实验1

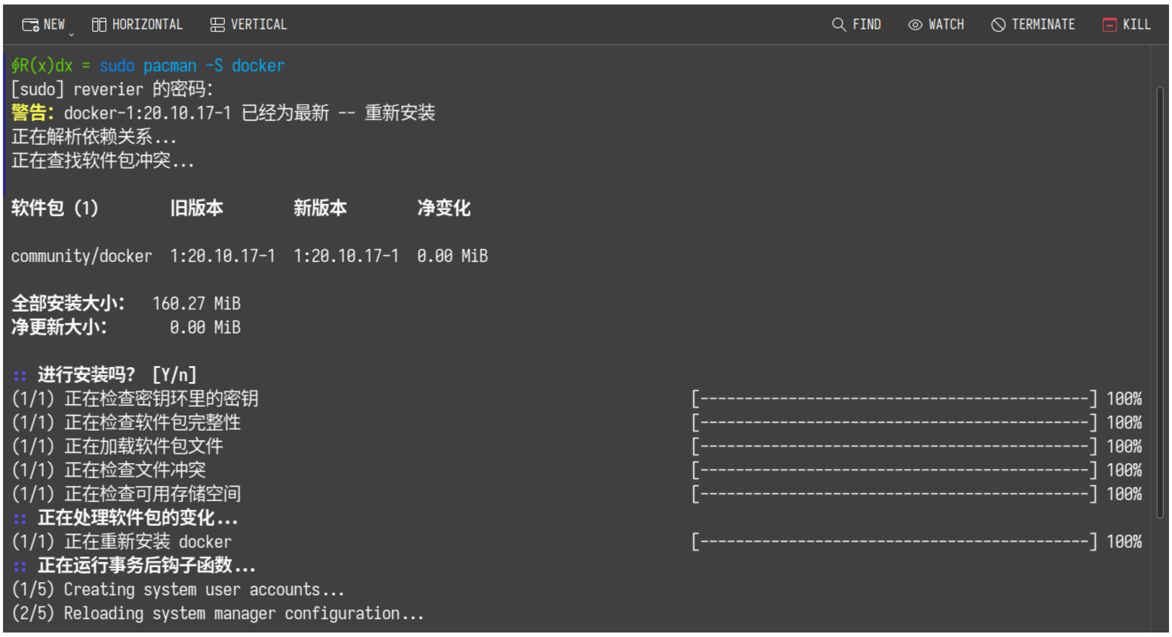
> 21009200991 盖乐

实验过程

实验环境

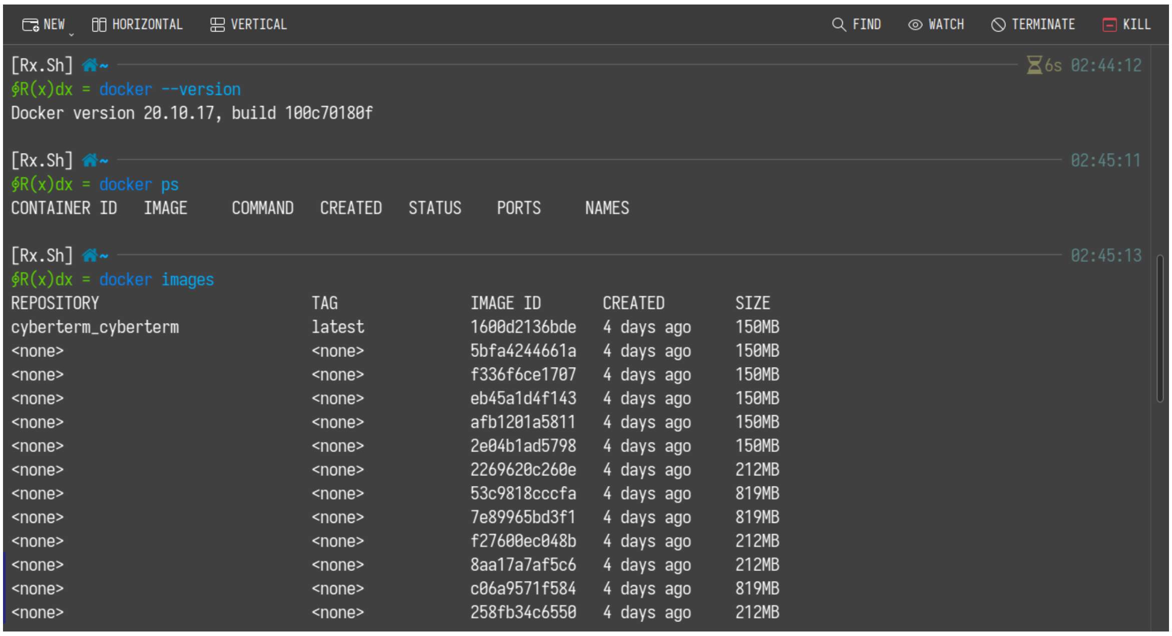
```
                  -`                    Reverier-Xu @ Arch Linux
                 .o+`
                `ooo/                   ===============================
               `+oooo:                  Hardware Information
              `+oooooo:                 MOD  =  AERO 15 Classic-XA
              -+oooooo+:                CPU  =  Intel i7-9750H (12) @ 4.500GHz
            `/:-:++oooo+:               GPU  =  NVIDIA GeForce RTX 2070 Mobile
           `/++++/+++++++:              GPU  =  Intel CoffeeLake-H GT2 [UHD Graphics 630]
          `/++++++++++++++:             RAM  =  4980MiB / 15855MiB (31%)
         `/+++ooooooooooooo/`           ===============================
        ./ooosssso++osssssso+`          Software Information
       .oossssso-````/ossssss+`         KER  =  Linux 5.18.3-arch1-1
      -osssssso.      :ssssssso.        DIS  =  Arch Linux x86_64
     :osssssss/        osssso+++.
    /ossssssss/        +ssssooo/-
  `/ossssso+/:-        -:/+osssso+-
 `+sso+:-`                 `.-/+oso:
`++:.                           `-/+/
```

