

10

İş Mantığı Zafiyetleri



İş Mantığı Zafiyetleri



<https://www.indusface.com/blog/business-logic-vulnerabilities/>

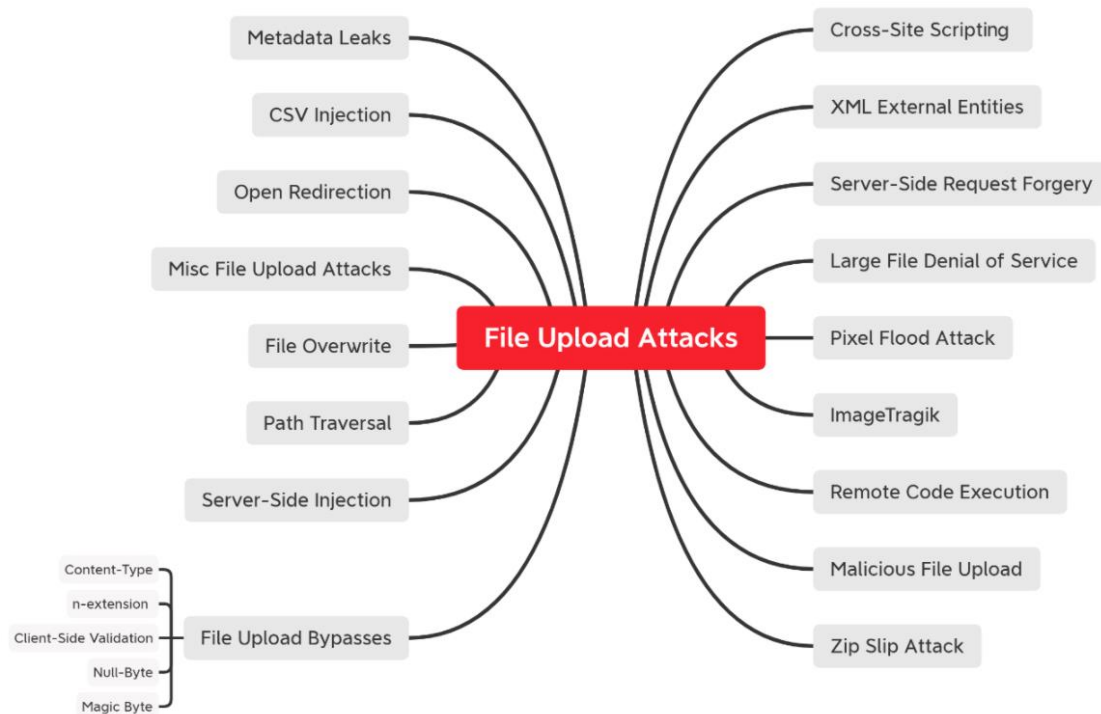
Örnek-1
Örnek-2

11

Dosya Yükleme Saldırıları



Dosya Yükleme Saldırıları



Güvensiz Dosya Yükleme



Zararlı dosyaların karşıdan yüklenebilmesi ve sunucu üzerinde çalıştırılması ile yapılan saldırılardır.



Dosya Yükleme Saldırıları

Atlatma Teknikleri

Client-side Kontrol

Blacklist

Content-Type Kontrolü

Magic Byte Kontrolü

file.PhP
file.php7

file.jpg.php
file.php.jpg
file.php%00

application/x-httpd-php → image/jpeg

Hex:
JPG: FF D8 FF EE
PNG: 89 50 4E 47 0D 0A 1A 0A
GIF: 47 49 46 38 39 61

Dosya Yükleme Saldırıları

Dosya Adı Üzerinden Oluşabilecek Zafiyetler

```
file$(whoami).png # Command Injection  
file';select+sleep(10);--.png # SQLi  
file"><script>alert(1)</script>.png # Cross-site Scripting (XSS)
```

```
../../file.jpg  
../../../../../../../../etc/passwd
```

Zip Slip

```
../../../../../../root/.ssh/authorized_keys  
dosya.txt
```

Dosya Yükleme Saldırıları

Potansiyel Atak Vektörleri

Denial of Service (DOS)
Metadata'ların Açığa Çıkması
XML External Entity (XXE) Injection
Zafiyetli Bileşen Kullanımı



