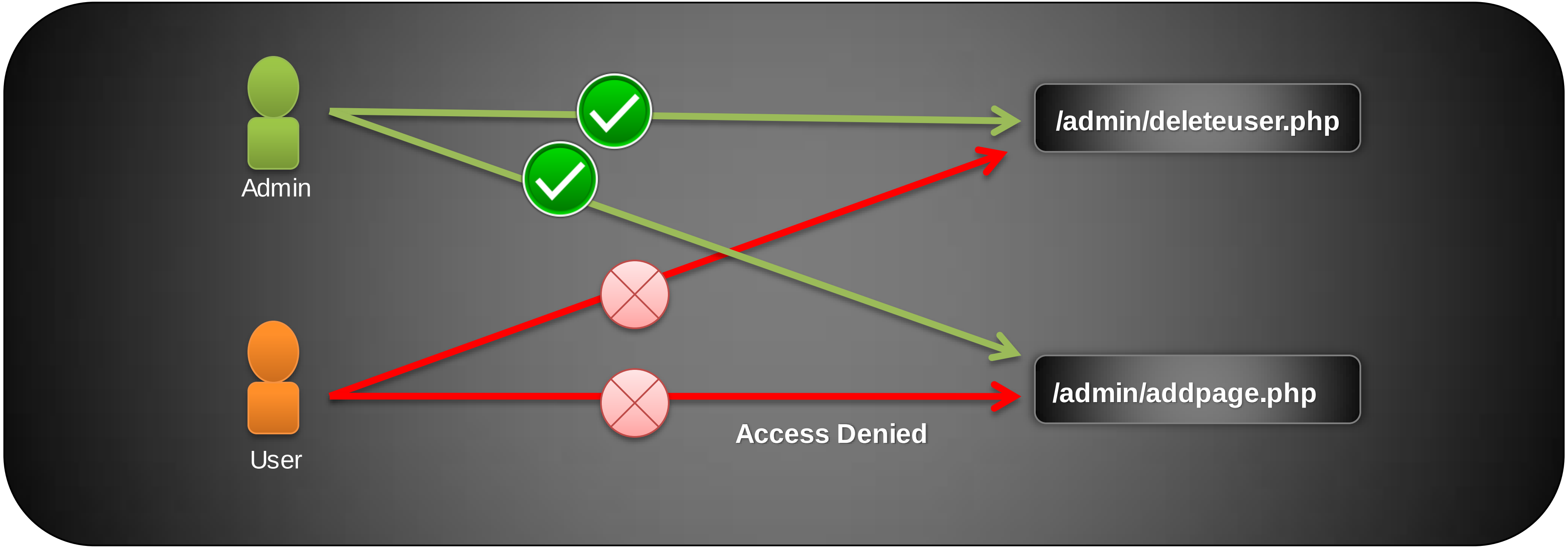
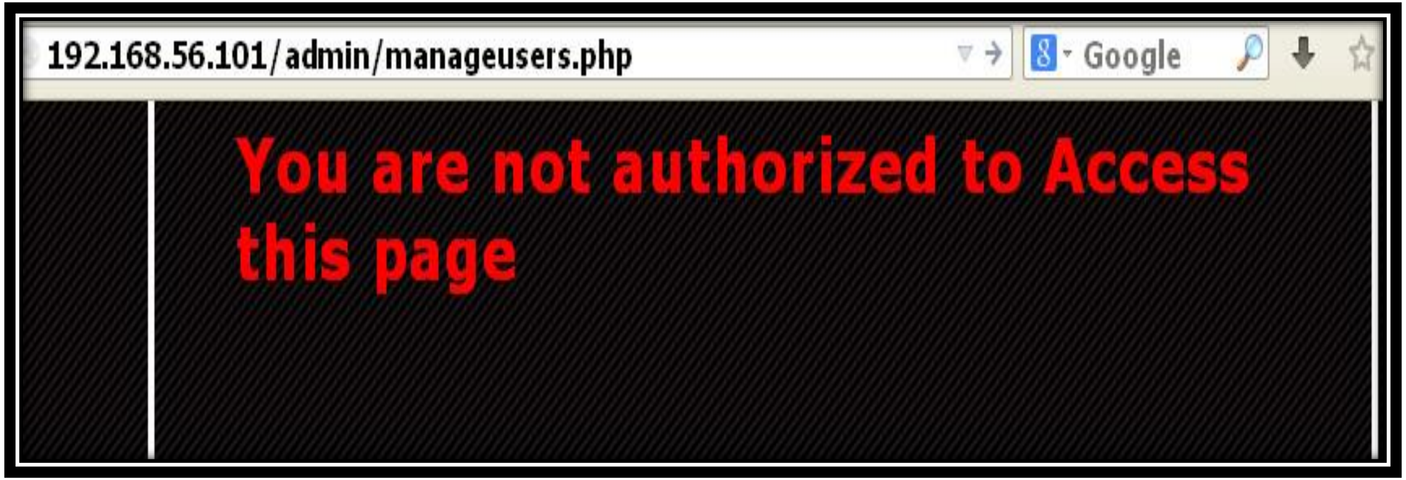
Missing Function Level Access Control Prevention