1，安装docker



```
∮R(x)dx = sudo pacman -S docker
[sudo] reverier 的密码:
警告: docker-1:20.10.17-1 已经为最新 -- 重新安装
正在解析依赖关系...
正在查找软件包冲突...

软件包 (1)        旧版本       新版本       净变化

community/docker  1:20.10.17-1  1:20.10.17-1  0.00 MiB

全部安装大小:   160.27 MiB
净更新大小:       0.00 MiB

:: 进行安装吗? [Y/n]
(1/1) 正在检查密钥环里的密钥                        [--------------------------------------------] 100%
(1/1) 正在检查软件包完整性                          [--------------------------------------------] 100%
(1/1) 正在加载软件包文件                            [--------------------------------------------] 100%
(1/1) 正在检查文件冲突                              [--------------------------------------------] 100%
(1/1) 正在检查可用存储空间                          [--------------------------------------------] 100%
:: 正在处理软件包的变化...
(1/1) 正在重新安装 docker                           [--------------------------------------------] 100%
:: 正在运行事务后钩子函数...
(1/5) Creating system user accounts...
(2/5) Reloading system manager configuration...
```

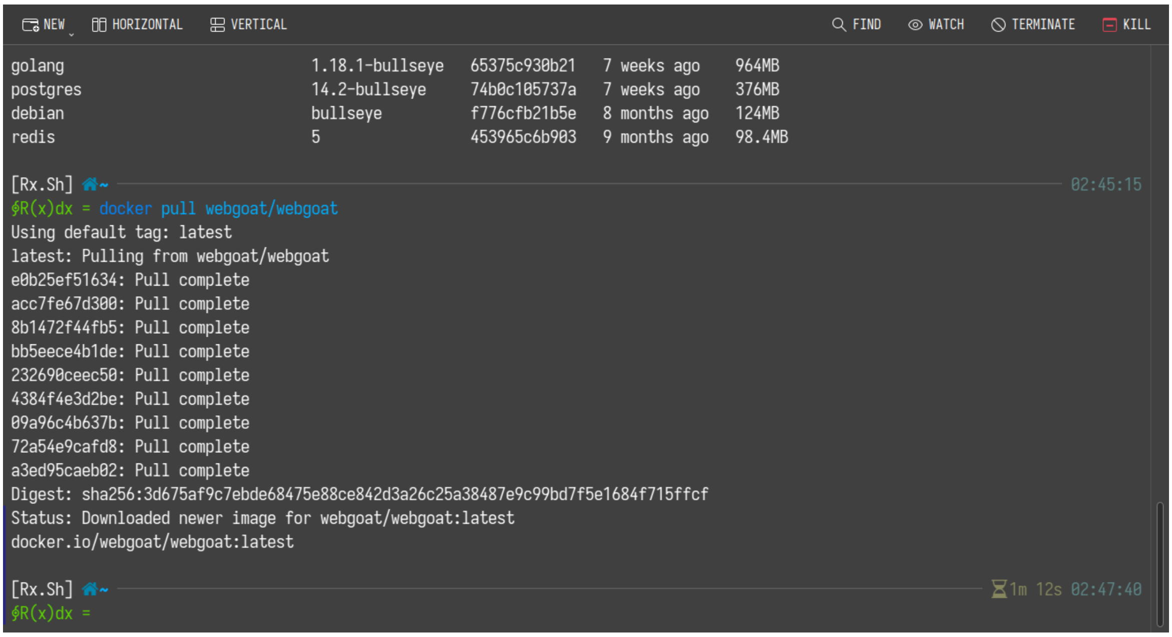
验证：



```
[Rx.Sh] 🏠~ ────────────────────────────────────────────────────── ⌛6s 02:44:12
∮R(x)dx = docker --version
Docker version 20.10.17, build 100c70180f

[Rx.Sh] 🏠~ ─────────────────────────────────────────────────────────── 02:45:11
∮R(x)dx = docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

[Rx.Sh] 🏠~ ─────────────────────────────────────────────────────────── 02:45:13
∮R(x)dx = docker images
REPOSITORY                          TAG                 IMAGE ID       CREATED        SIZE
cyberterm_cyberterm                 latest              1600d2136bde   4 days ago     150MB
<none>                              <none>              5bfa4244661a   4 days ago     150MB
<none>                              <none>              f336f6ce1707   4 days ago     150MB
<none>                              <none>              eb45a1d4f143   4 days ago     150MB
<none>                              <none>              afb1201a5811   4 days ago     150MB
<none>                              <none>              2e04b1ad5798   4 days ago     150MB
<none>                              <none>              2269620c260e   4 days ago     212MB
<none>                              <none>              53c9818cccfa   4 days ago     819MB
<none>                              <none>              7e89965bd3f1   4 days ago     819MB
<none>                              <none>              f27600ec048b   4 days ago     212MB
<none>                              <none>              8aa17a7af5c6   4 days ago     212MB
<none>                              <none>              c06a9571f584   4 days ago     819MB
<none>                              <none>              258fb34c6550   4 days ago     212MB
```

