



东塔网络安全学院

DoTa Cyber Security College

网络安全检测与防御技术国家地方联合工程技术研究中心

# 网络安全检测与防护技术国家地方联合工程研究中心

National Joint Engineering Research Center of Network Security Detection and Protection Technology



经国家发展改革委员会批准成立，由暨南大学牵头51位代表国际一流科研力量的院士、国家千人、长江学者、ACM Fellow、IEEE Fellow、教育部新世纪优秀人才、全国网络安全优秀教师等多名尖端学者成立“网络安全检测与防护技术国家地方联合工程中心”。



为解决我国网络空间安全人才紧缺、缺口巨大的问题，成立“网络安全检测与防护技术国家地方联合工程中心深圳分中心”。主要负责研究制定国家网络安全人才的教育与培养体系，开发出专门针对零基础人员的职业化实战训练课程以及一体化教学体系。



深圳分中心以网络安全检测与防护技术的研究成果为基础，设立“东塔网络安全学院”，通过培养大量的零基础人员加入网络安全人才大军，形成我国网络空间安全人才职业化等级梯队，铸造国家网络空间安全的“镇东之塔”。

# 其他数据库注入 SQLMAP详解



第二阶段 OWASP常见WEB漏洞利用及防御



## 强调声明

本次直播及相关资料仅用于信息防御技术教学，旨在培养白帽子安全工程师，请勿用于其他用途；

