



**Hasan Şuca Kayman**

**2017280030**

**Yazılım Proje Yönetimi Final Ödevi**

# İçindekiler

<b>1. Bölüm.....</b>	<b>3</b>
<b>1.1 SC-1.java .....</b>	<b>3</b>
<b>1.2 SC-2.java .....</b>	<b>4</b>
<b>1.1 SC-3.java .....</b>	<b>5</b>
<b>2. Bölüm.....</b>	<b>6</b>
<b>Alternatif B: <a href="http://bodgeit.herokuapp.com/">http://bodgeit.herokuapp.com/</a> .....</b>	<b>6</b>
Acunetix Screenshots.....	7
OWASP ZAP Screenshots .....	7

# 1. Bölüm

## 1.1 SC-1.java

Potansiyel Tehlike	Tespit	Seviye	Yorum	Çözüm
<b>STANDARD: FileInputStream</b> This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, careful checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename. Line: 4 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java import java.io.FileInputStream;	VCG	Orta	Manuel Kontrol Edilmesi Gerekliliği	Bu kütüphanenin her kullanılan yerlerin control edilmesi ve gerekli yerlerde hata atmasını sağlanması
<b>STANDARD: java.io.File</b> This functionality acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, careful checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename. Line: 5 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java import java.io.File;	VCG	Orta	Manuel Kontrol Edilmesi Gerekliliği	Bu kütüphanenin her kullanılan yerlerin control edilmesi ve gerekli yerlerde hata atmasını sağlanması
<b>POTENTIAL ISSUE: Public Class Not Declared as Final</b> The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practica (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final. Line: 9 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java public class TestIt extends AbstractTestCase	VCG	Düşük	Abstract Sınıfına kalıtım implement ile olur	Extend yerine implement yapılmalıdır.
<b>HIGH: java.lang.Runtime.exec Gets Path from Variable</b> The pathname used in the call appears to be loaded from a variable. Check the code manually to ensure that malicious filenames cannot be submitted by an attacker. Line: 33 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java Process process = Runtime.getRuntime().exec(osCommand + data);	VCG	Yüksek	Script Injection problem titizlikle kontrol edilmelidir.	Komut satırındaki önemli noktalama işaretleri elenmeli titizlikle engellenmelidir.
<b>STANDARD: FileInputStream</b> This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, careful checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename. Line: 53 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java streamFileInput = new FileInputStream(file);	VCG	Orta	Manuel Kontrol Edilmesi Gerekliliği	Try catch control edilip dikkatli bir şekilde kodlanması
<b>STANDARD: FileInputStream</b> This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, careful checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename. Line: 47 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java FileInputStream streamFileInput = null;	VCG	Orta	Manuel Kontrol Edilmesi Gerekliliği	Try catch control edilip dikkatli bir şekilde kodlanması
<b>LOW: Operation on Primitive Data Type</b> The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk. Line: 57 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java for (int i = 0; i >= 0; i = (i + 1) % 256)	VCG	Yüksek	Manuel Kontrol Edilmesi Gerekliliği	Sınırsız döngü var mutlaka sonlu hale getirilmelidir.
<b>STANDARD: FileInputStream</b> This function acts as an entry point for external data and the code should be manually checked to ensure the data obtained is correctly validated and/or sanitised. Additionally, careful checks/sanitisation should be applied in any situation where the user may be able to control or affect the filename. Line: 102 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java io.logger.log(Level.WARNING, "Error closing FileInputStream", exceptIO);	VCG	Düşük	Manuel Kontrol Edilmesi Gerekliliği	IO değişkeni kütüphaneden veya kalıttan geldiği varsayılır. Ayrıyeten Try catch control edilip dikkatli bir şekilde kodlanması
46 File file = new File("C:\\data.txt");	Manuel	Orta	Windows dışı OSlerinde bu dosya dizini yoktur.	Btd() methodunda olduğu gibi burada da işletim sistemi kontrol edilebilir.

