

New issue

[Jump to bottom](#)

XX vulnerability in index.php #80

🔴 Open enferas opened this issue on Jul 22 · 9 comments

enferas commented on Jul 22

Hello,

I would like to report for possible XSS vulnerability.

In file <https://github.com/xiebruce/PicUploader/blob/master/index.php>

```
$data = [
    'code' => 'success',
    'data' => [
        'filename' => $_FILES['file']['name'],
        'url' => $isWeb ? $link['formatLink'] : $link,
        //专用于web上传, 其它客户端上传该参数无用
        'notFormatUrl' => $isWeb ? $link['notFormatLink'] : '',
    ],
];

header('Content-Type: application/json; charset=UTF-8');
$json = json_encode($data, JSON_UNESCAPED_UNICODE);
echo $json;
```

It is possible to do the injection with the name of the file through `$_FILES['file']['name']`.

xiebruce commented on Jul 23

Owner

Thank you for reporting, I add a `htmlspecialchars()` to convert something like `<script>alert('sdfds')` to html entities.

```
htmlspecialchars($_FILES['file']['name'])
```

Don't know if this can solve the issue?

enferas commented on Jul 23

Author

Thank you for your response.

Yes exactly that solve the issue.

I would like also to mention to security issue in

<https://github.com/xiebruce/PicUploader/blob/master/settings/SettingController.php>

```
public function getStorageParams($params){
    $key = $params['key'];
    $jsonFile = $this->storagesDir.'/storage-'. $key.'.json';
    if(is_file($jsonFile)){
        $columns = json_decode(file_get_contents($jsonFile), true);
        $code = 0;
    }else{
        //....
    }
    unset($columns['name']);

    $returnArr = [
        'code' => $code,
        'data' => $columns,
    ];
    //....
    return json_encode($returnArr);
}

public function setStorageParams($params){
    //...
    $config = json_encode($_POST, JSON_UNESCAPED_SLASHES);
    //...
    $config = str_replace('\u202a', '', $config);
    file_put_contents($jsonFile, $config);
    //....
}
```

You are saving the \$_POST in a file through the function getStorageParams without sanitization. Then you use the function getStorageParams to retrieve the information. Are you using this file in your project ? if yes, we need to sanitize the input.

xiebruce commented on Jul 24

Owner

Thank you so much, now I update the code as below

```
$post = [];
foreach($_POST as $key=>$val){
    $post[$key] = htmlspecialchars($val);
}
```

```
}  
$config = json_encode($post, JSON_UNESCAPED_SLASHES);
```



enferas commented on Sep 21

Author

[CVE-2022-36748](#) is assigned to the first report in /master/index.php

xiebruce commented on Sep 22

Owner

[CVE-2022-36748](#) is assigned to the first report in /master/index.php

I've delete that tag v2.6.3



enferas commented on Oct 3

Author

[CVE-2022-41442](#) is assigned to the second report.

xiebruce commented on Oct 3

Owner

Thank you for your response.

Yes exactly that solve the issue.

I would like also to mention to security issue in

<https://github.com/xiebruce/PicUploader/blob/master/settings/SettingController.php>

```
public function getStorageParams($params){  
    $key = $params['key'];  
    $jsonFile = $this->storagesDir.'/storage-'. $key.'.json';  
    if(is_file($jsonFile)){  
        $columns = json_decode(file_get_contents($jsonFile), true);  
        $code = 0;  
    }else{  
        //....  
    }  
    unset($columns['name']);  
  
    $returnArr = [  
        'code' => $code,  
        'data' => $columns,
```

```

];
//....
return json_encode($returnArr);
}

public function setStorageParams($params){
    //...
    $config = json_encode($_POST, JSON_UNESCAPED_SLASHES);
    //...
    $config = str_replace('\u202a', '', $config);
    file_put_contents($jsonFile, $config);
    //....
}

```

You are saving the \$_POST in a file through the function getStorageParams without sanitization. Then you use the function getStorageParams to retrieve the information. Are you using this file in your project ? if yes, we need to sanitize the input.

Second report? did you mean this? but I've already fix it. If I didn't, please point it out(coz I can't understand you clearly.)

enferas commented on Oct 4

Author

Yes, the vulnerability already fixed. thanks for your confirmation.
It is just some process for gaining a CVE which will help me in my research.
When the person find a security issues he can ask for CVE, then it is assigned to the discovery
<https://www.cve.org/>

xiebruce commented on Oct 5

Owner

OK, got it.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestones

milestone

No milestone

Development

No branches or pull requests

2 participants

