



2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体



李亚楠

优雅而坚定的
和SQL注入说再见！

汉领信息科技有限公司
副总经理



中国互联网络安全大会



360互联网安全中心

目录

DT时代面临的数据库安全威胁

优雅而坚定的SQL注入说再见

应用场景



中国互联网安全大会



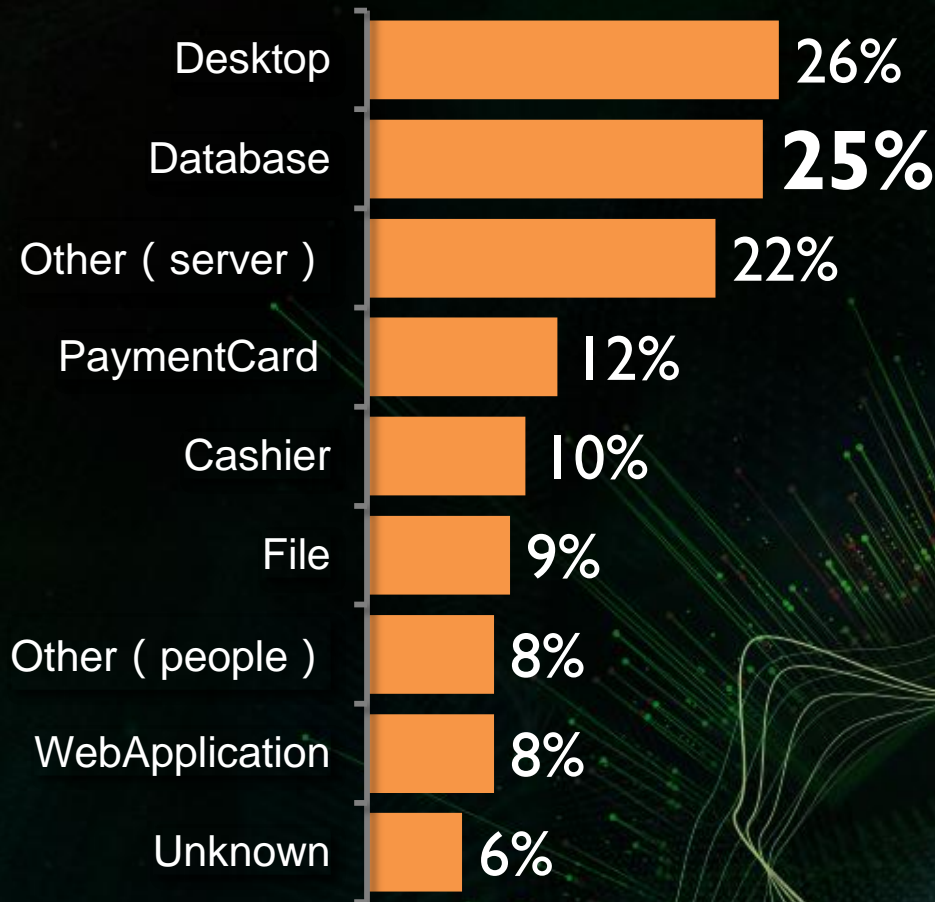
360互联网安全中心

DT时代的数据库安全威胁

Verizon 2015 十大内部资产滥用排名：

数据库在这些泄露事件成为了主角，这与我们在传统的安全建设中忽略了数据库安全问题有关。

#Verizon 2015



传统网络安全解决方案存在致命缺陷：

不对数据库通讯协议进行控制

对数据库通信协议的控制很弱

网络防火墙

IPS/IDS

绕过WAF的刷库行为屡见不鲜

无法解决来自业务本身的安全威胁

WAF

NGFW



中国互联网安全大会



360互联网安全中心

优雅而坚定的 和SQL注入说再见

SQL注入攻击

广泛存在 手段隐蔽 特征不可穷举

攻击手段及工具平民化

```
78 trim(preg_replace('/\\\\\\\\/', '\\', $image_src), '/');
79 $_SESSION['_CAPTCHA']['config'] = serialize($captcha_config);
80
81 return array(
82     'code' => $captcha_config['code'],
83     'image_src' => $image_src
84 );
85 }
86
87
88 if (function_exists('hex2rgb')) {
89     $rgb_array = hex2rgb($hex_str);
90     $rgb_array['r'] = hexdec(str_repeat(substr($hex_str, 0, 1), 2));
91     $rgb_array['g'] = hexdec(str_repeat(substr($hex_str, 1, 1), 2));
92     $rgb_array['b'] = hexdec(str_repeat(substr($hex_str, 2, 1), 2));
