

高校常见安全漏洞案例分析

Monster

高校网络安全问题

- 现状
- 困局
- 案例
- 解决方案

高校安全现状

几乎所有服务器被秒请问校长知道吗

WooYun-2013-47372

残雪 ==
2013-12-30 11:26

查看详情

XX大学 Structs2命令执行漏洞

WooYun-2013-45814

路人甲 ==
2013-12-13 18:46

查看详情

XX教务平台系统GETSHELL (涉及百万学生信息安全)

WooYun-2013-44986

hacker@sina.cn ==
2013-12-05 11:57

查看详情

XX course grading系统漏洞(按照名单涉及29所学校)

WooYun-2013-43524

HoerWing ==
2013-11-21 13:09

查看详情

XX srun3000网页验证可实现暴力破解(只需3小时全系新生账号到手)

WooYun-2013-43540

HoerWing ==
2013-11-21 12:10

查看详情

查看详情

山东18岁女孩被骗走全部学费 心脏骤停不幸离世～

只看楼主

收藏

回复

18岁的杜天禹，从小学五年级起经常去网吧打游戏，就读初中二年级时退学，他在打网络游戏的过程中，对黑客技术产生了兴趣，开始尝试使用黑客技术在网上获取他人的数据信息，杜天禹给自己起了个网名叫“法师”，意思是掌握了魔法。

取便宜，成本取低，而且在网上购买十八信息对于仅有准反。

了教育部门的电话，让她办理了助学金的相关手续，说钱过几天就能发下来。”徐玉玉的母亲李自云告诉记者，由于前一天接到的教育部门电话是真的，所以当时他们并没有怀疑这则电话的真伪。

困局

- 安全难做
- 人手不够
- 经费不够
- 流程复杂

- SQL 注入
- 任意文件上传
- 弱口令
- 命令注入
- XSS

漏洞概要

缺陷编号: [WooYun-2012-08241](#)

漏洞标题: ■■■■■ 出入证管理系统弱口令导致14000多名人员资料泄露

相关厂商: ■■■■■

漏洞作者: [circus](#)

提交时间: 2012-06-13 02:40

公开时间: 2012-07-28 02:40

漏洞类型: 服务弱口令

危害等级: 中

自评Rank: 6

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: [后台被猜解](#) [用户敏感信息泄漏](#) [admin/admin弱口令](#) [配置不当](#) [webserver服务配置不](#)

漏洞概要

缺陷编号: [WooYun-2013-37940](#)

漏洞标题: 某大学校园转账终端远程控制服务(VNC)存在统一密码

相关厂商: 

漏洞作者: [NetSeif](#)

提交时间: 2013-09-24 10:08

公开时间: 2013-11-08 10:09

漏洞类型: 重要敏感信息泄露

危害等级: 高

自评Rank: 10

漏洞状态: 未联系到厂商或者厂商积极忽略

漏洞来源: <http://www.wooyun.org>

Tags标签: [敏感信息泄露](#) [内部敏感信息泄漏](#)

漏洞概要

缺陷编号: [WooYun-2013-27114](#)

漏洞标题: 某等国内296所高校DNS域传送漏洞

相关厂商: [国内300所大学域传送漏洞](#)

漏洞作者: [红帽子](#)

提交时间: 2013-06-28 16:15

公开时间: 2013-08-12 16:15

漏洞类型: 系统/服务运维配置不当

危害等级: 中

自评Rank: 5

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: [DNS域传送](#) [国内高校](#)

强智科技教务管理系统注入漏洞可改成绩

[WooYun-2014-11355](#)

小孩 == 
2014-03-28 12:40

正邦教育管理系统SQL注入

[WooYun-2014-48622](#)

monster = 
2014-01-12 10:19

方正系统客户端无密码任意登陆（如JWC01），影响所有版本

[WooYun-2013-34912](#)

Yep == 
2013-08-21 19:56


方正教务管理系统存在XSS漏洞可威胁所有登陆用户

[WooYun-2013-26083](#)

Yep == 杭州正邦教育软件有限公司
2013-06-16 21:53

方正教务管理系统教师权限可查看任意学生信息-也以北京电影学院为例

[WooYun-2013-26298](#)

pplover == 
2013-06-19 10:02

通用漏洞

■ 简要描述:

教务管理系统SQL注入

■ 详细说明:

在毕业设计管理的个人信息维护页面 (lw_xsxx.aspx) 存在SQL注入漏洞

■ 漏洞证明:



住所填',/* Email填*/email='123

然后点提交就发现email的值变成123了。

这样的话就可以随便修改学生个人信息表里的内容了。。。鄙视谁的话把他的学号改掉什么的。。

如果支持多语句环境的话就可以执行任意语句了。

简要描述:

■ 教务系统客户端的漏洞。根本原因在于软件设计的时候，用户登陆的认证在本地实现。

所这个洞不是新洞，和之前 @独孤城 发的这个<http://www.wooyun.org/bugs/wooyun-2010-010453> 根源是一样的。就是211端口。

不过这次发现他的客户端不仅有传输不加密的问题，还有更劲爆的问题~

详细说明:

实现思路：直接爆破客户端。

开发客户端的程序猿貌似没什么保护程序不被反汇编的经验。总之那个客户端一下就给爆破了。用的方法。。。基本上就是最简单的，一般讲反汇编爆破，第一课都会讲的方法。。。爆破方法比较简单。网上看看教程，就能搞定。目测这个漏洞正方一时半会也不会去修，爆破过程就不截图了。。。



■ 简要描述:

正方教务系统某目录权限设置不当, 有可能通过猜测文件名获得用户名和密码。

■ 详细说明:

正方教务系统一些关键操作都会记录log, 而log所在默认位置就是根目录/log。
以我们学校为例:



里面的文件命名格式是 "YYYY-MM-DD"+"-log.txt"或"YYYY-MM-DD"+"-Errorlog.txt"



从zjdx.dll里面也可以找到关于log文件建立的代码:



在正方教务的安装文档中, 并没有提示学校要限制log目录的访问, 导致漏洞的存在。

■ 漏洞证明:

log记录了登录用户的关键行为, 提交过的参数, 或数据库语句。
通过default_idap.aspx进行登录的用户, 他们的账号密码都会被写入log中。



在log.txt中通过搜索"passwd"就能找到大量用户密码。



花点时间就能找到jwc01的密码了。



■ 披露状态:

```
def decode(src):
    key = 'Encrypt01'
    str3 = ''
    num3 = 0
    num4 = len(src)
    if len(src) % 2 == 0:
        str4 = src[:num4/2]
        str4 = str4[::-1]
        str5 = src[num4/2:]
        str5 = str5[::-1]
        src = str4 + str5
    for i in range(num4):
        str6 = src[i:i+1]
        str2 = key[num3:num3+1]
        if ((ord(str6[0]) ^ ord(str2[0])) < 0x20) or ((ord(str6[0]) ^ ord(str2[0])) > 0x7E) or (ord(str6[0]) < 0) or (ord(str6[0]) > 0xFF):
            str3 = str3 + str6
        else:
            str3 = str3 + str(chr(ord(str6[0]) ^ ord(str2[0])))
        num3 = num3 + 1
        if num3 == len(key):
            num3 = 0
    return str3
```

还附带exp。。

```
def login():
    global cookie
```

详细说明：

问题出在用户注册页面的参数上。

系统的注册页面URL为：<http://biotech.ustc.edu.cn/BiotechWeb/BioTech/Pages/BT10/BT100200.aspx?businessId=Default>

在这个页面上有一个参数为“角色”，根据网站的需求这个角色应当是仅能为“注册用户”

。但页面加载的过程中将这个参数的所有值都加载进来了，通过chrome的审查元素功能或ie f12 以及firebug插件均可以绕过页面锁定进行修改。

详细步骤如下：

1、进入注册页面：<http://biotech.ustc.edu.cn/BiotechWeb/BioTech/Pages/BT10/BT100200.aspx?businessId=Default>

2、使用chrome的审查元素功能，或其他的类似浏览器插件，找到“角色”的参数值；



3、修改这一段代码的disabled="enable"、下一行的value修改为 value="3"；



4、输入任意用户名，点击“检查用户名”就会发现，角色已经修改成了“系统管理员”。

5、输入注册信息，完成注册就可以得到中国科学技术大学生命科学实验中心大型仪器设备管理系统的超级管理员权限。

漏洞概要

缺陷编号: [WooYun-2015-141618](#)