<pre> 107 else 108 { 109     data = null; 110 } </pre>	Manuel	Düşük	Hiç bu satır çalışmayacaktır. Ait olduğu method private ve bu methoda erişen btd methodunda koşulu true yapıyor.	Silinmesi veya btd methodunun sonuna btdPrivate = false; satırı eklenmesi
<pre> 34 process.waitFor(); </pre>	Manuel	Yüksek	Ne kadar?	Methodun süre değişkenleri verilmesi
<pre> 59 IO.writeLine(i); </pre>	Manuel	Düşük	IO field'ı kalıtım sağlandığı abstract sınıfta tanımlanmış ve yazıldığı yerin konumu belirlenmiştir.	Eğer IO tanımlanmamışsa write işleminin tanımlanarak yapılması

## 1.2 SC-2.java

Potansiyel Tehlike	Tespit	Seviye	Yorum	Çözüm
<b>POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final</b> Line: 5 - C:\Users\sucu\Desktop\SC\finalKaynakKodlar\SC-2.java The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final. <pre>public class TestMe extends AbstractTestCaseServlet</pre>	VCG	Düşük	Abstract Sınıfına kalıtım implement ile olur	Extend yerine implement yapılmalıdır.
<b>LOW: Potentially Unsafe Code - Operation on Primitive Data Type</b> Line: 26 - C:\Users\sucu\Desktop\SC\finalKaynakKodlar\SC-2.java The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk. <pre>id = -1;</pre>	VCG	Orta	Manuel Kontrol Edilmesi Gerekli	Kesinlikle id'si -1 olan kayıt olmamalıdır.
<b>HIGH: Potentially Unsafe Code - Poor Input Validation</b> Line: 90 - C:\Users\sucu\Desktop\SC\finalKaynakKodlar\SC-2.java The application appears to use data contained in the HttpServletRequest without validation or sanitisation. No validator plug-ins were located in the application's XML files. <pre>data = request.getParameter("id");</pre>	VCG	Yüksek	Direk http sunucusundan çekiyor eğer id bilgisi yoksa null dönecektir bu da bzd methodunda problem çıkarabilecektir	Id bilgisini url den direk olarak url den alırsak daha güvenli olacaktır.
<b>31. Satır</b> <pre>dbConnection.prepareStatement</pre>	Manuel	Yüksek	SQL Injection Problemi	Dahil olan değişkenden noktalama işaretleri silinmeli veya tipi int gibi olmalı burada da öyle
<b>36. Satır</b> <pre>"bzd()"   result requested: " + data + "\n"</pre>	Manuel	Düşük	Sorgunun sonucu basılmalı	Print işleminde data değil resultSet basılmalı
<pre> 92 else 93 { 94     data = null; 95 } 96 </pre>	Manuel	Düşük	Hiç bu satır çalışmayacaktır. Ait olduğu method private ve bu methoda erişen btd methodunda koşulu true yapıyor.	Silinmesi veya btd methodunun sonuna btdPrivate = false; satırı eklenmesi

## 1.1 SC-3.java

Potansiyel Tehlike	Tespit	Seviye	Yorum	Çözüm
<b>POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final</b> Line: 8 - C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-3.java The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final. public class TestThis extends AbstractTestCase	VCG	Düşük	Abstract Sınıfına kalıtım implement ile olur	Extend yerine implement yapılmalıdır.
17 int x = (new SecureRandom()).nextInt(3); 18 switch (x) 19 { 20 case 0: 21 stringIntValue = "0"; 22 break; 23 case 1: 24 stringIntValue = "1"; 25 break; 26 27 }	Manuel	Düşük	Case 3 durumu yok default da yok	Case 3 durumu eklenmesi
87 else 88 { 89 data = 0; 90 }	Manuel	Düşük	PRIVATE_STATIC_FINAL_TRUE değişkeni sabit olarak true bu kısım hiçbir zaman çalışmayacaktır	Silinmesi
94. Satır (100 / data)	Manuel	Yüksek	0 a bölme hatası	işlemden önce control edilmeli
IO.logger.	Manuel	Düşük	IO field'ı kalıtım sağlandığı abstract sınıfta tanımlanmış ve yazıldığı yerin konumu belirlenmiştir.	Eğer IO tanımlanmamışsa write işleminin tanımlanarak yapılması

### STANDARD: FileInputStream

Line: 4 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
import java.io.FileInputStream;  
Line: 47 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
FileInputStream streamFileInput = null;  
Line: 53 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
streamFileInput = new FileInputStream(file);  
Line: 102 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
IO.logger.log(Level.WARNING, "Error closing FileInputStream", exceptIO);

