UbuCon Asia 2025

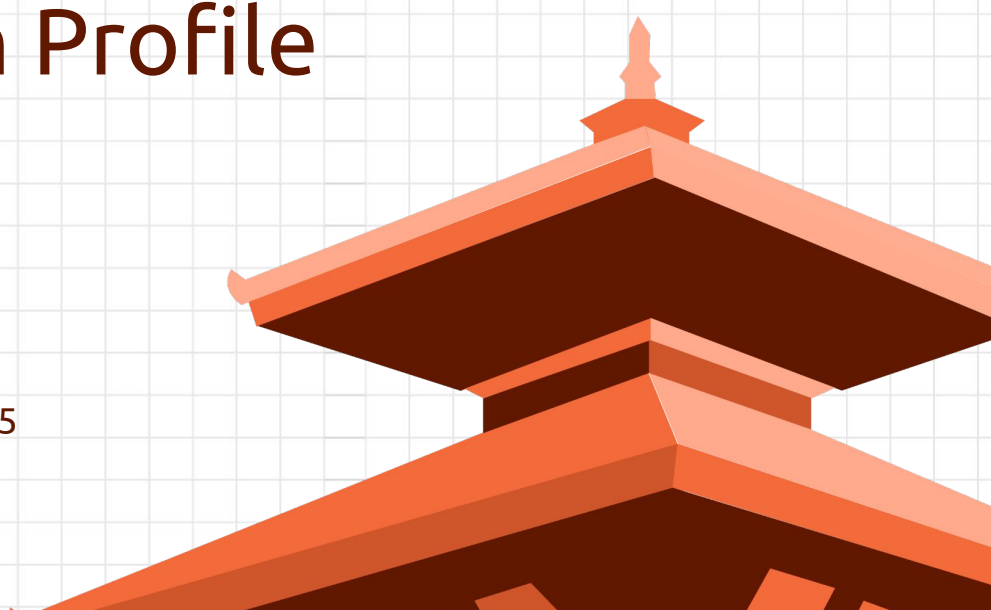
GNOME NEPAL

Apparmor in Action

Building Application Profile

Shishir Subedi @shishirsub10
Ubuntu Security Engineer, Canonical

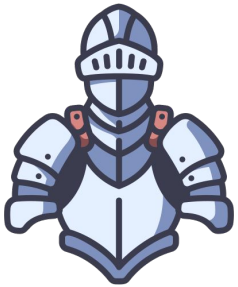
UbuCon Asia 2025 – Kathmandu – 30 August 2025



Ubuntu Security Engineer

Patching

Supply Chain



Apparmor

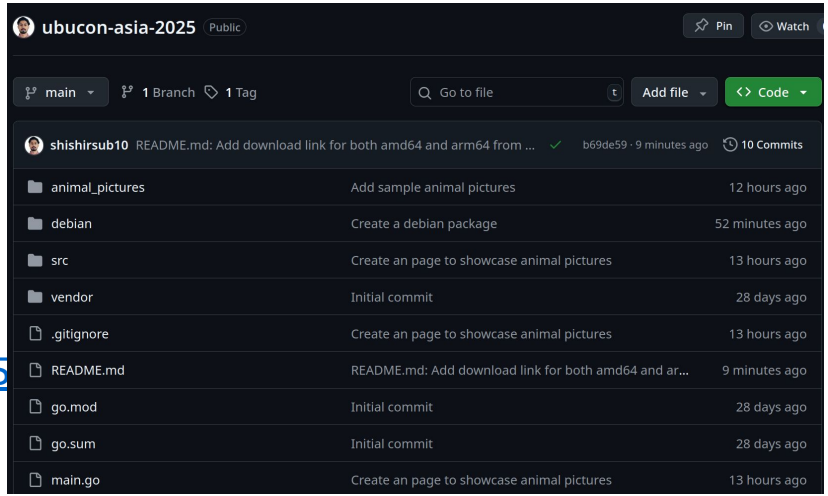
What we will do today?

