WebScan

某公司的网站遭受到黑客攻击，存放在Apache配置文件中的重要信息被黑客盗取了。公司员工为了验证成因，使用明鉴Web应用弱点扫描器扫描网站并导出漏洞报告，你能通过分析漏洞报告得出黑客可能是采用哪种漏洞盗取重要信息的么？被盗取的重要信息是什么？

IP：192.168.5.25

报告选摘

2.1.4 . 漏洞详细信息列表

2.1.4.1 . 紧急漏洞

2.1.4.1.1 . SQL盲注

URL	http://172.16.80.11/index.php?act=news%26id=1
弱点	参数：id=1，注入类型：数字型,数据库类型：MySQL,数据库名：ctf,用户名：ctfweb@localhost
等级	紧急

2.1.4.1.1.1 . 漏洞描述：

<bold>可能原因：</bold>

2.1.4.1.1.1 . 漏洞描述：

<bold>可能原因：</bold>

无论是内网环境还是外网环境（互联网），B/S架构的Web应用（以下指网站）都直接或者间接地受到以SQL注入攻击对危害，由于网站服务端语言自身的缺陷与程序员编写代码的安全意识不足，攻击者可以将恶意SQL语句注入到正常的数据库操作指令中去，从而使该恶意SQL语句在后台数据库中被解析执行。

2.1.4.1.2 . 跨站脚本

URL	http://172.16.80.11/index.php?act=ver%26msg=1.0
弱点	parameter: msg=1.0, xss: --><script>prompt(/Webscan6/)</script>
等级	紧急

2.1.4.1.2.1 . 漏洞描述：

<bold>可能原因：</bold>

未对用户输入字符正确执行危险字符清理。

<bold>技术描述：</bold>

跨站点脚本（XSS）是针对其他用户的重量级攻击。从某种程度上说，XSS是在Web应用程序中发现的最为普遍的漏洞，困扰着现在绝大多数的应用程序，包括因特网上一些最为注重安全的应用程序，如电子银行使用的应用程序。

2.1.4.2 . 高危漏洞

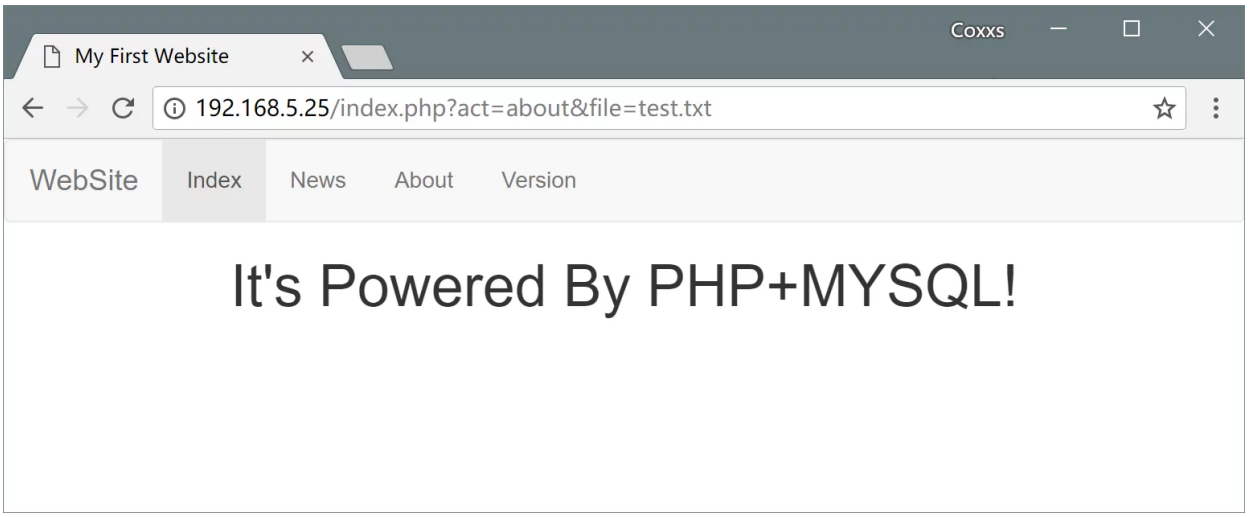
2.1.4.2.1 . 目录遍历

URL	http://172.16.80.11/index.php?act=about%26file=test.txt
弱点	http://172.16.80.11/index.php?act=about&file=/etc/hosts

MatriXay Web应用安全评估报告

等级	高危

2.1.4.2.1.1 . 漏洞描述：



考虑到题干中有提及：*存放在 Apache 配置文件中的重要信息*，因此直接利用报告中的目录遍历漏洞，读取 apache 配置文件（默认在 `/etc/httpd/conf/httpd.conf`）。