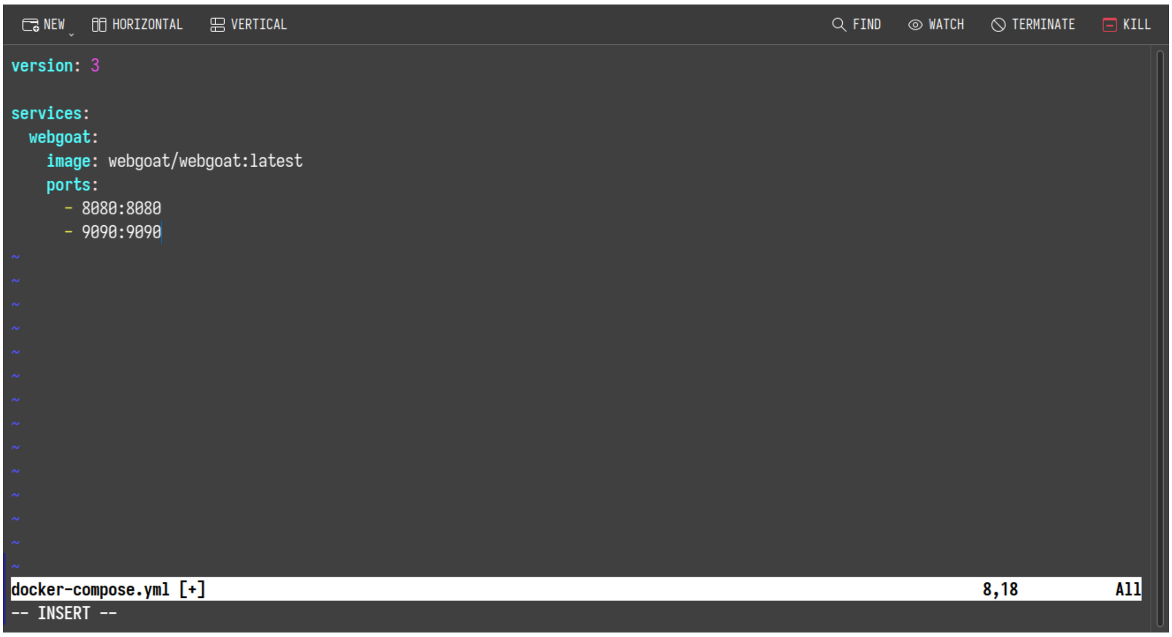
2，部署webgoat镜像

从dockerhub拉取最新的webgoat镜像：

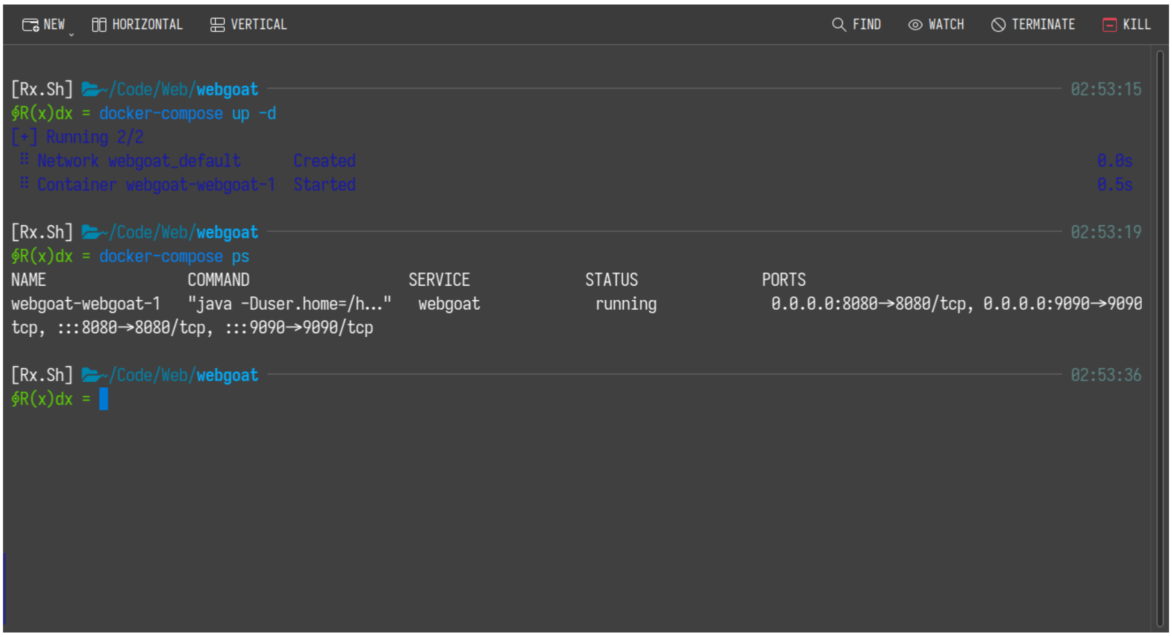


```
golang                              1.18.1-bullseye     65375c930b21   7 weeks ago    964MB
postgres                            14.2-bullseye       74b0c105737a   7 weeks ago    376MB
debian                              bullseye            f776cfb21b5e   8 months ago   124MB
redis                               5                   453965c6b903   9 months ago   98.4MB

[Rx.Sh] 🏠~ ─────────────────────────────────────────────────────────── 02:45:15
∮R(x)dx = docker pull webgoat/webgoat
Using default tag: latest
latest: Pulling from webgoat/webgoat
e0b25ef51634: Pull complete
acc7fe67d300: Pull complete
8b1472f44fb5: Pull complete
bb5eece4b1de: Pull complete
232690ceec50: Pull complete
4384f4e3d2be: Pull complete
09a96c4b637b: Pull complete
72a54e9cafd8: Pull complete
a3ed95caeb02: Pull complete
Digest: sha256:3d675af9c7ebde68475e88ce842d3a26c25a38487e9c99bd7f5e1684f715ffcf
Status: Downloaded newer image for webgoat/webgoat:latest
docker.io/webgoat/webgoat:latest

[Rx.Sh] 🏠~ ───────────────────────────────────────────────── ⌛1m 12s 02:47:40
∮R(x)dx =
```