- Play with a vulnerable app
- Introduction to apparmor
- Your first apparmor profile
- Break and fix things
- Learn how to contribute to profiles upstream

Our intentionally vulnerable app

- A small web application written in Go + Gin
- Deliberately vulnerable by design
- Source code hosted on GitHub:

  👉https://github.com/shishirsub10/ubucon-asia-2025
- Disclaimer:
  - Run in a VM if possible
  - Do not run the application in all interfaces



Installation

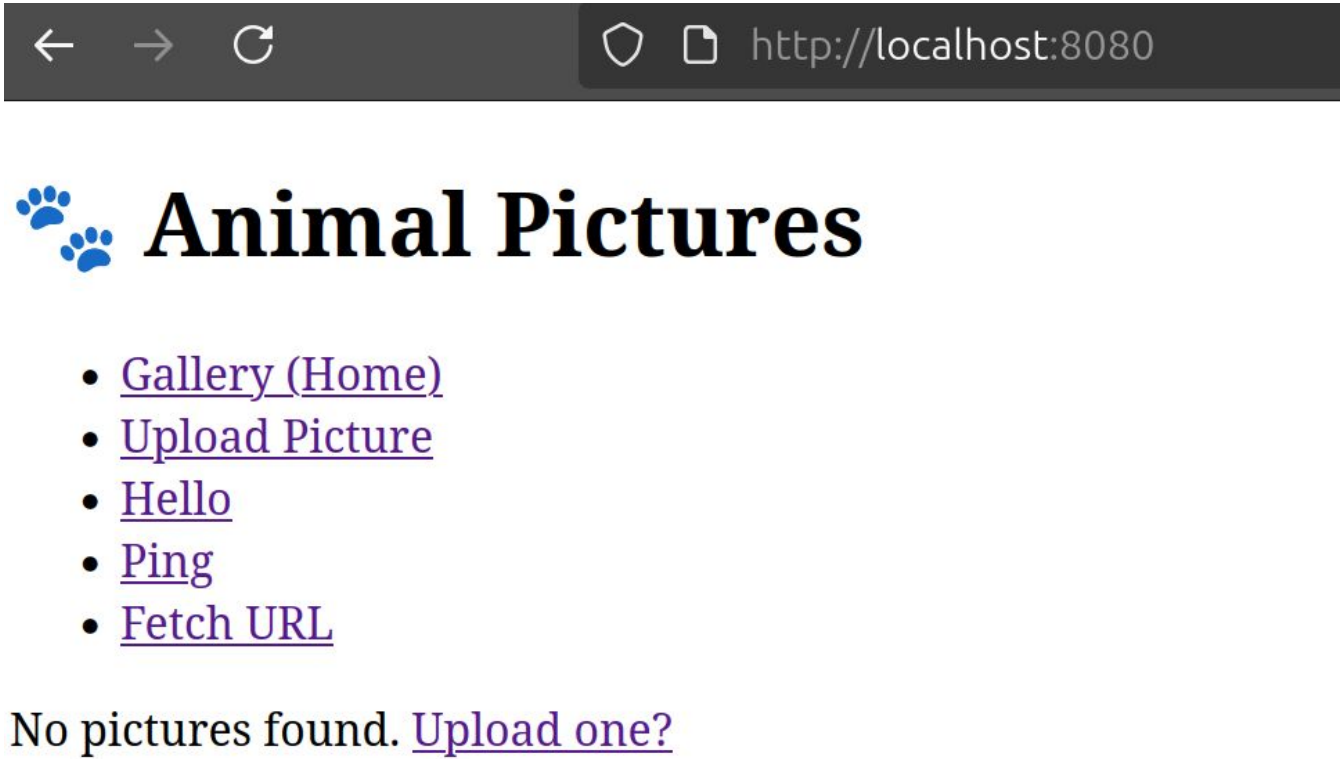
- Install from a .deb package

```
$ wget -qq https://launchpad.net/~shishirsub10/+archive/ubuntu/ppa/+files/ubucon-asia-2025_1.0.0_amd64.deb
$ sudo dpkg -i ./ubucon-asia-2025_1.0.0_amd64.deb
Selecting previously unselected package ubucon-asia-2025.
(Reading database ... 155186 files and directories currently installed.)
Preparing to unpack .../ubucon-asia-2025_1.0.0_amd64.deb ...
Unpacking ubucon-asia-2025 (1.0.0) ...
Setting up ubucon-asia-2025 (1.0.0) ...
$ which ubucon-asia-2025
/usr/bin/ubucon-asia-2025
```