漏洞标题: 某医科大学电子邮件系统设计缺陷导致多个邮箱密码被修改并非授权访问

相关厂商: [CCERT教育网应急响应组](#)

漏洞作者: [quiterr](#)

提交时间: 2015-09-20 16:25

公开时间: 2015-09-25 16:26

漏洞类型: 设计缺陷/逻辑错误

危害等级: 中

自评Rank: 10

漏洞状态: 已交由第三方合作机构(CCERT教育网应急响应组)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: [未授权访问](#) [设计不当](#) [信息泄露](#)

解决方案

发现问题

解决问题

WAF 需要解决的问题

- 防御 Web 攻击

判断 WAF 好坏的指标

- 准确率
- 召回率
- 检测性能

传统 WAF 面临的难题

- 规则维护费心费力
- 正则规则难以应对变化的攻击
- 人工维护规则容易出错
- 难以防御未知威胁
- 性能随规则累加越来越慢

下一代 WAF 需要解决的问题

- 精准定位攻击
- 通过攻击日志分析潜在威胁

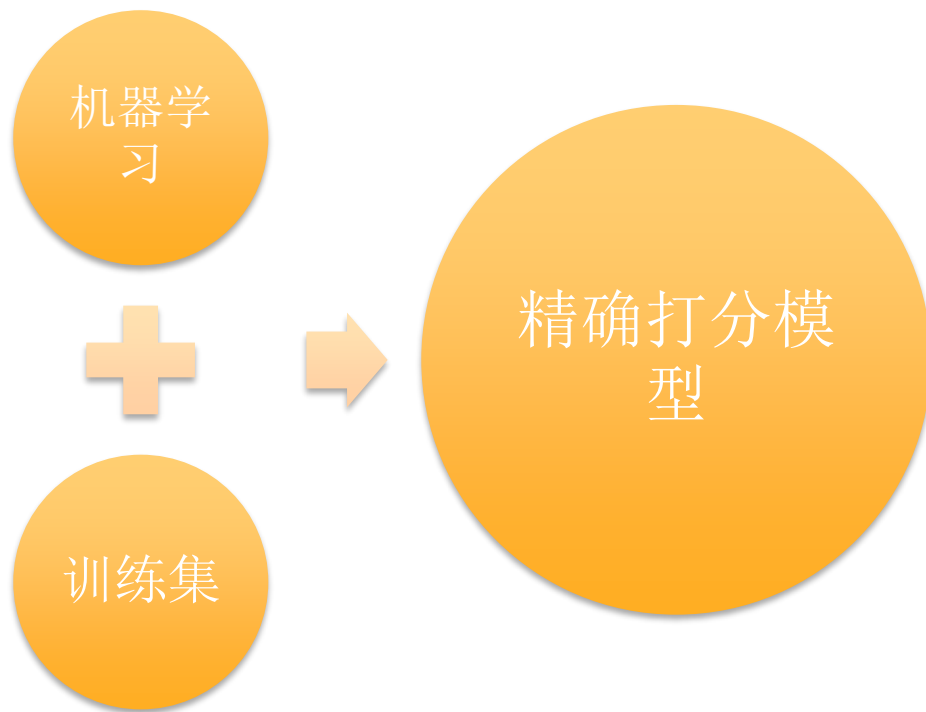
- 自动识别请求中存在的编码片段
- 自动解码
- 识别多层编码嵌套

词法、语法、语义分析

从更高的层面看攻击

具有更高级的形式语言抽象能力

攻击打分模型



攻击事件还原

- 攻击日志分析
- 攻击溯源

长亭雷池 Web 应用防火墙



高准确率、召回率，准确定位、深度发现攻击

高检测性能

高级日志分析

也许是一个新的解决思路

核心问题——人手不足

1. 精力不足
2. 不在攻防第一线

发动一切可以发动的力量

- 学生群体有着巨大的潜力
- 理论与动手有一定的距离
- 带学生进入攻防一线
- 形成正向循环