

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:56 交卷

展开 » 0 / 30 题

1. 单选题 (2分)

(2-7) 缓冲区溢出能被用于覆盖函数或数据指针，必须（ ）同时成立。

a、缓冲区与目标函数或者数据指针必须分配在同一个段内；  
b、缓冲区必须可以被缓冲区溢出利用；  
c、缓冲区的数据类型必须与目标指针的类型相同；  
d、缓冲区必须位于比目标函数或者数据指针更低的地址处；  
e、缓冲区必须位于比目标函数或者数据指针更高的地址处。

2. 填空题 (2分)

(1-5) 一致的内存管理约定包括  
输入答案 等。

请保持背景无变化且没有其他人出现在镜头内

1 2 3 4 5 6 7

Windows 搜索 菜单 文件 Internet Explorer Word 微信 13:29 2020/6/19 9

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:56 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

2. 填空题 (2分)  
(1-5) 一致的内存管理约定包括  
输入答案 等。

3. 主观题 (5分)  
【简答题】对比植入shellcode中静态淹没返回地址与JMP ESP两种方式的优缺点。

请保持背景无变化  
且没有其他人出现在镜头内

B I U ☰ 手机传图 Σ 代码语言

字数统计

文档将自动保存

Windows 搜索 菜单 Microsoft Edge Word 微信 13:29 2020/6/19 中文 拼音 9

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:56 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

4. 填空题 (2分)

(1-1) 侦测整数错误的方法主要有  
输入答案 和 输入答案。

5. 主观题 (5分)

【简单题】列举动态分配缓冲区的缺点。

B I U C 手机传图 Σ 代码语言

字数统计

文档将自动保存

?

13:29 2020/6/19

9

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:55 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

添加附件 (可上传1个附件, 文件不超过100M) ?

6. 主观题 (10分)

【分析题】简述虚函数的实现，并试述利用虚表对虚函数开展攻击的过程。假设声明了一个类vf，具有160字节的成员变量buf和虚函数test，main函数中可以通过溢出修改虚表，据此做答。

B I U C 手机传图 Σ 代码语言

字数统计

文档将自动保存

添加附件 (可上传1个附件, 文件不超过100M) ?

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:55 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

文档将自动保存

添加附件 (可上传1个附件, 文件不超过100M) ?

字数统计

7. 主观题 (3分)

【名词解释】整数回绕

手机传图 代码语言

字数统计

请保持背景无变化  
且没有其他人出现在镜头内

文档将自动保存

B I U ⌂ 手机传图 Σ 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:55 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

8. 主观题 (5分)

【简答题】指出下列代码在什么情况下时，就会发生缓冲区溢出。

```
01 void good_function(const char *str) {...}
02 void main(int argc, char **argv) {
03     static char buff[BUFFSIZE];
04     static void (*funcPtr)(const char *str);
05     funcPtr = &good_function;
06     strncpy(buff, argv[1], strlen(argv[1]));
07     (void)(*funcPtr)(argv[2]);
08 }
```

B I U 手机传图 代码语言 字数统计

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:54 交卷

展开 » 0 / 30题

1 文档将自动保存 字数统计

2 添加附件 (可上传1个附件, 文件不超过100M) ?

3 请保持背景无变化  
且没有其他人出现在镜头内

4 9. 主观题 (3分)

【名词解释】缓冲区溢出攻击

B I U C 手机传图 Σ 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:54 交卷

展开 » 0 / 30题

10. 单选题 (2分)

(2-2) 下列Windows机制中不是针对缓冲区溢出的技术为: ( )

A GS编译技术  
B S.E.H  
C ASLR (Address space layout randomization)  
D DEP

请保持背景无变化且没有其他人出现在镜头内

11. 主观题 (5分)

【简答题】请解释printf(“%s%s%s%s%s%s%s%s%s%s” )格式化输出可能导致程序崩溃?

B I U C 手机传图 Σ 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:54 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

添加附件 (可上传1个附件, 文件不超过100M) ?

12. 主观题 (1分)

【上传图片位置】此题仅作为上传图片使用。

B I U ⌂ 手机传图 代码语言

字数统计

文档将自动保存

添加附件 (可上传1个附件, 文件不超过100M) ?