<https://hackerone.com/reports/446238>



<https://hackerone.com/reports/135072>



<https://hackerone.com/reports/1062888>

Dosya Yükleme Saldırıları

Örnek - SVG dosyası üzerinden XSS

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full"
xmlns="http://www.w3.org/2000/svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900"
stroke="#004400"/>
  <script type="text/javascript">
    alert(document.domain);
  </script>
</svg>
```



Dosya Yükleme Saldırıları

Önlemler



İş ihtiyacı kapsamında gerekli olan dosya uzantıları belirlenerek, beyaz liste yaklaşımı ile kontrol edilmelidir. Sadece istenilen dosya uzantılarına izin verilmelidir.



Yüklenen dosyanın içeriği kontrol edilmelidir.



Yüklenebilecek dosyaların boyutu sınırlandırılmalıdır.



Uygulama tarafında yüklenen dosyaların adları değiştirilmelidir.



Sadece yetkili kişiler tarafından dosya yüklenebilmesine izin verilmelidir.



Yüklenen dosyalara erişim sağlanırken yetki kontrollerinin uygun bir şekilde yapıldığından emin olunmalıdır.

Dosya Yükleme Saldırıları

Önlemler



Dosya izinleri en az ayrıcalıklar ilkesine göre ayarlanmalıdır.



Yüklenen dosyaların, zararlı bir içeriğe sahip olup olmadığını doğrulamak için bir anti virüs veya sandbox çözümü kullanılabilir.



Kullanılan kütüphaneler güncel tutulmalı ve güvenli bir şekilde yapılandırılmalıdır.



Uygulama

Güvensiz Dosya Yükleme

Örnek-1



12

Server Side Request Forgery (SSRF)



Server Side Request Forgery (SSRF)



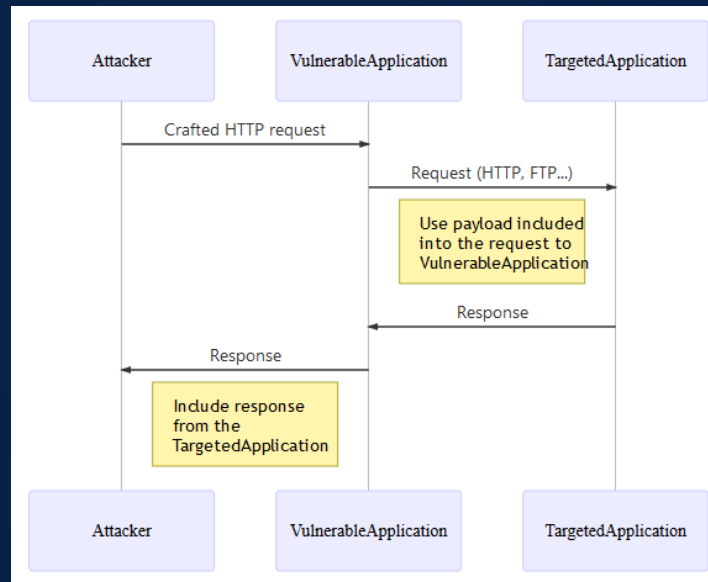
Kullanıcı kontrolünde olan girdiler üzerinden sunucu tarafı istekler yapıldığı durumlarda görülmektedir.



Harici kaynaklara olan erişim talepleri



file://, phar://, gopher://, data://, dict://





Uygulama

SSRF

Örnek-1

Örnek-2



Server Side Request Forgery (SSRF)

Önlem



Beyaz liste yaklaşımı ile girdi denetimi (String, IP, Domain name, URL)



İzin verilen adresler ve protokoller için **beyaz liste** yaklaşımı uygulanmalıdır.



Hem uygulama katmanında hem de Network katmanında güvenlik önlemleri alınmalıdır.



Web uygulama üzerinde, yönlendirmenin takip edilmesi desteği devre dışı bırakılmalıdır.

13

Open Redirection



Open Redirection



Güvenilmeyen girdi olarak sağlanan bir URL üzerinden yeniden yönlendirmeye izin veren uygulamalarda karşımıza çıkar.



Bir saldırgan, güvenilmeyen URL girişini **kötü amaçlı** bir siteye yönlendirerek kullanıcı kimlik bilgilerini çalabilir.