93 } else {
94     $color_val = hexdec($hex_str);
95     $color_val = ($color_val >> 0x10);
96     $color_val = ($color_val >> 0x8);
97     $color_val = ($color_val & 0xFF);
98     $rgb_array['r'] = ($color_val >> 0);
99     $rgb_array['g'] = ($color_val >> 8);
100     $rgb_array['b'] = ($color_val >> 16);
101 }
102 return $rgb_array;
103 }
104
105 // Draw the image
106 if (isset($_GET['image_src'])) {
107     $separator = '&';
108     $return_string = implode($separator, $return_array);
109 }
110 
```

有代码就有漏洞！

只要人类还在编写数据库应用
SQL注入漏洞就会一直存在

数据安全



中国互联网安全大会



360互联网安全中心

人

数据

拥有管理权限 (高危)

拥有使用权限 (中危)

拥有接触权限 (低危)

结构化数据
(高)

非结构化数据
(中)



B/S



业务系统



Oracle
SQL
Server
IBM-DB2
Sybase
Informix
Mysql

系统0day/应用程序0day

直接接触/间接接触数据

`http://leadsino.com/news/id=1`

`Select * from news where id=1`



`http://leadsino.com/news/id=1' and 1=2`
`union select * form users where id='1`

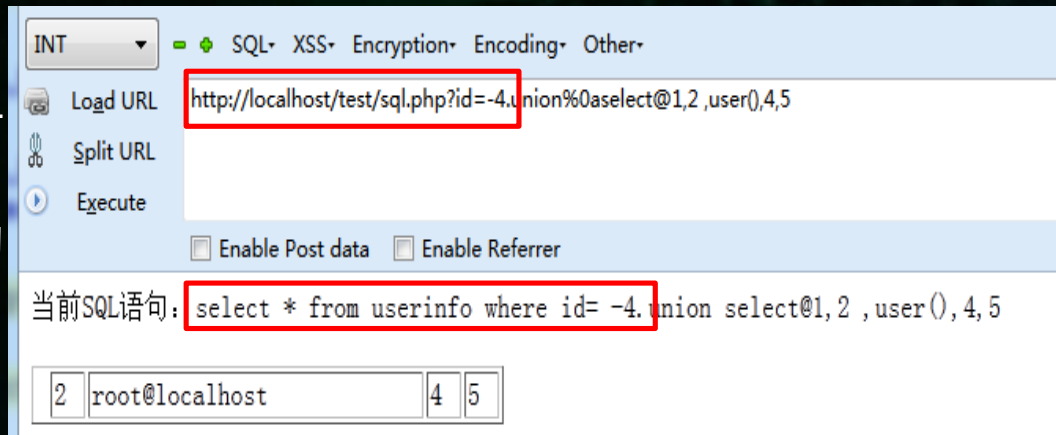
`Select * from news where id='1' and 1=2`
`union select * form users where id='1'`