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:54 交卷

展开 » 0 / 30题

1 文档将自动保存 2 3 4 5 6 7

添加附件 (可上传1个附件, 文件不超过100M) ②

请保持背景无变化  
且没有其他人出现在镜头内

13. 主观题 (5分)

【简答题】什么是空闲内存列表，并画出其关键数据结构。

B I U ⌂ 手机传图 Σ 代码语言

字数统计

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:53 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

**14. 单选题 (2分)**

(2-8) 考察下面的代码:

```
01 enum { BLOCK_HEADER_SIZE = 16 };
02 void *AllocateBlock(size_t length) {
03     struct memBlock *mBlock;
04     if (length + BLOCK_HEADER_SIZE > (unsigned long long)SIZE_MAX) {
05         return NULL;
06     }
07     mBlock = (struct memBlock *)malloc(
08         length + BLOCK_HEADER_SIZE
09     );
10     if (!mBlock) return NULL;
11     /* fill in block header and return data portion */
12     return mBlock;
13 }
```

这段程序最根本的漏洞是什么 ( )

A 非异常整数逻辑错误;  
B 有符号整数溢出;  
C 转换错误;  
D 无符号整数回环。

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:53 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

**15. 填空题 (2分)**

(1-4) 常见的字符串操作错误主要包括:  
输入答案 等。

**16. 单选题 (2分)**

(2-9) 关于限制字节写入的漏洞缓解方法, 下列说法错误的是 ( )。

A 缓冲区溢出可以通过严格控制函数写入的字节数来避免;  
B snprintf() 比 sprintf() 更安全, vsnprintf() 比 vsprintf() 更安全;  
C 函数 asprintf() 和 vasprintf() 为字符串分配足够大的空间以容纳包括末尾空字符在内的输出内容;  
D 使用更安全版本的格式化输出库函数可以杜绝缓冲区溢出问题。

**17 单选题 (2分)**

13:29 2020/6/19

请保持背景无变化  
且没有其他人出现在镜头内



雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:53 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

B snprintf() 比 sprintf() 更安全, vsnprintf() 比 vsprintf() 更安全;  
C 函数 asprintf() 和 vasprintf() 为字符串分配足够大的空间以容纳包括末尾空字符在内的输出内容;  
D 使用更安全版本的格式化输出库函数可以杜绝缓冲区溢出问题。

请保持背景无变化  
且没有其他人出现在镜头内

17. 单选题 (2分)

(2-6) 关于异常处理, 以下哪种说法是错误的 ( )

A 栈探测仪可以保护包括栈段在内的任何位置发生缓冲区溢出;  
B 攻击者可以通过覆写异常处理程序地址修改指令指针;  
C 在 try ... catch 块中, 如果 catch 块无法处理该异常, 那么它将被传回之前的范围块;  
D 已注册的异常处理程序列表是由 Thread Environment Block(TEB) 中的指针引用的。

18. 主观题 (5分)

Windows 搜索 菜单 文件 Microsoft Edge Word 微信 13:29 2020/6/19 9

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:53 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

D 已注册的异常处理程序列表是由Thread Environment Block(TEB) 中的指针引用的。

18. 主观题 (5分)

【简答题】指出并分析下面程序的整数溢出问题。

```
01 void getComment(size_t len, char *src) {  
02     size_t size;  
03     size = len - 2;  
04     char *comment = (char *)malloc(size + 1);  
05     memcpy(comment, src, size);  
06     return;  
07 }  
08  
09 int main(int argc, char *argv[]) {  
10     getComment(1, "Comment ");  
11     return 0;  
12 }
```

请保持背景无变化且没有其他人出现在镜头内

B I U 手机传图 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:52 交卷

展开 » 0 / 30题 文档将自动保存 字数统计

1 添加附件 (可上传1个附件, 文件不超过100M) ?

2

3

4

5

6

7

19. 单选题 (2分)

(2-1) 如下表赋值表达式所示, names是一个UTF-8的字符串:

```
01 char names[] = "\xD4\xBC\xF0\x9D\x90\x84\x45\xC6\xAC\x00"
```

那么该字符串的长度是( )

A 4  
B 10  
C 9  
D 5

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:52 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

20. 填空题 (2分)

(1-2) 采用补码表示, 采用补码表示, 一个8比特的数据, 无符号整数可以表示的范围是  
输入答案 \_\_\_\_\_ , 有符号整数可以表示的范围是 \_\_\_\_\_ 输入答案 \_\_\_\_\_ 。

请保持背景无变化  
且没有其他人出现在镜头内

21. 主观题 (5分)

【简答题】不安全的API是导致字符串错误的重要原因, 试列举并说明5个不安全的字符串API?

