在 php + mysql + apache 架构的 web 服务中输入 GET 参数 index.php?a=1&a=2&a=3 服务器端脚本 index.php 中$GET[a] 的值是？

正确答案: C 你的答案: 空 (错误)

1
2
3
1,2,3

以下哪些不是 CSRF 漏洞的防御方案？

正确答案: D 你的答案: 空 (错误)

检测 HTTPreferer
使用随机 token
使用验证码
html 编码

以下程序存在何种安全漏洞？

```
<tr>
   <td class="font_content" align="right">交易状态：</td>
   <td class="font_content" align="left"><?php echo $_GET['trade_status'];?></td>
</tr>
```

正确答案: A 你的答案: 空 (错误)

XSS
sql 注入
命令执行
代码执行

下列哪些工具可以作为离线破解密码使用？

正确答案: D 你的答案: 空 (错误)

hydra
Medusa
Hscan
OclHashcat

下列命令中不能用于 Android 应用程序反调试的是？

正确答案: C 你的答案: 空 (错误)

ps
cat/proc/self/status
cat/proc/self/cmdline
cat/proc/self/stat

用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？

正确答案: B 你的答案: 空 (错误)

缓存溢出攻击
钓鱼攻击
暗门攻击
DDOS 攻击

下列关于各类恶意代码说法错误的是？

正确答案: C 你的答案: 空 (错误)

蠕虫的特点是其可以利用网络进行自行传播和复制
木马可以对远程主机实施控制
Rootkit 即是可以取得 Root 权限的一类恶意工具的统称
pcshare 一种远程控制木马

关于 XcodeGhost 事件的正确说法是？

正确答案: B 你的答案: 空 (错误)

部分 Android 产品 也受到了影响
应用程序开发使用了包含后门插件的 IDE
当手机被盗时才有风险
苹果官方回应 APPSTORE 上的应用程序不受影响

下列关于各类恶意代码说法错误的是？

正确答案: C 你的答案: 空 (错误)

蠕虫的特点是其可以利用网络进行自行传播和复制
木马可以对远程主机实施控制
Rootkit 即是可以取得 Root 权限的一类恶意工具的统称
通常类型的病毒都只能破坏主机上的各类软件，而无法破坏计算机硬件

Unix 系统日志文件通常是存放在？

正确答案: A 你的答案: 空 (错误)

/var/log
/usr/adm
/etc/
/var/run

防止系统对 ping 请求做出回应，正确的命令是？

正确答案: C 你的答案: 空 (错误)

echo 0>/proc/sys/net/ipv4/icmp_ehco_ignore_all
echo 0>/proc/sys/net/ipv4/tcp_syncookies

```
echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all
echo 1>/proc/sys/net/ipv4/tcp_syncookies
```

文件名为 webshell.php.phpp1.php02 的文件可能会被那个服务器当做 php 文件进行解析？

正确答案: A 你的答案: 空 (错误)

Apache
IIS
nginx
squid

cookie 安全机制，cookie 有哪些设置可以提高安全性？

正确答案: A B C 你的答案: 空 (错误)

指定 cookie domain 的子域名
httponly 设置
cookie secure 设置，保证 cookie 在 https 层面传输
以上都不对

下列哪些方式对解决 xss 漏洞有帮助？

正确答案: B C 你的答案: 空 (错误)

csp
html 编码
url 编码
验证码

可以抓取 Windows 登录密码的安全工具有？

正确答案: A C 你的答案: 空 (错误)

mimikatz
sqlmap
pwdump7
hashcat

关于对称加密以下说法不正确的是？

正确答案: B D 你的答案: 空 (错误)

DES 属于对称加密
对称加密算法需要两个密钥来进行加密和解密
对称加密也叫单密钥加密
RSA 属于对称加密

以下哪些命令可以查看 windows 安全日志？

正确答案: A B 你的答案: 空 (错误)

wevtutil
eventquery.vbs
systeminfo
dsquery

以下 PHP 代码经过 mysql_real_escape_string 过滤还存在漏洞？为什么？

```
$id = $_GET['id'];
$id = mysql_real_escape_string($id);
$getid = "SELECT first_name, last_name FROM users WHERE user_id = $id";
$result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );
$num = mysql_numrows($result);
```

参考答案

这里$id 变量没有经过任何的过滤，直接传入了 sql 语句，造成数字型注入，mysql_real_escape_string 只对’“\ null 字符做转义，而数字型注入不需要’闭合，所以仍存在注入漏洞。