ourphp 1.8 后台任意文件读取漏洞

漏洞简介：

OurPHP（傲派建站系统）是一款使用PHP语言开发的网站内容管理系统，开发商为哈尔滨伟成科技有限公司。

OurPHP 1.8版本存在任意文件读取漏洞，攻击者可利用此漏洞读取敏感文件。

##漏洞分析## 漏洞在 \client\manage\ourphp_filebox.php 文件。

在 ourphp_filebox.php 第1383行开始。

```
switch($op) {

    case "home":
    home();
    break;

    case "up":
    up();
    break;

    case "yupload":
    if(!isset($_REQUEST['url'])){
        printerror('您没有输入文件地址！');
    }elseif(isset($_REQUEST['ndir'])){
        yupload($_REQUEST['url'], $_REQUEST['ndir'], @$_REQUEST['unzip']
,@$_REQUEST['delzip']);
    }else{
        yupload($_REQUEST['url'], './', @$_REQUEST['unzip']
,@$_REQUEST['delzip']);
    }
    break;

    case "upload":
    if(!isset($_FILES['upfile'])){
        printerror('您没有选择文件！');
    }elseif(isset($_REQUEST['ndir'])){
        upload($_FILES['upfile'], $_REQUEST['ndir'], @$_REQUEST['unzip']
,@$_REQUEST['delzip']);
    }else{
        upload($_FILES['upfile'], './', @$_REQUEST['unzip']
,@$_REQUEST['delzip']);
    }
    break;

    case "unz":
    unz($_REQUEST['dename']);
    break;

    case "unzip":
    unzip($_REQUEST['dename'],$_REQUEST['ndir'],@$_REQUEST['del']);
    break;
```

```
    case "sqlb":
    sqlb();
    break;

    case "sqlbackup":
    sqlbackup($_POST['ip'], $_POST['sql'], $_POST['username'],
$_POST['password']);
    break;

    case "ftpa":
    ftpa();
    break;

    case "ftpall":
    ftpall($_POST['ftpip'], $_POST['ftpuser'], $_POST['ftppass'],
$_POST['goto'], $_POST['ftpfile'], $_POST['del']);
    break;

    case "edit":
    edit($_REQUEST['fename']);
    break;
```

这里看 case edit 的时候 fename参数没有任何的过滤直接从request获取，并且传入到 edit方法。

edit方法在 文件 第645行。

```
function edit($fename) {
    global $meurl,$folder;
    $file = iconv("UTF-8", "GBK", $folder.$fename);
    if (file_exists($folder.$fename)) {
        maintop("编辑");
        echo "<div class=\"title\">编辑文件 ".$folder.$fename."</div>";
        $contents = file_get_contents($file);
        if(function_exists('mb_detect_encoding')){
            $encode = mb_detect_encoding($contents);
        }else{
            $encode = 'UTF-8';
        }
        if($encode!=="UTF-8" && !empty($encode)){
            $contents = iconv("UTF-8", $encode, $contents);
        }
        echo "<form action=\"".$meurl."?op=save&encode=".$encode."\"
method=\"post\">\n"
            ."<textarea rows=\"30\" name=\"ncontent\" id=\"code\">";

        echo htmlspecialchars($contents);
        echo "</textarea>"
            ."<br>\n"
            ."<input type=\"hidden\" name=\"folder\" value=\"".$folder."\">\n"
            ."<input type=\"hidden\" name=\"fename\" value=\"".$fename."\">\n"
```

```
            ."    [<a href='#'
onClick=window.open('tags.php','go','scrollbars=0,resizable=0,scrollbars=yes,wid
th=1300,height=500,left=150,top=150,screenX=50,screenY=50')>在新窗口中弹出模板标签
</a>]    [<a href='#'
onClick=window.open('ourphp_column.php?
id=ourphp','go','scrollbars=0,resizable=0,scrollbars=yes,width=1300,height=500,l
eft=150,top=150,screenX=50,screenY=50')>在新窗口中弹出栏目管理</a>]"
            ."<input type=\"submit\" value=\"保存\" class=\"right button\">\n"
            ."</form>\n";
        echo "<script id='script'>"
              ."var editor =
CodeMirror.fromTextArea(document.getElementById('code'), {\n"
              ."  lineNumbers: true,\n"
              ."  lineWrapping: true,\n"
              ."  mode: 'markdown'\n"
              ."});"
              ."</script>";
    }else{
        home();
    }
}
```

这里看重点 `$file = iconv("UTF-8", "GBK", $folder.$fename);` file参数是 `$folder` 和 `$fename` 拼接而成。并且 `$contents = file_get_contents($file);` 这里没有任何过滤直接读取文件。这里 `fename` 参数可控，导致任意文件读取漏洞。

漏洞证明

用管理员身份登录到后台，然后访问下面的url：

```
http://localhost/client/manage/ourphp_filebox.php?
op=edit&fename=../config/ourphp_config.php&folder=D:/phpStudy/WWW/templates/
```

这里我们把 `fename` 的值改为 `../config/ourphp_config.php`，就可以读取 `config/ourphp_config.php` 文件的内容。