火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

火龙果·整理
uml.org.cn

概 览

CONTENTS

1 背景概述
2 典型攻击
3 攻防原理

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

6 总结不足

WEB安全体制——攻击与防护

1

背景概述

Web成为主流的网络和应用技术

CNCERT/CC 网络安全监测系统对流量数据进行的抽样统计显示，Web 应用流量占整个TCP 流量的81.1%。

B/S居统治地位：网上银行、电子商务、电子政务、证券、手机上网。

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1

背景概述

SANS(美国信息组织部)发布的全球20大安全风险排行榜上，Web应用安全漏洞名列前茅，攻击者利用最多的漏洞是SQL注入及跨站脚本。

根据国家计算机网络应急技术处理协调中心(简称CNCERT/CC)上半年的工作报告显示，网站漏洞百出，被篡改的大陆网站数量明显上升，总数达到28367个，比去年全年增加近16%

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

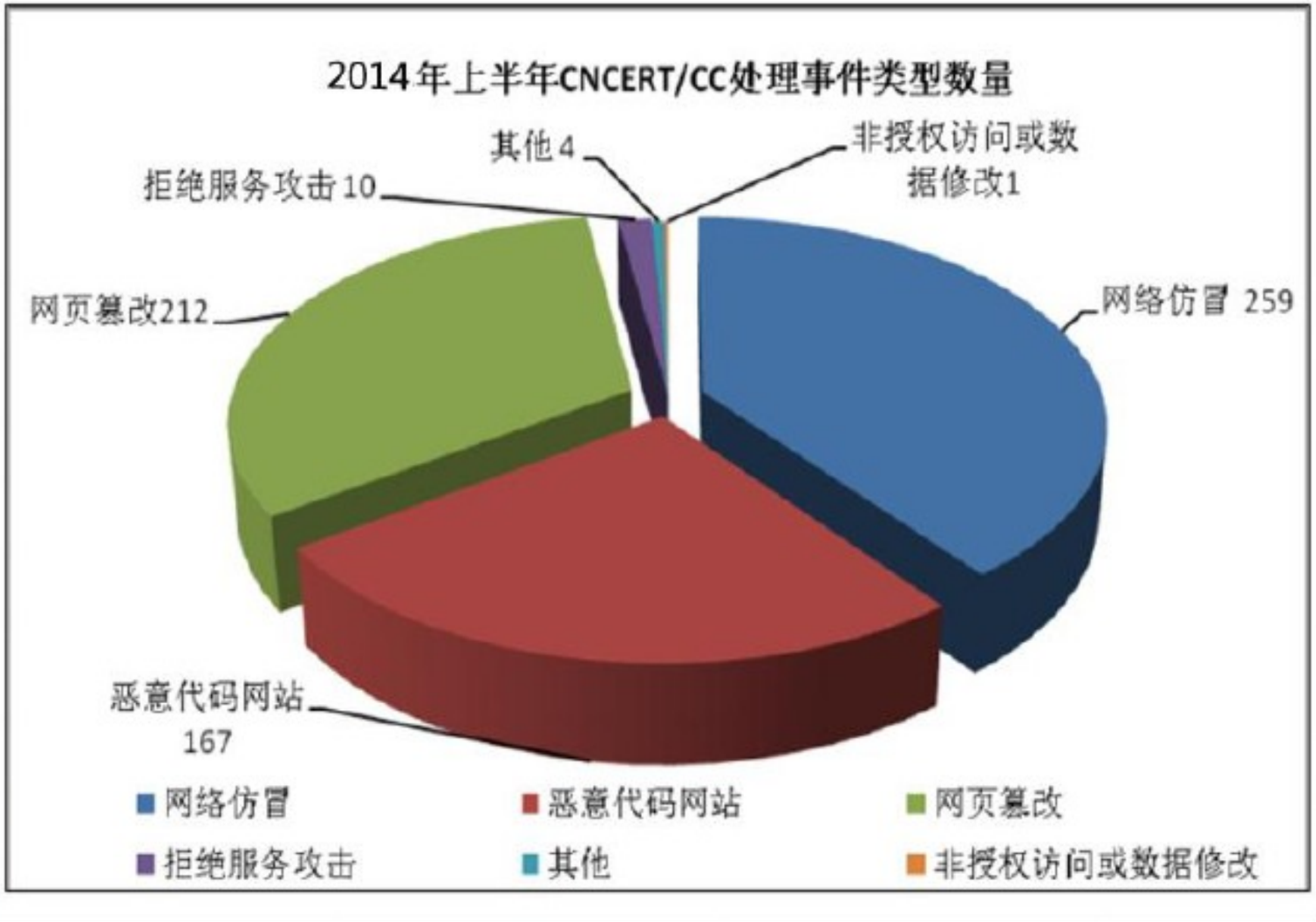
6 总结不足

