

WEBGOAT






WebGoat Nedir?

WebGoat, OWASP tarafından geliştirilen ve bilinçli olarak güvenlik zafiyetleri içeren bir web uygulamasıdır. Bu platform, güvenlik açıklarını öğretmek ve test etmek amacıyla özel olarak tasarlanmıştır. Özellikle web uygulama güvenliği konusunda eğitim almak isteyenler için ideal bir ortam sunar.

Nasıl Kurulur?

Kurulumundan önce Linux makinemizi update ve upgrade ediyoruz. Daha sonra [OWASP Web Goat](#) web sitesini ziyaret ediyoruz. Sağ tarafta bulunan Downloads bölümünden [Standalone jars](#)'a tıklayarak WebGoat'ın GitHub sayfasına erişiyoruz. Buradan son sürümü indirmemiz gerekiyor. Assets kısmından **webgoat-2023.8.jar**'ı indiriyoruz.

▼ Assets 3

 webgoat-2023.8.jar	113 MB	Dec 5, 2023
 Source code (zip)		Dec 5, 2023
 Source code (tar.gz)		Dec 5, 2023

İndirme işlemi tamamlandıktan sonra indirdiğimiz dizine gidiyoruz ve aşağıdaki komutu yazıyoruz.

```
sudo java -Dfile.encoding=UTF-8 -Dwebgoat.port=53666 -Dwebwolf.port=9090 -jar webgoat-2023.8.jar
```

```
(kali@kali)~[~/Downloads]
$ sudo java -Dfile.encoding=UTF-8 -Dwebgoat.port=53666 -Dwebwolf.port=9090 -jar webgoat-2023.8.jar
2024-07-14T14:45:24.774-04:00 INFO 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : Starting StartWebGoat v2023.8 using Java 17.0.10
with PID 12650 (/home/kali/Downloads/webgoat-2023.8.jar started by root in /home/kali/Downloads)
2024-07-14T14:45:24.789-04:00 INFO 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : No active profile set, falling back to 1 default
profile: "default"
2024-07-14T14:45:26.859-04:00 INFO 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : Started StartWebGoat in 3.703 seconds (process ru
nning for 5.906)

WebGoat

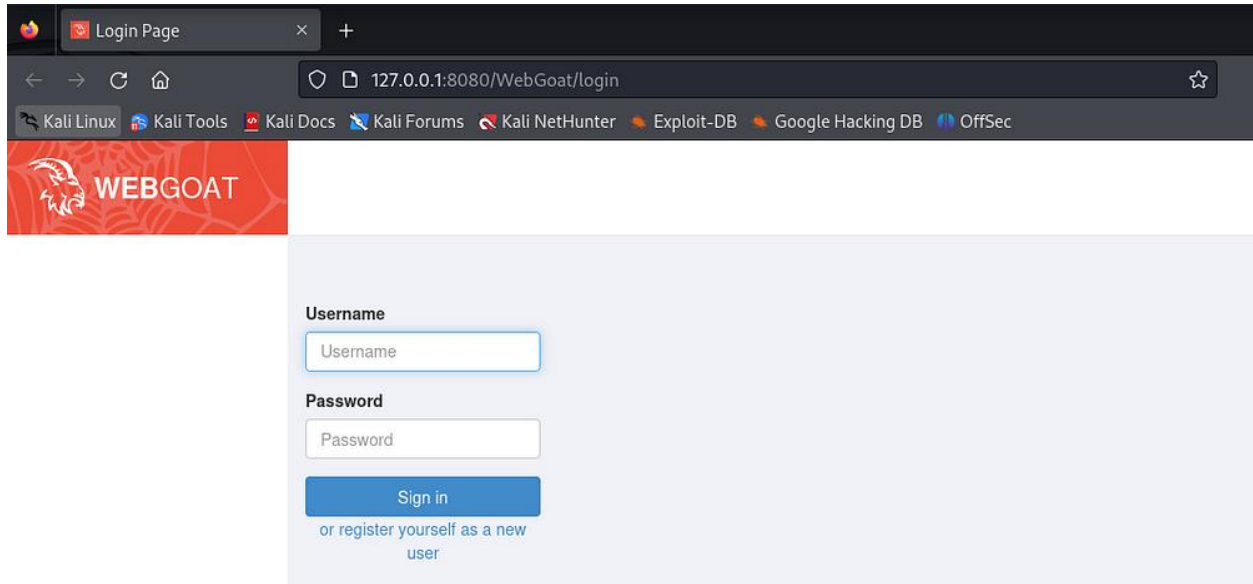
2024-07-14T14:45:27.165-04:00 INFO 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : No active profile set, falling back to 1 default
profile: "default"
2024-07-14T14:45:30.362-04:00 INFO 12650 --- [main] s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEF
AULT mode.
2024-07-14T14:45:30.603-04:00 INFO 12650 --- [main] s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 196 m
s. Found 2 JPA repository interfaces.