使用docker-compose托管并启动：

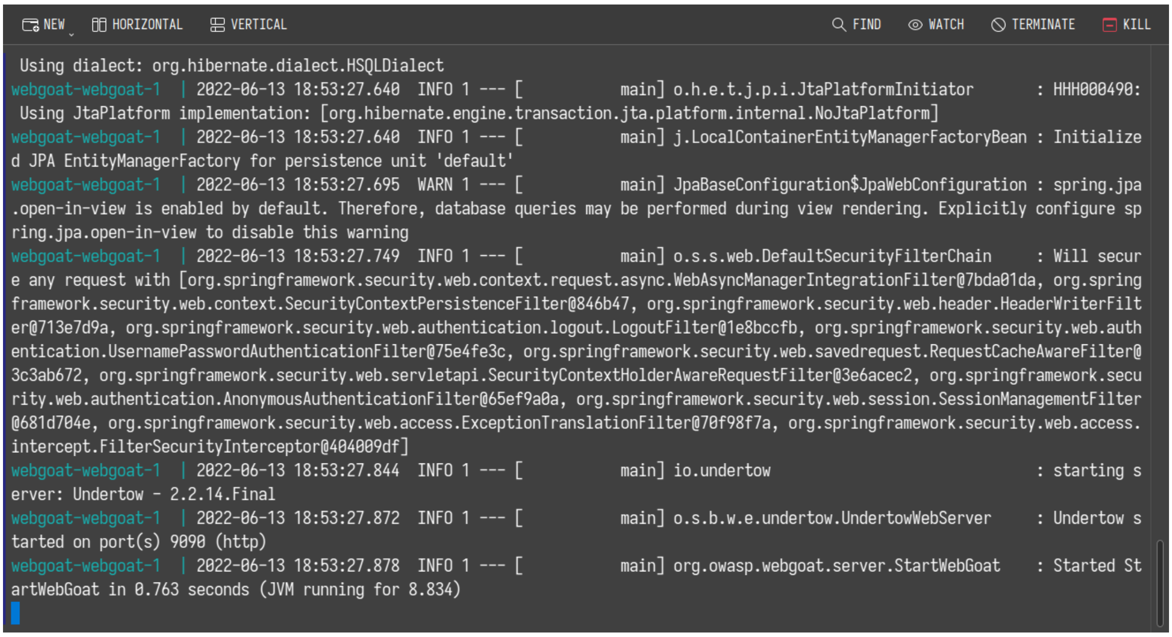


```
version: 3

services:
  webgoat:
    image: webgoat/webgoat:latest
    ports:
      - 8080:8080
      - 9090:9090
~
~
~
~
~
~
~
~
~
~
~
~
~
~
docker-compose.yml [+]                                                                          8,18          All
-- INSERT --
```



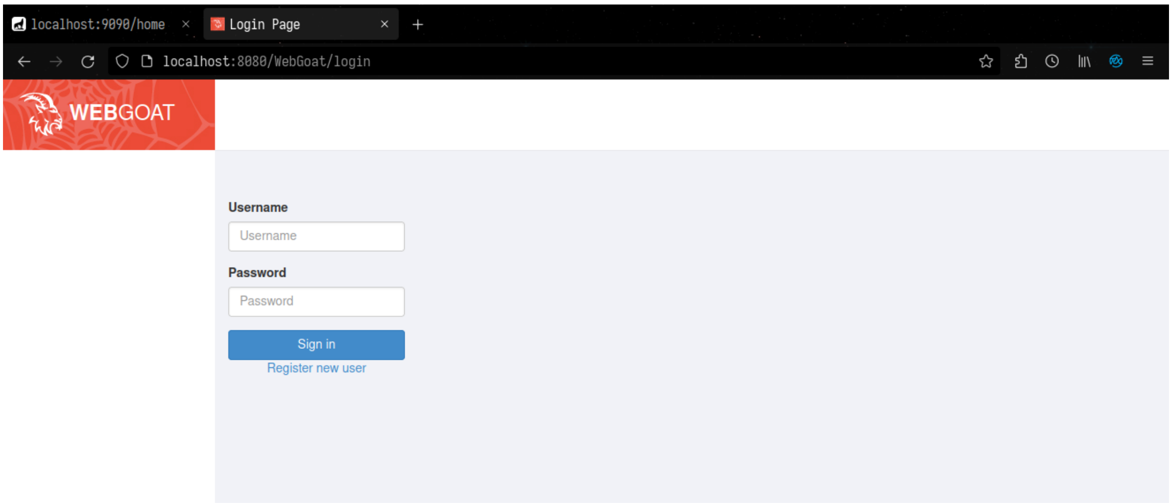
```
[Rx.Sh] ~/Code/Web/webgoat ──────────────────────────────────────────────────────────────────────── 02:53:15
∮R(x)dx = docker-compose up -d
[+] Running 2/2
 ⠿ Network webgoat_default      Created                                                                  0.0s
 ⠿ Container webgoat-webgoat-1  Started                                                                  0.5s

[Rx.Sh] ~/Code/Web/webgoat ──────────────────────────────────────────────────────────────────────── 02:53:19
∮R(x)dx = docker-compose ps
NAME                COMMAND                  SERVICE             STATUS              PORTS
webgoat-webgoat-1   "java -Duser.home=/h…"   webgoat             running             0.0.0.0:8080->8080/tcp, 0.0.0.0:9090->9090
tcp, :::8080->8080/tcp, :::9090->9090/tcp

[Rx.Sh] ~/Code/Web/webgoat ──────────────────────────────────────────────────────────────────────── 02:53:36
∮R(x)dx = 
```