在未得到网站授权前提下，禁止对政府、事业单位、企业或其他单位网站及系统进行渗透测试；

技术是把双刃剑，请遵纪守法，做一名合格的白帽子安全专家，为国家的网络安全事业做出贡献。

**本次直播及相关资料仅用于信息防御技术教学 请勿用于其他用途**



## 第一章 防御绕过

第1节 大小写混合

第2节 双写绕过

第3节 编码绕过

第4节 内联注释绕过

第5节 更改提交方式

第6节 等价函数替换

第7节 垃圾数据溢出

第8节 HTTP参数污染

第9节 借助符号混用

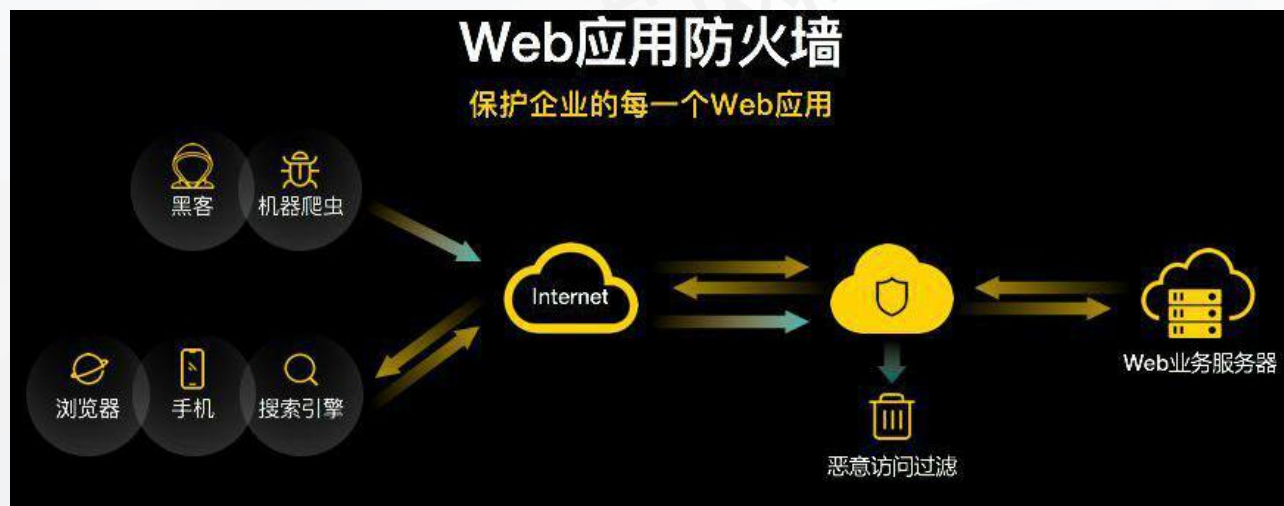
第10节 借助数据库特性

# 防御绕过-WAF概念

**WAF**是英文"**Web Applicaton Firewall**"的缩写，中文意思是"**Web应用防火墙**"，也称为"网站应用级入侵防御系统"。

WAF是集WEB防护、网页保护、负载均衡、应用交付于一体的WEB整体安全防护设备。WAF需要部署在Web服务器的前面，串行接入，不仅在硬件性能上要求高，而且不能影响Web服务，所以HA功能、Bypass功能都是必须的，而且还要与负载均衡、Web Cache等Web服务器前的常见的产品协调部署。

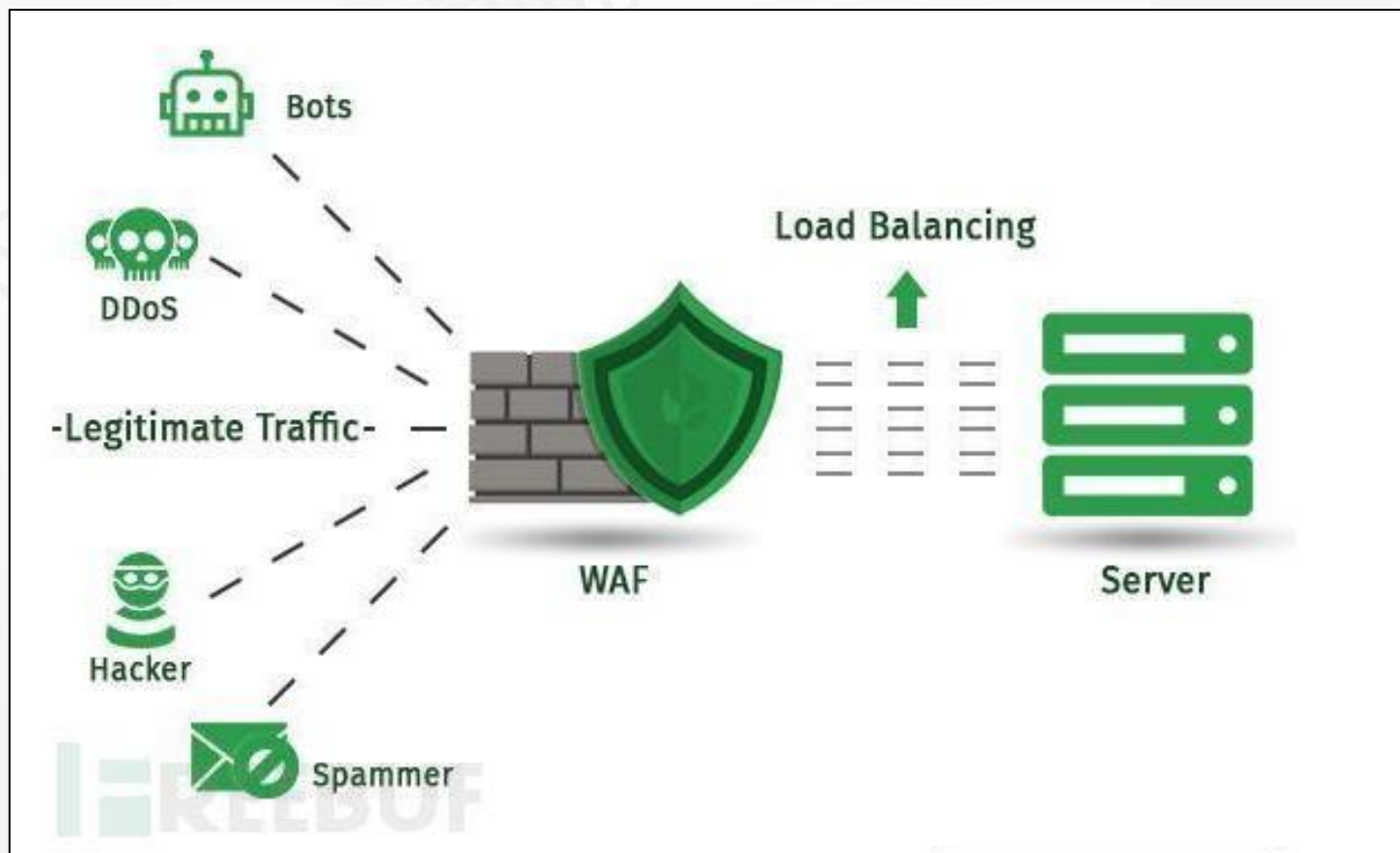
WAF的主要技术是对入侵的检测能力，尤其是对Web服务入侵的检测能力。常见的实现形式包括代理服务、特征识别、算法识别、模式匹配。