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1

背景概述



WEB安全体制——攻击与防护

SQL注入攻击（SQL Injection）

攻击者利用WEB应用程序对用户输入验证上的疏忽，在输入的数据中包含对某些数据库系统有特殊意义的符号或命令，让攻击者有机会直接对后台数据库系统下达指令，进而实现对后台数据库乃至整个应用系统的入侵。

WEB安全体制——攻击与防护

SQL注入的危害

泄露敏感信息

无需知道口令就能以用户身份登陆应用系统

篡改敏感数据

攻击者可以获取后台数据库的种类、版本，操作系统信息，数据库名、表名、字段名以及数据库中的数据信息。

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

6 总结不足

WEB安全体制——攻击与防护

SQL注入主要方式

拼接的SQL字符串改变了设计者原来的意图，执行了如泄露、改变数据等操作，甚至控制数据库服务器

拼接SQL字符串灵活方便，但是容易导致安全问题

火龙果·整理
uml.org.cn

SQL注入原理

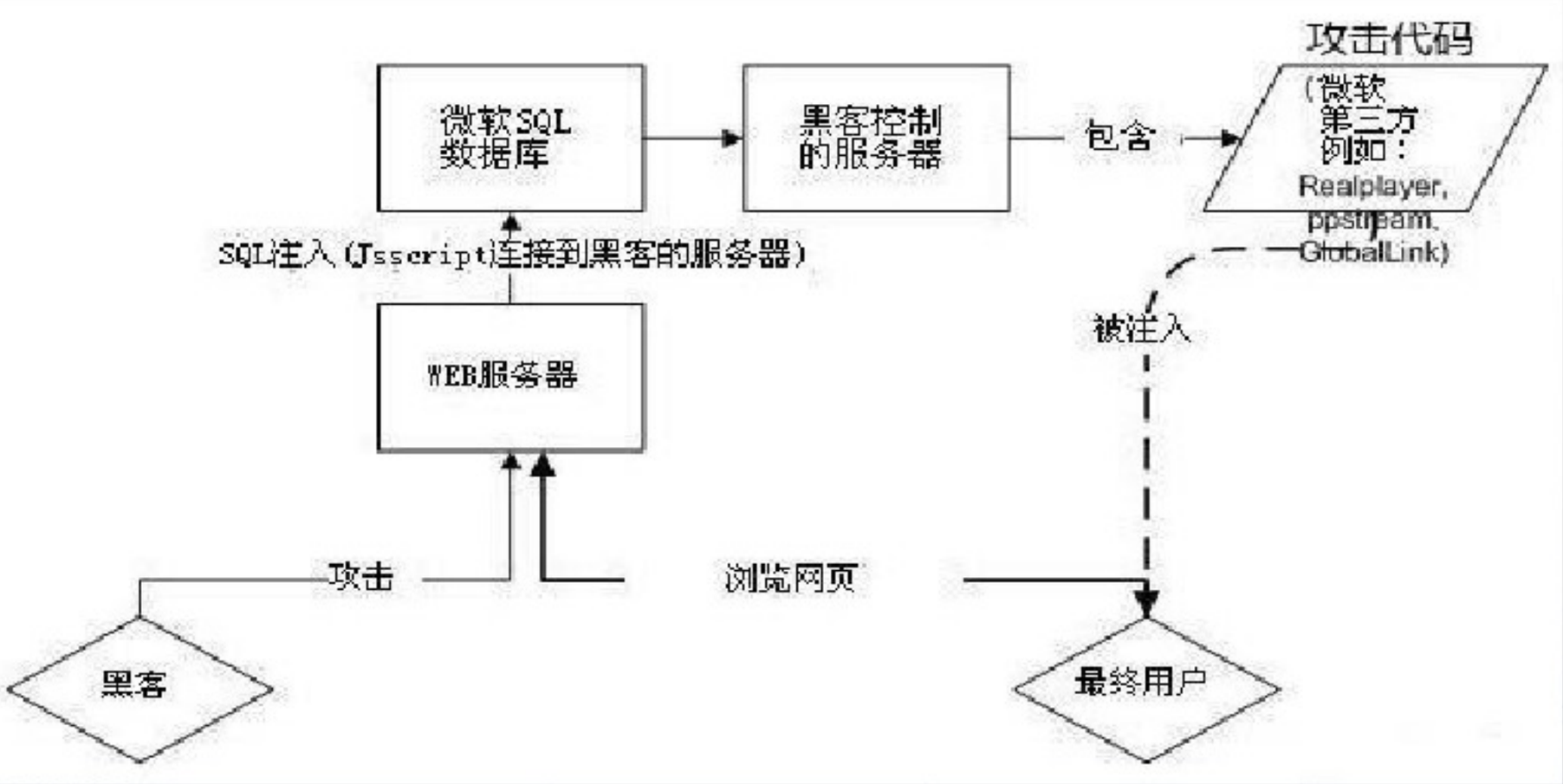
攻击者通过Web应用程序利用SQL语句或字符串将非法的数据插入到服务器端数据库中，获取数据库的管理用户权限，然后将数据库管理用户权限提升至操作系统管理用户权限，控制服务器操作系统，获取重要信息及机密文件。

