通过环境变量进行攻击

S3.1. 环境变量与 shell 变量有什么区别？

S3.2. 在 Bash 中执行 `"export foo=bar"` 时，它是否直接修改当前 shell 进程的环境变量？

S3.3. 以下两条命令都可显示环境变量。请说明它们的区别：

```
$ /usr/bin/env
$ /usr/bin/strings /proc/$$/environ
```

S3.4. 使用 `execve()` 执行外部程序 `xyz`，并把第三个参数传为 `NULL` 时，新程序会有多少个环境变量？

S3.5. Bob 说自己的应用代码从不读取环境变量，因此无需考虑环境变量带来的安全问题。他说得对吗？

S3.6. 程序 `abc` 通过 `system()` 调用外部程序 `xyz`，所以其行为会受到 `PATH` 环境变量影响。从命令行启动 `abc` 时，当前 shell 中的 `PATH` 变量如何一路影响 `system()` 的行为？

S3.7. 请解释在特权程序中，为什么 `secure_getenv()` 通常比 `getenv()` 更安全。

S3.8. 特权 `Set-UID` 程序需要确定当前工作目录。一种方法是读取包含当前目录完整路径的 `PWD` 环境变量，另一种是调用 `getcwd()`。应选择哪一种？为什么？

S3.9. 在 Linux 中，动态链接器会在执行 `Set-UID` 程序时忽略一些环境变量，例如 `LD_PRELOAD` 和 `LD_LIBRARY_PATH`。请阅读 `ld-linux` 手册（`https://linux.die.net/man/8/ld-linux`），并解释为什么下列变量也会被忽略：

- `LD_AUDIT`
- `LD_DEBUG_OUTPUT`

S3.10. 让普通用户完成特权任务通常有两种办法：提供由 root 拥有的 `Set-UID` 程序供用户直接执行，或由专用的 root 守护进程代表用户完成任务。请比较两种方案的攻击面，并说明哪种通常更安全。