# 防御绕过-WAF分类

安全防护软件划分为：云WAF、硬件WAF、主机防护软件、软件waf等。

在攻防实战中，我们往往需要掌握一些特性，比如服务器、数据库、编程语言等等，以便更灵活地去构造Payload，从而绕过安全防护进行漏洞利用。



# SQL注入绕过常见方式

1. 绕过空格 (注释符/\* \*/ , %a0)
2. 括号绕过空格
3. 引号绕过 (使用十六进制)
4. 逗号绕过 (limit使用from或者offset) (substr使用from for属于逗号)
5. 比较符号 (<>) 绕过 (使用greatest())
6. or and 绕过
7. 绕过注释符号 (#, --) 过滤
8. = 绕过
9. 绕过union, select, where等:
  - (1) 使用注释符绕过
  - (2) 使用大小写绕过
  - (3) 内联注释绕过
  - (4) 双关键字绕过
10. 通用绕过 (编码)
11. 等价函数绕过
12. 宽字节注入



# SQL注入绕过-大小写绕过

## 1、思路讲解

果程序中设置了过滤关键字，但是过滤过程中并没有对关键字组成进行深入分析过滤，导致只是对整体进行过滤。

例如：and 过滤。当然这种过滤只是发现关键字出现，并不会对关键字处理。

通过修改关键字内字母大小写来绕过过滤措施。例如：AnD 1=1

例如：在进行探测当前表的字段数时，使用order by 数字进行探测。如果过滤了order，可以使用OrdEr来进行绕过。

查询创建工具

查询编辑器

```
1 SELECT * FROM `users` where id=1 OrDEr by 2;
```

信息

结果1

概况

状态

id	username	password
1	Dumb	Dumb

# SQL注入绕过-大小写绕过-实战

首页 / 在线靶场 / SQL注入之大小写混合绕过

Web安全

SQL注入靶场

大小写混合绕过

Work hard and improve daily

初级

2 积分



SQL注入之大小写混合绕过

消耗 **2.00** 积分

人气: 靶场有564人完成/898人尝试

时间: 30分钟

收藏: ☆

启动靶场

# SQL注入绕过-使用注释绕过

## 1、思路讲解

SQL中常使用的注释符有

`//, --, /**/, #, --+, -- -, ;,%00,--a`

具体的用法如下:

`U/**/NION/**/SE/**/LECT/**/user, pwd from user`

查询创建工具 查询编辑器

```
1 SELECT * FROM `users` where id=1 union/**/select 1,2,3;
```

前后内容通过注释符连接在一起

信息 结果1 概况 状态

id	username	password
1	Dumb	Dumb
1 2		3

查询创建工具 查询编辑器

```
1 SELECT * FROM `users` where id=1 /*!50000union*//**/select 1,2,3;
```

特殊注释: 其中的数字和版本有关, 一般大于10000都行

信息 结果1 概况 状态

id	username	password
1	Dumb	Dumb
1 2		3

# SQL注入绕过-空格绕过

## 1、思路讲解

如果空格被过滤，括号没有被过滤，可以用括号绕过。

在MySQL中，括号是用来包围子查询的。因此，任何可以计算出结果的语句，都可以用括号包围起来。而括号的两端，可以没有多余的空格。

例如：

```
select(user())fromdualwhere(1=1)and(2=2)
```

这种过滤方法常常用于time based盲注,例如：

```
?id=1%27and(sleep(ascii(mid(database()from(1)for(1)))=109))%23
```

