第十二届全国大学生信息安全竞赛-创新实践能力赛

总决赛应用场景开发需求

依照《第十二届全国大学生信息安全竞赛—创新实践能力参赛规程与指南》要求，创新实践能力赛总决赛阶段的应用场景开发需求分为 WEB 、PWN 两类场景，入围战队需根据场景开发的功能特性需求，选择其中的一个场景，开发出符合要求的安全应用，并预设创新性的网络安全挑战，构建出在总决赛环节中使用的靶标环境。

一、题目设置规范：

WEB 方向出题要求

基本要求

1. 使用 php/python/java/c#等常用编程语言实现，运行在 Apache/Nginx/IIS/Weblogic 等服务器，后端数据库使用 mysql/T-SQL/sqlite3/mongodb 等；
2. 设计的 WEB 安全漏洞利用路线有且只有一条，禁止预设多种获取 flag 的途径；
3. 需要提供测试视频以验证 check.py 以及 exp.py 正常可用；
4. WEB 程序统一映射端口：80，请勿修改此端口；
5. flag 存放于`/flag`（Linux），`C:\flag.txt`（Windows），并提供更新 flag 的命令（默认 flag 请设置为 `flag{flag_test}`）；
6. 提供 3 个提示，按从难度从低到高填写；
7. 确保在 check 服务正常的情况下，能够修补漏洞；
8. linux 题目需要制作成 docker 镜像；
9. 制作模板请参照 '赛题设计模板'。

Check 要求

1. 检查 WEB 服务是否正常工作，关键页面能否访问；
2. 检查关键服务是否正常运行；
3. 检查 WEB 服务是否存在通用防护；
4. 检查 flag 是否被修改，如无法 getshell，不检测。

Exp 要求

1. 提供可以获取到 flag 的脚本

服务运行系统

WEB 服务运行允许的操作系统有：

1. Windows 包括：Win2003、winXP、win10
2. Linux 包括：CentOS 6-7 minimal，Ubuntu 14.04 - 18.04 server

特殊系统环境请于设计文档中说明，并补充下载地址。

赛题文件夹规范

1. 赛题设计说明.md 【Web design document】（内容包含制作过程 以及 解题方法）；
2. 附件 【Appendix】（供选手下载分析）：

   题目名小写 md5 值.zip （例：gift61846d544c13b6b91dc868e570071843.zip）；
3. 源码【source code】：

   docker （存放 Dockerfile 文件等，如无法使用 docker 情况，请在此文件夹中详细描述服务搭建过程）；

   source （存放赛题制作的源码、编译环境以及命令）；

4. 解题视频 【video】（供验证 check、exp 脚本正确性）：

   题目名.avi/题目名.mp4；

5. img【img】：

   （存放赛题设计说明.md 中图片内容）；

6. check 脚本【check script】：

   check.py（检查 WEB 程序正常工作的脚本）；

7. exp 脚本【exp script】：

   exp.py（验证 WEB 程序漏洞可用的脚本）。

PWN 方向出题要求

基本要求

1. 使用 C/C++ 源码编译 PWN 序，不可使用其他语言，允许的编译架构：X86-32、X86-64；
2. 设计的 PWN 程序漏洞利用路线有且仅有一条，禁止预设多种获取 flag 的途径；
3. 需要提供测试视频以验证 check.py 以及 exp.py 正常可用；
4. PWN 程序统一映射端口：8888，请勿修改此端口；
5. flag 存放于`/flag`（Linux），`C:\flag.txt`（Windows），并提供更新 flag 的命令（默认 flag 请设置为 `flag{flag_test}`）；
6. 提供 3 个提示，按从难度从低到高填写；
7. 确保在 check 服务正常的情况下，能够修补漏洞；
8. linux 题目需要制作成 docker 镜像；
9. 制作模板请参照 '赛题设计模板'。

Check 要求

1. 检查 PWN 服务是否正常工作，运行流程是否异常；

2. 检查 PWN 服务是否存在通防（防止选手恶意 patch）；
3. 如果有堆题，建议检测 free 函数是否被恶意修改；
4. 检查 flag 是否被修改，如无法 getshell，不检测。

