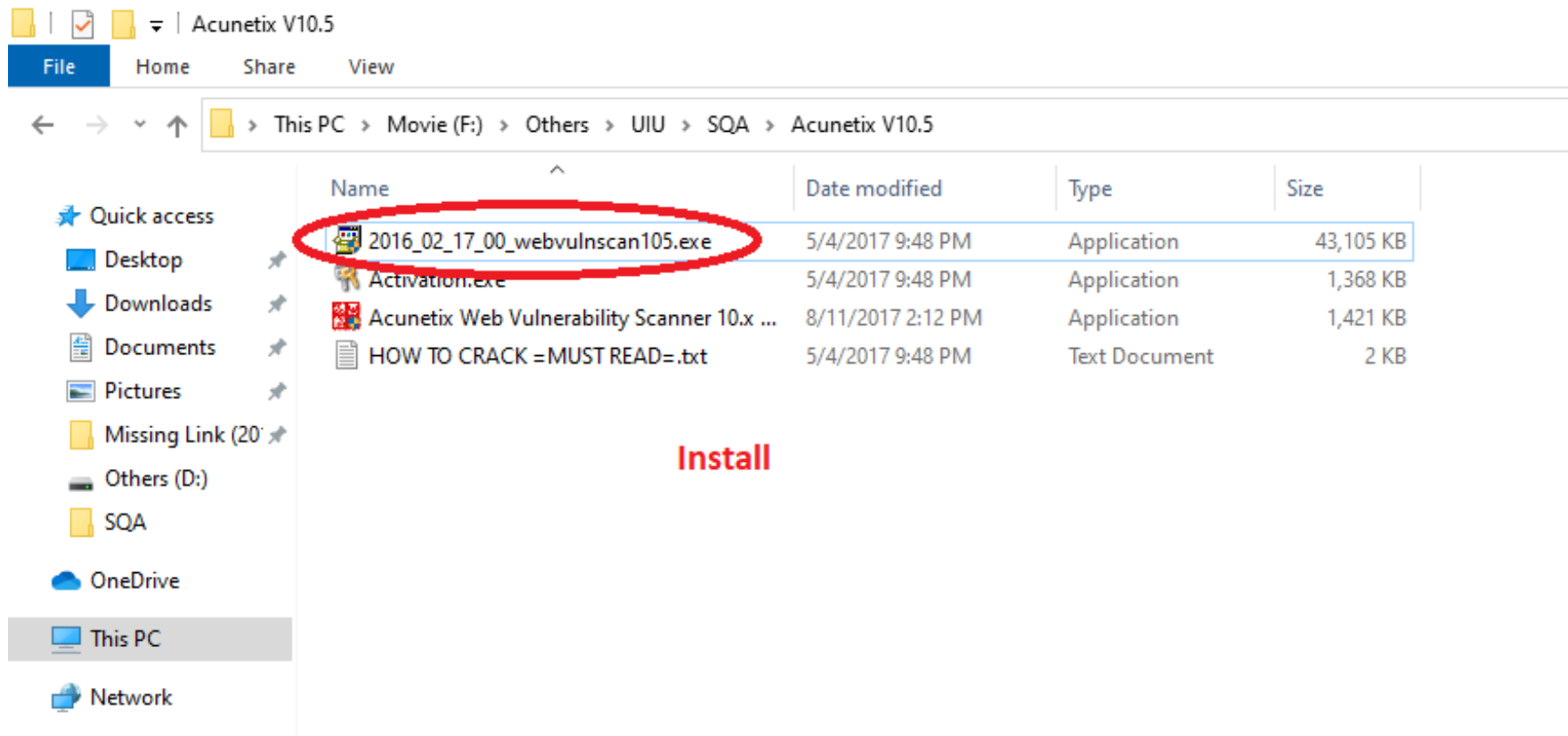


Acunetix Tutorial

Created by
Wahid Bin Mahbub

1. 1st download Acunetix .exe file
2. Then install the software



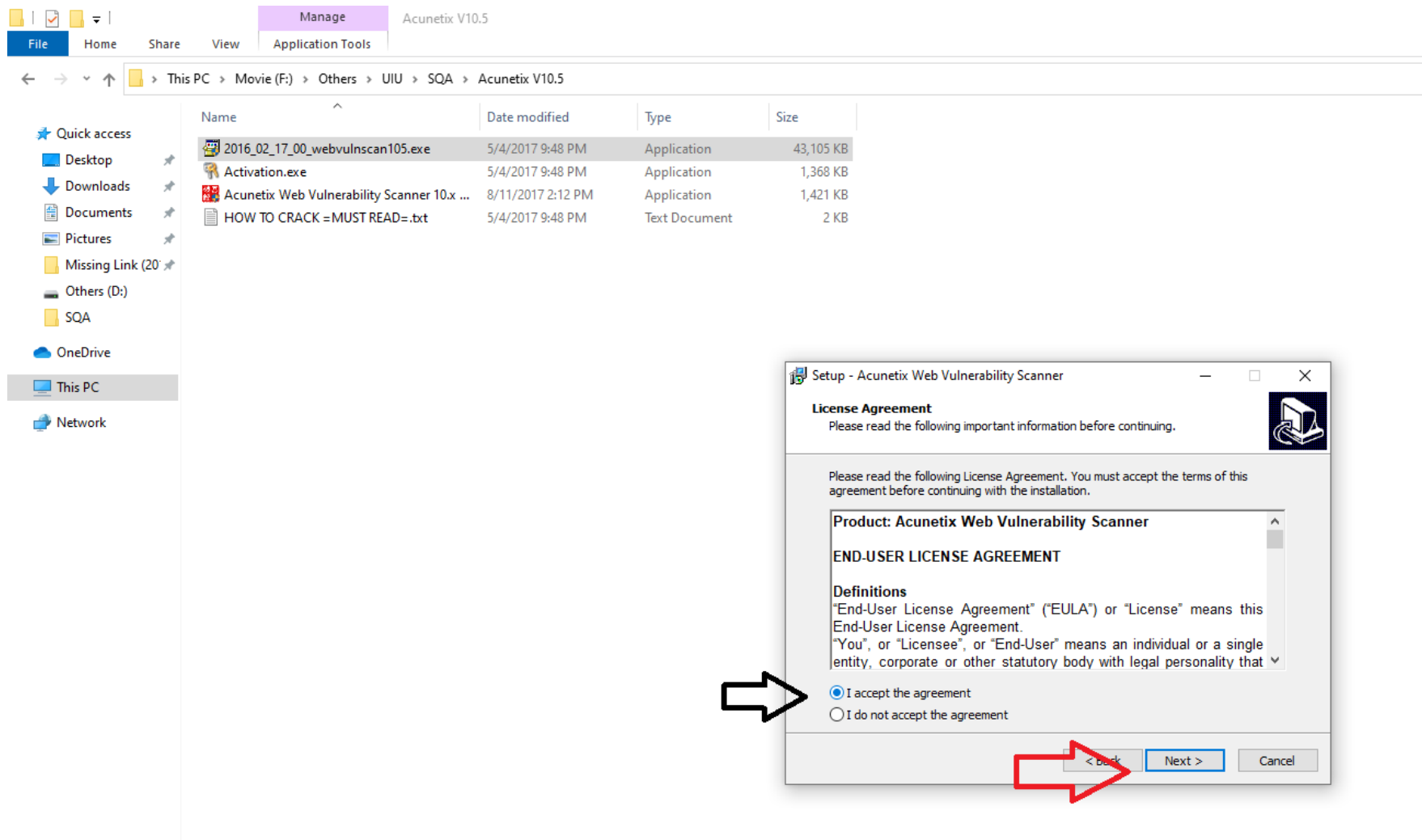
Press Next button.

File Explorer window showing the path: This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5. The file list shows:

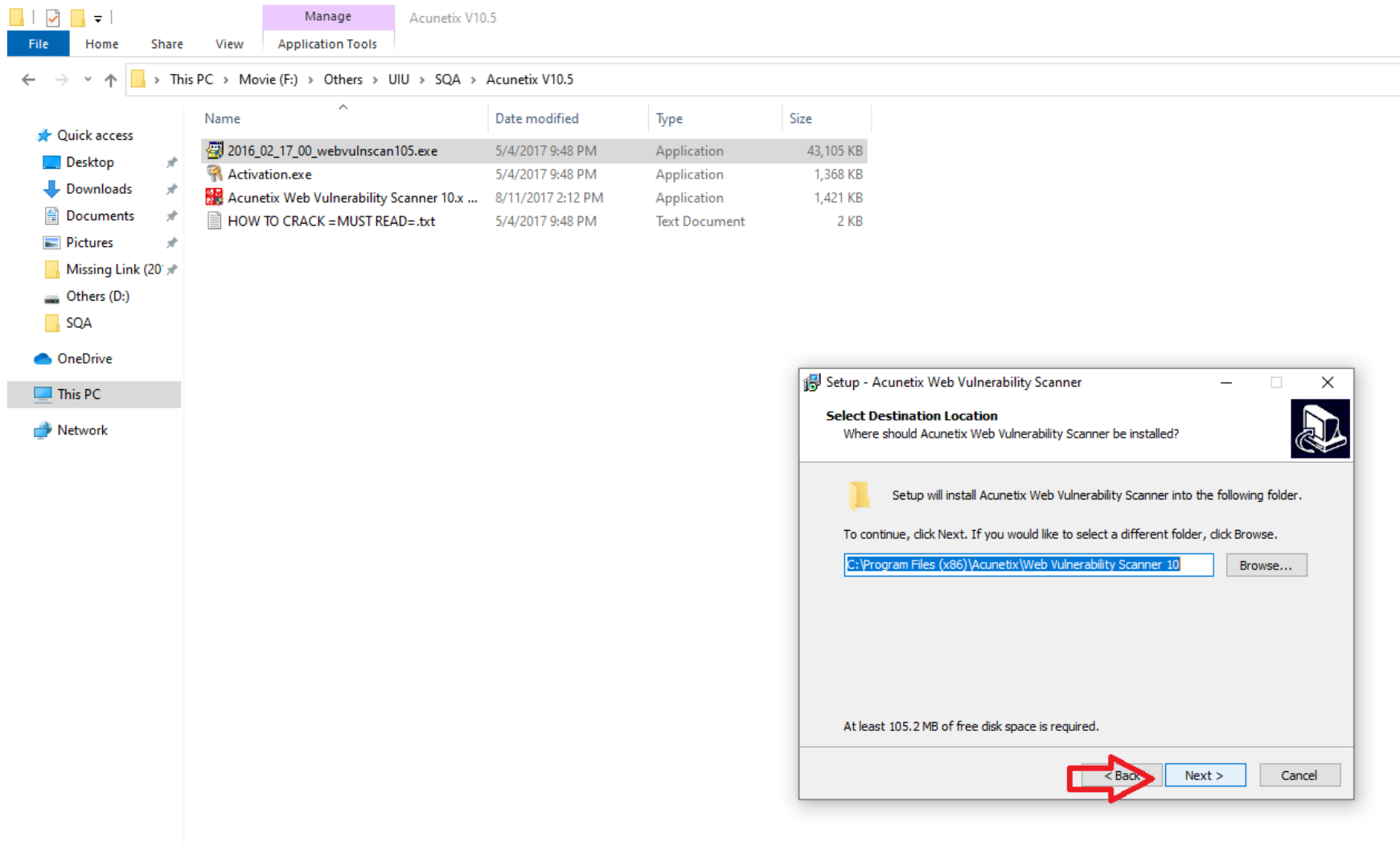
Name	Date modified	Type	Size
2016_02_17_00_webvulnscan105.exe	5/4/2017 9:48 PM	Application	43,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix Web Vulnerability Scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

The setup wizard window is titled "Setup - Acunetix Web Vulnerability Scanner". It displays the text: "Welcome to the Acunetix Web Vulnerability Scanner Setup Wizard". Below this, it states: "This will install Acunetix Web Vulnerability Scanner 10.5 on your computer." and "It is recommended that you close all other applications before continuing." The bottom of the window has a "Next >" button and a "Cancel" button. A red arrow points to the "Next >" button.