(from for属于逗号绕过下面会有)

上面的方法既没有逗号也没有空格。猜解database () 第一个字符ascii码是否为109，若是则加载延时。

在很多GET传参的网站，过滤函数对传入的内容有长度限制的时候，会导致GET传入一些垃圾数据，长于过滤的长度的时候就可以实现绕过

[illegible]

**东塔网络安全学院**  
DoTa Cyber Security College



# SQL注入绕过-更换提交方式绕过

## 1、思路讲解

后台获取参数通过REQUEST方式获取数据，但是过滤函数式针对GET方式或者POST方式传递的参数进行过滤，此时可以进行更换提交方式绕过；

首页 / 在线靶场 / SQL注入之更换提交方式绕过

Web安全

# SQL注入 更换提交方式绕过

Work hard and improve daily

中级  
3 积分



## SQL注入之更换提交方式绕过

消耗 **3.00** 积分

人气: 靶场有672人完成/902人尝试

时间: 30分钟

收藏: ☆

启动靶场

# SQL注入绕过-双写绕过

## 1、思路讲解

- 举例: ?id=1
  - 访问?id=1 and 1=1 页面报错 1=1, 发现and被过滤, 这时候尝试使用双写 的方式绕过, 如aanndd 1=1, 当and被过滤后, aanndd变成了and, 所以 这时传输数据库的语句是and 1=1, 如果当访问 order by 错误信息为'der by'这发现过滤了or, 这双写or, 后面注入和union注入的一致。
- 其他关键字也是, 如果过滤select关键字了, 可以使用seselectect, 双写绕过;


[首页](#) / [在线靶场](#) / [SQL注入之双写绕过](#)

Web安全

# SQL注入 双写绕过

Work hard and improve daily

初级  
2 积分



## SQL注入之双写绕过

消耗 **2.00** 积分

人气: 靶场有567人完成/783人尝试

时间: **30分钟** 剩余时间: 00:26:21

收藏: ☆

镜像

关闭靶场

提示: 你当前正运行靶场训练, 关闭将丢失当前训练进

# SQL注入绕过-HTTP参数污染绕过

## 1、思路讲解

HTTP 参数污染，简单的讲就是给**相同名称参数**赋上两个或两个以上的值，导致应用程序以意外方式解释值而出现漏洞。现在的 HTTP 标准没有提及在遇到相同参数多个赋值时应该怎样处理。因此 web 程序组件在遇到这类问题时采取的方法也不完全相同。

如以下案例：

search.php?id=110&id=911

这就是典型的相同参数，多个赋值的情况，针对于这种情况，由于 HTTP 标准没有规定如何处理，是由 Werserver 来处理这个事情，但是每个 Webserver 处理时又不相同，针对于这种情况我们可以进行攻击。

首页 / 在线靶场 / SQL注入之HTTP参数污染绕过

Web安全

SQL注入

HTTP参数污染绕过

Work hard and improve daily

初级  
2 积分

SQL注入之HTTP参数污染绕过

消耗 **2.00** 积分

人气: 靶场有718人完成/891人尝试

时间: 35分钟

收藏: ☆

启动靶场

# SQL注入绕过-URL编码绕过

## 1、思路讲解

一般来说，URL只能使用英文字母、阿拉伯数字和某些标点符号，不能使用其他文字和符号。比如，世界上有英文字母的网址"http://www.abc.com"，但是没有希腊字母的网址"http://www.aβγ.com"（读作阿尔法-贝塔-伽玛.com）。这是因为网络标准[RFC 1738](#)做了硬性规定：

"...Only alphanumerics [0-9a-zA-Z], the special characters "\$-\_.+!\*'()," [not including the quotes - ed], and reserved characters used for their reserved purposes may be used unencoded within a URL."

