1. 网络空间安全概论

授课教师：游伟 副教授

授课时间：周五10:00 – 11:30（立德楼909）

课程主页：https://www.youwei.site/course/cybersecurity

引子

为什么当代大学生爱用匿名墙：

- 匿名性
- 言论自由

匿名墙中的当代大学生关注热点：

by 潘俊达（21图灵）

现场演示


RUC小喇叭
分享你的快乐，分担你的忧愁
昵称
发表
Web安全研讨课
搜索
我发
我回
我赞
新发
新回
最热
#2144970 管理员 | 置顶
1天前
小喇叭服务号来啦！关注以后能收到评论提醒🔔，以后发帖再也不用盯着有没有人回复啦～！
留言时间：2024 年 2 月20 日 19:26
详情
客户留言通知
2月20日
客户名称：谁来评论一下这条，我测试消息提醒功能
留言内容：你好
留言时间：2024 年 2 月20 日 19:26
详情
客户留言通知

人大小助手

手手子你好，我是人大信息学院21级图灵班的崔钰锟。我们这学期学习了《网络空间的安全攻防》新生研讨课，我和同班同学潘俊达一起对新版人大墙的安全性进行了探究，发现了其中存在一些安全漏洞，可以被攻击者利用来获取管理员权限。下附攻击效果图和漏洞报告。我们承诺在研究过程中，没有做任何有损他人的事。匿名墙是我们日常学习生活的调味剂，珍惜希望它能长久稳定地运行，希望我们的报告能够帮助更好地提升匿名墙的安全性。谢谢。

新人大墙漏洞报告.pdf
218.4 KB
PDF
微信电脑版

14:31

天呐

大神👍👍👍

谢谢你！马上反馈给技术修复漏洞🍌

新人大墙漏洞报告

作者：人大信息学院21级图灵班崔钰锟、潘俊达

邮箱：1572161937@qq.com

我们针对新人大墙展开了一系列安全测试和攻击测试，发现其存在比较明显的可利用的安全漏洞。

我们的发现如下：

漏洞	严重性
敏感接口未进行权限验证	高危
`openid` 可篡改	中危
管理员权限仅通过 `openid` 检验	高危

……

可能影响

控制台一行命令就可以使用和管理员一样的功能，操作难度比发包还低，传播开后极度容易被各种人利用。

修改建议

管理员应该用更强的验证手段保护，至少加入密码，同时应该是强密码，否则可能会被爆破出来。

总结

我们重点关注了 `openid` 的问题。

首先为了匿名墙的匿名性，他人的 `openid` 是绝不可以被任何手段获取的。

另外是管理员的 `openid` 已经泄露了，所以如今再修补隐蔽获取 `openid` 的接口可能为时已晚。我们建议慎重考虑是完善服务端对管理员 `openid` 的验证，还是直接抛弃，转而用密码等方式。

目录

1.1 网络空间安全的国内外现状

- 国际网络空间安全事件盘点
  - “冲击波”蠕虫病毒事件
  - 伊朗核电站“震网”病毒事件
  - ……
- 国内网络空间安全事件盘点
  - 国内政府网站遭受攻击事件
  - 用户信息数据库泄露事件
  - ……

“冲击波”蠕虫病毒事件

- 发生时间： 2003年8月
- 攻击目标：全球安装Windows系统的计算机
- 利用漏洞：MS03-026（微软Windows RPC DCOM漏洞）
- 攻击方式： Blaster利用微软Windows RPC DCOM漏洞进行传播，可在用户毫无知觉的情况下感染未打补丁的Windows计算机
- 损失危害：据微软数据显示，至少有800万台计算机被感染。有的数据显示Blaster蠕虫病毒至少攻击了全球80%的Windows用户。据评估，Blaster蠕虫病毒在全球造成的经济损失逾30亿美元

