



% docker for **hackers**
intro, tips, tricks and fun things you can do



```
% id
```

```
uid=0 gid=hacker username=@syndrowm euid=root job=technology,founder
```



Docker is an open platform for developing, shipping, and running applications.

Docker takes advantage of several features of the Linux kernel to deliver its functionality.



```
% uname -a
```

```
Darwin evans-MacBook-Air.local 22.3.0 Darwin Kernel Version 22.3.0: Mon Jan 30  
20:39:35 PST 2023; root:xnu-8792.81.3~2/RELEASE_ARM64_T8103 arm64
```

```
% docker run --platform linux/amd64 -it ubuntu:22.04 bash
```

```
root@f8eb9d320b9b:/# uname -a
```

```
Linux f8eb9d320b9b 5.15.49-linuxkit #1 SMP PREEMPT Tue Sep 13 07:51:32 UTC 2022  
x86_64 x86_64 x86_64 GNU/Linux
```



```
% docker help
```

```
Usage:  docker [OPTIONS] COMMAND
```

```
A self-sufficient runtime for containers
```

```
Options:
```

```
    --config string          Location of client config files (default Management
```

```
...

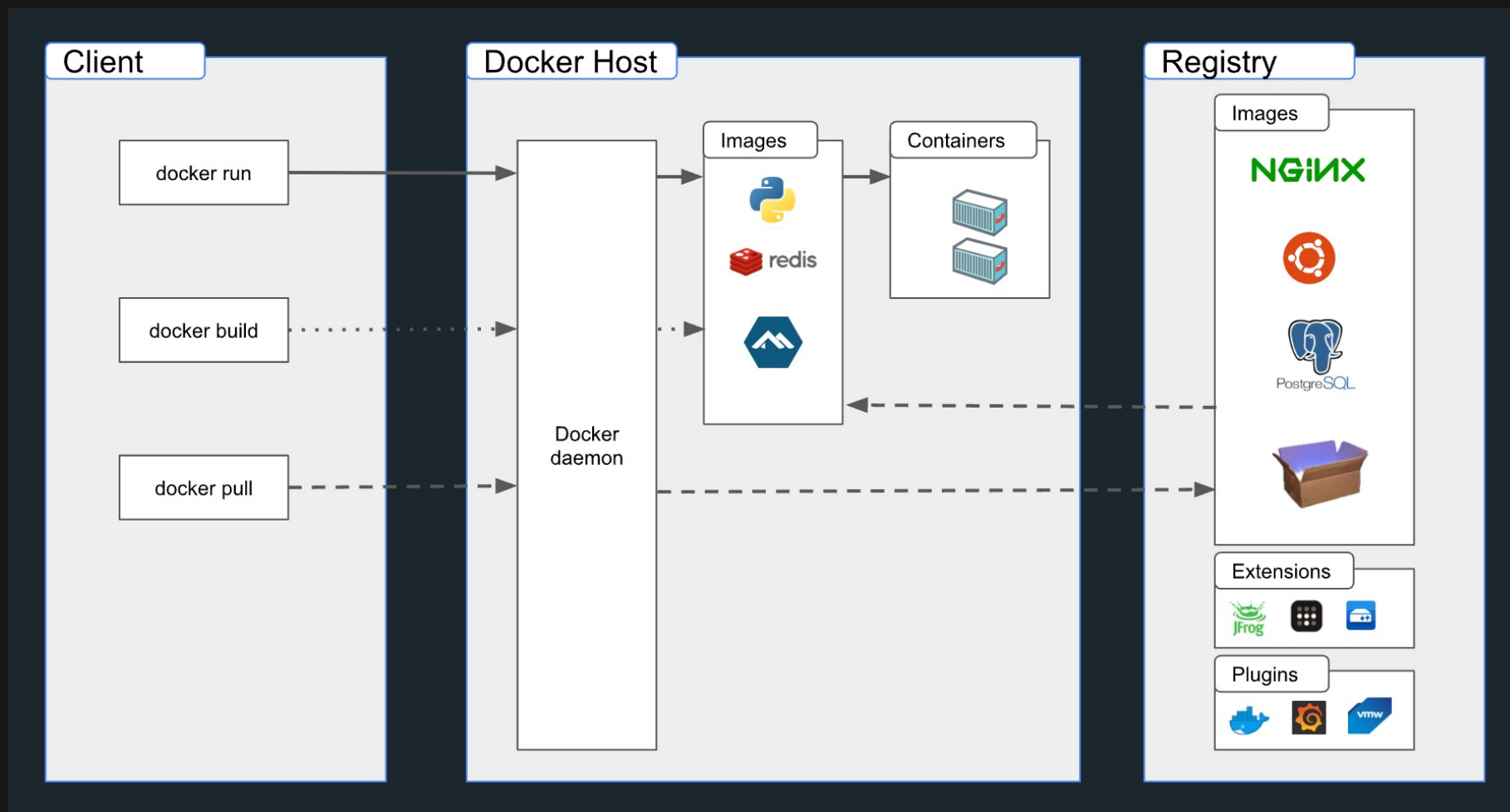
```

```
Commands:
```