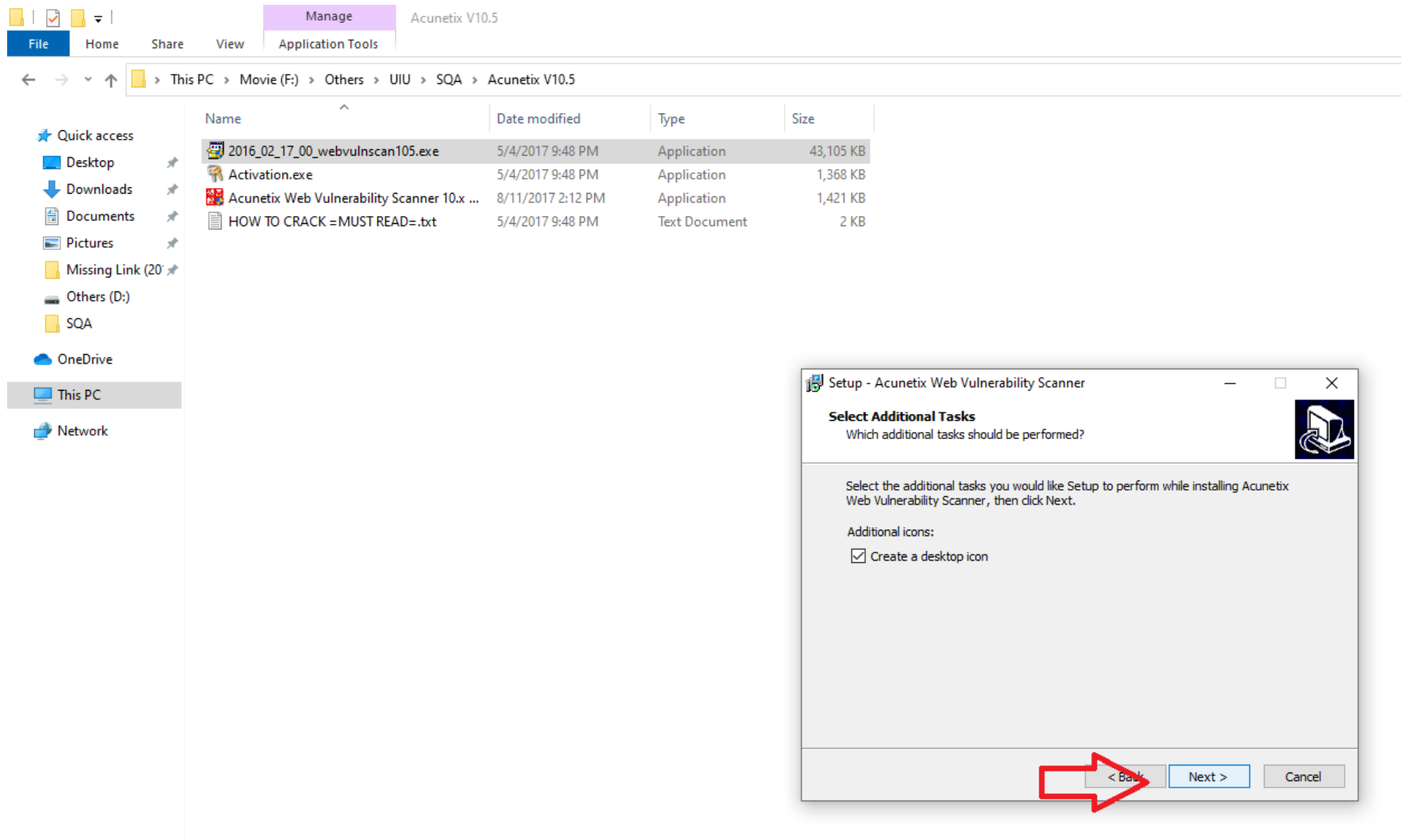
1st Press “I accept the agreement” than press Next button.



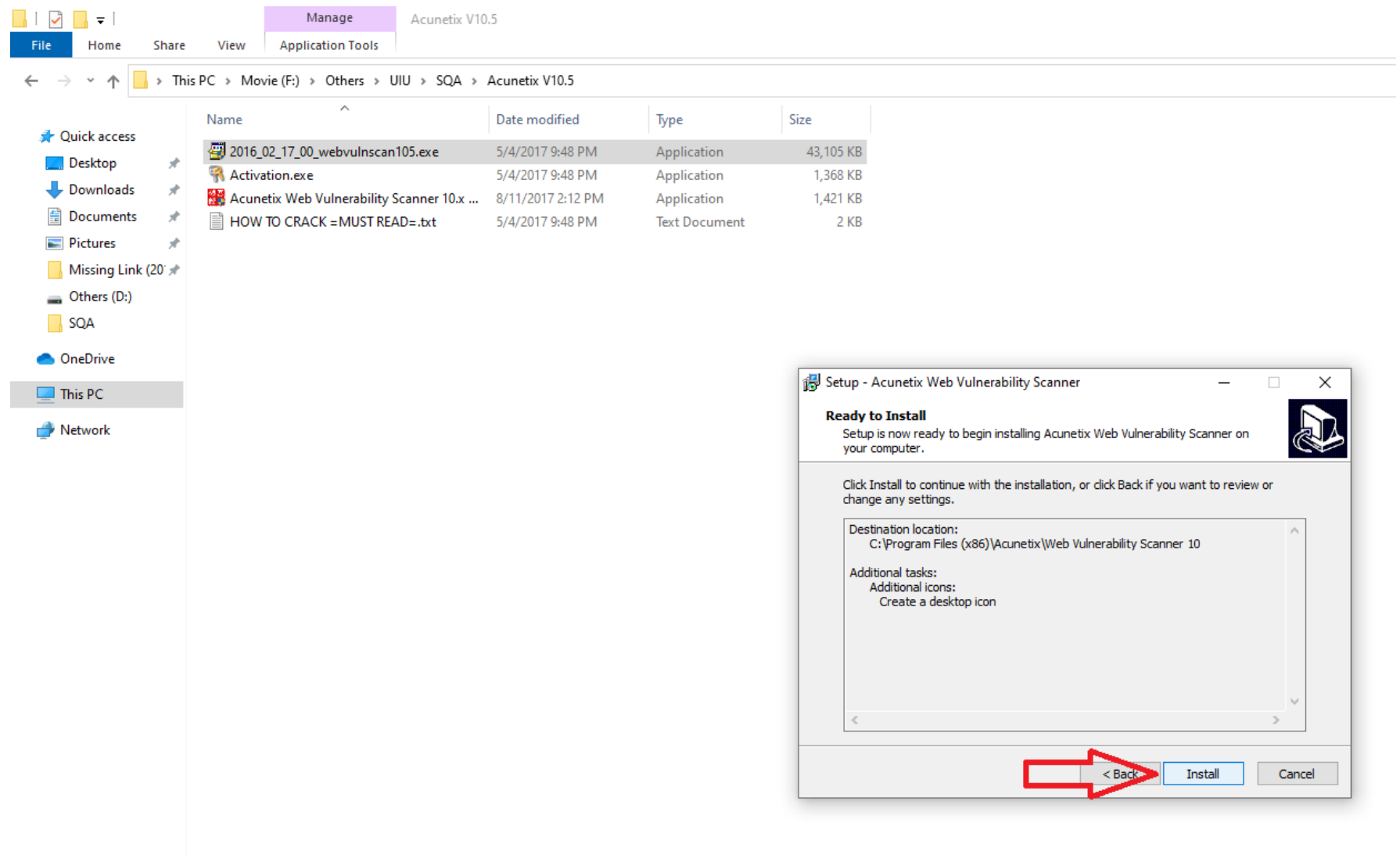
Press Next button.



1st check “Create a dextop ican” than press Next button.



Click "Install" button



Now installing

File Home Share View Manage Application Tools Acunetix V10.5

← → ↕ ↑ This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Missing Link (20)
- Others (D:)
- SQA
- OneDrive
- This PC
- Network

Name	Date modified	Type	Size
2016_02_17_00_webvulnscan105.exe	5/4/2017 9:48 PM	Application	43,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix Web Vulnerability Scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

Setup - Acunetix Web Vulnerability Scanner

Installing

Please wait while Setup installs Acunetix Web Vulnerability Scanner on your computer.

Extracting files...
C:\ProgramData\Acunetix WVS 10\Data\Reports\content.txt

Installing

Cancel

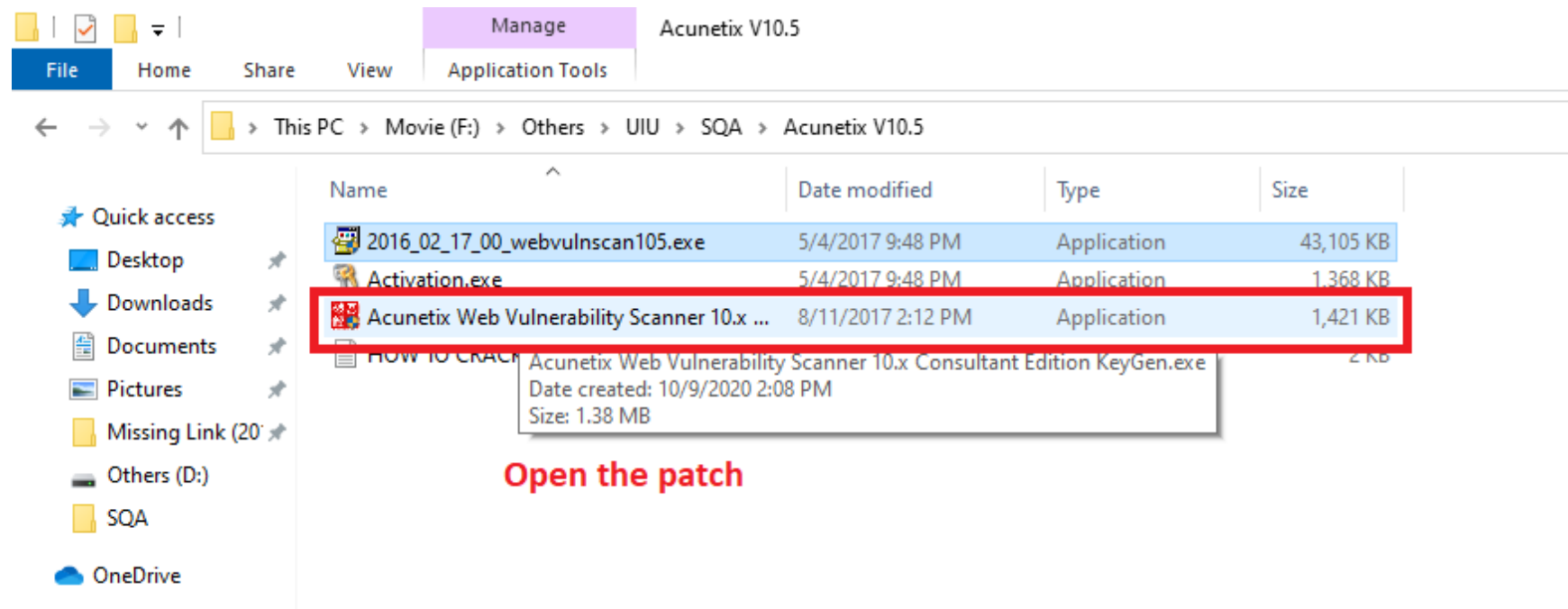
Installation DONE

File Explorer window showing the installation path: This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5. The file list includes:

Name	Date modified	Type	Size
2016_02_17_00_webvulnscan105.exe	5/4/2017 9:48 PM	Application	43,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix Web Vulnerability Scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

On the right, the "Setup - Acunetix Web Vulnerability Scanner" window is displayed, showing the "Completing the Acunetix Web Vulnerability Scanner Setup Wizard" screen. The window includes instructions to click Finish to exit Setup and a checkbox for "Launch Acunetix Web Vulnerability Scanner". The "Finish" button is circled in red.

Now open the patch file



In here press patch button

File Explorer window showing the directory path: This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5. The file list includes:

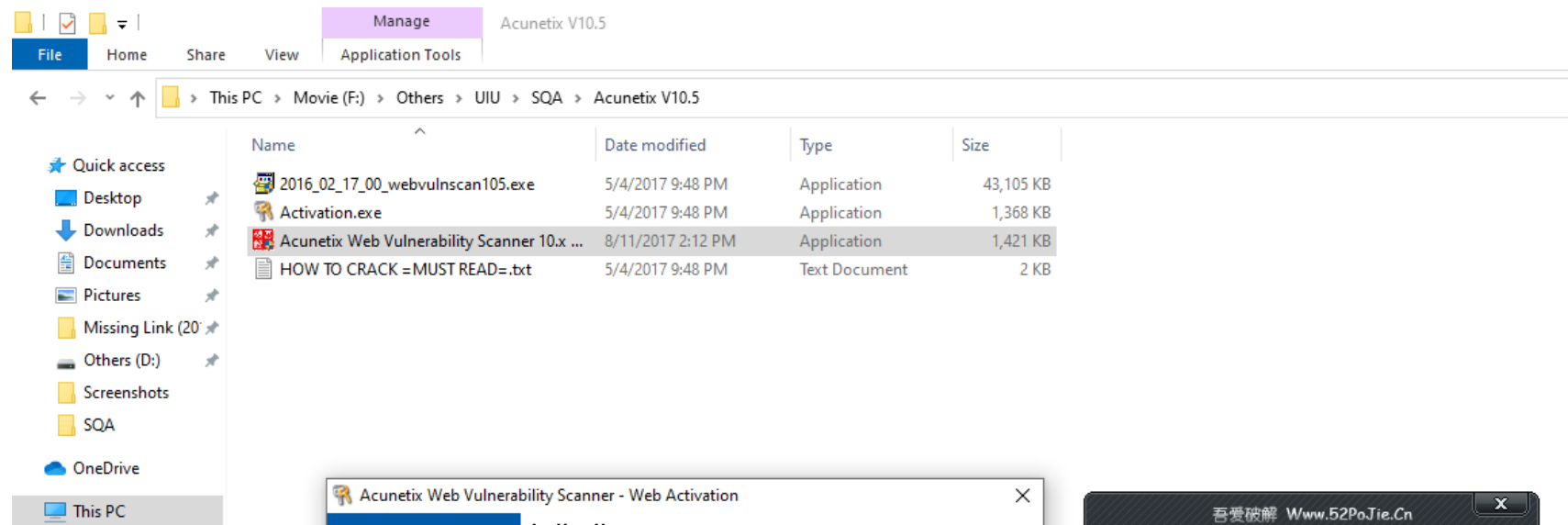
Name	Date modified	Type	Size
2016_02_17_00_webvulnscan105.exe	5/4/2017 9:48 PM	Application	43,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix Web Vulnerability Scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

Overlaid on the bottom right is a crack patch application window titled "Cracked By Hmily". It contains the following information:

- Acunetix Web Vulnerability Scanner 10.x
- FILENAME: Activation.exe
- WEBSITE: <http://www.52pojie.cn/thread-214819>
- AUTHOR: Hmily[LOG]
- Acunetix Web Vulnerability Scanner 10.x Consultant Edition KeyGen By Hmily[LOG]
- E-Mail: Hmily[at]52PoJie.Cn

At the bottom of the window, there are three buttons: "MAKE BACKUP", "ACTIVATION", and "PATCH". A red arrow points to the "PATCH" button, which is also circled in red. The word "Patch" is written in red text to the left of the arrow.

In the patch file a new window pop up. Now press “Next” button



File Home Share View Manage Application Tools Acunetix V10.5

← → ↕ ↑ This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5

Name	Date modified	Type	Size
2016_02_17_00_webvulnscan105.exe	5/4/2017 9:48 PM	Application	43,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix Web Vulnerability Scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

Quick access: Desktop, Downloads, Documents, Pictures, Missing Link (20), Others (D:), Screenshots, SQA, OneDrive, This PC, Network

Acunetix Web Vulnerability Scanner - Web Activation

Activation

You need to activate your copy of Acunetix Web Vulnerability Scanner. Internet connection is required for web activation.

Activation details

Please enter the license key and contact information below:

License Key: 8C43-8CB1-8326-CE87

Name: Hmily[LCG]

Company: Wwww.52PoJie.Cn

Email: Hmily@Acunetix.com

Telephone: 110

Country: China

Offline Activation

Next > Cancel

吾爱破解 Wwww.52PoJie.Cn

Cracked By Hmily

Acunetix Web Vulnerability Scanner 10.x

FILENAME: Activation.exe

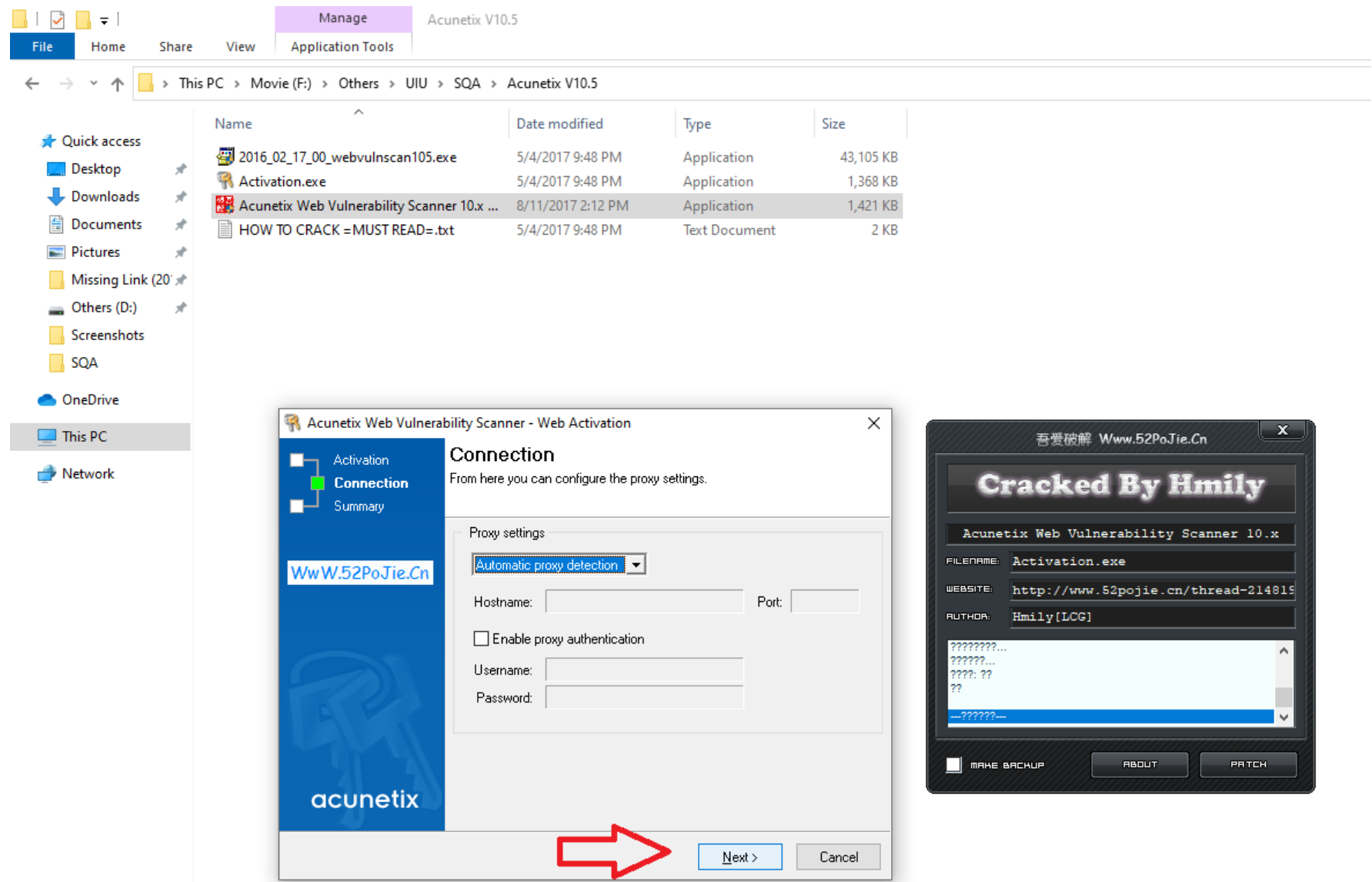
WEBSITE: http://www.52pojie.cn/thread-214819

AUTHOR: Hmily[LCG]

