Безопасность веб приложений

Выполнила Троеглазова М.А гр 22\2

1)Уязвимости Include, Upload.

Для данного сайта обеспечение безопасности для Include и Upload нет необходимости, поскольку директивой include подключаются только внутренние части системы, а загрузки через upload не происходит.

2)Уязвимости CSRF

Так как обеспечение безопасности от межсайтовых подделок запросов достаточно актуальная проблема, то решением защиты формы от подобных атак может быть использование так называемых токенов(token), которые используются при добавлении скрытых полей к каждому заполнению формы для удостоверения в ее подлинности. Если отправленное формой значение не соответствует хранящемуся на сервере для каждого пользователя, то такая форма не будет восприниматся сервером.

Пример

Создание «токена»

$token=(substr(md5(uniqueid()),0,8).$_SERVER['REMOTE_ADDR'].$_SESSION['login'];

$_SESSION['token']=$token;

Помещение в скрытое поле формы

<?php if(isset($_SESSION['token']))

print'<input type = "hidden" name="client-token" value=" '.$_SESSION['token'].'">'?>

Его проверка в основном коде

if($_SESSION['token']!=$_POST['client-token']{

setcoookie('token_error','1',time()+30*24*60*60);

header('Location:index.php');

exit();}

3)Уязвимости SQl Injection

Обеспечение защиты определяется тем, Что подготовленные запросы и отсутствие именованных меток позволяет избегать подобных ситуаций

```
if (preg_match('/^[a-z]+$/u',$_SERVER['PHP_AUTH_USER']) && preg_match('/^[a-
zA-Z0-9]+$/u',$_SERVER['PHP_AUTH_PW'])){
                $user = 'u20397';
                $pass = '5245721';
                $db = new PDO('mysql:host=localhost;dbname=u20397', $user,
$pass, array(PDO::ATTR_PERSISTENT => true));
                try {
                    $stmt = $db->prepare("SELECT * FROM atable WHERE alog=?
AND apar=md5(?)");
                    $stmt-
>execute(array($_SERVER['PHP_AUTH_USER'],$_SERVER['PHP_AUTH_PW']));
```

```
                }
                catch(PDOException $e){
                    print('Error : ' . $e->getMessage());
                    exit();
                }
                $count = $stmt->rowCount();
```

(этот пример находится ф файле админ)

4)Xss

Для обеспечения безопасности в данной области достаточно предусмотреть корректную проверку заполнения формы, а также проверку данных, получаемых из бд

(получение из базы):

```
$values['day'] = !empty($user_data[0]['day']) ? date("Y-m-
d",$user_data[0]['day']) : '';
                                                $values['pol'] =
!empty($user_data[0]['pol']) ? strip_tags($user_data[0]['pol']) : '';
```

Складывание полученных значений в массив value

```
$values = array();

    if (isset($_COOKIE['fio_value']))
        $values['fio'] = !preg_match('/^[a-яA-Я ]+$/u',$_COOKIE['fio_value'])
|| empty($_COOKIE['fio_value']) ? '' : $_COOKIE['fio_value'];
        else $values['fio']='';

        if (isset($_COOKIE['email_value']))
            $values['email'] = !preg_match('/^((([0-9A-Za-z]{1}[-0-9A-
z\.]{1,}[0-9A-Za-z]{1})|([0-9A-Яа-я]{1}[-0-9A-я\.]{1,}[0-9A-Яа-я]{1}))@([-A-
Za-z]{1,}\.){1,2}[-A-Za-z]{2,})$/u'
                ,$_COOKIE['email_value']) || empty($_COOKIE['email_value']) ?
'' : $_COOKIE['email_value'];
                else $values['email']='';

                if (isset($_COOKIE['day_value']))
                    $values['day'] = !preg_match('/^\d\d\d\d\-\d\d\-\d\d$/'
,$_COOKIE['day_value']) || empty($_COOKIE['day_value']) ? '' :
$_COOKIE['day_value'];
                    else $values['day']='';
```

и так далее

В файле формы происходит такая обработка данных

```
<input name="email" <?php if ($errors['email']) {print 'class="error"';} ?>
value="<?php print $values['email']; ?>" type="email"
placeholder="yourmail@gmail.com">
            </label>
            <br>
            <label>
            Дата рождения
            <br>
            <input name="day" <?php if ($errors['day']) {print
'class="error"';} ?> value="<?php print $values['day']; ?>" type="date">
            </label>
            <br>
            <p>
```

в файле admin

```
$users_data= $stmt->fetchAll();
        $values=[];
        foreach ($users_data as $row){
            $fio = strip_tags($row['fio']);
            $email = strip_tags($row['email']);
            $day = date("Y-m-d",intval($row['day']));
```