

Laravel Production Hardening Checklist

1. System-Level Hardening (Ubuntu 22.04)

- `sudo apt update && sudo apt upgrade -y`
- `sudo ufw allow OpenSSH`
- `sudo ufw allow 'Apache Full'`
- `sudo ufw enable`
- `sudo apt install fail2ban -y`
- `sudo systemctl enable fail2ban`
- `sudo systemctl start fail2ban`

2. Apache Hardening

- Disable directory listing in `apache2.conf` (Options `-Indexes`)
- Hide Apache version in `security.conf`:
`ServerTokens Prod`
`ServerSignature Off`
- Enable modules: `rewrite, headers, ssl`
`sudo a2enmod rewrite headers ssl`
`sudo systemctl restart apache2`

3. Laravel File Permissions

- `chown -R www-data:www-data /var/www/html/sudheerkt_live`
- Directories: `755`
- Files: `644`
- `storage & bootstrap/cache`: `775`
- `.env`: `600`
- `artisan`: `755`

4. Protect .env File

```
Add inside public/.htaccess:  
<Files .env>  
    Require all denied  
</Files>
```

5. Disable PHP Execution in Writable Folders

```
Create storage/.htaccess:  
<FilesMatch "\.php$">  
    Require all denied  
</FilesMatch>
```

6. Secure php.ini

```
expose_php = Off
display_errors = Off
allow_url_fopen = Off
allow_url_include = Off
disable_functions = exec,passthru,shell_exec,system,proc_open,popen,curl_exec,parse_ini_file,show_source
sudo systemctl restart apache2
```

7. Force HTTPS & Production Settings

```
.env settings:
APP_ENV=production
APP_DEBUG=false
APP_URL=https://yourdomain.com
```

```
In AppServiceProvider:
URL::forceScheme('https');
```

8. Security Headers

```
Add to public/.htaccess:
Header set X-Content-Type-Options "nosniff"
Header set X-XSS-Protection "1; mode=block"
Header set X-Frame-Options "SAMEORIGIN"
Header set Referrer-Policy "strict-origin-when-cross-origin"
```

9. Optimize Laravel

```
php artisan config:cache
php artisan route:cache
php artisan view:cache
php artisan optimize
```

10. Database Security

- Use strong DB password
- bind-address = 127.0.0.1 in mysqld.cnf
- Restart MySQL

11. Post-Hack Actions

- Replace vendor folder
- composer install --no-dev --optimize-autoloader
- php artisan key:generate
- Rotate all passwords
- Clear cache and sessions