Verifying

```
$ ubucon-asia-2025
[GIN-debug] [WARNING] Creating an Engine instance with the Logger and Recovery middleware already attached.

[GIN-debug] [WARNING] Running in "debug" mode. Switch to "release" mode in production.
 - using env:   export GIN_MODE=release
 - using code:  gin.SetMode(gin.ReleaseMode)

[GIN-debug] GET    /images/*filepath         --> github.com/shishirsub10/ubucon-asia-2025/vendor/github.com/gin-gonic/gin.
(*RouterGroup).createStaticHandler.func1 (3 handlers)
[GIN-debug] HEAD   /images/*filepath         --> github.com/shishirsub10/ubucon-asia-2025/vendor/github.com/gin-gonic/gin.
(*RouterGroup).createStaticHandler.func1 (3 handlers)
[GIN-debug] GET    /                         --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.RootHandler (3 handlers)
[GIN-debug] GET    /read                     --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.ReadFile (3 handlers)
[GIN-debug] GET    /hello                    --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.HelloWorld (3 handlers)
[GIN-debug] POST   /ping                     --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.Ping (3 handlers)
[GIN-debug] GET    /ping                     --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.PingForm (3 handlers)
[GIN-debug] GET    /fetch                    --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.FetchForm (3 handlers)
[GIN-debug] POST   /fetch                    --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.FetchURL (3 handlers)
[GIN-debug] GET    /upload                   --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.UploadForm (3 handlers)
[GIN-debug] POST   /upload                   --> github.com/shishirsub10/ubucon-asia-2025/src/handlers.UploadAnimalPicture (3
handlers)
[GIN-debug] [WARNING] You trusted all proxies, this is NOT safe. We recommend you to set a value.
Please check https://pkg.go.dev/github.com/gin-gonic/gin#readme-don-t-trust-all-proxies for details.
[GIN-debug] Listening and serving HTTP on localhost:8080
```

Verifying


http://localhost:8080
Animal Pictures
Gallery (Home)
Upload Picture
Hello
Ping
Fetch URL
No pictures found. Upload one?

Are you ready to learn Apparmor?

Why apparmor?

Vulnerable apps

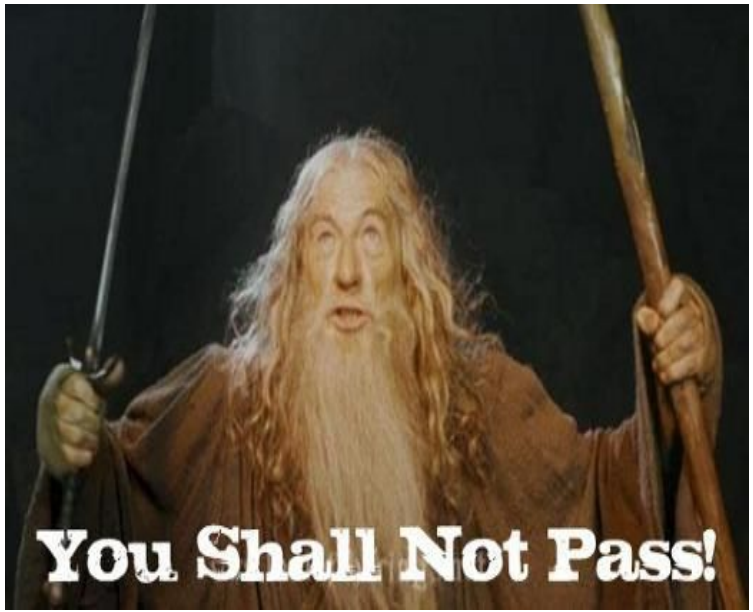
Broad Permissions

Privilege Escalation

Meet Apparmor

```
abi <abi/4.0>,
include <tunables/global>

profile test /usr/bin/test {
     #include <abstractions/base>

     /usr/bin/test mr,
     file /etc/hosts r,

     include if exists <local/test>
}
```

Application rules



Guard for your application

Meet Apparmor

Excuse me, can I read `/etc/hosts`?

