《Web 安全》期末考试题型说明

一、辨析题（5 分×4 题，共 20 分）

说明：分析每组名词所涉及概念、技术等方面的区别，也就是名词解释的升级版

举例：

存储型 XSS vs 基于 DOM 的 XSS

二、简答题（7 分×5 题，共 35 分）

说明：有些题目考查基本概念和原理，有些题目考查实际应用能力

举例：

1. XSS 攻击的原理是什么？

2. 为了提高网站防范 XSS 的能力，Web 开发者通过编写正则表达式并忽略大小写，实现过滤所有包含<script>字符的功能，请问可以防范下面的测试代码吗？请说明原因

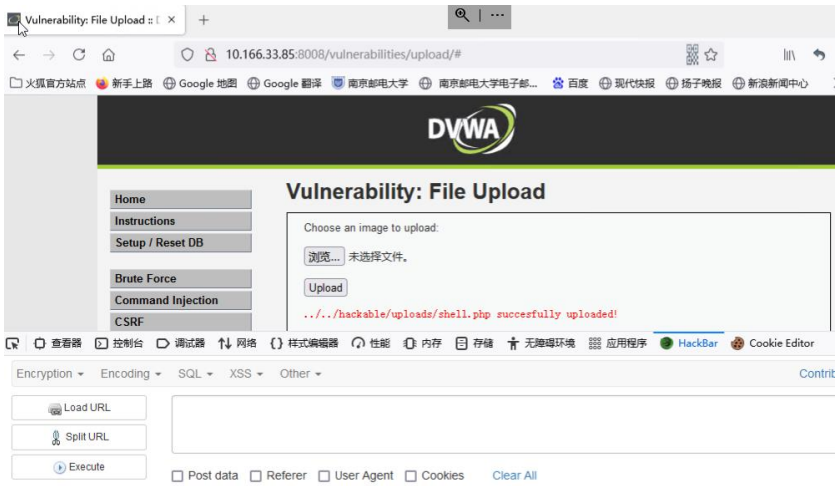
<scr<script>ipt>alert(/XSS/)</script>

三、分析题（4 题，分值不等，共 30 分）

说明：结合一些实际操作案例，包括实验和课堂演示，分析实际操作中的一些问题

举例：

1. 在一次网络攻防演练中，渗透测试人员成功的上传了 shell.php 文件，如图所示，为了测试上传的 shell.php 木马是否成功，下面准备使用 hackbar 进行测试，请列出测试的主要步骤.



四、代码审计题（1 题，共 15 分）

说明：主要针对 DVWA 的源码进行审计分析，主要包括几种常见的 Web 攻击：XSS、SQL 注入、文件上传、文件包含等，如果是 Low、Medium 级别的代码，能给出绕过的方法，如果是 impossible 级别的代码，能分析出为什么安全性很高的原因，里面有哪些关键的代码

举例：

1.由于 Web 开发人员缺乏安全能力和法律责任意识，在开发一个用户查询页面时，没有对其安全性进行关注，导致该页面存在 SQL 注入的风险。请分析下面代码中的漏洞点，并给出 SQL 手工注入攻击的具体步骤。

```php
<?php
if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );

    // Get results
    $num = mysql_numrows( $result );
    $i   = 0;
    while( $i < $num ) {
        // Get values
        $first = mysql_result( $result, $i, "first_name" );
        $last  = mysql_result( $result, $i, "last_name" );

        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";

        // Increase loop count
        $i++;
    }

    mysql_close();
}

?>
```