builder	Manage builds
buildx*	Docker Buildx (Docker Inc., v0.10.0)
compose*	Docker Compose (Docker Inc., v2.15.1)
config	Manage Docker configs
container	Manage containers
context	Manage contexts

```
...

```





```
% docker ps
```

```
Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the  
docker daemon running?
```



```
% docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
ubuntu	<none>	3c2df5585507	4 months ago	69.2MB
ubuntu	22.04	a8780b506fa4	4 months ago	77.8MB



```
% docker container list
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
e9724eee3b6c	ubuntu:22.04	"bash"	About an hour ago	Up About an hour		busy_bhabh



```
% docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
e9724eee3b6c	ubuntu:22.04	"bash"	About an hour ago	Up About an hour		busy_bhabh



```
% docker network ls
```

NETWORK ID	NAME	DRIVER	SCOPE
80e852e3908b	bridge	bridge	local
9c7395f42c0d	host	host	local
36632286003d	none	null	local



```
% docker run -it python:3.11 bash
root@7709f12587bf:/# python
Python 3.11.2 (main, Mar 1 2023, 10:41:09) [GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```



```
% docker run --platform linux/amd64 -it ubuntu:22.04 bash
root@f8eb9d320b9b:/# uname -a
Linux f8eb9d320b9b 5.15.49-linuxkit #1 SMP PREEMPT Tue Sep 13 07:51:32 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
```



```
$ sudo apt-get install qemu binfmt-support qemu-user-static # Install the qemu packages
```



```
% docker run -it --privileged --pid=host debian nsenter -t 1 -m -u -n -i sh
/ # uname -a
Linux docker-desktop 5.15.49-linuxkit #1 SMP PREEMPT Tue Sep 13 07:51:32 UTC 2022 aarch64 Linux
/ #
```



```
% docker run -it --platform linux/amd64 --volume $PWD:/w -w /w ubuntu:22.04 bash
root@ce0e2c61b5ec:/w# ls -al
total 8
drwxr-xr-x 3 root root  96 Mar  8 22:12 .
drwxr-xr-x 1 root root 4096 Mar  8 22:17 ..
-rw-r--r-- 1 root root  115 Mar  8 22:12 main.c
```




```
% docker run -it --platform linux/amd64 -v $PWD:/w --workdir /w ubuntu:22.04 bash
root@ce0e2c61b5ec:/w# ls -al
total 8
drwxr-xr-x 3 root root  96 Mar  8 22:12 .
drwxr-xr-x 1 root root 4096 Mar  8 22:17 ..
-rw-r--r-- 1 root root  115 Mar  8 22:12 main.c
```



```
% docker run -it --platform linux/amd64 -v $PWD:/w -w /w ubuntu:22.04 bash
root@e9724eee3b6c:/w# apt-get update && apt-get install build-essential
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
...
root@e9724eee3b6c:/w# gcc -static -o exploit fancy_LPE.c
root@e9724eee3b6c:/w# exit
% file exploit
exploit: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically
linked, BuildID[sha1]=7a265e2f07601b4fd630fac4265278da7fb325c0, for GNU/Linux
3.2.0, not stripped
```



```
% cat Dockerfile
FROM ubuntu:22.04
ENV DEBIAN_FRONTEND=noninteractive
RUN apt-get update && \
    apt-get install -y build-essential file iproute2
CMD ["bash"]
```



```
% docker build -t builder --platform linux/amd64 .  
[+] Building 32.5s (6/6) FINISHED  
=> [internal] load build definition from Dockerfile  
=> => transferring dockerfile: 179B  
=> [internal] load .dockerignore  
=> => transferring context: 2B  
=> [internal] load metadata for docker.io/library/ubuntu:22.04  
=> [1/2] FROM  
docker.io/library/ubuntu:22.04@sha256:2adf22367284330af9f832ffefb717c78239f6251d9d0f58de50b86229ed1427  
=> => resolve  
docker.io/library/ubuntu:22.04@sha256:2adf22367284330af9f832ffefb717c78239f6251d9d0f58de50b86229ed1427  
=> => sha256:730eeb702b69e53ae1c79541a48af6303d1bd240014dc6b4208ee4f3fab7b681 2.32kB / 2.32kB  
=> => sha256:d0a4bfa485d176c141f6b88493559f4802a12bdeb8249869bfc276bc48a3db35 27.35MB / 27.35MB  
=> => sha256:2adf22367284330af9f832ffefb717c78239f6251d9d0f58de50b86229ed1427 1.13kB / 1.13kB  
=> => sha256:b885cc8d4c735d3f407f4318c7ba917f4d95e90599238b25705fa0052490216e 424B / 424B  
=> => extracting sha256:d0a4bfa485d176c141f6b88493559f4802a12bdeb8249869bfc276bc48a3db35  
=> [2/2] RUN apt-get update && apt-get install -y build-essential file  
=> exporting to image  
=> => exporting layers  
=> => writing image sha256:2d214b845e4cf660c34c7216d0bf6202303aeff37a34fa097304f96d82e7fdae  
=> => naming to docker.io/library/buildbox
```