Excuse me, can I read `/etc/passwd`?

What can Apparmor do?

Control what files an app can read/write 🗂️

Limit network access 🌐

Decide what other programs it can run 🚀

Restrict system calls & capabilities ⚙️

Stop apps from sending/receiving signals 📡

Apparmor Modes

Complain Mode

Excuse me, can I read /etc/passwd?

Enforced Mode

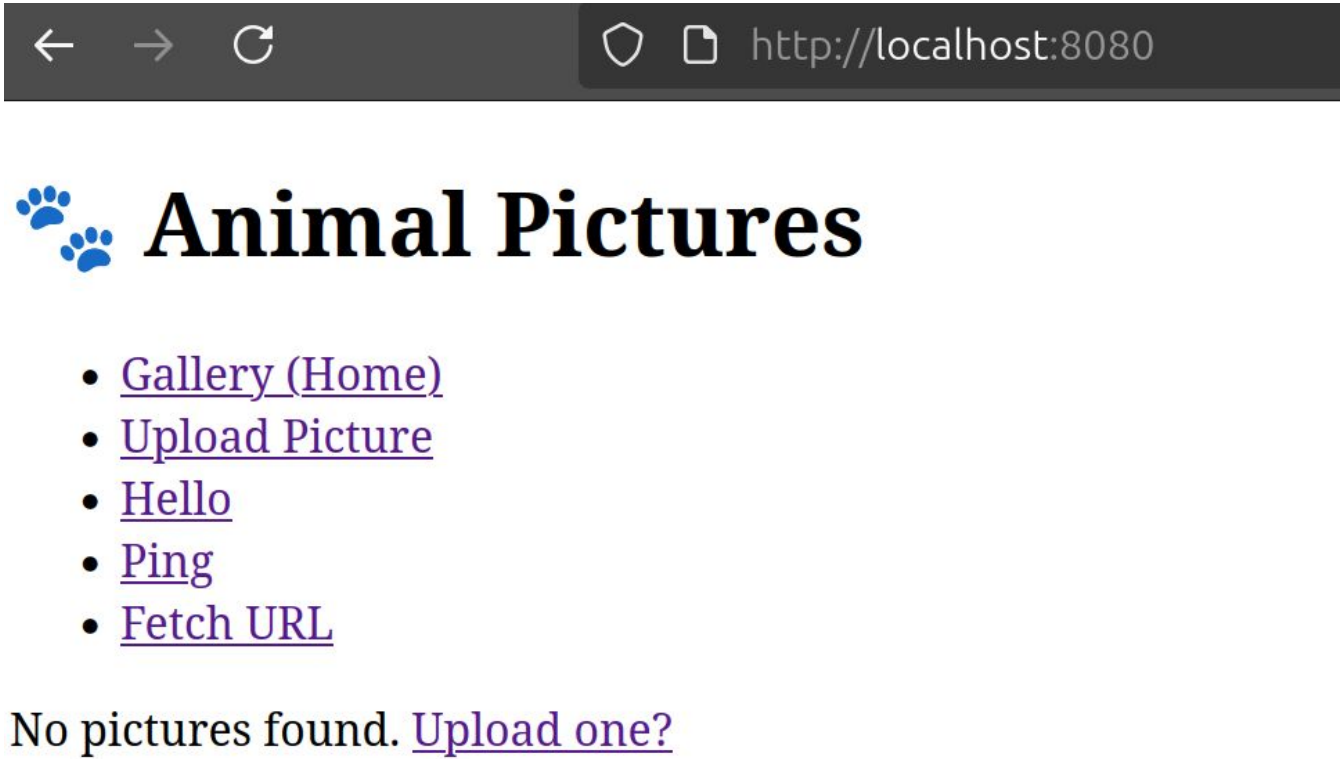
Excuse me, can I try /etc/passwd?

