir.

SELECT * FROM kullanicilar WHERE adi=‘muhittin’

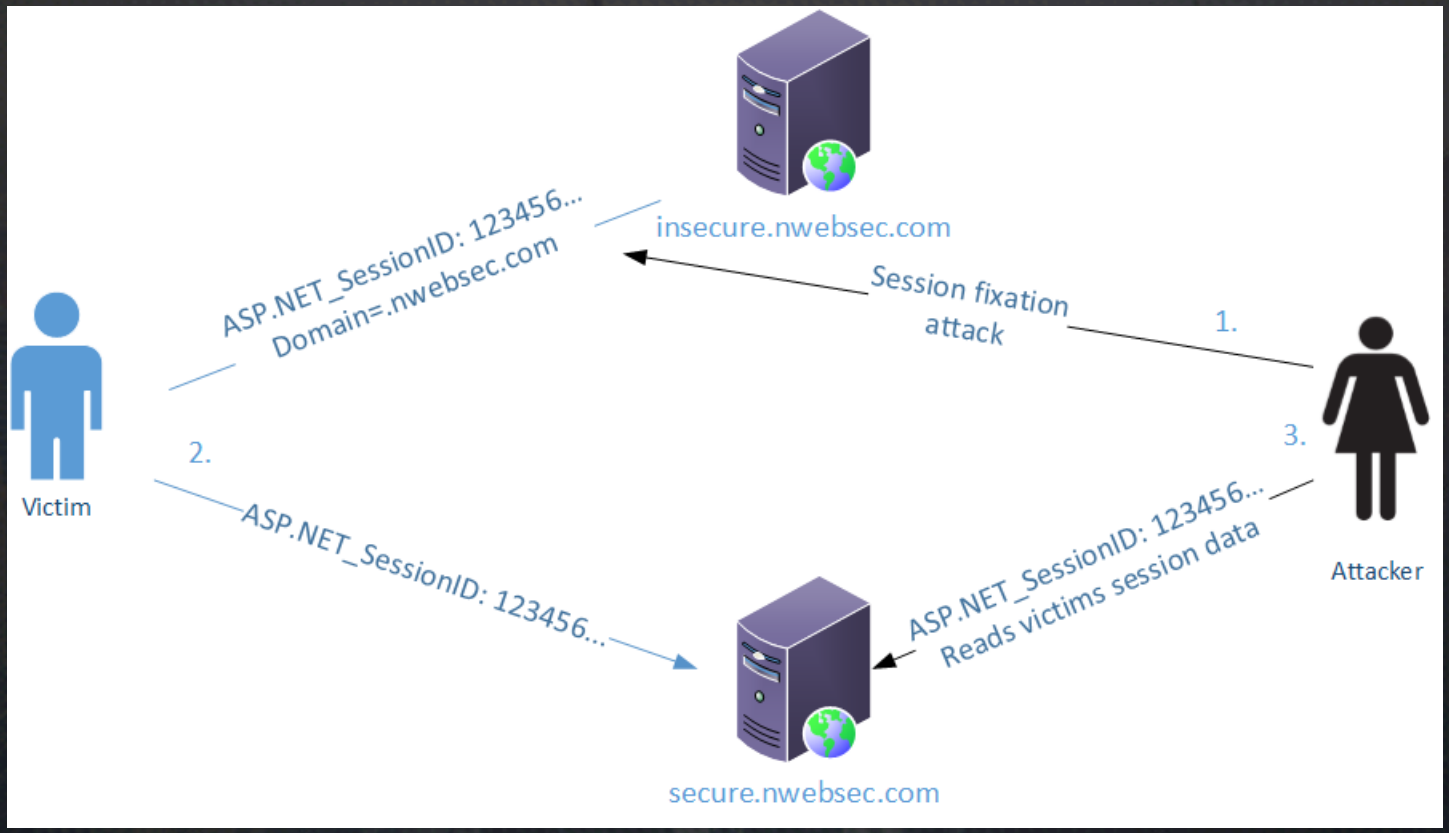
SQL Injection Aşamaları

1. Sql injection tespit et. (tırnak at ☺) ‘
2. Sorguda kaç kolon çekildiğini öğren. (order by)
3. Database adını öğren. (database())
4. Databasedeki tablo isimlerini öğren. (select table_name from information_schema.tables)
5. Tablodaki kolon isimlerini öğren. (select column_name from information_schema.cloumns from table_name=‘users’
6. Union select kolon1, kolon2 from table_name