### STANDARD: java.io.File

Line: 4 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
import java.io.File;  
Line: 5 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
import java.io.File;

### POTENTIAL ISSUE: Public Class Not Declared as Final

Line: 9 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
public class TestIt extends AbstractTestCase  
Line: 5 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-2.java  
public class TestMe extends AbstractTestCaseServlet  
Line: 8 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-3.java  
public class TestThis extends AbstractTestCase

### HIGH: java.lang.Runtime.exec Gets Path from Variable

Line: 33 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
Process process = Runtime.getRuntime().exec(osCommand + data);

### LOW: Operation on Primitive Data Type

Line: 57 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-1.java  
for (int i = 0; i <= 255; i++)  
Line: 26 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-2.java  
id = -1;

### STANDARD: getParameter

Line: 90 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-2.java  
data = request.getParameter("id");

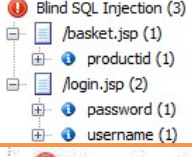
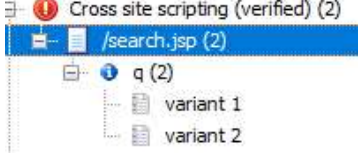
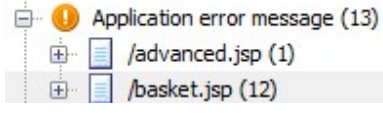
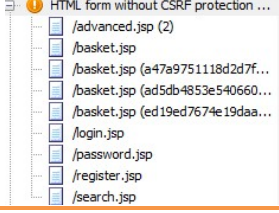
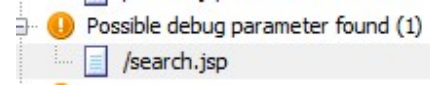
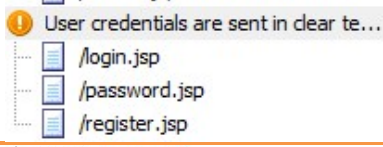
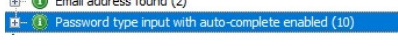
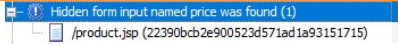

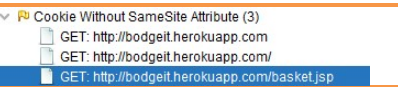
### HIGH: Poor Input Validation

Line: 90 - Filename: C:\Users\suca\Desktop\SC\finalKaynakKodlar\SC-2.java  
data = request.getParameter("id");

Tüm Sonuçlar değerlendirildi. False pozitif mi diye control edildi. Manuelde control edildi.