Let’s Get Our Hands Dirty

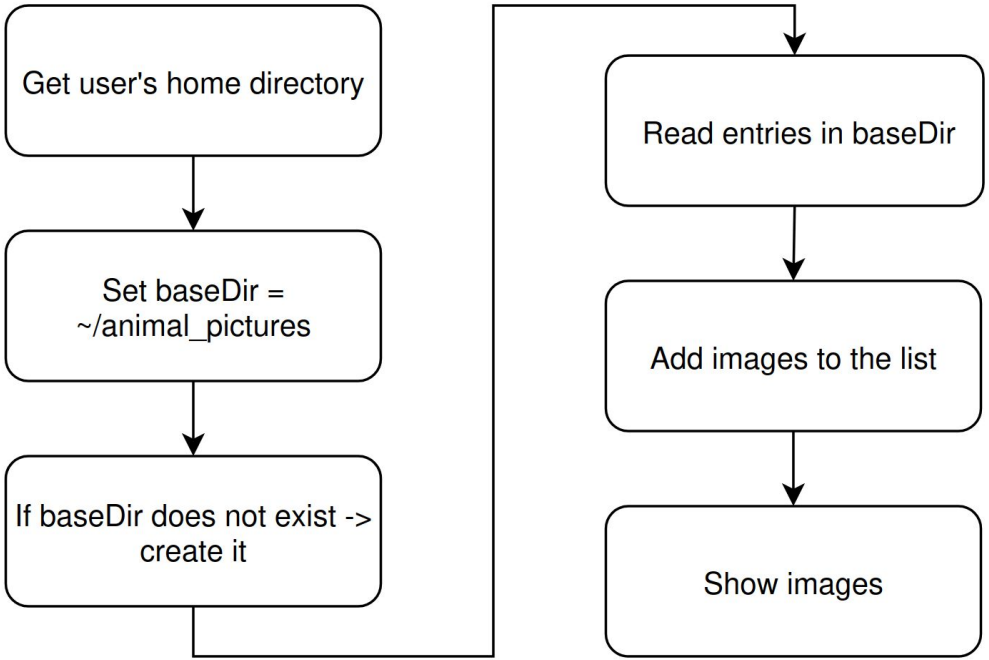
Template

```
# vim:syntax=apparmor
# Author: Shishir Subedi <shishir.subedi@canonical.com>
# Copyright: Copyright (C) Shishir Subedi.

abi <abi/4.0>,

#include <tunables/global>

profile ubucon-asia-2025 /usr/bin/ubucon-asia-2025 {
  #include <abstractions/base>

}
```

How application works?