```
response.sendRedirect(request.getParameter("url"));
```

```
http://example.com/example.php?url=http://malicious.example.com
```



Uygulama

Open Redirection

Örnek-1



Open Redirection



Mümkünse kullanıcı girdisine bağımlı olarak yönlendirme işlemlerinden kaçınılmalıdır.



Kullanıcı girdisinden kaçınılamıyorsa, sağlanan değerin geçerli, uygulama için uygun ve kullanıcı için yetkilendirilmiş olduğundan emin olunmalıdır.



Uygulamada yönlendirme yapılan noktalarda beyaz liste yöntemi ile doğrulama yapılarak sadece izin verilen adreslere yönlendirme sağlanmalıdır.



Yönlendirme işlemlerinde, kullanıcılara sitenizden çıkacaklarını bildiren, hedefin adresin gösterildiği bir bilgilendirme gösterilmeli ve onaylamak için bağlantıyı tıklamaları sağlanmalıdır.

14

Directory Traversal



Directory Traversal



Kullanıcıdan alınan girdiler üzerinden herhangi bir kontrole tabii tutulmadan, dinamik olarak dosyalara/dizinlere erişim sağlanması durumunda Directory Traversal zafiyeti ortaya çıkar.



Sunucu üzerindeki dosyalara/dizinlere yetkisiz erişim sağlanması

```
https://example.com/get-files.jsp?file=report.pdf
```

Directory Traversal

```
<?php
$template = 'red.php';
if (isset($_COOKIE['TEMPLATE'])) {
    $template = $_COOKIE['TEMPLATE'];
}
include "/home/users/phpguru/templates/" . $template;
```

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../../../../etc/passwd
```



Uygulama

Directory Traversal

Örnek-1

Örnek-2

Örnek-3



Directory Traversal



İzin verilen dosya isimleri **beyaz listeye** eklenerek, kontrol edilmelidir.



../ gibi ifadelerin kara listeye eklenmesi, çeşitli yöntemlerle atlatılabilir!



Uygulama kullanıcısı en az yetki prensibini ile çalışmalıdır.

15

Güvensiz Yapılandırma Kaynaklı Zafiyetler

Zafiyetli Bileşen Kullanımı
Bilgi Ifşaları
Dizin Listeleme
Debug Mod Kullanımı
Uygunsuz Varlık Yönetimi
Rate Limiting
Client Side Filtering

Soru



File | /Users/anilbas/Desktop/siberkamp.html

Turkcell Siberkamp

Bu sayfada girdi yok

Zafiyetli Bileşen Kullanımı



Uygulamalarda çoğunlukla kütüphaneler veya bazı ürünler kullanılır.



Eğer kullanılan bileşenlerde bilinen güvenlik zafiyetleri varsa, bu bileşen üzerinden hedef uygulama da risk altında kalacaktır.

Zafiyetli Bileşen Kullanımı

Önlem



Uygulamada kullanılan bileşenlerin bilinen bir güvenlik açığı olup olmadığı kontrol edilmelidir.



Uygulamalarda kullanılan bağımlılıkların envanteri tutulmalı ve belirli aralıklarla kontrol edilmelidir.



Uygulamalarımızda kullanılan bileşenlerin güncel tutulması / güncel sürümlerin kullanılması gerekmektedir.

Zafiyetli Bileşen Kullanımı

Equifax Breach



Uygunsuz Varlık Yönetimi



Saldırganlar, tespit ettikleri test ortamları ve API eski sürümleri üzerinden saldırılar gerçekleştirebilir.



Bu ortamların, PROD ortamlar gibi iyi korunmadığı bilinen bir gerçektir.

Uygunsuz Varlık Yönetimi

Önlem



Envanter sürekli güncellenmeli ve takip edilmelidir.



API'lerin eski sürümlerinin kullanımdan kaldırılması önerilmektedir.



Yalnızca geçerli PROD ortam için değil, kullanımda olan tüm sürümler için harici koruma önlemleri uygulanmalıdır.



Test ortamlarına erişimin kısıtlanması ve bu ortamların ayrılması önerilir.





API dokümantasyonlarının sadece yetkili kişiler tarafından erişilmesi sağlanmalıdır.

Rate Limiting



LIMITATION

 API çağrıları yapılırken, istek sınırlaması olmaması sunucunun kaynaklarını gereksiz yere tüketerek, servis dışı kalmasına sebep olabilir.