Architectures officially supported by Docker, Inc.

- * ARMv6 32-bit (arm32v6): <https://hub.docker.com/u/arm32v6/>
- * ARMv7 32-bit (arm32v7): <https://hub.docker.com/u/arm32v7/>
- * ARMv8 64-bit (arm64v8): <https://hub.docker.com/u/arm64v8/>
- * Linux x86-64 (amd64): <https://hub.docker.com/u/amd64/>
- * Windows x86-64 (windows-amd64): <https://hub.docker.com/u/winamd64/>

Other architectures built by official images:

- * ARMv5 32-bit (arm32v5): <https://hub.docker.com/u/arm32v5/>
- * IBM POWER8 (ppc64le): <https://hub.docker.com/u/ppc64le/>
- * IBM z Systems (s390x): <https://hub.docker.com/u/s390x/>
- * MIPS64 LE (mips64le): <https://hub.docker.com/u/mips64le/>
- * RISC-V 64-bit (riscv64): <https://hub.docker.com/u/riscv64/>
- * x86/i686 (i386): <https://hub.docker.com/u/i386/>

https://github.com/dockcross/dockcross

☰ README.md

dockcross

Cross compiling toolchains in Docker images.

🔄 Dockcross CI passing 🔄 Shellcheck CI passing

license MIT commit activity 173/year


Features

- Pre-built and configured toolchains for cross compiling.
- Most images also contain an emulator for the target system.
- Clean separation of build tools, source code, and build artifacts.





hub.docker.com/search?q=kalilinux



Filters



Products

☐ Images


☐ Extensions

☐ Plugins




Trusted Content

☐  Docker Official Image 

1 - 25 of 174 results for **kalilinux**.



kalilinux/kali-rolling

 SPONSORED OSS ·  5M+ ·  634

By Kali · Updated 4 days ago

Official Kali Linux Docker image (weekly snapshot of kali-rolling)