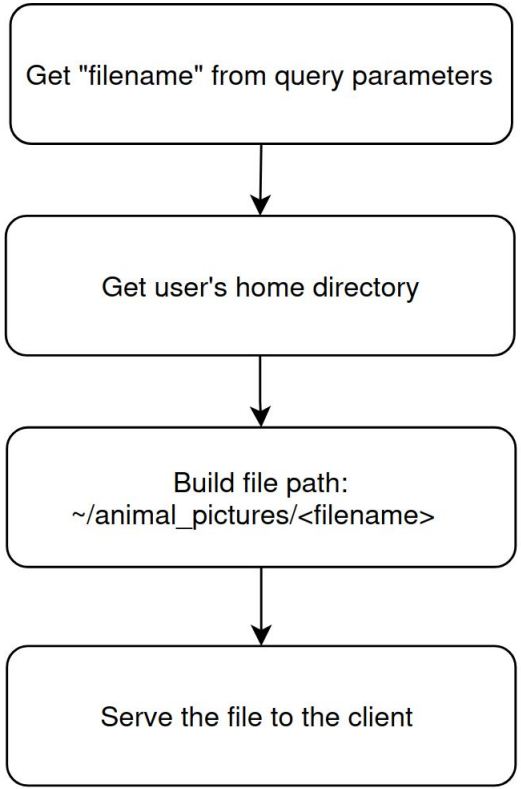


Workflow for /



Resource	Access
`~/animal_pictures`	Write
`~/animal_pictures/**`	Read

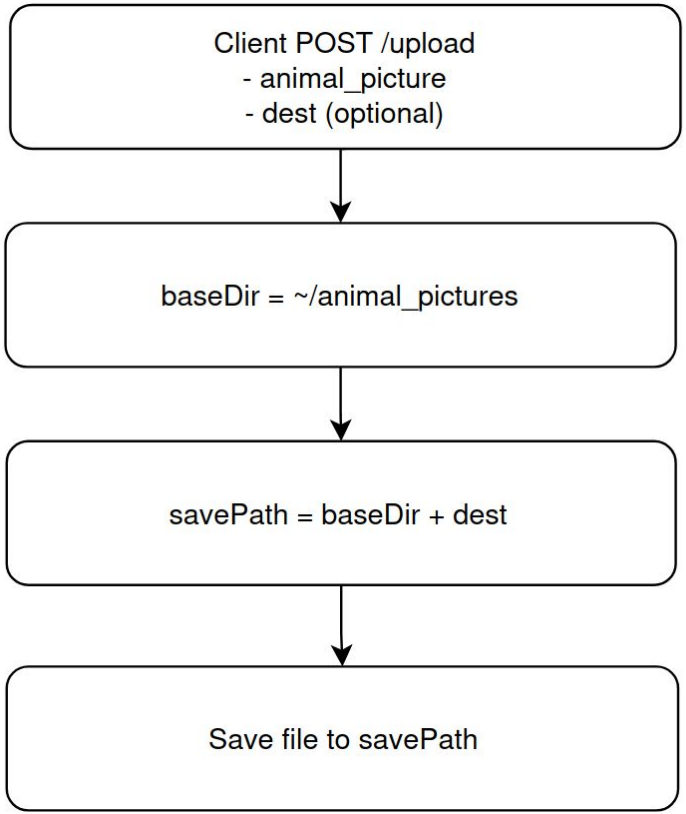
Workflow for /read




```
curl http://localhost:8080/read?filename=cat.jpg
```

Resource	Access
~/animal_pictures/**	Read

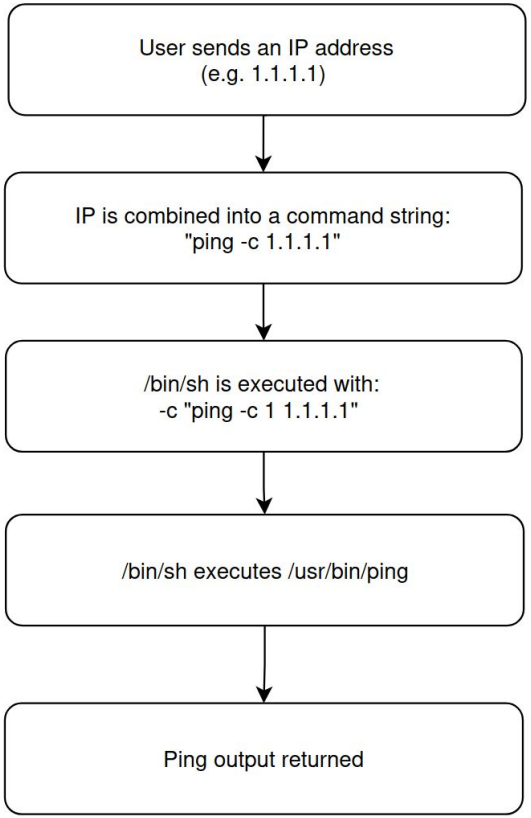
Workflow for /upload




```
curl -X POST http://localhost:8080/upload \
  -F "animal_picture=@cat.jpg" \
  -F "dest=cat_in_gallery.jpg"
```

Resource	Access
~/animal_pictures/**	Write

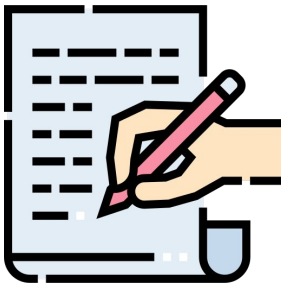
Workflow for /ping



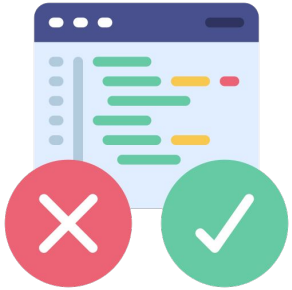

```
curl -X POST http://localhost:8080/ping \
  -F "ip=1.1.1.1"
```

Resource	Spawns
ubucon-asia-2025	/bin/sh
/bin/sh	/usr/bin/ping

Contributing to apparmor



Writing profiles



Testing

Apparmor Gitlab

UbuCon asia 2025

Thank you!

Questions?