Exp 要求

1. 能够 getshell 的脚本。

服务运行系统

PWN 服务运行允许的操作系统有：

1. Windows 包括：Win2003、winXP、win10
2. Linux 包括：CentOS 6-7 minimal，Ubuntu 14.04 - 18.04 server

特殊系统环境请于设计文档中说明，并补充下载地址。

赛题文件夹规范

8. 赛题设计说明.md 【PWN design document】（内容包含制作过程 以及 解题方法）；
9. 附件 【Appendix】（供选手下载分析）：

    题目名小写 md5 值.zip （例：gift61846d544c13b6b91dc868e570071843.zip）；
10. 源码【Source code】：

    docker （存放 Dockerfile 文件等，如无法使用 docker 情况，请在此文件夹中详细描述服务搭建过程）；

    source （存放赛题制作的源码、编译环境以及命令）；
11. 解题视频【Video】 （供验证 check、exp 脚本正确性）：

    题目名.avi/题目名.mp4；
12. img【img】：

（存放赛题设计说明.md 中图片内容）；

13. check 脚本【check script】：

check.py（检查 WEB 程序正常工作的脚本）；

14. exp 脚本【exp script】：

exp.py（验证 WEB 程序漏洞可用的脚本）。

二、Build It 环节积分规则

环节	分值		说明
Build It	20	0 或 2	【EXP 通过率】 对参赛队提供的 EXP 脚本进行测试，以能成功获取平台方配置的 Flag，则获取该部分得分。
		0-2.5	【能力符合度】 1、安全技术点、漏洞利用点具有一定实用性、新颖性； 2、体现网络空间安全及相关专业应具备知识技能的综合应用；

			3、赛题场景反应了常见应用的新问题，或是热点应用的新问题，能反应信息安全/网络安全技术应用的方向和趋势。
		0 或 2	【选中作为大赛赛题】 符合分区赛赛题使用标准，被纳入大学生信息安全竞赛——创新实践能力赛题库中的题目获得该部分分值。

		0 或 4.5	【功能实现度-完整性】 1、场景设计部分以战队为单位提交，场景必须由晋级分区赛的选手独立完成； 2、场景设计中不得包含违反法律法规和违背社会道德的敏感词汇； 3、场景设计中不得有侵害他人知识产权、品牌及名誉的内容，设计者需要对场景享有完全的知识产权或对借鉴他人的部分享有充分授权； 4、场景中不得含有关于场景设计者信息的描述或暗示； 5、分区赛现场不允许任何人通过任何形式外接网络，所以场景设计时请考虑避免需要联网的内容，如有外链请下载到本地并改为使用本地链接； 6、请不要附带无关文件，最后提供压缩包以及其文件哈希值（如 md5 值），并以“md5 验证.txt”为文件名放到场景的压缩包中；

			7、如有特殊情况的请备注。

		0 或 4.5	【功能实现度-可用性】 1、场景考点设计是否有一定的逻辑性、合理性（拒绝纯脑洞出题）； 2、web 题目的静态资源（如 js、css）是否要使用外链； 3、pwn 题的源码是否能编译； 4、check 和 exp 脚本必须可用； 5、解题的路径仅是否只有一条。
		0 – 4.5	【功能实现度-实用性】 1、可能在信息安全/网络安全等领域产生影响； 2、是否和业务实践紧密结合。

三、题目设置要求：

1. 场景文档描述和设计需要符合国家法律法规和社会道德共识；不得包含违反法律法规和违背社会道德的敏感词汇；
2. 场景设计部分以战队为单位提交，场景必须由晋级总决赛的选手独立完成；
3. 场景设计中不得有侵害他人知识产权、品牌及名誉的内容，设计者需要对场景享有完全的知识产权或对借鉴他人的部分享有充分授权；
4. 在本年度全国大学生信息安全竞赛创新实践能力赛结束前，不得通过任何形式向组委会指定邮箱以外的地方泄露，违者将直接取消比赛资格；

5. 场景设计模板中的样题仅为示例，供参赛战队参考；

6. 场景中不得含有关于场景设计者或相关人员信息的描述或暗示；

7. 请仔细阅读该出题标准，并按照标准来设计赛题；

8. 题目设计应该有一定的逻辑性、合理性、禁止长时间 猜测/爆破 相关行为设计；

9. 赛题文件夹中的所有文件需要全部提供，否则扣除相应分数；

10. 更新的 flag 默认格式为 flag{uuid} （例如：flag{8ba868f2-71b6-477b-bc7a-255302c881e1}），如有特殊情况请说明原因，flag 的格式至少需要有 flag{}，禁止使用其它格式。

11. 文件夹内所有子文件均以英文命名，文件夹统一命名规范【战队名-学校名-题目类型】.zip

12. 晋级队伍需要在7月8日24点前提交自行创新赛题的源码、设计文档、视频演示、题目提示、exp脚本、check脚本等至技术委员会提供的邮箱（ciscn2019@126.com），提交后将按照提交时间进行编号，由技术委员会负责审核；

13. 7月8日- 10日期间提交赛题者该环节得分将扣 5 分（权重20%），不提交赛题的队伍该环节得分为 0。赛题若存在高度雷同的情况下，将直接通报大赛组委会，该环节得分为 0；

14. 如有特殊情况的请备注。

教育部高等学校网络空间安全专业教学指导委员会

第十二届全国大学生信息安全竞赛—创新实践能力赛技术委员会

第十二届全国大学生信息安全竞赛-创新实践能力赛组委会

2019 年 6 月 29 日