Linux x86-64 arm arm64 386



```
% docker run --rm -it kalilinux/kali-rolling bash
Unable to find image 'kalilinux/kali-rolling:latest' locally
latest: Pulling from kalilinux/kali-rolling
37c459033527: Pull complete
Digest: sha256:334e48190163888e8b0588d40031c5ac193d9a501be587856051f9ecbadea1dd
Status: Downloaded newer image for kalilinux/kali-rolling:latest
└─(root@fbb97a3a3388)-[/]
└─#
```




```
% docker run --rm -it kalilinux/kali-rolling bash
Unable to find image 'kalilinux/kali-rolling:latest' locally
latest: Pulling from kalilinux/kali-rolling
37c459033527: Pull complete
Digest: sha256:334e48190163888e8b0588d40031c5ac193d9a501be587856051f9ecbadea1dd
Status: Downloaded newer image for kalilinux/kali-rolling:latest
└─(root@fbb97a3a3388)-[/]
└─#
```



```
% docker network ls
```

NETWORK ID	NAME	DRIVER	SCOPE
80e852e3908b	bridge	bridge	local
9c7395f42c0d	host	host	local
36632286003d	none	null	local



```
% docker run --rm -it --network none buildbox bash
root@cee09de08855:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
3: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
    link/tunnel6 :: brd :: permaddr f2ad:67f9:fd53::
root@cee09de08855:/#
```

```
% docker run --rm -i -t --network host kalilinux/kali-rolling bash
```

```
└─(root@docke-desktop)-[/]
```

```
# ip a
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
3: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
    link/tunnel6 :: brd :: permaddr eef8:ae2b:a2e::
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:89:08:8e:65 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:89ff:fe08:8e65/64 scope link
        valid_lft forever preferred_lft forever
8: eth0@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 8a:a3:ef:66:84:e7 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.65.4 peer 192.168.65.5/32 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::88a3:efff:fe66:84e7/64 scope link
        valid_lft forever preferred_lft forever
```





Compose is a tool for defining and running multi-container Docker applications.

With Compose, you use a YAML file to configure your application's services.

Then, with a single command, you create and start all the services from your configuration.



PUBLIC
100.126.0.0/27

PRivate
10.10.10.0/27



OWASP Juice Shop



```
version: "3.9"

services:

  # This will be our public target
  juice-shop:
    image: bkimminich/juice-shop
    ports:
      - 3000:3000
    networks:
      - public
      - private

  # This will be our private target
  web-dvwa:
    image: vulnerables/web-dvwa
    ports:
      - 8000:80
    networks:
      - private

  # This is our attacker system
  kali:
    build: ./kali
    command: tail -f /dev/null
    networks:
      - public

networks:
  public:
    ipam:
      driver: default
      config:
        - subnet: 100.126.0.0/27
  private:
    ipam:
      driver: default
      config:
        - subnet: 10.10.10.0/27
```





```
networks:
  public:
    ipam:
      driver: default
      config:
        - subnet: 100.126.0.0/27
  private:
    ipam:
      driver: default
      config:
        - subnet: 10.10.10.0/27
```




```
# This will be our public target
juice-shop:
  image: bkimminich/juice-shop
  ports:
    - 3000:3000
  networks:
    - public
    - private
```



```
# This will be our private target
web-dvwa:
  image: vulnerables/web-dvwa
  ports:
    - 8000:80
  networks:
    - private
```



```
# This is our attacker system
kali:
  build: ./kali
  command: tail -f /dev/null
  networks:
    - public
```



% **docker compose up**

[+] Running 3/4

⌘ Container docker-for-hackers-web-dvwa-1

⌘ Container docker-for-hackers-kali-1

⌘ Container docker-for-hackers-juice-shop-1

⌘ web-dvwa The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm64)

Attaching to docker-for-hackers-juice-shop-1, docker-for-hackers-kali-1, docker-for-hackers-web-dvwa-1

docker-for-hackers-web-dvwa-1 | [+] Starting mysql...

docker-for-hackers-juice-shop-1 | info: All dependencies in ./package.json are satisfied (OK)

docker-for-hackers-juice-shop-1 | info: Chatbot training data botDefaultTrainingData.json validated (OK)

docker-for-hackers-juice-shop-1 | info: Detected Node.js version v18.14.0 (OK)

docker-for-hackers-juice-shop-1 | info: Detected OS linux (OK)



```
% docker compose ps
```