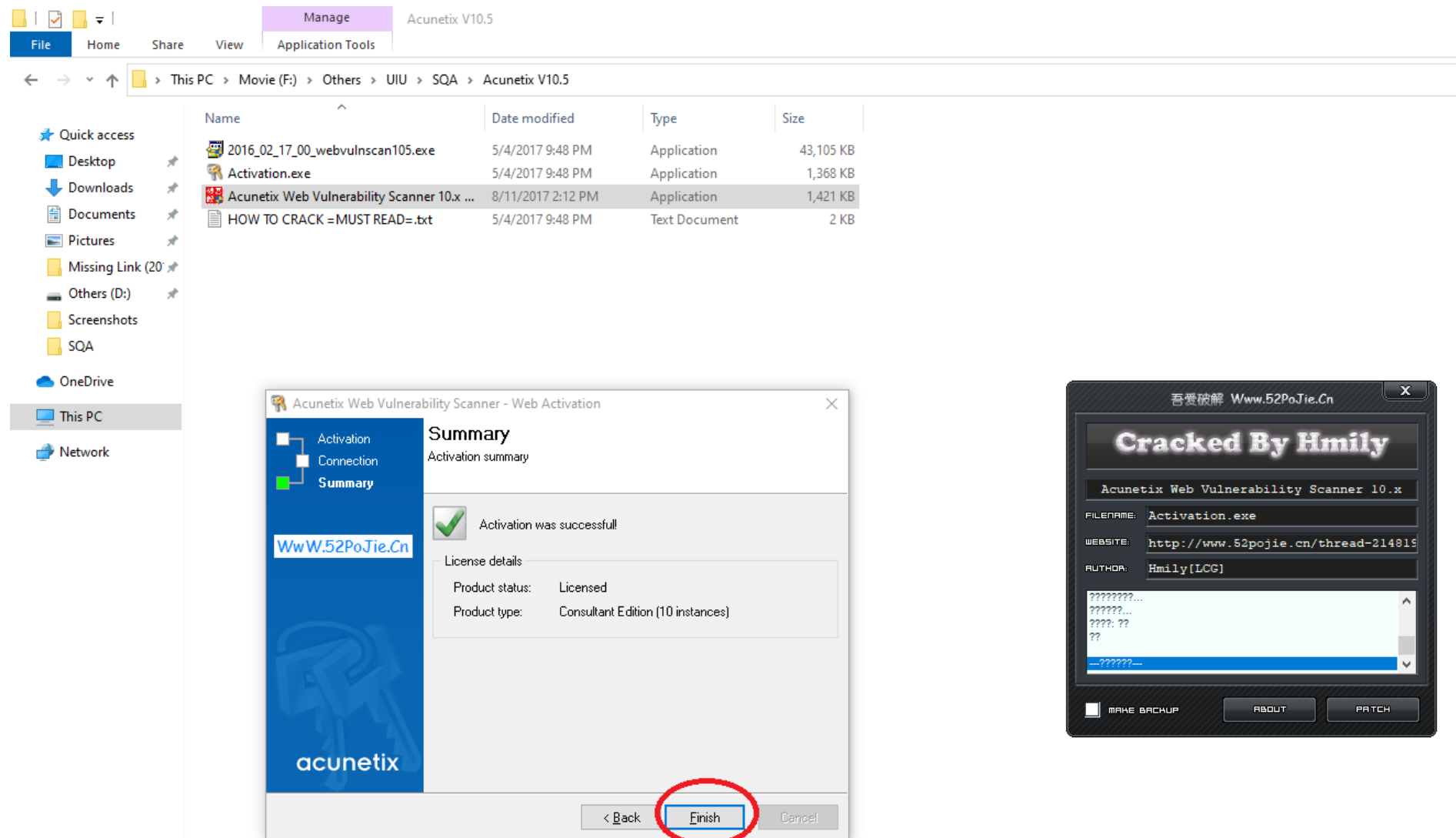
?????????
??????
???? ??
??
-?????-

MAKE BACKUP ABOUT PATCH

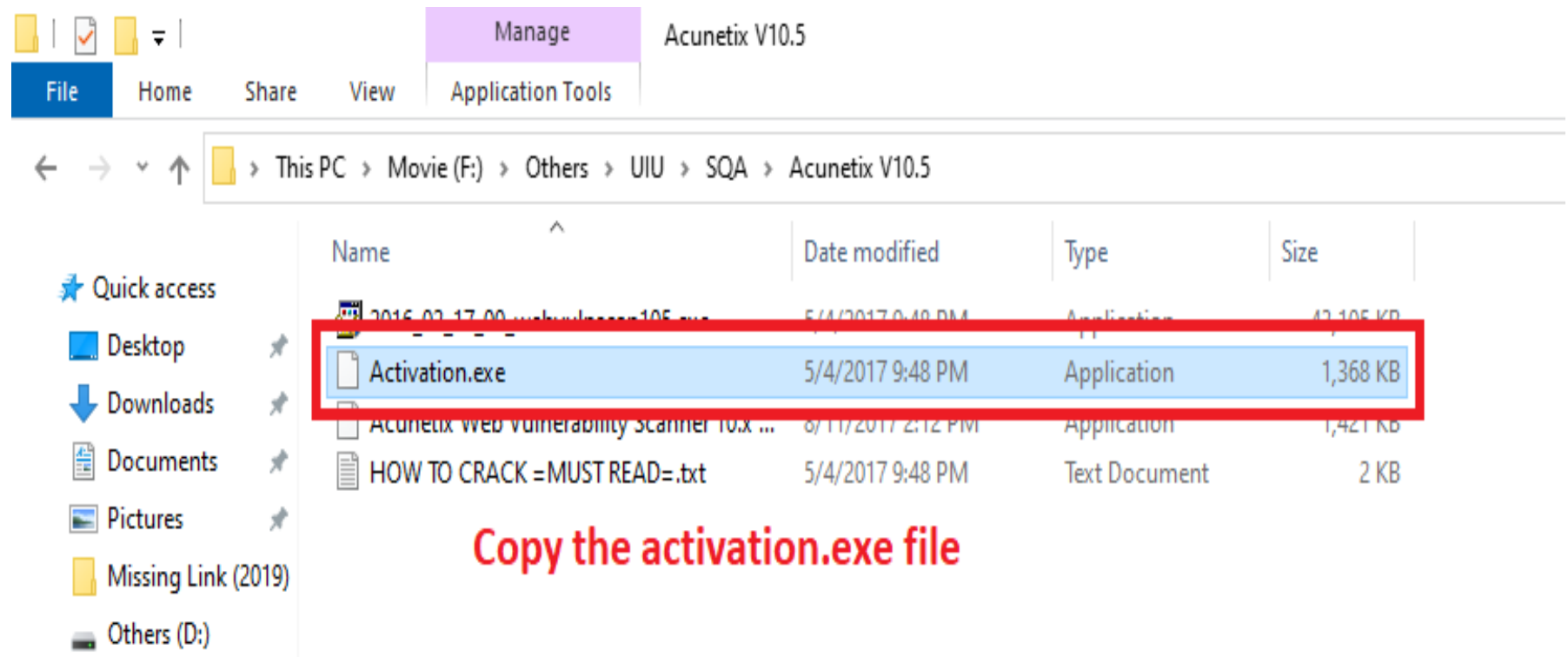
Press "Next" button.



Press "Next" button.



Now copy the activation.exe file



File Explorer window showing the file structure and details of the 'Activation.exe' file.

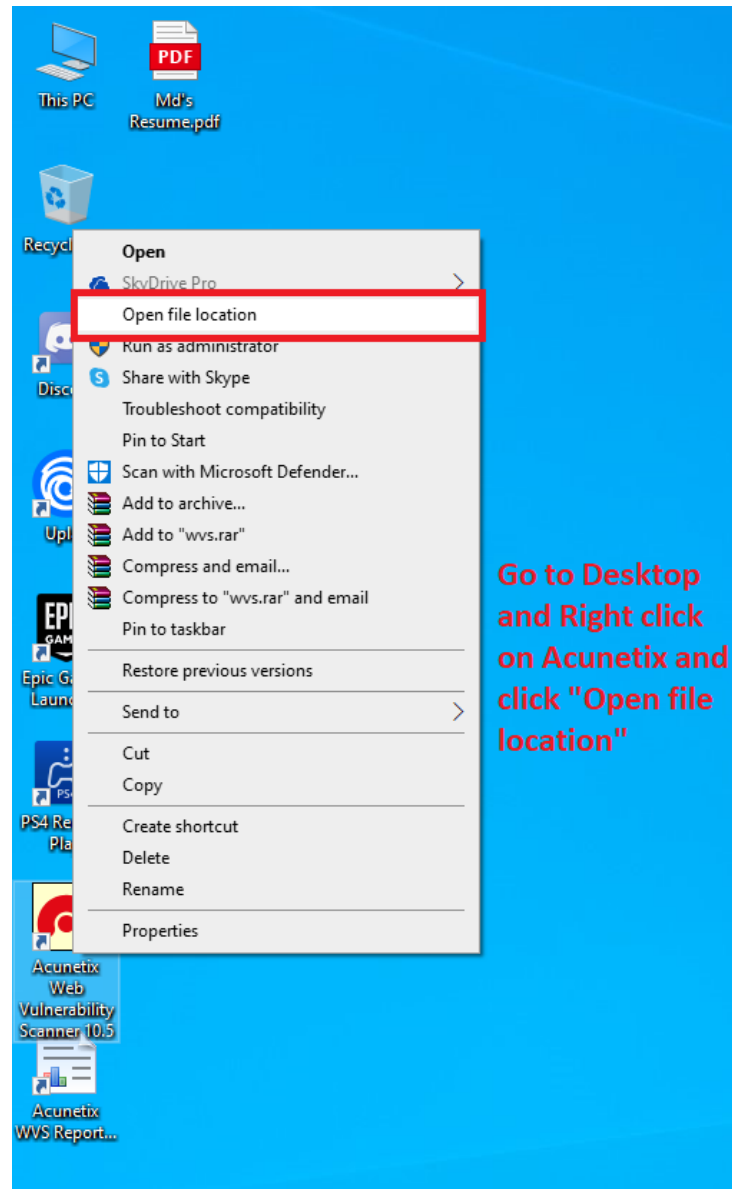
Path: This PC > Movie (F:) > Others > UIU > SQA > Acunetix V10.5

Name	Date modified	Type	Size
2016_02_17_00_...105.exe	5/4/2017 9:48 PM	Application	42,105 KB
Activation.exe	5/4/2017 9:48 PM	Application	1,368 KB
Acunetix web vulnerability scanner 10.x ...	8/11/2017 2:12 PM	Application	1,421 KB
HOW TO CRACK =MUST READ=.txt	5/4/2017 9:48 PM	Text Document	2 KB

Quick access links: Desktop, Downloads, Documents, Pictures, Missing Link (2019), Others (D:)

Copy the activation.exe file

Go to Desktop and Right click on Acunetix shortcut and click "Open file location".



Press here the copied activation.exe file.