WEB安全体制——攻击与防护

3

典型攻击

SQL注入过程



火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

6 总结不足

WEB安全体制——攻击与防护

4

案例介绍

SQL注入过程

http://victim/news.php?id=3721

⇩

select * from news where id=$id

⇩

select * from news where id=3721

WEB安全体制——攻击与防护

4

案例介绍

SQL注入过程

http://victim/news.php?id=0 union select name,pw from users

⇩

select * from news where id=$id

⇩

select * from news where id=**0 union select name,pw from users**

WEB安全体制——攻击与防护

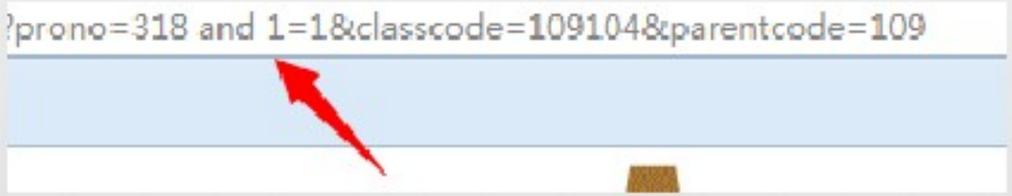
4

案例介绍

SQL注入过程

Step2：test and条件

构造类似如下格式：



id=1 and 1=1　　返回了信息

Id=1 and 1=2　　没有返回信息

由于没有对get请求提交的参数prono进行过滤，因此我们猜想其大概的SQL查询语句类似如下：

“Select article From news Where id = “+prono;而注入后则为

Select article from News where id = 318 and 1=2　**此时条件为假**

所以显示不出来,相关信息。但是这基本可以判定存在注入.

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

6 总结不足

火龙果·整理
uml.org.cn

5

讨论学习

SQL注入讨论

1、网页前端的参数有时与数据库列名息息相关！

2、对于数据库是MySQL、SQL的，很多时候是不需要注入！因为： 他们的表名，字段名是可以查出来的！

3、or 1=1 # 也可以很的简单，就进入了某网站的后台

火龙果·整理
uml.org.cn

WEB安全体制——攻击与防护

1 背景概述

2 典型攻击

3 攻防原理

4 案例介绍

5 讨论学习

6 总结不足