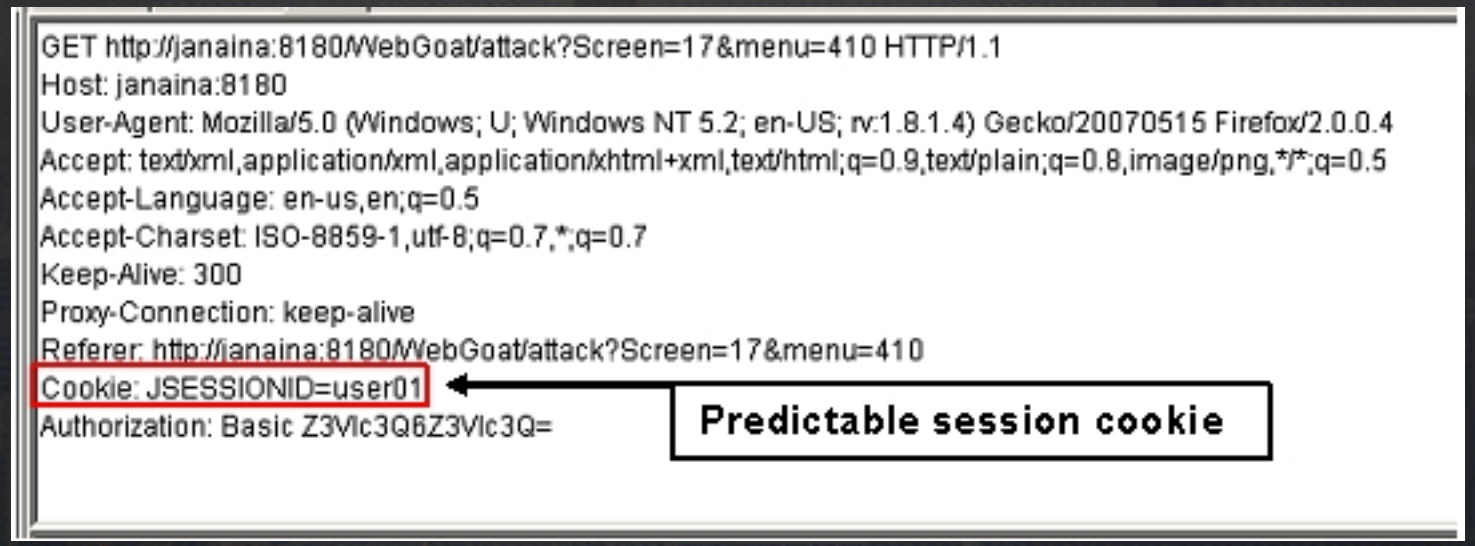
Broken Authentication and Session Management

1. Session Fixation (Oturum Sabitleme)
2. Session Prediction (Oturum Tahmin Etme)

Session Fixation



Session Prediction



Cross Site Scripting (XSS)

HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılmasıdır.

1. Reflected XSS
2. Stored XSS
3. DOM XSS (Document Object Model)

DOM XSS

- www.site.com/index.php#deger
- DOM Elementleri
- location.hash

Javascript kodları

document.write(..)
document.writeln(…)
document.body.innerHTML=…

Insecure Direct Object Reference

- Güvensiz Doğrudan Nesne Erişimi
- Yetkisiz erişim.

http://www.site.com/fatura.php?faturaID=4571

Security Misconfiguration

- Web Server
  - Versiyon bilgisi
  - Debug mod
  - Kullanılmayan sayfalar
  - Dosya/dizin izinleri
  - Sistem bilgisi
- Database
  - Varsayılan tablo isimleri
  - Varsayılan user

Sensitive Data Exposure

- Hassas bilgiler(kimlik numarası, kredi kartı, kullanıcıları bilgileri) korunamaması
- Hash
- Encryption