使用`docker-compose logs -f`查看输出：

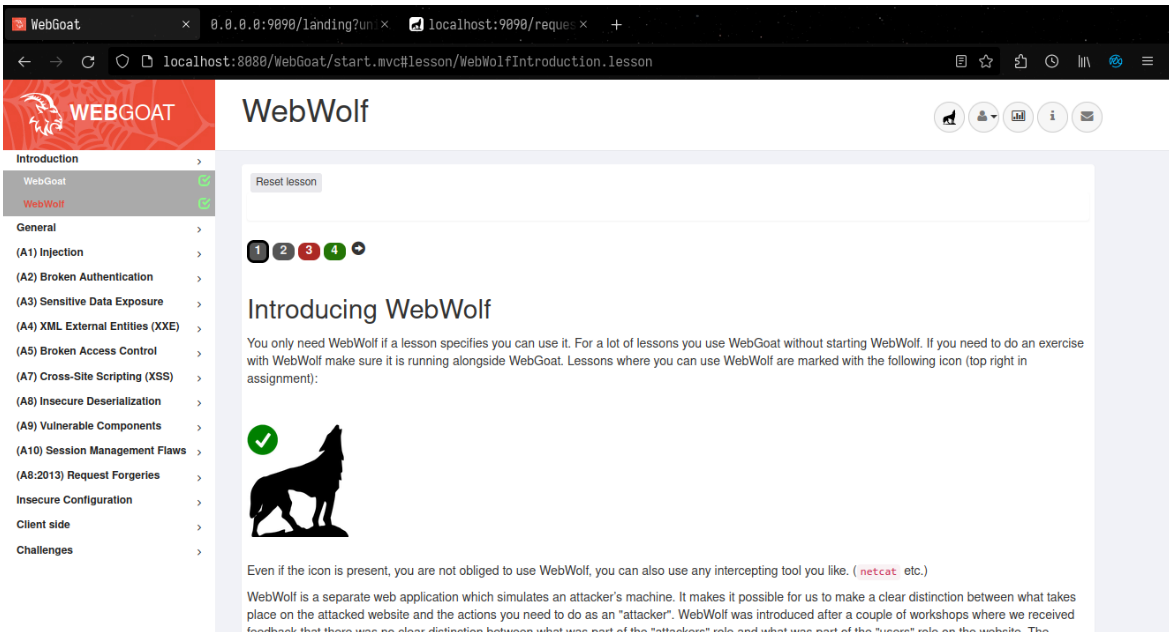


```
 Using dialect: org.hibernate.dialect.HSQLDialect
webgoat-webgoat-1  | 2022-06-13 18:53:27.640  INFO 1 --- [           main] o.h.e.t.j.p.i.JtaPlatformInitiator       : HHH000490:
 Using JtaPlatform implementation: [org.hibernate.engine.transaction.jta.platform.internal.NoJtaPlatform]
webgoat-webgoat-1  | 2022-06-13 18:53:27.640  INFO 1 --- [           main] j.LocalContainerEntityManagerFactoryBean : Initialize
d JPA EntityManagerFactory for persistence unit 'default'
webgoat-webgoat-1  | 2022-06-13 18:53:27.695  WARN 1 --- [           main] JpaBaseConfiguration$JpaWebConfiguration : spring.jpa
.open-in-view is enabled by default. Therefore, database queries may be performed during view rendering. Explicitly configure sp
ring.jpa.open-in-view to disable this warning
webgoat-webgoat-1  | 2022-06-13 18:53:27.749  INFO 1 --- [           main] o.s.s.web.DefaultSecurityFilterChain     : Will secur
e any request with [org.springframework.security.web.context.request.async.WebAsyncManagerIntegrationFilter@7bda01da, org.spring
framework.security.web.context.SecurityContextPersistenceFilter@846b47, org.springframework.security.web.header.HeaderWriterFilt
er@713e7d9a, org.springframework.security.web.authentication.logout.LogoutFilter@1e8bccfb, org.springframework.security.web.auth
entication.UsernamePasswordAuthenticationFilter@75e4fe3c, org.springframework.security.web.savedrequest.RequestCacheAwareFilter@
3c3ab672, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@3e6acec2, org.springframework.secu
rity.web.authentication.AnonymousAuthenticationFilter@65ef9a0a, org.springframework.security.web.session.SessionManagementFilter
@681d704e, org.springframework.security.web.access.ExceptionTranslationFilter@70f98f7a, org.springframework.security.web.access.
intercept.FilterSecurityInterceptor@404009df]
webgoat-webgoat-1  | 2022-06-13 18:53:27.844  INFO 1 --- [           main] io.undertow                              : starting s
erver: Undertow - 2.2.14.Final
webgoat-webgoat-1  | 2022-06-13 18:53:27.872  INFO 1 --- [           main] o.s.b.w.e.undertow.UndertowWebServer     : Undertow s
tarted on port(s) 9090 (http)
webgoat-webgoat-1  | 2022-06-13 18:53:27.878  INFO 1 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Started St
artWebGoat in 0.763 seconds (JVM running for 8.834)
```