 Mail gönderme, iletişim formu, OTP gönderim servisleri, büyük cevaplar dönebilecek servislerde bu durum değişik etkilere sebep olabilir.

Rate Limiting

Önlem



Yapılan istekler için boyut sınırlaması belirlenerek, sunucu tarafında kontrol edilmelidir.



Cevapta döndürülecek kayıt sayısı kontrol edilmelidir.



Belirli bir süre içerisinde API'nin ne sıklıkla çağırılacağına sınırlama getirilmelidir.

Client-side Filtering



Genellikle, sunucudan toplu bir şekilde veriyi döndürüp, kullanıcı tarafında filtreleme yapılması ve sadece istenilen bilgilerin kullanıcıya gösterilmesi ile risk oluşturur.

532-000-11-22



5XX-XXX-XX-XX

Client-side Filtering

Önlem



Kullanıcı tarafında yapılan filtrelemelere asla güvenilmemelidir.



Uygulamadan veri dönen noktalar incelenmeli, gereksinimi belirleyerek en az miktarda veri döndürülmelidir.

Bilgi İfşaları & Hata Ayıklama Modu



Sistem hakkında bilgi açığa çıkartan durumlar;
Server versiyonu ve teknoloji ifşaları, detaylı hata mesajları vs.



Hata ayıklama modu geliştirme aşamasında geliştiricilere
kolaylık sağlar.



Üretim ortamında hata ayıklama modunun açık bırakılması
saldırganlara uygulama hakkında hassas veri ifşaları
sağlayabilir.

Server Error in '/' Application.

Failed to generate a user instance of SQL Server due to failure in retrieving the user's local application data path. Please make sure the user has a local user profile on the computer. The connection will be closed.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Failed to generate a user instance of SQL Server due to failure in retrieving the user's local application data path. Please make sure the user has a local user profile on the computer. The connection will be closed.

Source Error:

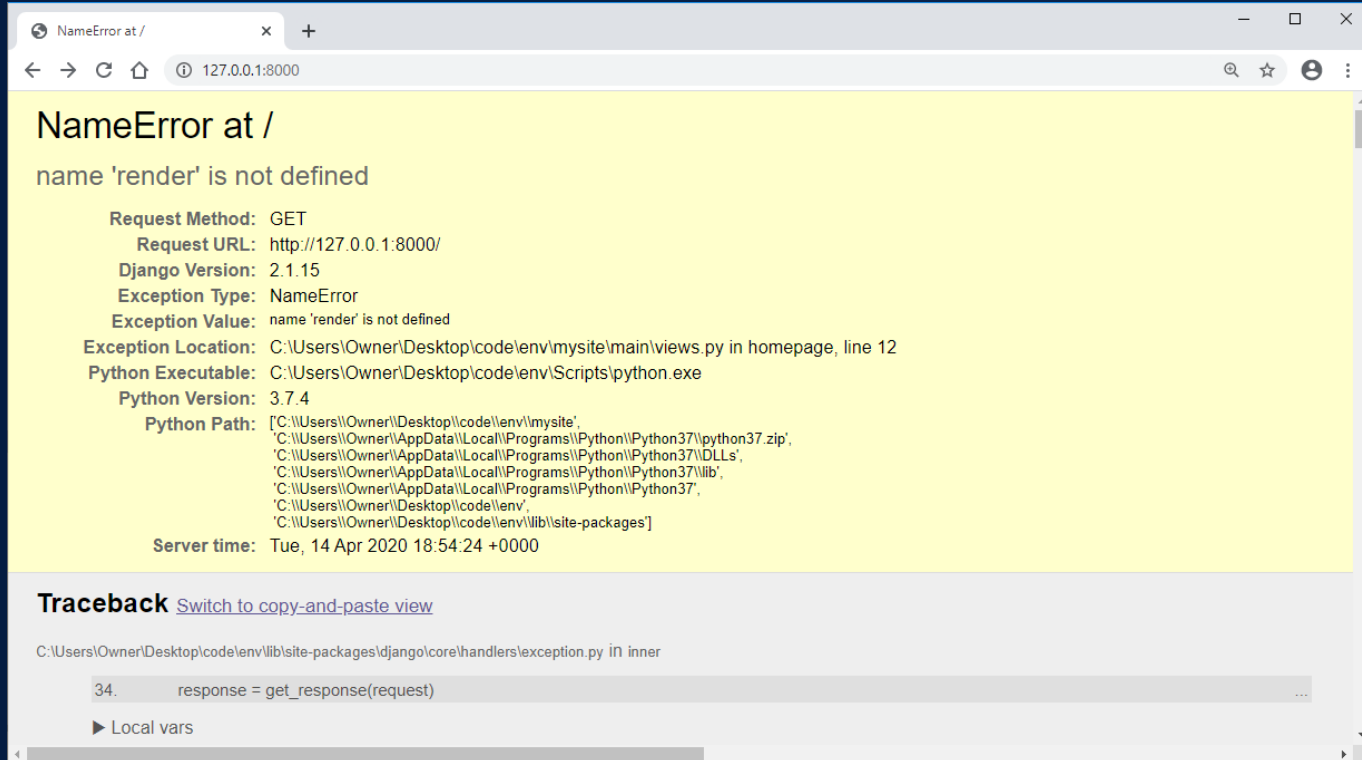
```
Line 139:         DbConnection conn = provider.CreateConnection();
Line 140:         conn.ConnectionString = connectionString;
Line 141:         conn.Open();
Line 142:
Line 143:         s_connectionPool[i] = conn;
```