2024-07-14T14:45:32.103-04:00 WARN 12650 --- [main] io.undertow.websockets.jsr : UT026010: Buffer pool was not set on WebSocketDep
loymentInfo, the default pool will be used
2024-07-14T14:45:32.157-04:00 INFO 12650 --- [main] io.undertow.servlet : Initializing Spring embedded WebApplicationContext
2024-07-14T14:45:32.160-04:00 INFO 12650 --- [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization comple
ted in 4707 ms
2024-07-14T14:45:32.836-04:00 INFO 12650 --- [main] com.zaxxer.hikari.HikariDataSource : HikariPool-1 - Starting...
2024-07-14T14:45:34.329-04:00 INFO 12650 --- [main] com.zaxxer.hikari.pool.PoolBase : HikariPool-1 - Driver does not support get/set ne
twork timeout for connections. (feature not supported)
2024-07-14T14:45:34.332-04:00 INFO 12650 --- [main] com.zaxxer.hikari.pool.HikariPool : HikariPool-1 - Added connection org.hsqldb.jdbc.J
DBCConnection@41382722
2024-07-14T14:45:34.337-04:00 INFO 12650 --- [main] com.zaxxer.hikari.HikariDataSource : HikariPool-1 - Start completed.
2024-07-14T14:45:34.464-04:00 INFO 12650 --- [main] o.hibernate.jpa.internal.util.LogHelper : HHH000204: Processing PersistenceUnitInfo [name:
default]
2024-07-14T14:45:34.749-04:00 INFO 12650 --- [main] org.hibernate.Version : HHH0000412: Hibernate ORM core version 6.2.13.Final
2024-07-14T14:45:34.765-04:00 INFO 12650 --- [main] org.hibernate.cfg.Environment : HHH0000406: Using bytecode reflection optimizer
2024-07-14T14:45:35.757-04:00 INFO 12650 --- [main] o.s.o.j.p.SpringPersistenceUnitInfo : No LoadTimeWeaver setup: ignoring JPA class trans
former
2024-07-14T14:45:35.932-04:00 WARN 12650 --- [main] org.hibernate.orm.deprecation : HHH90000025: HSQLDialect does not need to be spec
ified explicitly using 'hibernate.dialect' (remove the property setting and it will be selected by default)
2024-07-14T14:45:39.197-04:00 INFO 12650 --- [main] o.h.e.t.j.p.i.JtaPlatformInitiator : HHH0000489: No JTA platform available (set 'hibern
ate.transaction.jta.platform' to enable JTA platform integration)
2024-07-14T14:45:39.218-04:00 INFO 12650 --- [main] j.LocalContainerEntityManagerFactoryBean : Initialized JPA EntityManagerFactory for persiste
nce unit 'default'
```