B I U ⌂ 手机传图 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:52 交卷

展开 » 0 / 30题

1 文档将自动保存 2 添加附件 (可上传1个附件, 文件不超过100M) ?

3 4 5 6 7

请保持背景无变化  
且没有其他人出现在镜头内

22. 主观题 (9分)

**【分析题】**  
先写出frontlink技术实现代码, 分析它并给出实现攻击者提供4字节的数据写入到同样是攻击者指定的4字节地址的实例详细过程。

B I U 手机传图 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:51 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

添加附件 (可上传1个附件, 文件不超过100M) ?

23. 单选题 (2分)

(2-10) 要成功地利用双重释放漏洞, 需满足的条件不包括: ( )

A 被释放的内存块必须在内存中独立存在;  
B 被释放的内存块相邻的内存块必须是已分配的;  
C 被释放的内存块相邻的内存块必须是未分配的;  
D 被释放的内存块所被放入的筐 (bin) 必须为空。

请保持背景无变化  
且没有其他人出现在镜头内

24. 填空题 (2分)

(1-3) 操作系统中进程所使用的内存根据用途不同, 按照功能主要可分成  
输入答案 、 输入答案 、 输入答案 和  
输入答案 四大部分。

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:50 交卷

展开 » 0 / 30 题

1 2 3 4 5 6 7

24. 填空题 (2分)

(1-3) 操作系统中进程所使用的内存根据用途不同，按照功能主要可分成  
输入答案 、 输入答案 、 输入答案 和  
输入答案 四大部分。

请保持背景无变化  
且没有其他人出现在镜头内

25. 主观题 (3分)

【名词解释】恶意软件

B I U ☰ 手机传图 Σ 代码语言

字数统计

文档将自动保存

Windows 搜索 菜单 Microsoft Edge Microsoft Word Microsoft Excel Microsoft PowerPoint 微信 13:29 2020/6/19 9

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:50 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

文档将自动保存

添加附件 (可上传1个附件, 文件不超过100M) ?

26. 单选题 (2分)

(2-3) 该段代码第三行该如何为变量prog\_name分配内存? ( )

```
1. int main(int argc, char *argv[]) {  
2.     const char *const name = argv[0] ? argv[0] : "";  
3.     //补充: 声明prog_name并分配内存  
4.     if(prog_name != NULL){  
5.         strcpy(prog_name, name);  
6.     }  
7. }
```

请保持背景无变化  
且没有其他人出现在镜头内

字数统计

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:50 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

**27. 单选题 (2分)**

(2-5) 根据以下代码, 任何长度大于( )字节的字符串都会导致越界写:

```
char buffer[512];
sprintf(buffer, "Wrong command: %s\n", user);
```

A char \*prog\_name = malloc(strlen(name));  
B char \*prog\_name = malloc(strlen(name)+1);  
C char \*prog\_name = (char \*)malloc(strlen(name));  
D char \*prog\_name = (char \*)malloc(strlen(name)+1);

请保持背景无变化  
且没有其他人出现在镜头内

Windows taskbar icons: File Explorer, Edge, Word, Camera, Chat, Network, Battery, Volume, Language, Date/Time (13:29, 2020/6/19), Notifications (9).

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:50 交卷

展开 » 0 / 30 题

28. 单选题 (2分)

(2-4) gets()、puts()、strcpy()、strcat()、strlen()、printf()、memcpy()和memset()等8个API均来自标准C，其中能够导致无界字符串越界写操作的有( )个。

A 3  
 B 4  
 C 5  
 D 6

请保持背景无变化且没有其他人出现在镜头内

29. 主观题 (3分)

【名词解释】有效用户ID

B I U 手机传图 代码语言

13:29 2020/6/19

雨课堂 考试系统

https://examination.xuetangx.com/exam/86163?isFrom=2

分类: Compile Princ... 编译原理 (哈工大...) 脚本之家 腾讯云 youzack Ryzentosh CTF Wiki Ac1d\_blog h0lyduck's 树洞 h0lyduck后台 其他收藏夹

2019~2020学年第二学期软件安全期末考试试卷 考试剩余: 02:14:50 交卷

展开 » 0 / 30题

1 2 3 4 5 6 7

添加附件 (可上传1个附件, 文件不超过100M) ?

30. 主观题 (3分)

(3-1) 【名词解释】竞争条件

B I U C 手机传图 Σ 代码语言

字数统计

文档将自动保存

添加附件 (可上传1个附件, 文件不超过100M) ?

请保持背景无变化  
且没有其他人出现在镜头内

13:29 2020/6/19