环境已经启动成功，打开浏览器进行验证：



完成情况

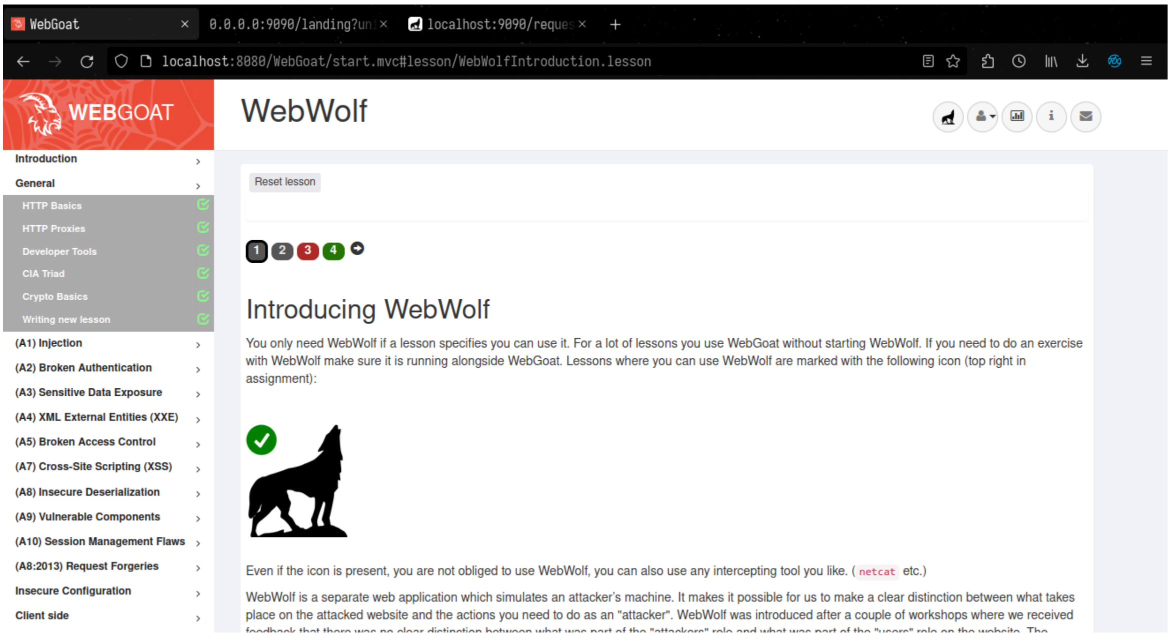

WebGoat
0.0.0.0:9090/landing?uni
localhost:9090/reques
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
Introduction
WebGoat
WebWolf
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
WebWolf
Reset lesson
1 2 3 4

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The

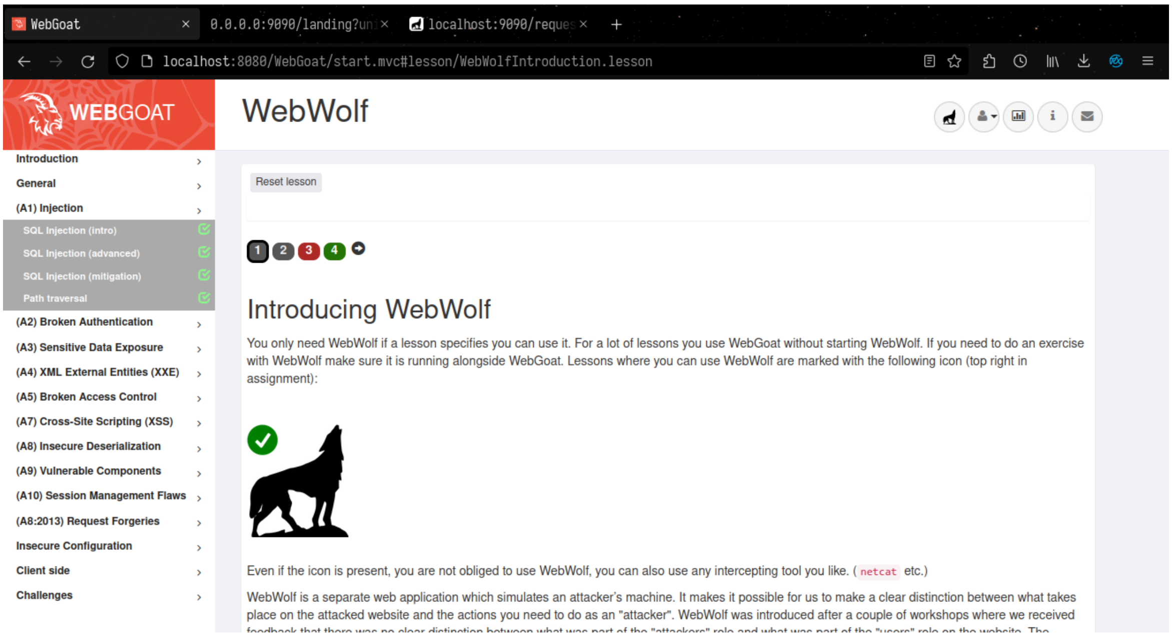

WebGoat
0.0.0.0:9090/landing?uni
localhost:9090/reques
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
Introduction
General
HTTP Basics
HTTP Proxies
Developer Tools
CIA Triad
Crypto Basics
Writing new lesson
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
WebWolf
Reset lesson
1 2 3 4