Tamamlandığında şu şekilde görünecektir.

```
kali@kali: ~/Downloads

File Actions Edit View Help
2024-07-14T14:45:51.849-04:00 INFO 12650 --- [main] o.o.w.lessons.logging.LogBleedingTask : Password for admin: OWFiYtC3YjYtYzVhYy00OGExLWE5N
jUtZGJhMGMyZlJmWZj
2024-07-14T14:45:52.174-04:00 WARN 12650 --- [main] o.o.w.c.lessons.CourseConfiguration : Lesson: webgoat.title has no endpoints, is this i
ntentionally?
2024-07-14T14:45:53.716-04:00 INFO 12650 --- [main] o.s.b.a.e.web.EndpointLinksResolver : Exposing 3 endpoint(s) beneath base path '/actual
or'
2024-07-14T14:45:53.788-04:00 INFO 12650 --- [main] o.s.s.web.DefaultSecurityFilterChain : Will secure any request with [org.springframework
.security.web.session.DisableEncodeUrlFilter@5c5c7cc4, org.springframework.security.web.context.request.async.WebAsyncManagerIntegrationFilter@6c27e700, org
.springframework.security.web.context.SecurityContextHolderFilter@d66502, org.springframework.security.web.authentication.logout.LogoutFilter@2707c790, org
.springframework.security.oauth2.client.web.OAuth2AuthorizationRequestRedirectFilter@32b112a1, org.springframework.security.oauth2.client.web.OAuth2LoginAuth
enticationFilter@5635bcd2, org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@2b936b04, org.springframework.security.web.s
avedrequest.RequestCacheAwareFilter@78545d40, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@34549979, org.springframew
ork.security.web.authentication.AnonymousAuthenticationFilter@56b9d43f, org.springframework.security.web.access.ExceptionTranslationFilter@2bc16fe2, org.spr
ingframework.security.web.access.intercept.AuthorizationFilter@6dece1f9]
2024-07-14T14:45:57.880-04:00 [main] WARN FileNoUtil : Native subprocess control requires open access to the JDK IO subsystem
Pass '--add-opens java.base/sun.nio.ch=ALL-UNNAMED --add-opens java.base/java.io=ALL-UNNAMED' to enable.
2024-07-14T14:46:04.951-04:00 WARN 12650 --- [main] ion$DefaultTemplateResolverConfiguration : Cannot find template location: classpath:/templat
es/ (please add some templates, check your Thymeleaf configuration, or set spring.thymeleaf.check-template-location=false)
2024-07-14T14:46:05.010-04:00 INFO 12650 --- [main] io.undertow : starting server: Undertow - 2.3.10.Final
2024-07-14T14:46:05.014-04:00 INFO 12650 --- [main] o.s.b.w.e.undertow.UndertowWebServer : Undertow started on port(s) 8080 (http) with cont
ext path '/WebGoat'
2024-07-14T14:46:05.060-04:00 INFO 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : Started StartWebGoat in 18.386 seconds (process r
unning for 44.107)
2024-07-14T14:46:05.064-04:00 WARN 12650 --- [main] org.owasp.webgoat.server.StartWebGoat : Please browse to http://127.0.0.1:8080/WebGoat to
start using WebGoat...
```

<http://127.0.0.1:8080/WebGoat> adresine gidiyoruz.