数据建模：

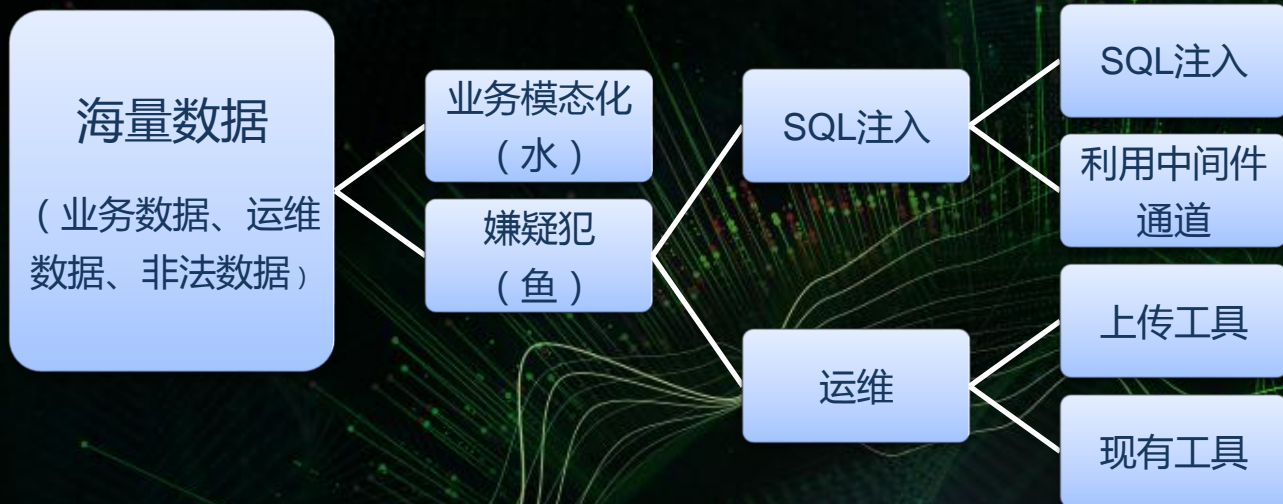
扩展“无危险不审计”白名单，通过对业务SQL语句的关键字、逻辑关系等特征自动采样学习，并结合高性能的SQL语义分析计算，构建对应的SQL语法树，完成模态数据建模：

此模块对SQL注入的探测与防御有特别的意义

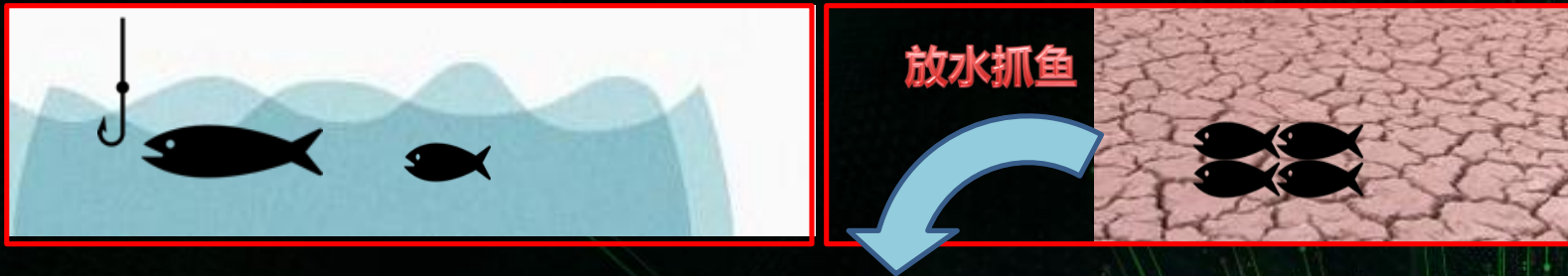
- 来源地址
- 目标地址
- 端口
- 数据库账号名
- 客户端主机名
- 客户端用户名
- 客户端程序名
- SQL语句
- 底层交互信息



计算SQL语法树：select * from userinfo where id=?