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The

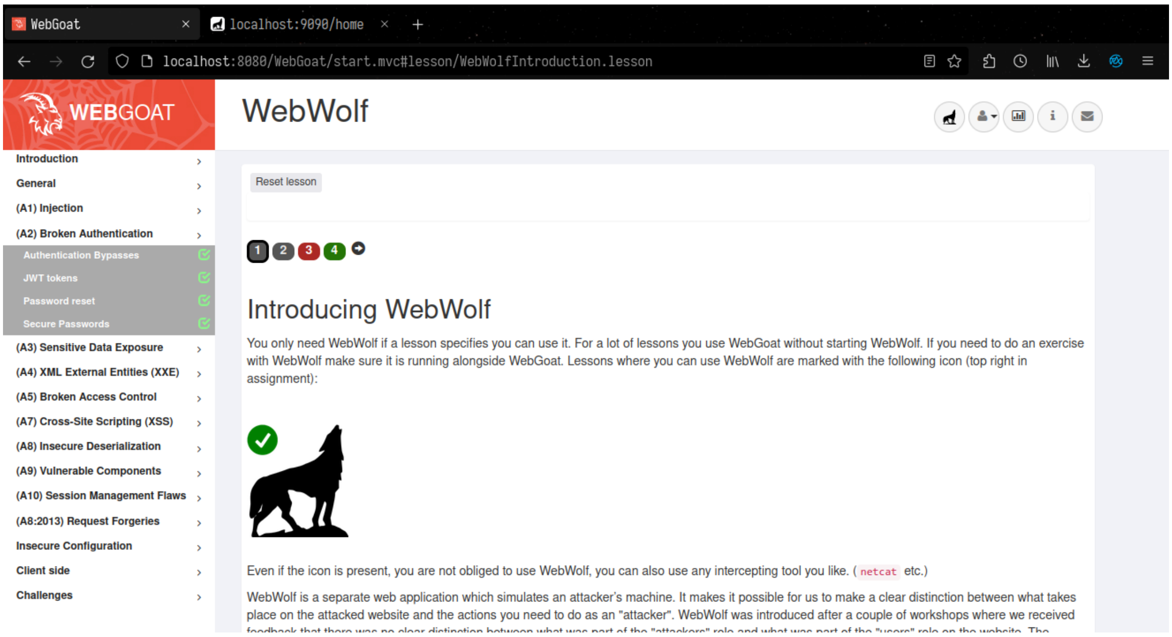

WebGoat
0.0.0.0:9090/landing?un
localhost:9090/reques
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
WebWolf
Introduction
General
(A1) Injection
SQL Injection (intro)
SQL Injection (advanced)
SQL Injection (mitigation)
Path traversal
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
Reset lesson
1 2 3 4

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The

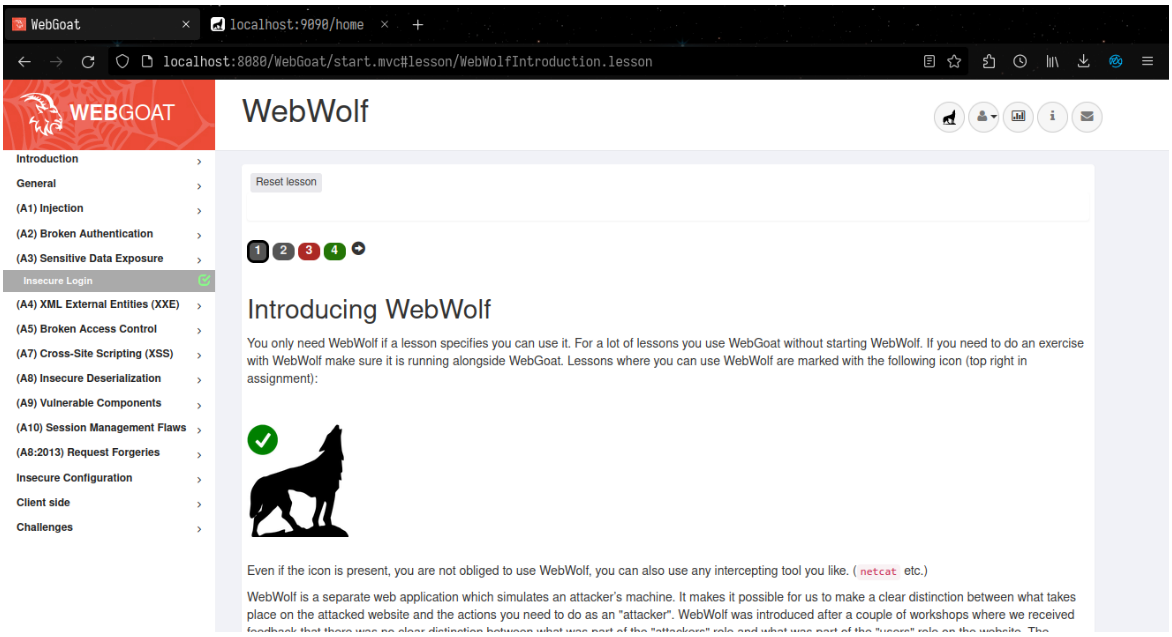

WebGoat
localhost:9090/home
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
WebWolf
Introduction
General
(A1) Injection
(A2) Broken Authentication
Authentication Bypasses
JWT tokens
Password reset
Secure Passwords
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
Reset lesson
1 2 3 4

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The


WebGoat
localhost:9090/home
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
Insecure Login
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
Reset lesson
1 2 3 4