伊朗核电站“震网”病毒事件

- 发生时间：2010年7月
- 攻击目标：伊朗核电站（物理隔离网络）
- 利用漏洞： MS10-046（西门子SIMATIC WinCC系统0-Day漏洞）
- 攻击方式：利用漏洞成功控制离心机的控制系统，修改了离心机参数，让其生产不出制造核武器的物质，但在人工检测显示端正常
- 损失危害：美国利用“震网”蠕虫病毒攻击伊朗的轴浓缩设备，造成伊朗核电站离心机损坏，推迟发电达两年之久。感染全球超过45000个网络
- 入侵方式：
  - 收集核电站工作人员和其家庭成员信息
  - 针对家用电脑发起攻击，成功控制家用电脑
  - 感染所有接入的USB移动介质通过U盘将病毒摆渡核电站内部网络

国内政府网站遭受攻击事件

- 2013年5月，中国干部网被篡改，导致用户电脑在浏览该网站时被植入木马，在影响用户正常浏览网页信息的同时，造成账号密码的泄露
- 2013年8月，国家.cn顶级域名系统遭受大规模拒绝服务攻击，DSN域名系统陷入全线故障。部分网站解析受到影响，导致访问缓慢或中断
- ……

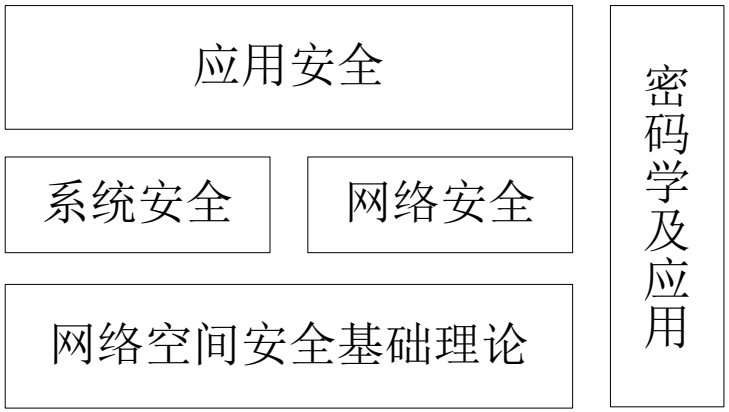
国家体育总局网站因漏洞被篡改

用户信息泄露事件

- 十大酒店泄露大量房客开房信息
  - 2015年2月11日，知名连锁酒店桔子、锦江之星、速八、布丁；高端酒店万豪（丽思卡尔顿酒店 等）、喜达屋（喜来登、艾美酒店等）、洲际（假日酒店等）网站存在高危漏洞——房客开房信息大量泄露，一览无余，黑客可轻松获取到千万级的酒店顾客的订单信息
  - 泄露信息包括顾客姓名、身份证、手机号、房间号、房型、开房时间、退房时间、家庭住址、信用卡后四位、信用卡截止日期、邮件等等大量敏感信息
- 机锋被曝泄露2300万用户信息：
  - 2015年1月5日，机锋科技旗下机锋论坛被曝出存在高危漏洞，多达2300万用户的信息遭遇安全威胁
  - 泄露的信息包括用户名、注册邮箱、加密后的密码等信息，由于机构数据库对用户密码仅使用了简单的MD5加密，黑客能快速破解出绝大部分明文密码
- ……

1.2 网络空间安全的知识体系

- 安全基础为其他方向的研究提供理论、架构和方法学指导
- 系统安全保证网络空间中单元计算系统的安全
- 网络安全保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全
- 应用安全保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用
- 密码学及应用为系统安全、网络安全和应用安全提供密码机制；



