Unexpected expected exception

ZeroNights 2014, 14th November 2014, @d0znpp
@d0znpp BIO

- Web applications security researches since 2009
- Bug hunting (Facebook, Google, Nokia, Yandex rewards)
- CEO of Wallarm since 2013
atomicity
call1()
call2()
call1()
call2()
call1()  
...black magic  
call2()
function checkToken(String token) {
    boolean check_passed = true;
    try {
        if (tokenIsReallyValid(token))
    } catch (Exception e) {
        ...
    }
    return check_passed;
}
function checkToken(String token) {
  boolean check_passed = true;
  try {
    if (tokenIsReallyValid(token) ..)
  } catch (Exception e) {
    ...
  }
  return check_passed;
}
if(strcmp($_GET['token'], '53CR37-value')==0){
    echo 'all is OK!';
}
if(strcmp($_GET['token'],'53CR37-value') == 0){
    echo 'all is OK!';
}

Warning: strcmp() expects parameter 1 to be string, array given in a.php on line 4

all is OK!
Resource exhaustion

- CPU: tick
- disk subsystem: iops
- filesystem: inodes
- PID, items in pools (i.e. database)
Locks (async and parallelism)

- lock files
- database locks
max_execution_time
max_input_nesting_level
max_input_time
memory_limit
pcre.backtrack_limit
pcre.recursion_limit
post_max_size
upload_max_filesize
max_file_uploads

POST ...

…

a[..][a…a][…]=…
One exception
Many trace parts
Order it!
Obtain full stack trace
PHP
rlimit_core = unlimited
My request
My PID for processing me
What’s wrong?

What’s in **CORE DUMPS**
Attack Target

Configure the details of the target for the attack.

Host: phptest.troll.onsec.ru
Port: 80

[ ] Use HTTPS
1. Process init phase – malloc()
2. Page allocated
3. Request processing phase – malloc()
4. Request finalizing phase free()
5. Page is still used by process
6. New request comes
7. Request processing phase...
sysctl kernel.core_pattern

- core.%p
- %e.core
- ...

Where is CORE DUMPS CWD of PID
Atomicity control
Try/catch for all
CONFERECE
ZERONIGHTS 2014
NOVEMBER 13-14

Thanks for listening!

http://wallarm.com
in@wallarm.com, @d0znpp
WWW.ZERONIGHTS.ORG