File

Home

Share

View

← → ↕

This PC > Local Disk (C:) > Program Files (x86) > Acunetix > Web Vulnerability Scanner 10

Quick access

Desktop

Downloads

Documents

Pictures

Missing Link (2019)

Others (D:)

Screenshots

SQA

OneDrive

This PC

Network

Name	Date modified	Type	Size
libeay32.dll	1/15/2016 11:35 AM	Application exten...	1,232 KB
libEGL.dll	1/15/2016 11:35 AM	Application exten...	11 KB
libGLESv2.dll	1/15/2016 11:35 AM	Application exten...	1,264 KB
license.rtf	2/2/2016 3:27 PM	Rich Text Format	258 KB
lsr.exe	1/15/2016 11:35 AM	Application	606 KB
marvin.exe	1/15/2016 11:35 AM	Application	88 KB
msvcp120.dll	5/6/2015 3:07 PM	Application exten...	445 KB
msvcr120.dll	5/6/2015 3:07 PM	Application exten...	949 KB
pcre.dll	5/6/2015 3:07 PM	Application exten...	148 KB
ProcessTracer.exe	5/6/2015 3:07 PM	Application	1,169 KB
Qt5Core.dll	1/15/2016 11:35 AM	Application exten...	4,054 KB
Qt5Gui.dll	1/15/2016 11:35 AM	Application exten...	3,413 KB
Qt5Multimedia.dll	1/15/2016 11:35 AM	Application exten...	551 KB
Qt5MultimediaWidgets.dll	1/15/2016 11:35 AM	Application exten...	81 KB
Qt5Network.dll	1/15/2016 11:35 AM	Application exten...	826 KB
Qt5OpenGL.dll	1/15/2016 11:35 AM	Application exten...	256 KB
Qt5Positioning.dll	1/15/2016 11:35 AM	Application exten...	163 KB
Qt5PrintSupport.dll	1/15/2016 11:35 AM	Application exten...	261 KB
Qt5Qml.dll	1/15/2016 11:35 AM	Application exten...	2,528 KB
Qt5Quick.dll	1/15/2016 11:35 AM	Application exten...	2,373 KB
Qt5Sensors.dll	1/15/2016 11:35 AM	Application exten...	145 KB
Qt5Sql.dll	1/15/2016 11:35 AM	Application exten...	151 KB
Qt5WebChannel.dll	1/15/2016 11:35 AM	Application exten...	79 KB
Qt5WebKit.dll	1/15/2016 11:35 AM	Application exten...	16,954 KB
Qt5WebKitWidgets.dll	1/15/2016 11:35 AM	Application exten...	194 KB
Qt5Widgets.dll	1/15/2016 11:35 AM	Application exten...	4,317 KB
Qt5Xml.dll	1/15/2016 11:35 AM	Application exten...	147 KB
Qt5XmlPatterns.dll	1/15/2016 11:35 AM	Application exten...	2,403 KB
Reporter.exe	2/17/2016 10:07 AM	Application	4,877 KB
reporter_console.exe	2/17/2016 10:07 AM	Application	51 KB
SciLexer.dll	5/6/2015 3:07 PM	Application exten...	332 KB
sduutils.dll	2/17/2016 10:08 AM	Application exten...	179 KB
SecureEngineSDK32.dll	7/16/2015 8:50 AM	Application exten...	28 KB
sqlite3.dll	5/6/2015 3:07 PM	Application exten...	598 KB
ssleay32.dll	1/15/2016 11:35 AM	Application exten...	291 KB
unins000.dat	10/9/2020 2:11 PM	KMP - MPEG Mov...	153 KB
unins000.exe	10/9/2020 2:11 PM	Application	704 KB
Uninstall.exe	2/17/2016 10:08 AM	Application	944 KB
ve.exe	2/17/2016 10:07 AM	Application	3,241 KB

Paste Here Activation.exe file

AMD Radeon Software

View

Sort by

Group by

Refresh

Customize this folder...