网络空间安全基础理论

- **网络空间安全数学理论**

  系统与网络建模、网络行为与演化建模

- **网络空间安全体系结构**

  顶层设计架构、网络空间安全模型与技术体系

- **网络空间安全数据分析**

  大数据分析理论与技术、为安全分析提供重要基础

- **网络空间博弈理论**

  网络空间行为与对抗的建模、攻防双方效益与行为的博弈建模

- **网络空间安全治理与策略**

  统一的网络空间安全政策架构、国家战略、安全法律法规、安全协助、安全底线等

- **网络空间的安全标准与评测**

  网络和信息系统在安全方面的标准规范和安全测评

系统安全

- **系统硬件和物理环境安全**

  计算机系统各组成部件和外设安全、设备认证、监控、信息泄露、访问控制、信息取证

- **系统软件安全**

  操作系统与中间件、数据库系统、语言处理系统等安全检测与防护、检测与恢复、安全生命周期管理、安全性评测等

- **恶意代码分析与防护**

  病毒、蠕虫、木马等恶意代码防御技术、分析与检测技术、隔离与清除技术

- **可信计算**

  基于硬件可信根的可信计算平台软硬件和方法理论

- **虚拟化计算平台安全**

  虚拟化计算平台安全保障技术、虚拟机监控、虚拟机迁移、虚拟机间安全通信等

- **漏洞挖掘、利用与修复**

  源代码审计、二进制代码审计、漏洞自动挖掘、漏洞利用代码自动生成、漏洞自动修复

网络安全

- **通信基础设施及物理环境安全**

  媒体电缆等固网安全、无线通信、移动通信网络、卫星网络等物理和链路层安全技术，窃听、信道加密、无线信道干扰阻塞、设备与链路的安全防护

- **互联网基础设施安全**

  路由系统安全、域名系统安全、通信协议安全、用户认证和访问控制如Radius认证协议、防火墙等

- **网络安全管理**

  安全风险和态势感知检测、接入与访问控制、入侵检测与防护、应急响应和网络攻击溯源取证、网络攻防

- **网络安全防护与主动攻防**

  网络安全漏洞的发现、分析和利用、攻防与对抗

- **端到端的安全通信**

  安全通信协议、VPN、IPsec、SSL、匿名通信

- **Web安全**

  Web应用安全、浏览器安全

应用安全

- **关键应用系统安全**

  关键信息基础设施：金融、能源、电力、化工、交通、医疗，安全体系结构、Web应用安全、安全态势感知与风险评估、动态安全防护、安全增强、安全产品认证与审查）

- **社会网络安全**

  包括内容安全、隐私威胁、恶意内容攻击、社会工程学、身份盗窃、网上滋扰、数字取证、网络内容识别和不良信息过滤、网络舆情与预警

- **隐私保护**

  隐私数据和数据所表征的特性、位置隐私、标识匿名、多敏感属性隐私保护

- **工控系统与物联网安全**

  关键信息基础设施、工控系统漏洞挖掘技术、入侵与异常检测技术、安全设计技术、APT防护技术、纵深防御技术

- **先进计算安全**

  云计算安全、移动计算安全、大数据安全

密码学及应用

- **对称密码设计与分析**

  分组密码、序列密码、消息认证码、哈希函数

- **公钥密码设计与分析**

  单向陷门函数、RSA类公钥密码、Elgmal类数字签名、ECC公钥密码、格密码等

- **安全协议设计与分析**

  密钥协商、秘密共享、身份认证、群签名、安全多方计算、电子投票

- **侧信道分析与防护**

  计时攻击、能量攻击、电磁辐射攻击、错误攻击等

- **量子密码与新型密码**

  量子计算环境下的密码体制设计与分析，包括加密、协议等、DNA密码、混沌密码

1.3 网络空间安全的意义与价值

- 发表学术论文

acm SIGSOFT

Distinguished Paper Award

FSE 2016

ACM SIGSOFT International Symposium on the Foundations of Software Engineering

November 13-18, 2016 Seattle, WA, USA

Presented to

Jianjun Huang, Xiangyu Zhang and Lin Tan

For

Detecting Sensitive Data Disclosure via Bi-directional Text Correlation Analysis

Thomas Zimmermann, General Chair
Jane Cleland-Huang, Program Chair
Zhendong Su, Program Chair

acm SIGPLAN

OOPSLA'19: International Conference on Object-Oriented Programming, Systems, Languages, and Applications