"只有字母和数字[0-9a-zA-Z]、一些特殊符号"\$-\_.+!\*'(),"[不包括双引号]、以及某些保留字，才可以不经过编码直接用于URL。"

这意味着，如果URL中有汉字，就必须编码后使用。但是麻烦的是，RFC 1738没有规定具体的编码方法，而是交给应用程序（浏览器）自己决定。这导致"URL编码"成为了一个混乱的领域。

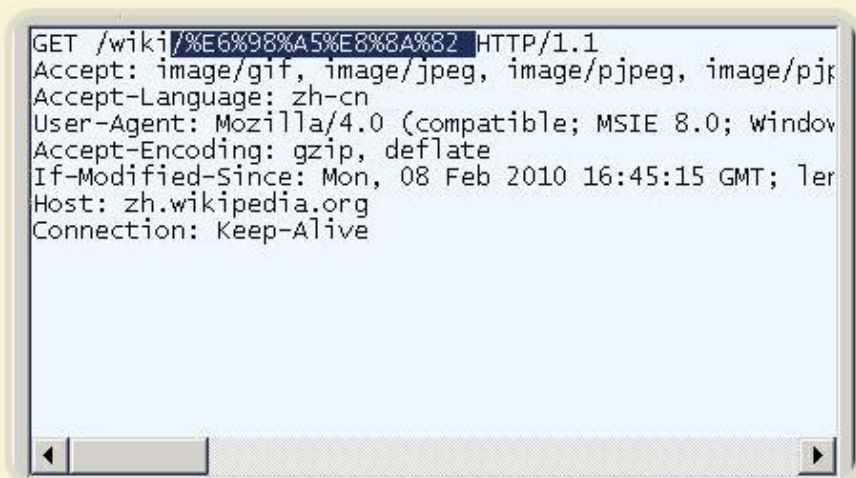


# SQL注入绕过-URL编码绕过

打开IE（我用的是8.0版），输入网址“<http://zh.wikipedia.org/wiki/春节>”。注意，“春节”这两个字此时是网址路径的一部分。



查看HTTP请求的头信息，会发现IE实际查询的网址是“<http://zh.wikipedia.org/wiki/%E6%98%A5%E8%8A%82>”。也就是说，IE自动将“春节”编码成了“%E6%98%A5%E8%8A%82”。



我们知道，“春”和“节”的utf-8编码分别是“E6 98 A5”和“E8 8A 82”，因此，“%E6%98%A5%E8%8A%82”就是按照顺序，在每个字节前加上%而得到的。



# SQL注入绕过-URL编码绕过

首页 / 在线靶场 / SQL注入之URL编码绕过

Web安全

## SQL注入 URL编码绕过

Work hard and improve daily

初级

2 积分



### SQL注入之URL编码绕过

消耗 **2.00** 积分

人气: 靶场有577人完成/745人尝试

时间: 30分钟

收藏: ☆

启动靶场

# SQL注入绕过-等价函数绕过

## 1、思路讲解

hex()、bin() ==> ascii()

sleep() ==> benchmark()

concat\_ws() ==> group\_concat()

mid()、substr() ==> substring()

**@@user** ==> user()

**@@datadir** ==> datadir()

举例：substring()和substr()无法使用

时： ?id=**1+and+ascii(lower(mid((select+pwd+from+users+limit+1,1),1,1)))=74**

或者： substr((select 'password'),**1,1**) = **0x70** strcmp(left('password',**1**), **0x69**) = **1**

strcmp(left('password',**1**), **0x70**) = **0** strcmp(left('password',**1**), **0x71**) = **-1**

# SQL注入绕过-等价函数绕过-实战

首页 / 在线靶场 / SQL注入之等价函数绕过

Web安全

## SQL注入 等价函数绕过

Work hard and improve daily

初级

2 积分



### SQL注入之等价函数绕过

消耗 **2.00** 积分

人气: 靶场有636人完成/894人尝试

时间: 30分钟

收藏: ☆

启动靶场

# 感谢各位的用心聆听!

网络安全国家工程研究中心  
——东塔网络安全学院