Paste

Paste shortcut

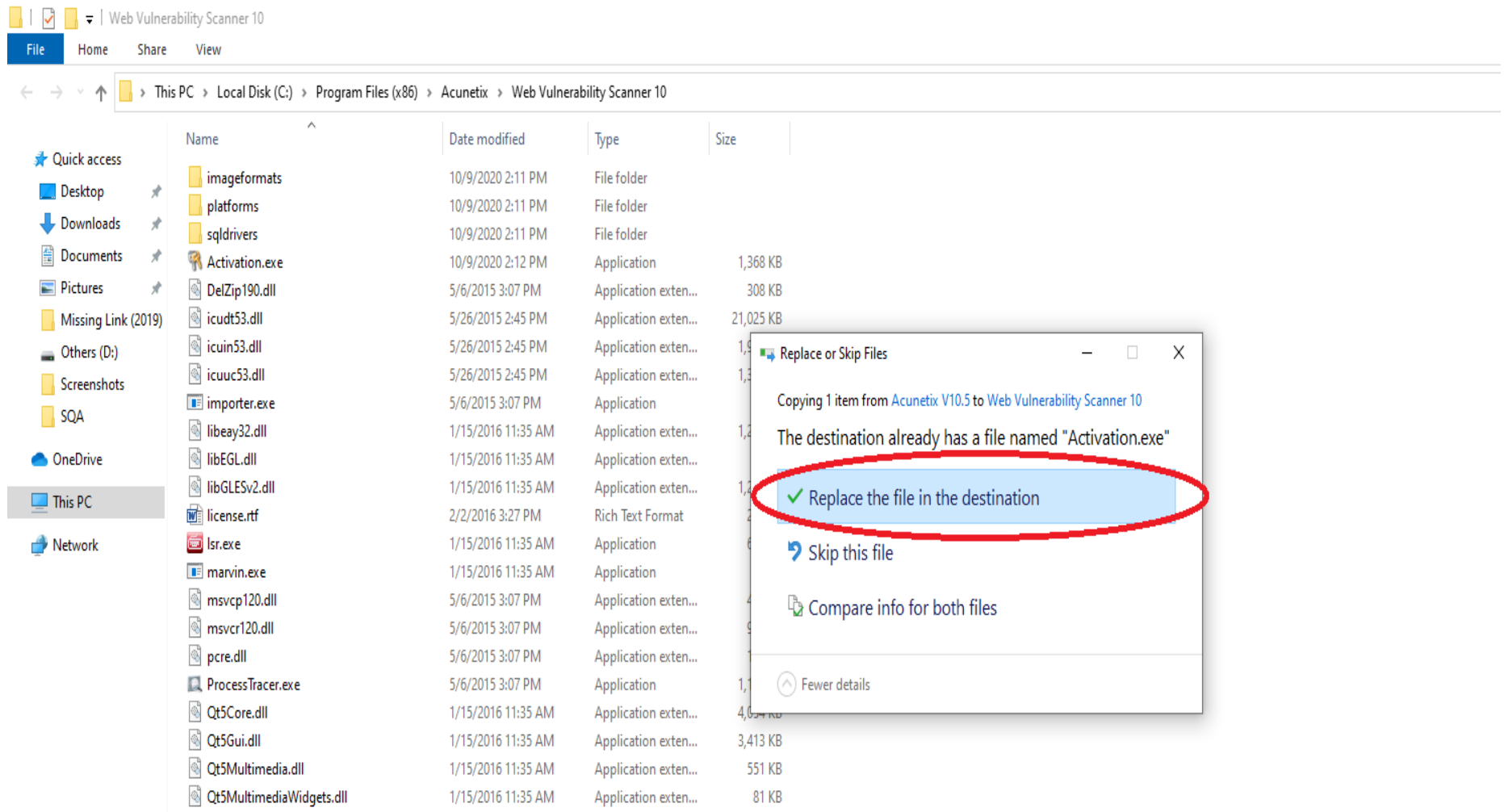
Undo Move

Give access to

New

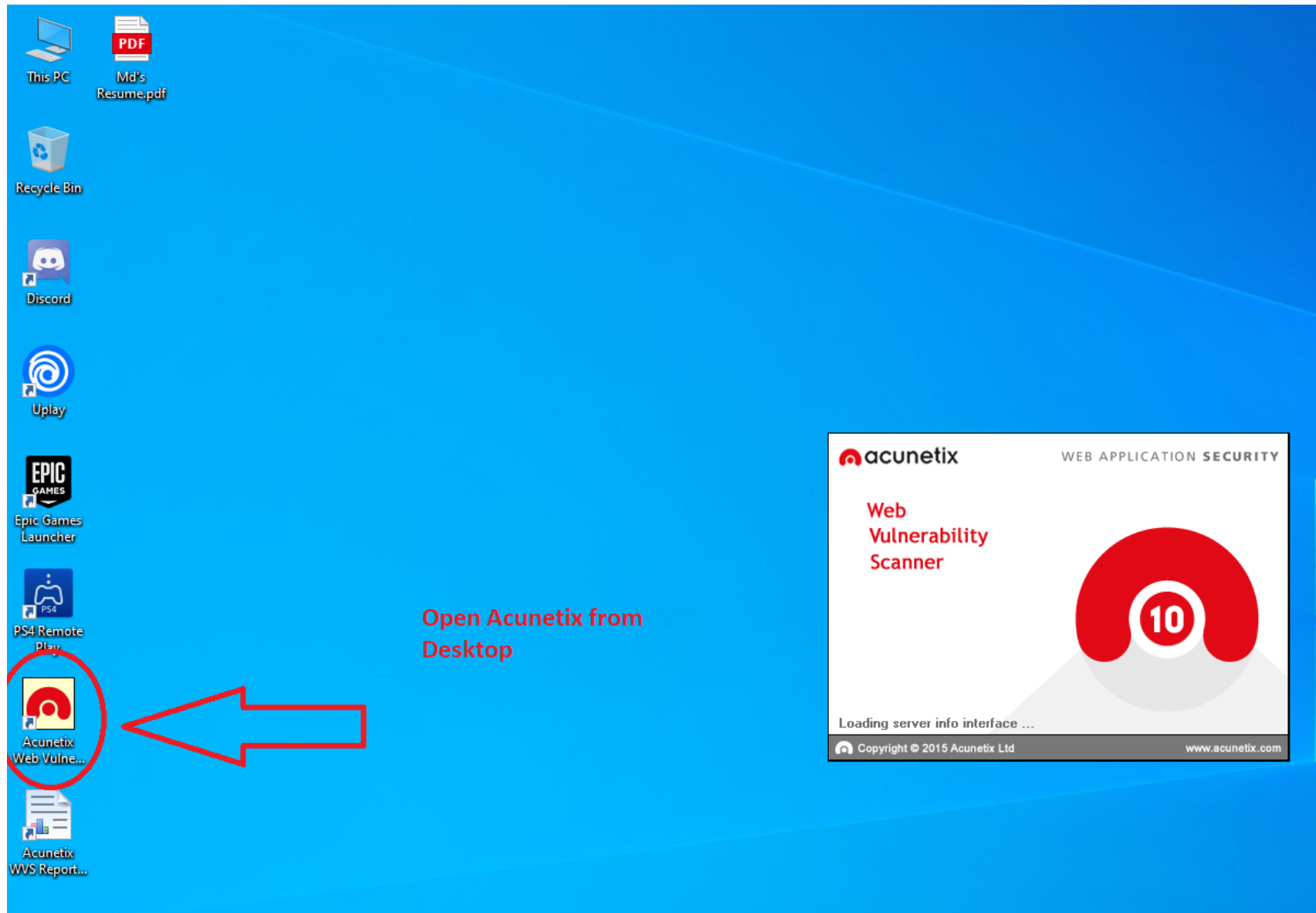
Properties

Ctrl+Z

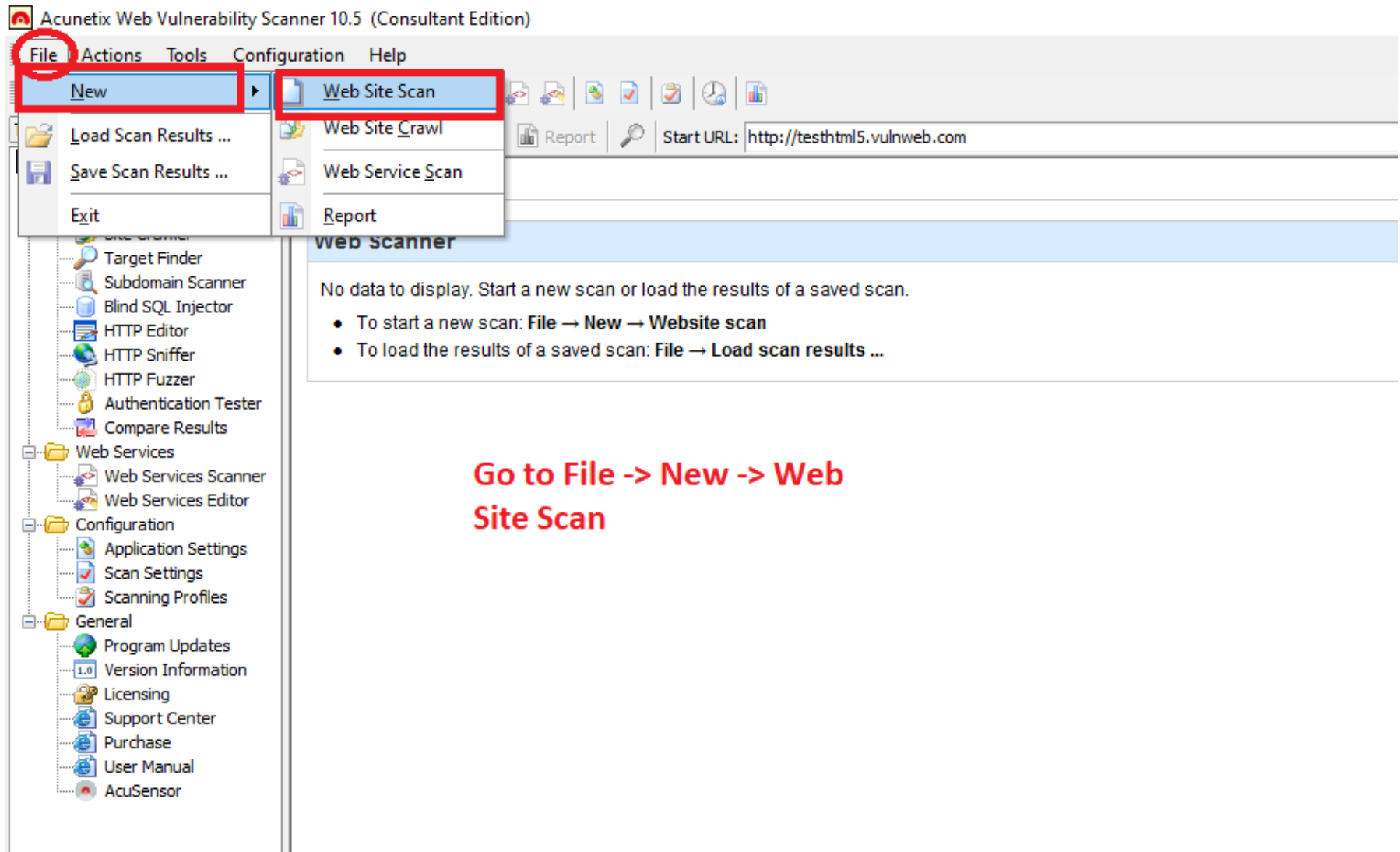


Our activation installation complete.

Go to Desktop and double click on Acunetix shortcut file.



Go to File -> New -> Web Site Scan



Write the website name that we want to test. Then press the Next button.

Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

File Actions Tools Configuration Help

New Scan

Tools Explorer

- Web Vulnerability Scanner
- Web Scanner
- Tools
 - Site Crawler
 - Target Finder
 - Subdomain Scanner
 - Blind SQL Injector
 - HTTP Editor
 - HTTP Sniffer
 - HTTP Fuzzer
 - Authentication Tester
 - Compare Results
- Web Services
 - Web Services Scanner
 - Web Services Editor
- Configuration
 - Application Settings
 - Scan Settings
 - Scanning Profiles
- General
 - Program Updates
 - Version Information
 - Licensing
 - Support Center
 - Purchase
 - User Manual
 - AcuSensor

Scan Results

Scan Thread 1 (http://google.com:80/) Status: Finished

Web Alerts

- Knowledge Base (3)
 - List of file extensions
 - List of files with inputs
 - List of external hosts
- Site Structure
 - / robots.txt Moved Permanently
 - Variation 1 for user-agent Moved Permanently
 - Cookies Moved Permanently

Scan Wizard

Scan Type

Select whether you want to scan a single website or analyze the results of a previous crawl.

Write the website name that you want to test

Scan type

Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites.

☒ Scan single website

Website URL:

If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again.

☐ Scan using saved crawling results

Filename:

If you want to scan a list of websites, use the Acunetix Scheduler. You can access the scheduler interface by clicking the link below.
<http://localhost:8183/>

Then click Next

< Back Next > Cancel

Alerts summary

Acunetix threat level

Acunetix Threat Level 0

No vulnerabilities have been discovered by the scanner.

Total alerts found: 0

- High: 0
- Medium: 0
- Low: 0
- Informational: 0

Target information: http://google.com:80/

Statistics: 2079 requests

Progress: Scan is finished 100.00%

Activity Window

10.09 14:25:26, CSRF testing finished.

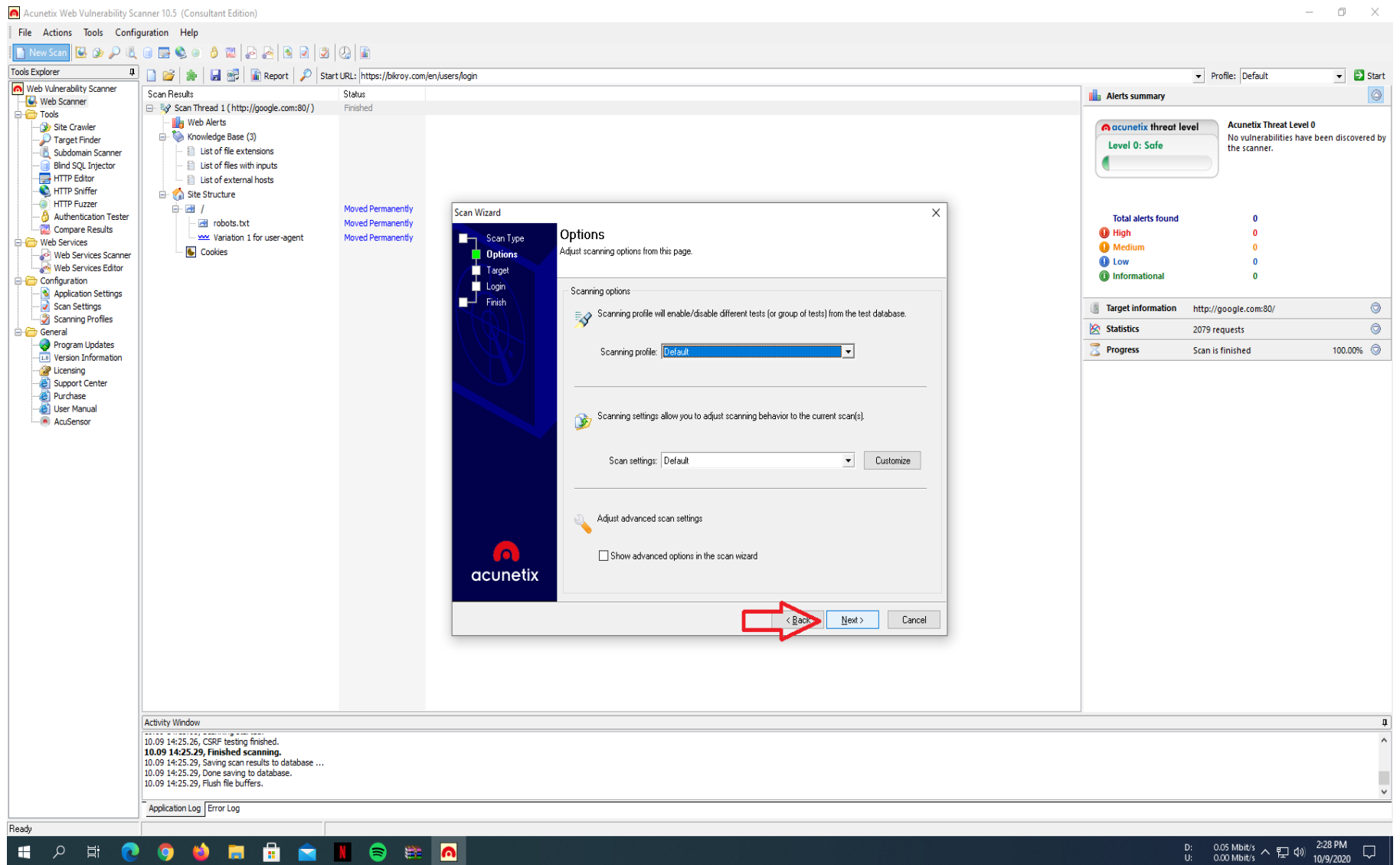
10.09 14:25:29, Finished scanning.

10.09 14:25:29, Saving scan results to database ...

10.09 14:25:29, Done saving to database.

10.09 14:25:29, Flush file buffers.

Press the next button.



Click which type to technology you want to test. Then press Next button.

The screenshot displays the Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition) interface. A 'Scan Wizard' dialog box is open, showing the 'Target' tab. The 'Optimize for following technologies' checkbox is highlighted with a red box. The 'Next >' button is also highlighted with a red circle. The background shows the main interface with a Tools Explorer, Scan Results, and Alerts summary.

Tools Explorer

- Web Vulnerability Scanner
- Web Scanner
- Tools
 - Site Crawler
 - Target Finder
 - Subdomain Scanner
 - Blind SQL Injector
 - HTTP Editor
 - HTTP Sniffer
 - HTTP Fuzzer
 - Authentication Tester
 - Compare Results
 - Web Services
 - Web Services Scanner
 - Web Services Editor
- Configuration
 - Application Settings
 - Scan Settings
 - Scanning Profiles
- General
 - Program Updates
 - Version Information
 - Licensing
 - Support Center
 - Purchase
 - User Manual
 - AcuSensor

Scan Results

Scan Thread 1 (http://google.com:80/)	Status
Web Alerts	Finished
Knowledge Base (3)	
List of file extensions	
List of files with inputs	
List of external hosts	
Site Structure	
/	Moved Permanently
robots.txt	Moved Permanently
Variation 1 for user-agent	Moved Permanently
Cookies	

Scan Wizard

Target

Please wait until the scanning is finished. You can also adjust details such as operating system, webserver, technology or change the base path. By entering these details you can reduce the scanning time.

