**CNNVD漏洞信息外部提交表**

|  |  |
| --- | --- |
| **漏洞基本信息** | |
| **漏洞名称** | 对漏洞进行命名，命名包括厂商信息、产品信息、漏洞类型等内容。具体要求和命名方法，参考附件1：《CNNVD漏洞命名规范》。 |
| **受影响实体版本号** | 明确漏洞针对的最新版本号以及之前的版本号，采用文字描述和网站截图进行表述。例如：SP3、V1.1等。 |
| **漏洞类型** | 根据漏洞成因对漏洞进行分类，从26种类型中选择其中一种。具体类型，参考附件2：《CNNVD漏洞分类指南》。 |
| **危害等级** | 对漏洞进行评分，填写附件3：《CNNVD漏洞评分表》，**务必**清楚说明“判定依据”。参考附件4：《CNNVD漏洞分级指南》。 |
| **漏洞简介** | 对**受影响实体**的生产厂商及功能信息，**漏洞**的产生原因、条件、漏洞危害性（如执行任意指令、本地提权、获取网站敏感信息等）等两方面信息进行描述。参考附件5：《CNNVD漏洞内容描述规范》。 |
| **提交人员基本信息** | |
| **提交机构** | 填写提交人员的单位信息，包括：所属单位、部门等。例如：XX公司。 |
| **提交人员** | 填写漏洞提交人员姓名。例如：张三。 |
| **联系方式** | 填写漏洞提交人员联系电话、邮箱等联系方式。例如：18622222222，vulpro@itsec.gov.cn。 |
| **提交日期** | 填写漏洞提交的日期。例如：2013年1月1日。 |
| **漏洞验证** | |
| **漏洞定位** | 描述漏洞在受影响实体中的位置。包括：模块名称及版本（例如：文件位置、文件名称、组件名称、插件名称等）、具体的漏洞位置（例如：源代码文件行号、二进制代码、函数名称、接口名称、参数名称等）触发漏洞的调用路径、代码行位置等。   1. 如果有源代码，需要指出具体的文件位置、漏洞代码行； 2. 如果有二进制代码，需要描述代码在可执行文件中的位置和内存中的位置； 3. 如果上述条件均不具备，需要尽可能提供漏洞产生的具体位置或原因，例如：漏洞模块接口信息、错误信息、调试信息等。   例如：该漏洞出现的文件路径为：软件安装根目录\dir1\dir2\dir3\dir4\index.php，具体代码位置如下图所示 |
| **漏洞触发条件** | 指在默认安装部署基础上进行配置修改，如：安装哪些模块、修改哪些配置、需要在哪种权限下触发、是否需要登录、是否需要数据表中存储数据等。  例如：在默认安装的基础上，开启用户操作日志模块，当系统管理员浏览日志时触发漏洞，同时需要攻击者注册用户登录系统才能利用漏洞。 |
| **漏洞验证过程** | 采用文字、截图、图形等方式，按步骤详细阐述验证过程。同时提交**漏洞验证录像视频**。  例如：  首先，注册用户登录系统，上传文件到网络硬盘中的默认分类文件夹中。    分别点击默认分类文件夹，并用burpsuite劫持数据，获取各个分类文件夹的parent\_id，本次验证中，我的多媒体、我的软件、我的图片、我的文档、我的音乐的分类文件夹对应的parent\_id分别为18,19,20,16,17。    选择我的软件中的文件，将其移动到我的文档，并用burpsuite进行劫持    将上述请求地址与payload拼接成完整的URL，判断admlog表中的管理员名称的一个字母是什么。  如果错误，我的软件中的文件不会移动到我的文档中。  http://mail.domain.com/ index.php?module=operate&action=move&file=3) and ascii(substring((select username from admlog where id=1),1,1))=96 %23&folder=&fid=16    如果正确，我的软件中的文件会移动到我的文档中。  http://www.test.com/ index.php?module=operate&action=move&file=3) and ascii(substring((select username from admlog where id=1),1,1))=97 %23&folder=&fid=16 |