CYBER SECURITY & PRIVACY FOUNDATION

- By default, Deny Access.
- Provide access to functions based on roles



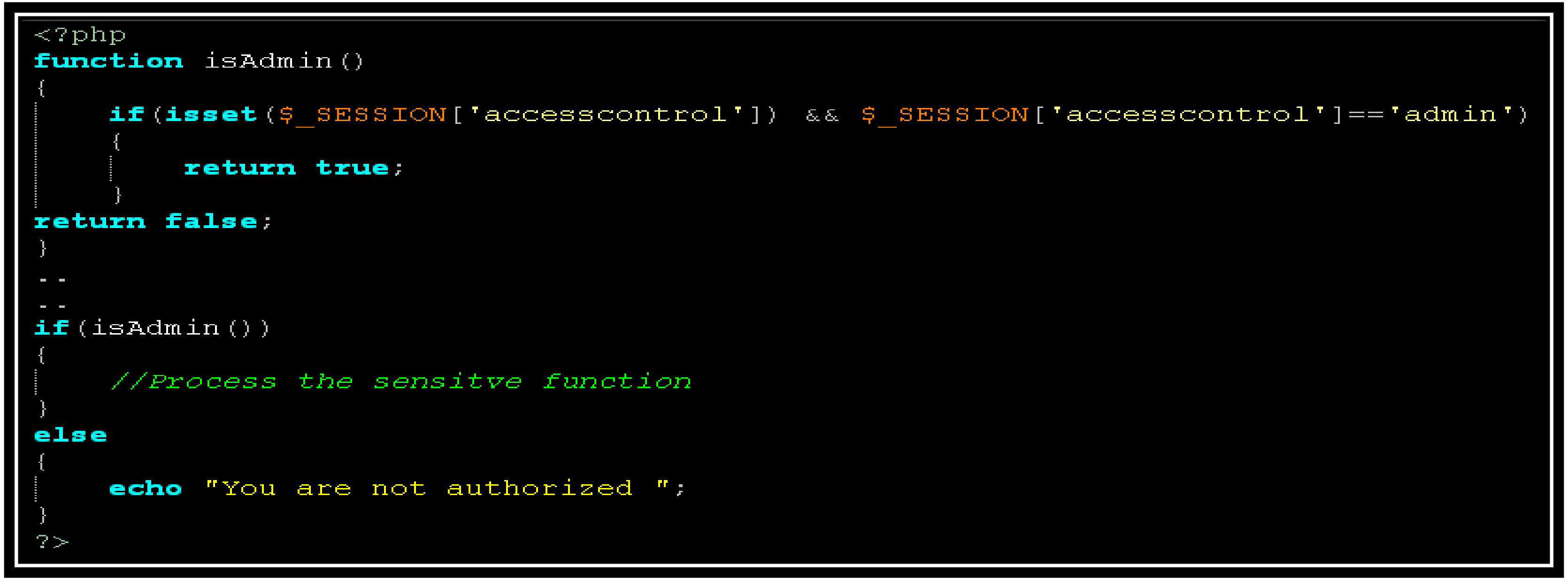
- Enforce “**Access Control**” not only in Presentation Layer but also in **Business Logic**.
- Hiding Links to sensitive function is not the solution. You must check whether the user is authorized or not, when there is a request to the function.



192.168.56.101/admin/manageusers.php

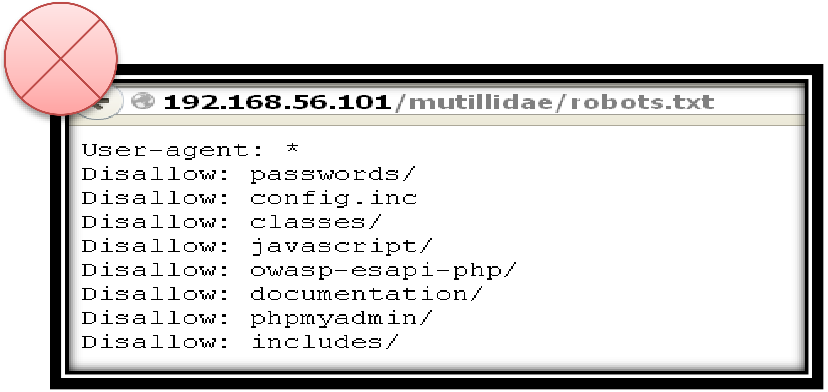
You are not authorized to Access this page

- PHP Code that only allows administrators to access the sensitive functions.



```
<?php
function isAdmin()
{
    if(isset($_SESSION['accesscontrol']) && $_SESSION['accesscontrol']=='admin')
    {
        return true;
    }
return false;
}
--
--
if(isAdmin())
{
    //Process the sensitve function
}
else
{
    echo "You are not authorized ";
}
?>
```

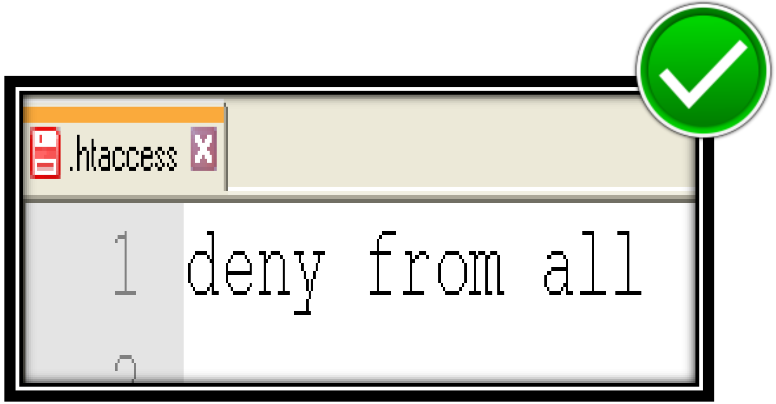
- Restrict directories/pages that you don’t want normal users and search engines to access with .htaccess rather than adding “Disallow” in robots.txt file



✗

192.168.56.101/mutillidae/robots.txt

```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi-php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```



✓

```
deny from all
```