Distinguished Paper Award

Presented to

Zhuo Zhang, Wei You, Guanhong Tao, Guannan Wei, Yonghwi Kwon, Xiangyu Zhang

for

BDA: Practical Dependence Analysis for Binary Executables by Unbiased Whole-Program Path Sampling and Per-Path Abstract Interpretation

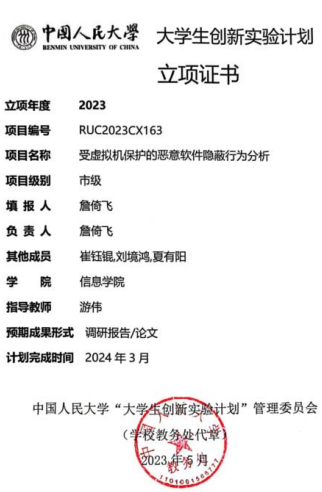
Eelco Visser
OOPSLA 2019 Program Chair

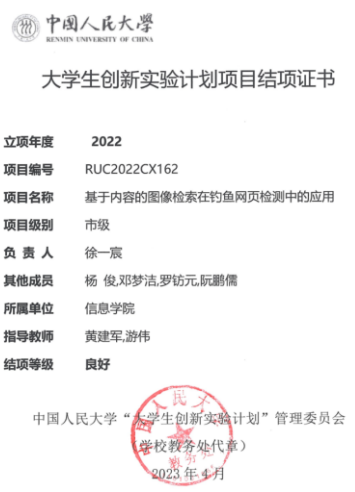
Yannis Smaragdakis
SPLASH 2019 General Chair

SPLASH 2019 – Athens, October 20-25, 2019

1.3 网络空间安全的意义与价值

- 参加学科竞赛和创新创业实践，将所学知识应用于实际





1.3 网络空间安全的意义与价值

- 助力构建更加安全的网络空间应用生态

Security bulletins

Addressed a potential issue where the application could be exposed to Out-of-Bounds Read Information Disclosure vulnerability and crash when processing certain arguments. This occurs due to the access of illegal memory as the application fails to restrict the access to an array outside its bounds when calling the *util.scand* function.	Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China
Addressed a potential issue where the application could be exposed to Out-of-Bounds Read Information Disclosure vulnerability and crash when processing certain arguments. This occurs due to the access of illegal memory as the application fails to restrict the access to an array outside its bounds when calling the *util.scand* function.	Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China
Addressed potential issues where the application could be exposed to Denial of Service, Null Pointer Reference, Out-of-Bounds Read, Context Level Bypass, Type Confusion, or Buffer Overflow vulnerability and crash, which could be exploited by attackers to execute remote code. This occurs during the implementation of certain functions in JavaScript due to the use of incorrect parameters or objects without proper validation (CNVD-C-2020-305224/CNVD-C-2020-305182/CNVD-C-2020-305095/EIP-2018-0045/CNVD-C-2020-305100/CVE-2021-31461/CVE-2021-31476).	Xinyu Wan, Yiwei Zhang, and Wei You from Renmin University of China China National Vulnerability Database mnhFly of Aurora Infinity WeiZhen Security Team Exodus Intelligence cor3sm4sh3r working with Volon Cyber Security Pvt Ltd working with Trend Micro Zero Day Initiative Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense cece working with Trend Micro Zero Day Initiative

- Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China (CVE-2020-9611, CVE-2020-9610, CVE-2020-9605, CVE-2020-9604, CVE-2020-9603, CVE-2020-9598, CVE-2020-9595, CVE-2020-9593)
- Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China (CVE-2020-9705, CVE-2020-9711, CVE-2020-9713)
- Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China (CVE-2020-3806, CVE-2020-3807, CVE-2020-3795, CVE-2020-3797)
- Xinyu Wan, Yiwei Zhang and Wei You from Renmin University of China (CVE-2020-3743, CVE-2020-3745, CVE-2020-3746, CVE-2020-3749, CVE-2020-3750, CVE-2020-3752, CVE-2020-3754)

Case offer: KMFL0002 Inbox ×

zdi@trendmicro.com
to me

Wed, Mar 16, 1:51 AM (5 days ago)

Hello KMFL,

Thank you for your submission. We have successfully verified your submitted advisory in our lab and are interested in purchasing it from you. We would like to officially extend an offer of 625 USD for the rights to your vulnerability.

Case offer: KMFL0003 Inbox ×

zdi@trendmicro.com <zdi@trendmicro.com>
to me

Tue, Mar 8, 6:51 PM (13 days ago)

Hello KMFL,

Thank you for your submission. We have successfully verified your submitted advisory in our lab and are interested in purchasing it from you. We would like to officially extend an offer of 550 USD

Case offer: KMFL0004 Inbox ×

zdi@trendmicro.com
to me

Wed, Mar 16, 10:47 PM (5 days ago)

Hello KMFL,

Thank you for your submission. We have successfully verified your submitted advisory in our lab and are interested in purchasing it from you. We would like to officially extend an offer of 650 USD for the rights to your vulnerability.

Case offer: RUCSESEC0005 Inbox ×

zdi@trendmicro.com <zdi@trendmicro.com>
to me

Wed, Mar 16, 11:03 PM (5 days ago)

Hello RUCSESEC,

Thank you for your submission. We have successfully verified your submitted advisory in our lab and are interested in purchasing it from you. We would like to officially extend an offer of 900 USD for the rights to your vulnerability.

This offer is valid for 7 calendar days. After 7 calendar days, the offer is rescinded. The same way, if all required documentation/information for the payment is not provided within the 10 days after acceptance of the offer, the offer will also be rescinded. If, after that time, you would like ZDI to re-offer, please let us know. We may be willing to do so.

Acceptance of this offer is your commitment to abide by the terms of the current ZDI Researcher Agreement (https://zerodayinitiative.com/documents/zdi_researcher_agreement.pdf).

Upon acceptance of this offer you will have achieved a total of 900 reward points.

For details on reward benefits please visit: http://www.zerodayinitiative.com/about/benefits/

As a reminder you selected wire_transfer as the payment method for this case, if that is incorrect let us know in your response and we will update it.

Please allow between 5 and 10 business days for payment to arrive. If this is your first time being paid by the ZDI, an additional 5-10 days should be expected.

Kind regards,
Zero Day Initiative
zdi@trendmicro.com

14天4个漏洞赏金收入：$625+$550+$630+$900 = $2705 ≈ ￥17215

1.3 网络空间安全的意义与价值

- 助力增强国家网络空间安全
  - 研发系统被华为公司采用，用于实际产品的检测
  - 研发工具被国家安全相关部门采用，用于国际安全攻防实际
  - ……
- 为政府和官方组织出谋划策
  - 区块链安全、大数据安全等多项国家标准的制定工作
  - 研究报告被中央网信办等部门采纳
  - ……

1.3 网络空间安全的伦理规范

- 告知实验对象即将参与的实验内容和可能造成的危害
- 将危害降低到最小限度
- 尽有能在测试环境而非真实中进行实验
- 实验完成后，尽可能恢复所造成的损害
- 不用所掌握的知识作恶和非法牟利

1.3 网络空间安全的伦理规范

- 匿名墙给我们的启示
  - 网络不是法外之地，言论自由要建立在法律和道德框架内
  - 互联网是有记忆的，黑历史会长久留下痕迹
  - 理性吐槽、合理发表意见，避免肆无忌惮、无端谩骂地匿名“喷喷”