Target information

Property	Value
Base path	/en/users/login
Server banner	cloudflare
Target URL	https://bikroy.com:443/en/users/login
Operating system	Unknown
Webserver	Unknown

Optimize for following technologies

Technology	Check
ASP.NET	<input type="checkbox"/>
PHP	<input type="checkbox"/>
Perl	<input type="checkbox"/>
Java/J2EE	<input type="checkbox"/>
ColdFusion/Jrun	<input type="checkbox"/>
Python	<input type="checkbox"/>
Rails	<input type="checkbox"/>
FrontPage	<input type="checkbox"/>

Check which type of technology you want to test

Status: Done

< Back Next > Cancel

Alerts summary

Acunetix threat level

Level 0: Safe

Acunetix Threat Level 0
No vulnerabilities have been discovered by the scanner.

Total alerts found

Severity	Count
High	0
Medium	0
Low	0
Informational	0

Target information http://google.com:80/

Statistics 2079 requests

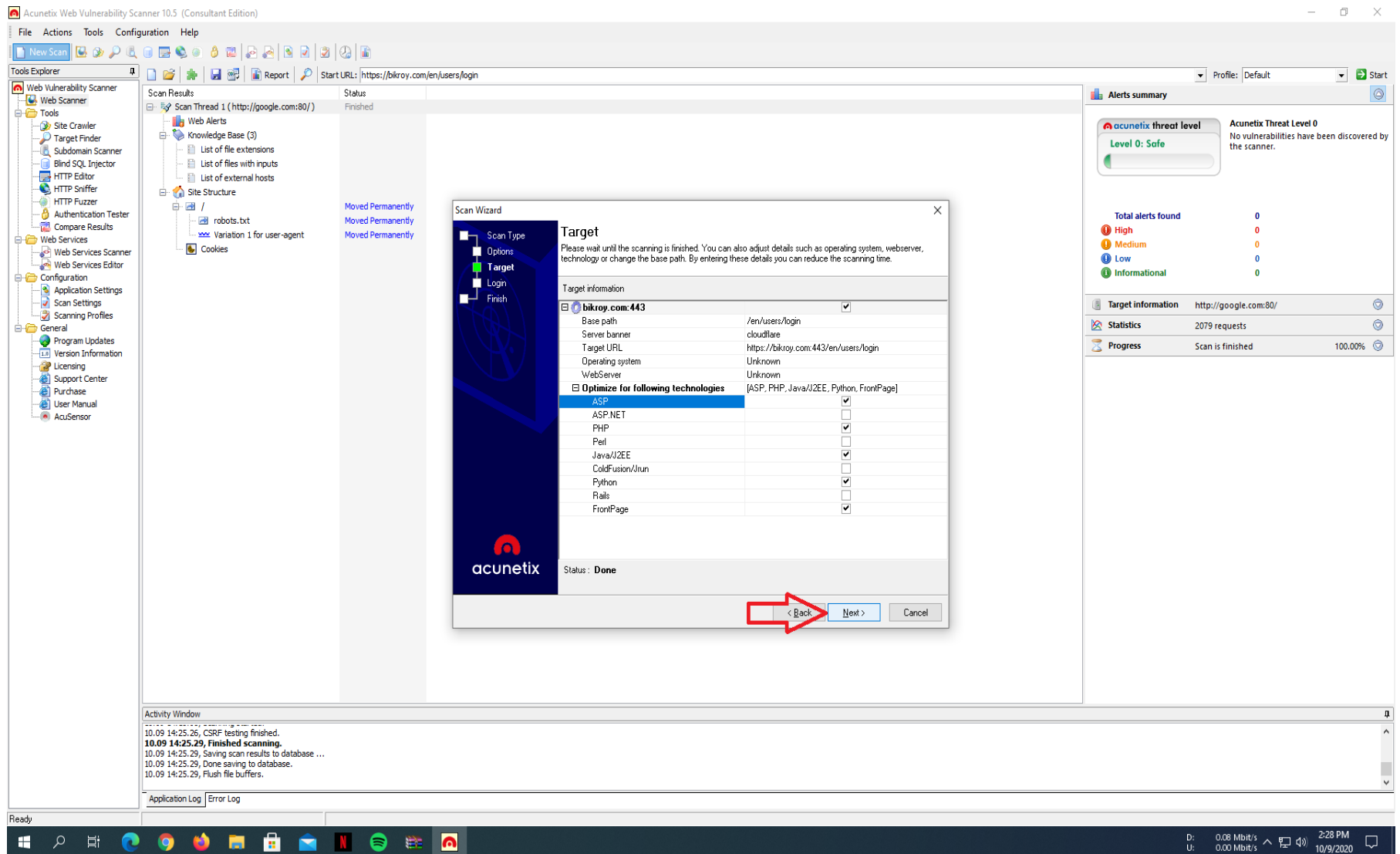
Progress Scan is finished 100.00%

Activity Window

```
10.09 14:25:26, CSRF testing finished.
10.09 14:25:29, Finished scanning.
10.09 14:25:29, Saving scan results to database ...
10.09 14:25:29, Done saving to database.
10.09 14:25:29, Flush file buffers.
```

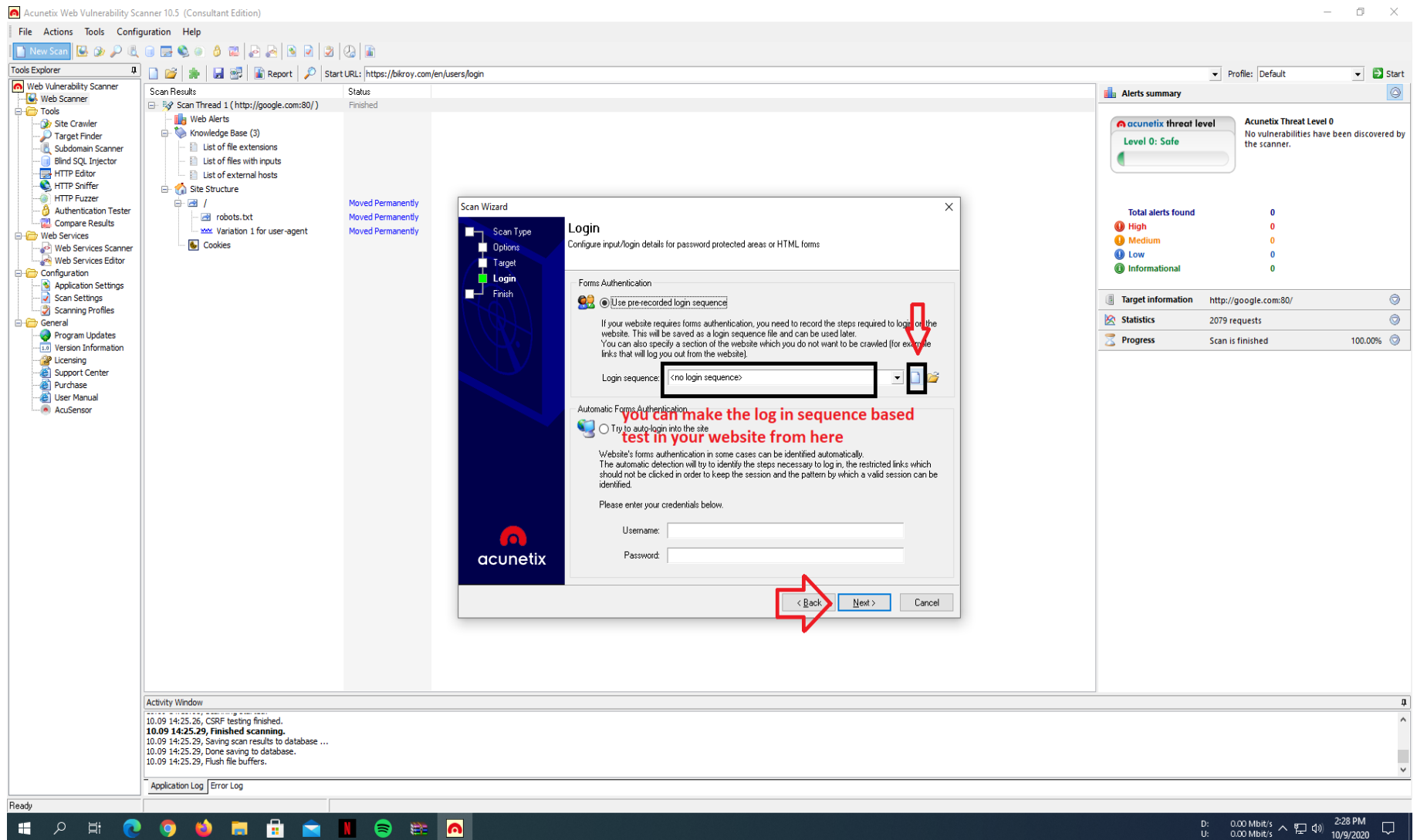
Application Log Error Log

Press Next button.

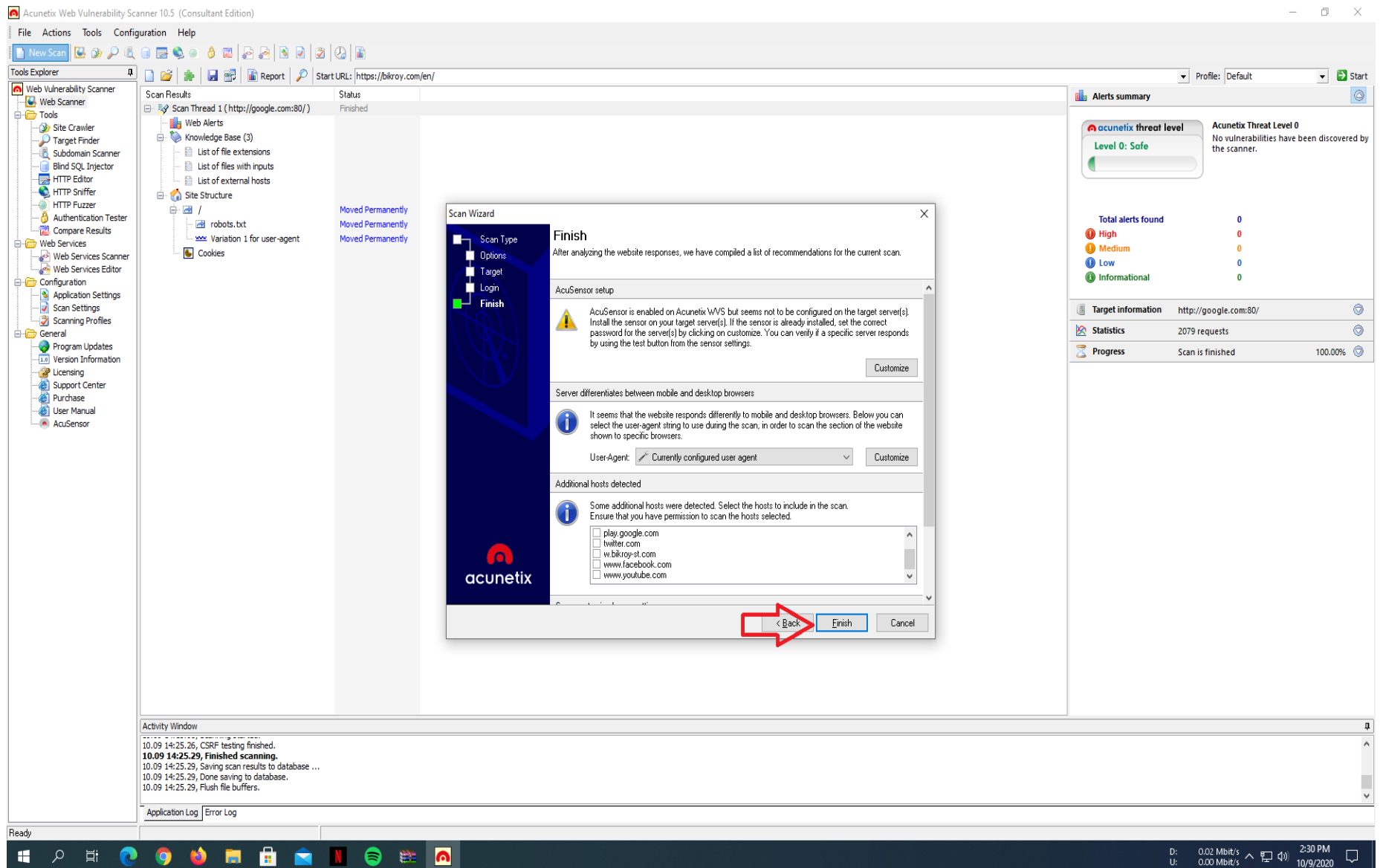


We can make the login sequence based test in our website from here.