Username

Username

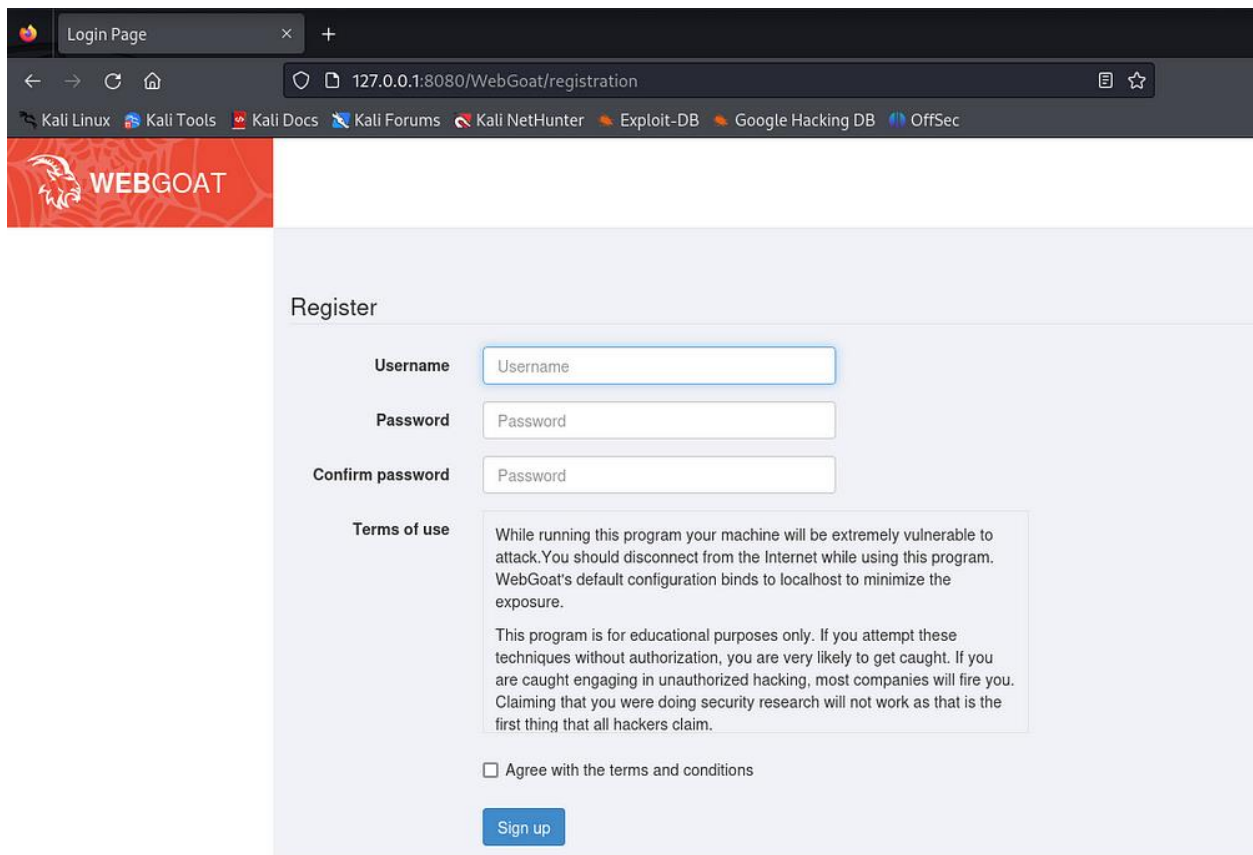
Password

Password

Sign in

[or register yourself as a new user](#)

Register diyerek kayıt oluyoruz.



Register

Username

Username

Password

Password

Confirm password

Password

Terms of use

While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.

This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

☐ Agree with the terms and conditions

Sign up

Kayıt bilgilerini doldurduktan sonra bizi WebGoat'ın ana sayfasına yönlendiriyor.

WEBGOAT

WebWolf



Search lesson

Reset lesson

1 2 3 4

Introducing WebWolf

You only need WebWolf if a lesson specifies that you can use it. For many lessons, you use WebGoat without using WebWolf. Lessons where you can use WebWolf, are marked with the following icon (top right in the assignment):

Even if the icon is present, you are not obliged to use WebWolf. You can also use any intercepting tool you like. (netcat etc.)

You can always open WebWolf by clicking the icon in the top right corner.

WebWolf opens in a new browser tab and is a separate web application that simulates an attacker's machine. It makes it possible for us to distinguish between what takes place on the attacked website and what actions you need to take as an "attacker." The idea for WebWolf came about after a couple of workshops where we received feedback that there was no clear distinction between what was part of the "attackers" role and what was part of the "users" role on the website. WebWolf supports the following functionality:

- Hosting a file
- Receiving email
- Landing page for incoming requests


Böylece WebGoat'ı başarıyla yüklemiş oluyoruz.

