XXXXX网址敏感信息泄露

目录

[一 漏洞存在网址及证明复现 2](#_Toc505430567)

[1 漏洞存在网址 2](#_Toc505430568)

[2 漏洞复现 2](#_Toc505430569)

[二 漏洞产生原因及危害 2](#_Toc505430570)

[1漏洞产生原因 2](#_Toc505430571)

[2漏洞可能造成的危害 2](#_Toc505430572)

[三 漏洞临时解决方案 2](#_Toc505430573)

危害等级：高级

发现时间：2018年2月3日

# 一 漏洞存在网址及证明复现

## 1 漏洞存在网址

## 2 漏洞复现

# 二 漏洞产生原因及危害

## 1漏洞产生原因

1 网站自动备份，备份文件名和路径容易被猜解。

2 管理员手动备份文件名，用的域名作为备份文件名称，并且放置在根目录。

## 2漏洞可能造成的危害

1网站存在备份文件：网站存在备份文件，例如数据库备份文件、网站源码备份文件等，攻击者利用该信息可以更容易得到网站权限，导致网站被黑。

2敏感文件泄露是高危漏洞之一，敏感文件包括数据库配置信息，网站后台路径，物理路径泄露等，此漏洞可以帮助攻击者进一步攻击，敞开系统的大门。

3 由于目标备份文件较大（xxx.G），可能存在更多敏感数据泄露

4 该备份文件被下载后，可以被用来做代码审计，进而造成更大的危害

5 该信息泄露会暴露服务器的敏感信息，使攻击者能够通过泄露的信息进行进一步入侵。

# 三 漏洞临时解决方案

1删除检测出的备份文件，或者将这类文件从网站目录下移走。

2使用非常规的文件名称。

3特定的文件设置合理的权限。

4 删除一些不需要的敏感文件。