Source File: c:\inetpub\BuySpySwiss\App_Code\Configuration.cs **Line:** 141

Stack Trace:

```
[SqlException (0x80131904): Failed to generate a user instance of SQL Server due to failure in retrieving
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataSt
System.Data.SqlClient.SqlInternalConnectionTds.CompleteLogin(Boolean enlistOK) +35
System.Data.SqlClient.SqlInternalConnectionTds.AttemptOneLogin(ServerInfo serverInfo, String newPassword
System.Data.SqlClient.SqlInternalConnectionTds.LoginNoFailover(String host, String newPassword, Boolean
System.Data.SqlClient.SqlInternalConnectionTds.OpenLoginEnlist(SqlConnection owningObject, SqlConnecti
System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionSt
System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbClientImplic
```

Bilgi İfşaları & Hata Ayıklama Modu



NameError at /

name 'render' is not defined

Request Method: GET
Request URL: http://127.0.0.1:8000/
Django Version: 2.1.15
Exception Type: NameError
Exception Value: name 'render' is not defined
Exception Location: C:\Users\Owner\Desktop\code\env\mysite\main\views.py in homepage, line 12
Python Executable: C:\Users\Owner\Desktop\code\env\Scripts\python.exe
Python Version: 3.7.4
Python Path: [C:\\Users\\Owner\\Desktop\\code\\env\\mysite',
C:\\Users\\Owner\\AppData\\Local\\Programs\\Python\\Python37\\python37.zip',
C:\\Users\\Owner\\AppData\\Local\\Programs\\Python\\Python37\\DLLs',
C:\\Users\\Owner\\AppData\\Local\\Programs\\Python\\Python37\\lib',
C:\\Users\\Owner\\AppData\\Local\\Programs\\Python\\Python37',
C:\\Users\\Owner\\Desktop\\code\\env',
C:\\Users\\Owner\\Desktop\\code\\env\\lib\\site-packages]
Server time: Tue, 14 Apr 2020 18:54:24 +0000

Traceback [Switch to copy-and-paste view](#)

C:\\Users\\Owner\\Desktop\\code\\env\\lib\\site-packages\\django\\core\\handlers\\exception.py in inner

```
34.     response = get_response(request)
```

► Local vars

Dizin Listeleme












Web sunucuları, bir index sayfası bulunmayan dizinlerin içeriğini listeler.



Bu durum, webroot klasörü altında yer alan gizli ve hassas dosyaların açığa çıkmasına sebep olacaktır.

Index of /content

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory			-
 license.txt	2019-01-02 02:07	19K	
 readme.html	2019-04-09 04:29	7.3K	
 wp-activate.php	2019-01-12 12:11	6.8K	
 wp-config-sample.php	2019-01-08 10:00	2.8K	
 wp-config.php	2017-12-07 17:00	3.1K	
 wp-content/	2012-01-08 22:31	-	
 wp-includes/	2019-05-21 23:54	-	
 xmlrpc.php	2018-08-17 07:21	3.0K	