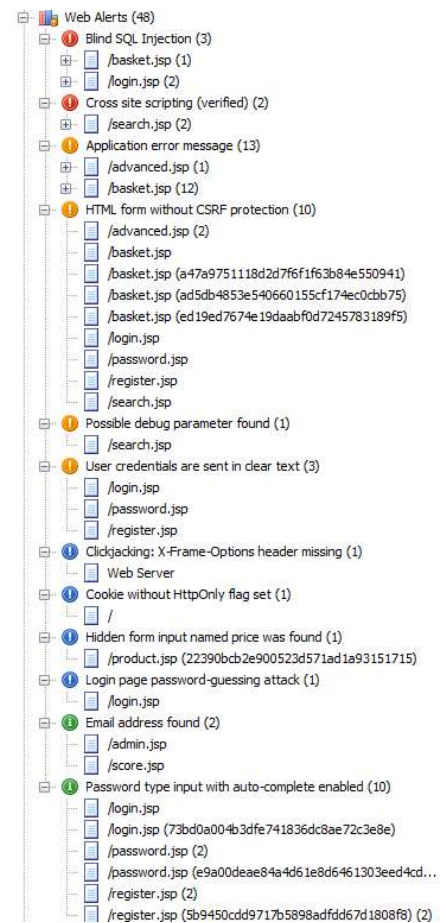
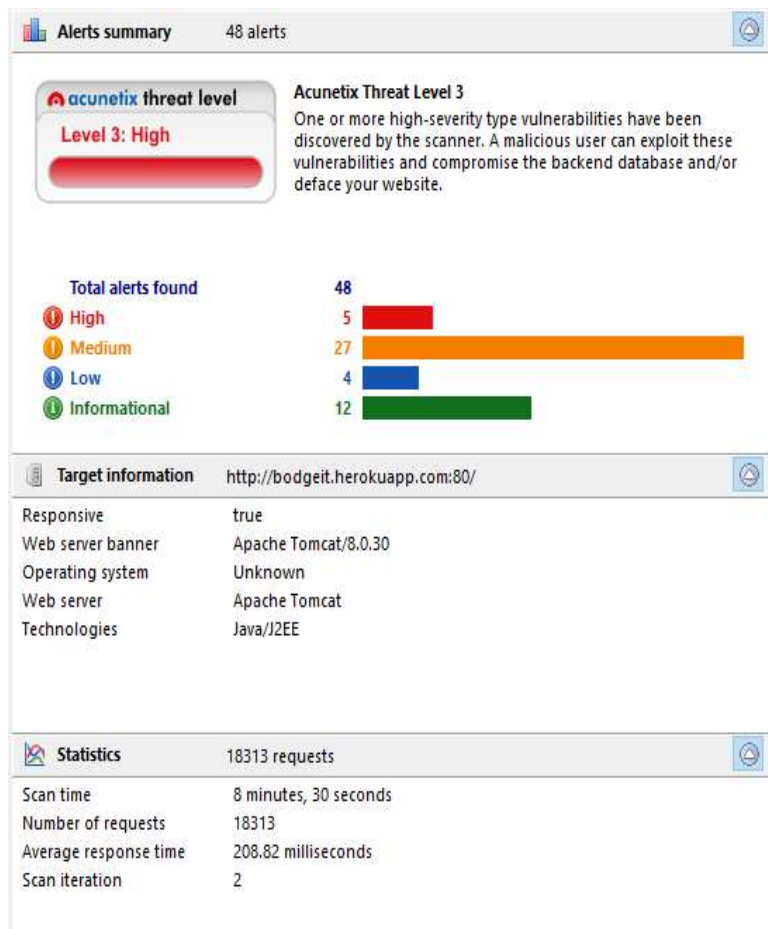
## 2. Bölüm

Alternatif B: <http://bodgeit.herokuapp.com/>

Potansiyel Tehlike	Tespit	Seviye	Yorum	Çözüm
	Acunetix	Yüksek	Sql Injection	Girdinin içindeki “,’,OR,AND gibi stringleri çıkarmak
	Acunetix - Owasp Zap	Yüksek	Script	Girdinin içindeki <Script> ifadesini silmek ve <Sc<Script>ript> bu gibi durumlarda ifade bitene kadar peşpeşe silmek
	Acunetix- Owasp Zap	Orta	Bu gibi hataları kodların içini görebilmek için muhteşem bir zafiyeti vardır.	Kaynak kodu kontrol edip bu gibi hataları (fırlatmak)throw yapılmalı
	Acunetix	Yüksek	CSRF zafiyeti, araya vpn koyup get, post lardaki değerleri değiştirmek	kaynak koda CSRF koruması eklenmeli
	Acunetix	Orta	Olası Debug parametresi CSRF gibi get, post lardaki değerleri değiştirmektedir	Debug parametresini silmek
	Acunetix	Orta	Kimlik bilgileri şifrelenmemiş	Md5 hash gibi fonksiyonlardan birini kullanıp veritabanına öyle kaydetmek
	Acunetix	Problem Değil	Egitim amaçlı zafiyetinden ötürü About sekmesinde gözüküyor	
	Acunetix	Düşük	Gizli formlarda hassas bilgilerin olması	Gizli formlarda hassas bilgi olmamalıdır.
	Owasp Zap	Düşük	HttpFlag olmaması	HttpFlagı ayarlanması
	Owasp Zap	Düşük	CSRF zafiyetinin bir adımı	Cookie leri katı olarak ayarlamak.



## Acunetix Screenshots



## OWASP ZAP Screenshots

- > Cross Site Scripting (Reflected)
- > Buffer Overflow (3)
- > X-Frame-Options Header Not Set (56)
- > Absence of Anti-CSRF Tokens (73)
- > Application Error Disclosure
- > Cookie No HttpOnly Flag
- > **Cookie Without SameSite Attribute (3)**
- > X-Content-Type-Options Header Missing (62)
- > Information Disclosure - Suspicious Comments (59)