NAME	IMAGE	COMMAND	SERVICE	CREATED	STATUS	PORTS
docker-for-hackers-juice-shop-1	bkimminich/juice-shop	"/nodejs/bin/node /j..."	juice-shop	7 minutes ago	Up 7 minutes	0.0.0.0:3000->3000/tcp
docker-for-hackers-kali-1	docker-for-hackers-kali	"tail -f /dev/null"	kali	7 minutes ago	Up 7 minutes	
docker-for-hackers-web-dvwa-1	vulnerables/web-dvwa	"/main.sh"	web-dvwa	7 minutes ago	Up 7 minutes	0.0.0.0:8000->80/tcp



OWASP Juice Shop



localhost:3000/#/

Account EN

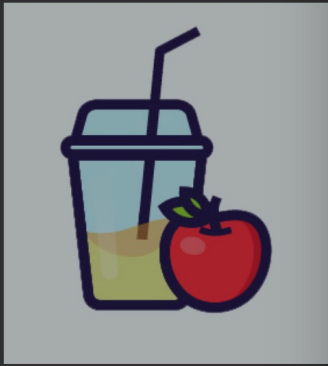
Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the **OWASP Juice Shop** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The **OWASP Juice Shop** is an open-source project hosted by the non-profit [Open Web Application Security Project \(OWASP\)](#) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.


