Securing PHP web application

Resources

|  |  |
| --- | --- |
| Name | URL |
| Common Vulnerabilities and Exposures | https://cve.mitre.org/ |
| *The Open Web Application Security Project* (*OWASP*) | https://www.owasp.org |

Global Variable

|  |  |
| --- | --- |
| Name | Description |
| $\_GET | URL data |
| $\_POST | HTTP Body data |
| $\_FILES | File uploads |
| $\_COOKIE | File uploads ( Cookies) |
| $\_SERVER | HTTP request data from server |
| $\_REQUEST | Contains data from $\_GET or $\_POST or other global variables |
| $\_ENV | Environment variables |
| $\_SESSION | Session Information |

Validation

|  |  |
| --- | --- |
| Type | Steps |
| is\_int(arg) | To check if passed variable s is integer |
| isset(arg) | To check if variable is set |
| ?? | To set default value for vairalbe rather than using isset  i.e:  $id=$\_GET[‘id’] ?? -1; |
| is\_\*() | A lot of function start with is\_ for checking purposes |
| ctype\_\* | ctype function to validate input field |
| filter\_\* | To filter and validate data |
| declare(strict\_types=1) | Provided arguments has to be in the same datatype |
| strip\_tags(arg) | To remove html tags |
| preg\_replace(arg,expression,’’) | to replace specific data based on regular expression |
| htmlspecialchars(arg,options) | To replace html tags with html entities |
| htmlentities(arg,options) | Similar to htmlspecilachars but with more filtering |

Cross-site Scripting (XSS)

|  |  |
| --- | --- |
| Type | Steps |
| header(‘content-type:application/json’); |  |

SQL Injection

|  |  |
| --- | --- |
| Type | Steps |
| mysqli\_real\_escape\_string($db,$value) | To escape unwanted characters |

State Management

|  |  |
| --- | --- |
| Type | Steps |
| document.cookie | To get session cookie |
| document.cookie=new key | To set session cookie |
| setcookie(‘name’,rand(100,999),0,’/’,’’,false,true) | To make httpOnly cookie which means that cookies can be access via http header not document.cookie |
| $\_SESSION[‘name’] = value | To set session value |
| session\_start() | To start a session then you can set any value you want |
| isset() | To check if variable is set |
| session.cookie\_httpOnly=true | In php.ini , you can disable visibility of the cookies |
| if(isset($\_GET[‘setHeader’])&&  $\_GET[‘setHeader’] ===1){  Header(‘X-FRAME-OPTIONS:DENY’);  } | To prevent IFRAMES |

Storing Passwords

|  |  |
| --- | --- |
| Type | Steps |
| MD5 (not recommended)  SHA1 (not recommended)  bcrypt (recommended) | Hashing Algorithm |
| crypt()  hash() | Generic hashing functions |
| password\_get\_info()  password\_hash()  password\_needs\_rehash()  password\_verify() | Password hashing API |
| $pwd=password\_hash(‘Your Password’,PASSWORD\_DEFAULT)  $pwd=password\_hash(‘Your Password’,PASSWORD\_DEFAULT,  [‘cost’=> 11]) | Create password hash  Increase the algorithmic cost for hashing |
| $result=password\_verify(‘Entered Password’, $hashedPassword\_From\_DB) | Verify that a hash belongs to a password |
| password\_get\_info(‘hashedPassword’) | To get info about the hashed password its type |
| password\_needs\_rehash() | To rehash the password |

Error Handling

|  |  |
| --- | --- |
| Type | Steps |
|  |  |