(A1) Broken Access Control







Broken Access Control, bir web uygulamasında veya sistemde kullanıcıların erişim kontrol mekanizmalarının doğru şekilde uygulanmaması veya hatalı yapılandırılması durumunu ifade eder. Bu durum, kullanıcıların yetkilerinden daha fazla erişim elde edebilmelerine veya beklenmeyen kaynaklara erişebilmelerine olanak tanır.

Hijack a session

Session hijacking, bir kullanıcının oturum kimlik bilgilerini ele geçirerek veya başka bir şekilde kontrol ederek yetkisiz erişim elde etmesidir.

WEBGOAT

Hijack a session



Introduction >

General >

(A1) Broken Access Control >

Hijack a session

Insecure Direct Object References

Missing Function Level Access Control

Spoofting an Authentication Cookie

(A2) Cryptographic Failures >

(A3) Injection >

(A5) Security Misconfiguration >

(A6) Vuln & Outdated Components >

(A7) Identity & Auth Failure >

(A8) Software & Data Integrity >

(A9) Security Logging Failures >

(A10) Server-side Request Forgery >

Client side >

Challenges >

Reset lesson

1 2 +

Concept

Application developers who develop their own session IDs frequently forget to incorporate the complexity and randomness necessary for security. If the user specific session ID is not complex and random, then the application is highly susceptible to session-based brute force attacks.

Goals

Gain access to an authenticated session belonging to someone else.

Hijack a session

[Show hints](#)[Reset lesson](#)

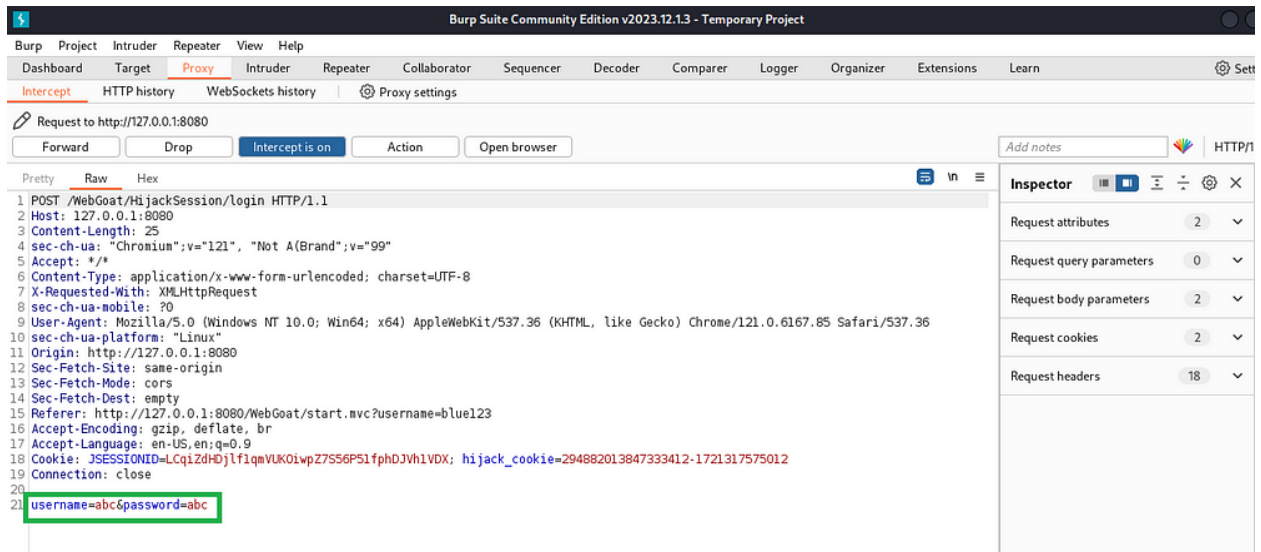
+ 1 2

Account Access






Random bir şeyler girerek Burp Suite'den takip ediyorum ve girmiş olduğum username ve password bilgilerini görüyoruz.



