

PHP Info Output



In a PHP software environment, the PHP info function is used to output detailed info about the PHP environment, configuration settings, installed modules, and more

PHP Info Output



If PHP info output can be accessed on a web app,
it could point malicious users to important
configuration info, loaded modules, username
info, and more

PHP Info Output

```
core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd  
mod_access_compat mod_alias mod_auth_basic mod_authn_core mod_authn_file mod_authz_core  
mod_authz_host mod_authz_user mod_autoindex mod_backdoor mod_deflate mod_dir mod_env  
mod_filter mod_mime prefork mod_negotiation mod_php mod_reqtimeout mod_setenvif mod_status
```

In this case, the PHP output for loaded modules indicates that there is a **mod_backdoor** module loaded, which is usual, to say the least

Privilege Escalation

Sudo Service

```
service apache2 start
```

The Linux Service program is used to manage and interact with system services. It acts as a wrapper for starting, stopping, restarting and checking the status of services

Privilege Escalation

Sudo Service

```
sudo service ../../bin/sh
```

If we have Sudo access with the Service program, we can escalate our privileges by using a command similar to the one above

Privilege Escalation

Sudo Joe

The Joe program is a terminal text editor, and it's considered to be more complex and feature-rich than the Nano text editor



Privilege Escalation

Sudo Joe

```
Program to run: /bin/bash
```

The Joe editor can run commands during program execution, we can elevate our privileges if we can run the program as Sudo by using the Ctrl + K shortcut, followed by !, then /bin/bash