<https://owasp-juice.shop>

All Products



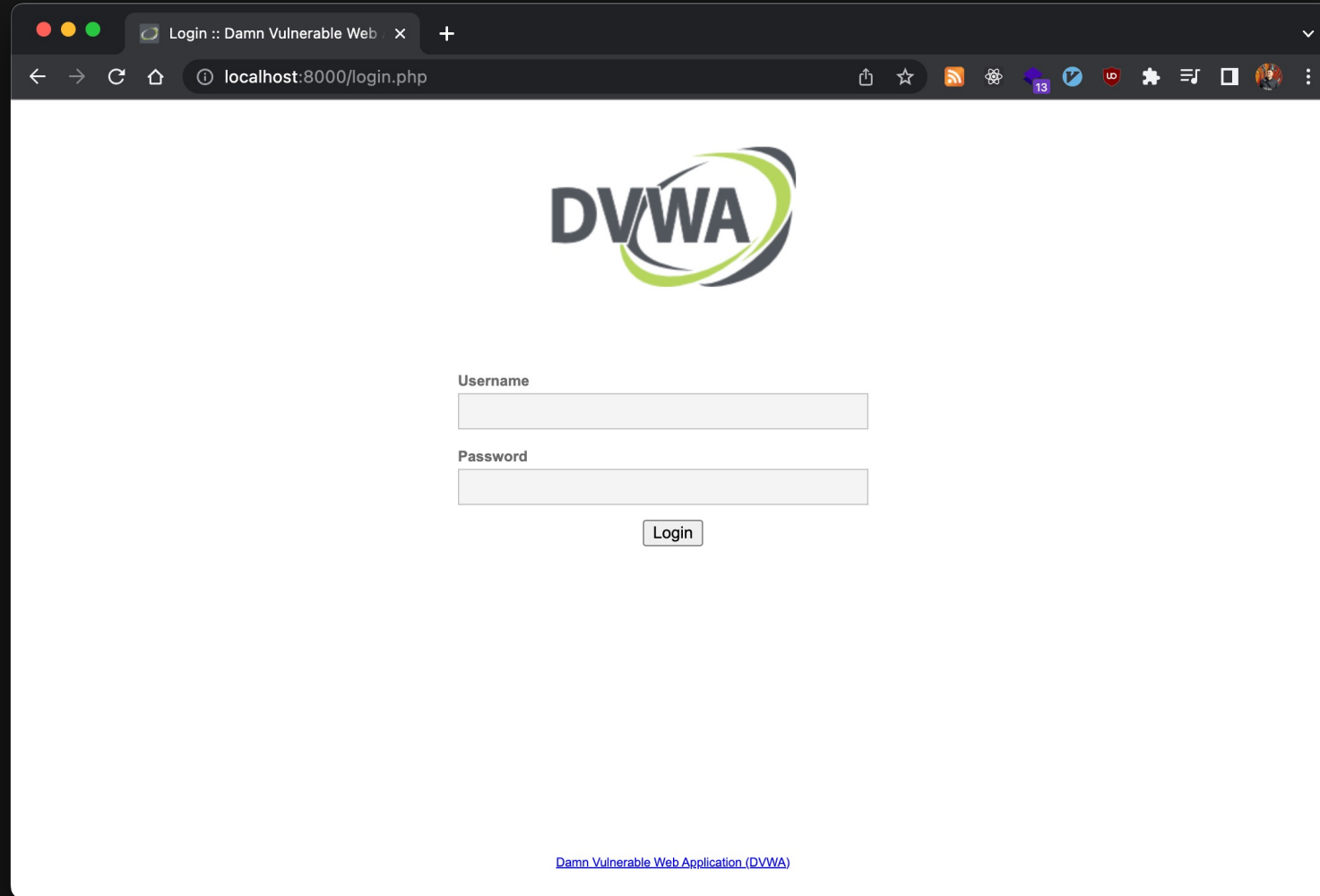
Apple Pomace
0.89€



Only 1 left

This website uses fruit cookies to ensure you get the juiciest tracking experience. [But me wait!](#)

Me want it!





```
% docker compose exec kali bash
```

```
└─(root@fdb6420e87a8)-[/]
```

```
└─# nmap 100.126.0.3
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 19:35 UTC
```

```
Nmap scan report for docker-for-hackers-juice-shop-1.docker-for-hackers_public (100.126.0.3)
```

```
Host is up (0.0000080s latency).
```

```
Not shown: 999 closed tcp ports (reset)
```

```
PORT      STATE SERVICE
```

```
3000/tcp  open  ppp
```

```
MAC Address: 02:42:64:7E:00:03 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```








```
% docker run --rm -it --network docker-for-hackers_private docker-for-hackers-kali bash
└─(root@a9e0ff714048)-[/]
└─# ip a s eth0
109: eth0@if110: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0a:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.10.4/27 brd 10.10.10.31 scope global eth0
        valid_lft forever preferred_lft forever
```




 Containers

 Images

 Volumes

 Dev Environments BETA

Extensions

 Add Extensions

Containers




























[Give feedback](#) 

A container packages up code and its dependencies so the application runs quickly and reliably from one computing environment to another. [Learn more](#)

☐ Only show running containers

 Search



<input type="checkbox"/>	Name	Image	Status	Port(s)	Last started	Actions
<input type="checkbox"/>	 docker-for-hackers	-	Running (4/4)		35 seconds ago	  
<input type="checkbox"/>	 web-dvwa-1 c6114bd50eec  	vulnerables/web-dvwa	Running	8000:80 	2 minutes ago	  
<input type="checkbox"/>	 juice-shop-1 ab3748f35e03 	bkimminich/juice-shop	Running	3000:3000 	2 minutes ago	  
<input type="checkbox"/>	 kali-1 554358ca21cb 	docker-for-hackers-kali	Running		2 minutes ago	  
<input type="checkbox"/>	 goofy_germain 040aaa41b6c6 	docker-for-hackers-kali	Running		35 seconds ago	  



```
% docker compose down
```

```
[+] Running 5/3
```

```
:: Container docker-for-hackers-kali-1    Removed
:: Container docker-for-hackers-juice-shop-1 Removed
:: Container docker-for-hackers-web-dvwa-1 Removed
:: Network docker-for-hackers_private    Removed
:: Network docker-for-hackers_public     Removed
```



```
% docker kill $(docker ps -q) 2>/dev/null  
e27e0d92e918  
% docker rm $(docker ps -aq) 2>/dev/null  
E27e0d92e918  
% docker rmi $(docker images -q) 2>/dev/null
```



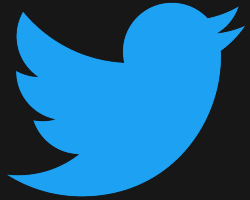
Docker is an open platform for developing, shipping, and running applications.

Docker takes advantage of several features of the Linux kernel to deliver its functionality.

Thank you!



github.com/syndrowm/docker-for-hackers



[syndrowm](https://twitter.com/syndrowm)