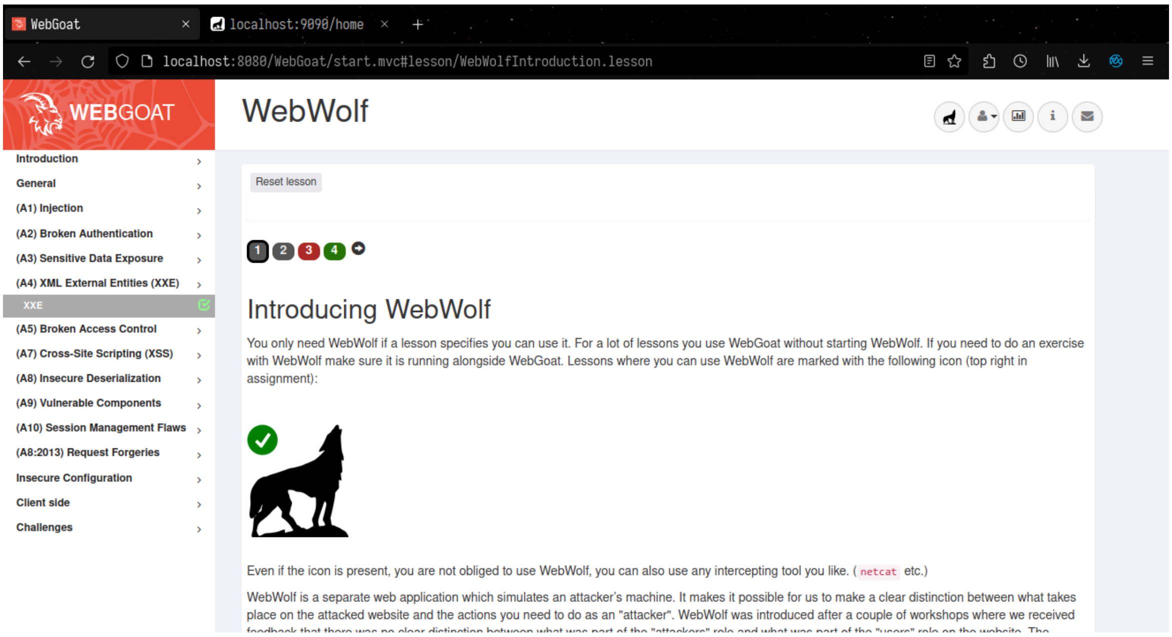
WebWolf

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The


WebGoat
localhost:9090/home
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
XXE
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
Reset lesson
1 2 3 4

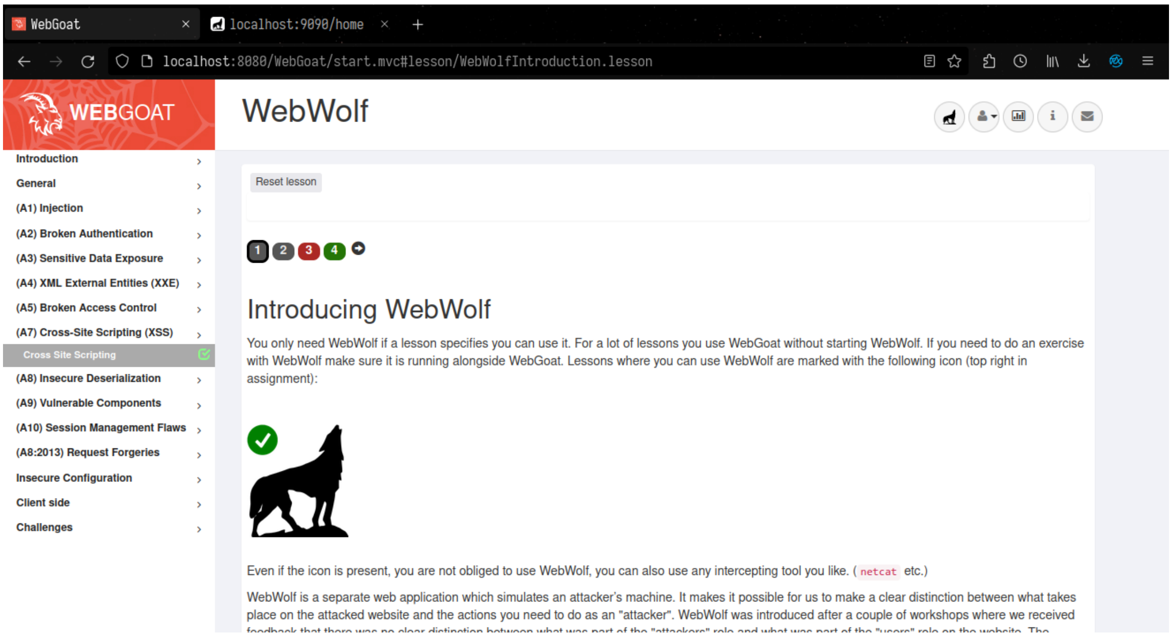
WebWolf

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The


WebGoat
localhost:9090/home
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson
WEBGOAT
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
Cross Site Scripting
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A10) Session Management Flaws
(A8:2013) Request Forgeries
Insecure Configuration
Client side
Challenges
WebWolf
Reset lesson
1
2
3
4

Introducing WebWolf

You only need WebWolf if a lesson specifies you can use it. For a lot of lessons you use WebGoat without starting WebWolf. If you need to do an exercise with WebWolf make sure it is running alongside WebGoat. Lessons where you can use WebWolf are marked with the following icon (top right in 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.)

WebWolf is a separate web application which simulates an attacker's machine. It makes it possible for us to make a clear distinction between what takes place on the attacked website and the actions you need to do as an "attacker". WebWolf was introduced 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. The