核心思想：放水抓鱼





中国互联网安全大会



360互联网安全中心

白模型鉴别 非常态阻断



中间件/应用服务器

NGDAP

数据库



SQL语句鉴别白模型

自动学习

正常功能请求，放行！

其他所有SQL请求，阻断！

攻击告警，攻击日志

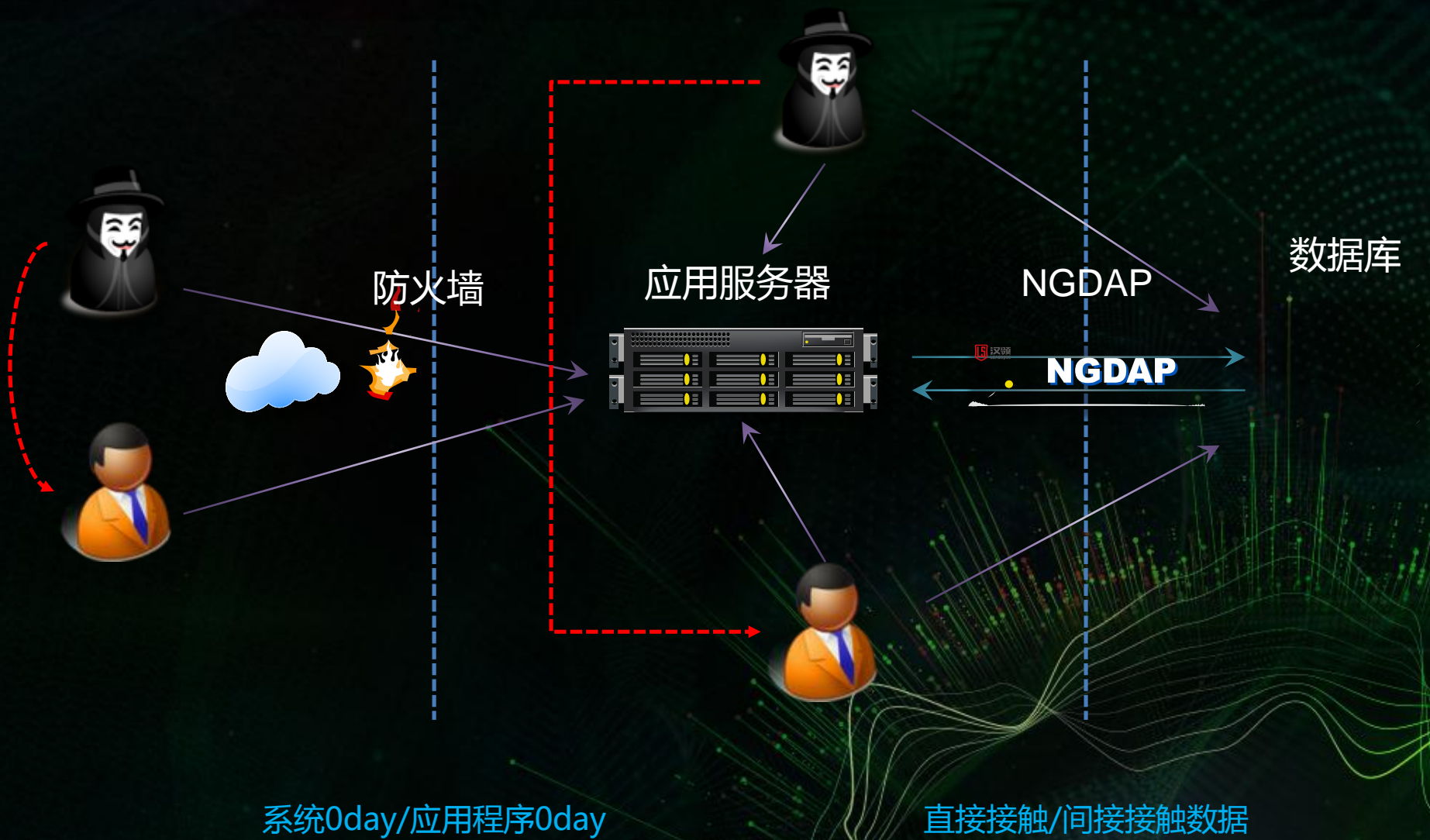


中国互联网安全大会



360互联网安全中心

应用场景



数据库全协议解码

Oracle

DB2

SQLServer

InforMIX

SYBASE

MySQL PostgreSQL



中国互联网安全大会



360互联网安全中心

超低延时，透明网桥模式部署

三层Bypass，健壮可靠



中国互联网安全大会



360互联网安全中心

高效

及时

精准

阻断



中国互联网安全大会



360互联网安全中心



数据边界安全

汉领将围绕『数据安全威胁的发现与防御』的核心贡献目标，构建和持续完善『数据边界安全』产品线。针对数据全生命周期的不同场景，提供相匹配的数据安全保护产品及解决方案。

谢 谢



中国互联网安全大会



360互联网安全中心