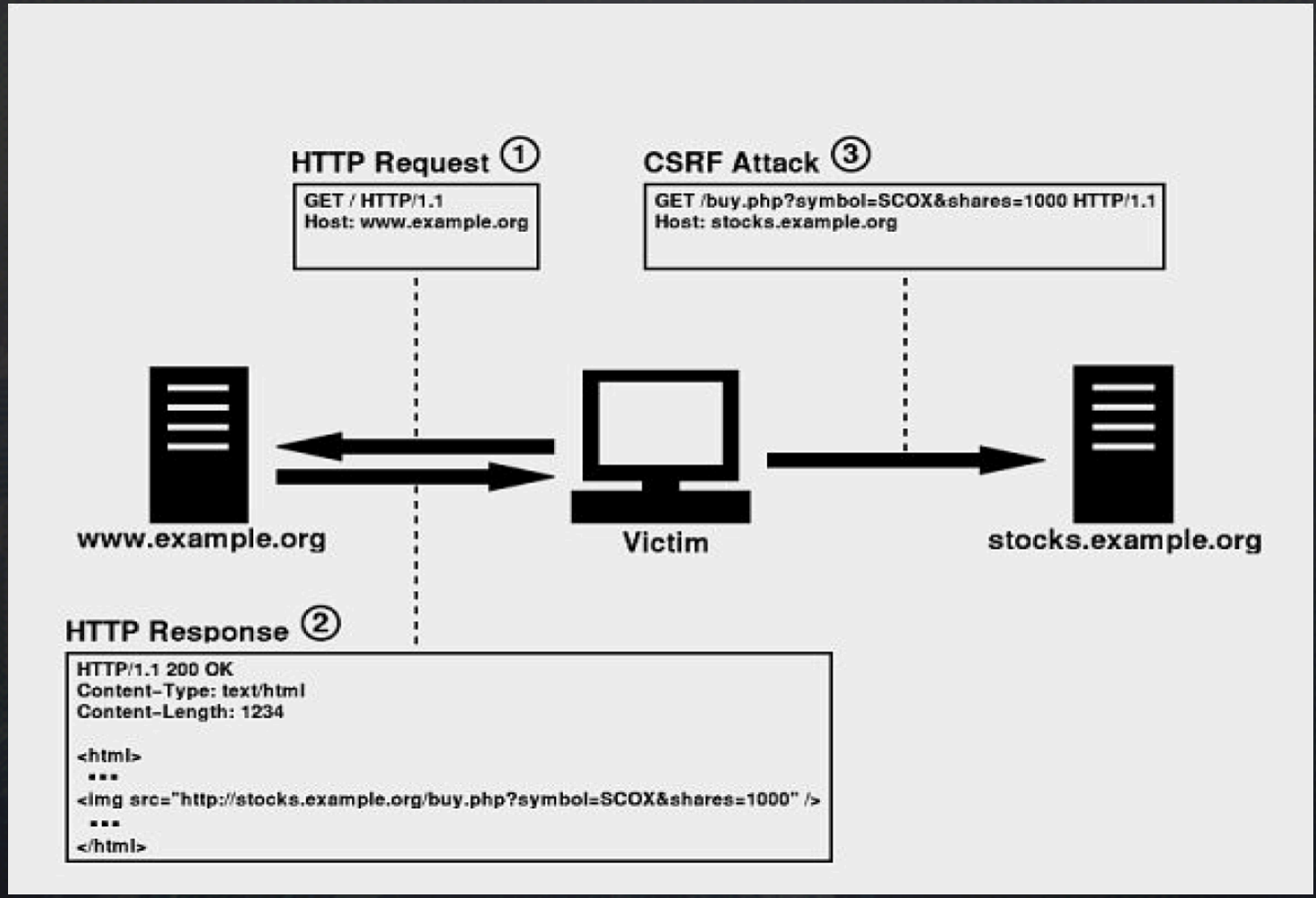
Missing Function Level Access Control

- Herkesin görebileceği link
  - www.site.com/readNews/5

- Sadece yetkili kişilerin görmesi gereken linkler
  - www.site.com/deleteNews/5
  - www.site.com/editNews/5

Bu tarz linklere erişim sırasında kontrol yapılmadığı durumlarda oluşur.

Cross-Site Request Forgery



Cross-Site Request Forgery

- GET

Cross-Site Request Forgery

- POST

```
<form action="http://bank.com/transfer.do" method="POST">
<input type="hidden" name="acct" value="MARIA"/>
<input type="hidden" name="amount" value="100000"/>
<input type="submit" value="View my pictures"/>
</form>

<body onload="document.forms[0].submit()">
<form...
```

Cross-Site Request Forgery

- POST

```
{ "acct":"BOB", "amount":100 }
```

```
<script>
function put() {
        var x = new XMLHttpRequest();
        x.open("PUT","http://bank.com/transfer.do",true);
        x.setRequestHeader("Content-Type", "application/json");
        x.send(JSON.stringify({"acct":"BOB", "amount":100}));
}
</script>
<body onload="put()">
```

Using Components with Known Vulnerabilities

3.parti yazılımlar

Unvalidated Redirect and Forwards

- www.site.com/login/?next=/page
- www.site.com/login/?next=www.phishing.com

TEŞEKKÜRLER