Insecure Direct Object Reference

Kısaca IDOR, bir web uygulamasında veya sisteminde, kullanıcıların doğrudan bir nesneye veya kaynağa (örneğin, veritabanı kaydına veya dosya sistemine) erişmesini sağlayan ve bu erişimi kontrol etmeyen bir güvenlik zafiyetidir. Bu zafiyet, kullanıcıların erişim yetkilerini doğrulamak veya sınırlamak için gerekli kontrollerin eksik veya yetersiz olduğu durumlarda ortaya çıkar.

**WEBGOAT**

- Introduction
- General
- (A1) Broken Access Control
 - Hijack a session
 - Insecure Direct Object References**
 - Missing Function Level Access Control
 - Spoofing an Authentication Cookie
- (A2) Cryptographic Failures
- (A3) Injection
- (A5) Security Misconfiguration
- (A6) Vuln & Outdated Components
- (A7) Identity & Auth Failure
- (A8) Software & Data Integrity
- (A9) Security Logging Failures
- (A10) Server-side Request Forgery
- Client side
- Challenges

Insecure Direct Object Reference

Reset lesson

1

2

3

4

5

6

+

Direct Object References

Direct Object References are when an application uses client-provided input to access data & objects.

Examples

Examples of Direct Object References using the GET method may look something like

<https://some.company.tld/dor?id=12345>

<https://some.company.tld/images?img=12345>

<https://some.company.tld/dor/12345>

Other Methods

POST, PUT, DELETE or other methods are also potentially susceptible and mainly only differ in the method and the potential payload.

Insecure Direct Object References

These are considered insecure when the reference is not properly handled and allows for authorization bypasses or disclose private data that could be used to perform operations or access data that the user should not be able to perform or access. Let's say that as a user, you go to view your profile and the URL looks something like:

<https://some.company.tld/app/user/23398>

... and you can view your profile there. What happens if you navigate to:

<https://some.company.tld/app/user/23399> ... or use another number at the end. If you can manipulate the number (user id) and view

Bize id ve password'ün tom ve cat olduğu söyleniyor. Giriyorum ve tom olarak oturum açıyorum.

123456

Authenticate First, Abuse Authorization Later

Many access control issues are susceptible to attack from an authenticated-but-unauthorized user. So, let's start by legitimately authenticating. Then, we will look for ways to bypass or abuse Authorization.

The id and password for the account in this case are 'tom' and 'cat' (It is an insecure app, right?).

After authenticating, proceed to the next screen.

✓

user/pass user: pass:

You are now logged in as tom. Please proceed.

Burp Suite'den de inceliyorum.

Burp Suite Community Edition v2023.12.13 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:8080

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1

Pretty Raw Hex

1 POST /WebGoat/IDOR/login HTTP/1.1

2 Host: 127.0.0.1:8080

3 Content-Length: 25

4 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"

5 Accept: */*

6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

7 X-Requested-With: XMLHttpRequest

8 sec-ch-ua-mobile: ?0

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

10 sec-ch-ua-platform: "Linux"

11 Origin: http://127.0.0.1:8080

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Dest: empty

15 Referer: http://127.0.0.1:8080/WebGoat/start.mvc?username=blue123

16 Accept-Encoding: gzip, deflate, br

17 Accept-Language: en-US,en;q=0.9

18 Cookie: JSESSIONID=LQqiZdHDjlf1qWVUK0iwpZ7S56P51fphDVh1VOX; hijack_cookie=294882013847333412-1721317575012

19 Connection: close

20

21 username=tom&password=cat

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 2

Request headers 18

Kurulum için takip ettiğim kaynak: <https://vishnushivalalp.medium.com/what-is-webgoat-and-how-to-setup-webgoat-in-linux-2fc91ed325e2>