Press Next button.



Press Next button.



In this window we can view the results, threats level, progress bar etc.

The screenshot displays the Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition) interface. The main window is divided into several sections:

- Tools Explorer:** A sidebar on the left containing various tools like Site Crawler, Target Finder, Subdomain Scanner, Blind SQL Injector, HTTP Editor, HTTP Sniffer, HTTP Fuzzer, Authentication Tester, Compare Results, Web Services, Web Services Scanner, Web Services Editor, Configuration, Application Settings, Scan Settings, Scanning Profiles, General, Program Updates, Version Information, Licensing, Support Center, Purchase, User Manual, and AcuSensor.
- Scan Results:** A central pane showing the results of a scan. It includes a tree view of findings such as "Clickjacking: X-Frame-Options header missing", "Cookie without HttpOnly flag set", "Cookie without Secure flag set", "Knowledge Base", "SSL server running", "Site Structure", "en", "robots.txt", and "Cookies". The status of the scan is "Scanning".
- Threats Level:** A section on the right showing the "Acunetix threat level" as "Level 1: Low". It includes a description: "One or more low-severity type vulnerabilities have been discovered by the scanner."
- Alerts Type:** A section on the right showing the "Total alerts found" as 4. It includes a breakdown of alert types: High (0), Medium (0), Low (4), and Informational (0).
- Progress Bar:** A section on the right showing the "Progress" of the scan as 70.00%.
- Activity Window:** A section at the bottom showing the "Application Log" and "Error Log" with timestamps and details of the scan process.

Annotations in red text and arrows highlight the "Scan Results", "Threats Level", and "Progress Bar" sections.

We can generate report from here.

The screenshot displays the Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition) interface. The main window shows the 'Scan Results' for 'Scan Thread 1 (https://bikroy.com:443/en/)', which is 'Finished (4 alerts)'. A red arrow points to the 'Reporter' button in the top toolbar, with the text 'You can generate Report from here' next to it. The left sidebar contains a 'Tools Explorer' with various tools like Site Crawler, Target Finder, and Subdomain Scanner. The right sidebar shows an 'Alerts summary' with 4 alerts, a threat level of 'Level 1: Low', and a progress bar. The bottom status bar shows 'Ready' and the system clock at 2:35 PM on 10/9/2020.

Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

File Actions Tools Configuration Help

New Scan

Tools Explorer

Web Vulnerability Scanner

Web Scanner

Tools

Site Crawler

Target Finder

Subdomain Scanner

Blind SQL Injector

HTTP Editor

HTTP Sniffer

HTTP Fuzzer

Authentication Tester

Compare Results

Web Services

Web Services Scanner

Web Services Editor

Configuration

Application Settings

Scan Settings

Scanning Profiles

General

Program Updates

Version Information

Licensing

Support Center

Purchase

User Manual

AcuSensor

Scan Results

Scan Thread 1 (https://bikroy.com:443/en/) Finished (4 alerts)

Web Alerts (4)

Clickjacking: X-Frame-Options head...

Cookie without HttpOnly flag set (1)

Cookie without Secure flag set (2)

Knowledge Base (3)

SSL server running [443]

List of file extensions

List of files with inputs

Site Structure

/

en

robots.txt

Cookies

Moved Permanently OK

Reporter

Status

Alerts summary 4 alerts

acunetix threat level

Level 1: Low

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Total alerts found 4

High 0

Medium 0

Low 4

Informational 0

Target information https://bikroy.com:443/en/

Statistics 2378 requests

Progress Scan is finished 100.00%

Activity Window

10.09 14:34:20, CSRF testing finished.

10.09 14:34:21, Finished scanning.

10.09 14:34:21, Saving scan results to database ...

10.09 14:34:21, Done saving to database.

10.09 14:34:21, Flush file buffers.

Application Log Error Log

Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

File Actions Tools Configuration Help

New Scan

Tools Explorer

- Web Vulnerability Scanner
- Web Scanner
- Tools
 - Site Crawler
 - Target Finder
 - Subdomain Scanner
 - Blind SQL Injector
 - HTTP Editor
 - HTTP Sniffer
 - HTTP Fuzzer
 - Authentication Tester
 - Compare Results
- Web Services
 - Web Services Scanner
 - Web Services Editor
- Configuration
 - Application Settings
 - Scan Settings
 - Scanning Profiles
- General
 - Program Updates
 - Version Information
 - Licensing
 - Support Center
 - Purchase
 - User Manual
 - AcuSensor

Start URL: <https://bikroy.com:443/en/>

Scan Results

Scan Thread 1 (<https://bikroy.com:443/en/>)

Status: Finished (4 alerts)

Web Alerts (4)

- Clickjacking: X-Frame-Options heade...
- Cookie without HttpOnly flag set (1)
- Cookie without Secure flag set (2)

Knowledge Base (3)

- SSL server running [443]
- List of file extensions
- List of files with inputs

Site Structure

- /
- en
- robots.txt
- Cookies

Moved Permanently OK

acunetix WEB APPLICATION SECURITY

WVS Reporter

Initializing GUI ...

Copyright © 2015 Acunetix Ltd www.acunetix.com

Alerts summary 4 alerts

Profile: Default Start

acunetix threat level

Level 1: Low

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Total alerts found 4

- High 0
- Medium 0
- Low 4
- Informational 0

Target information <https://bikroy.com:443/en/>

Statistics 2378 requests

Progress Scan is finished 100.00%

Activity Window

10.09 14:34:20, CSRF testing finished.

10.09 14:34:21, Finished scanning.

10.09 14:34:21, Saving scan results to database ...

10.09 14:34:21, Done saving to database.

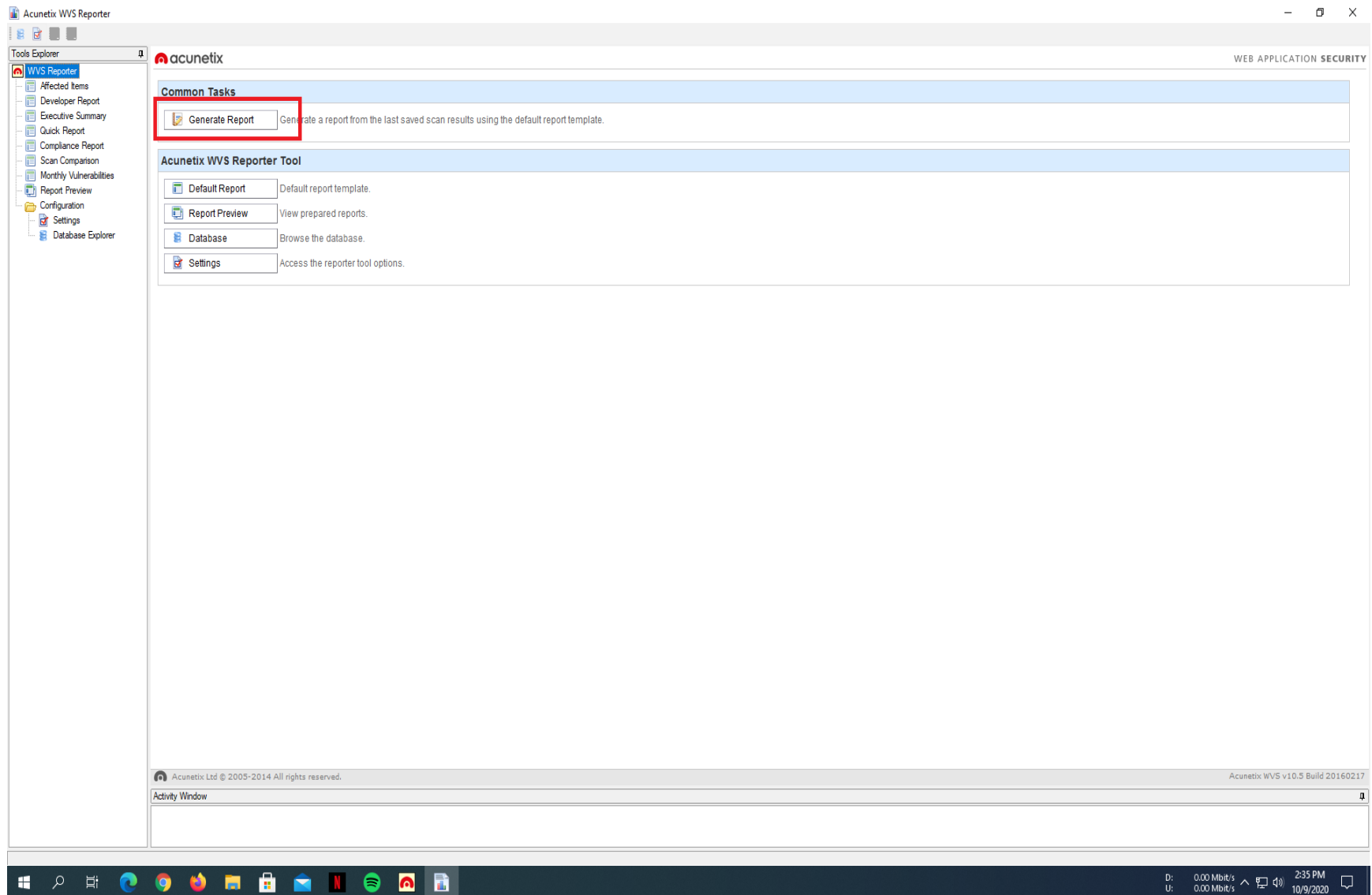
10.09 14:34:21, Flush file buffers.

Application Log Error Log

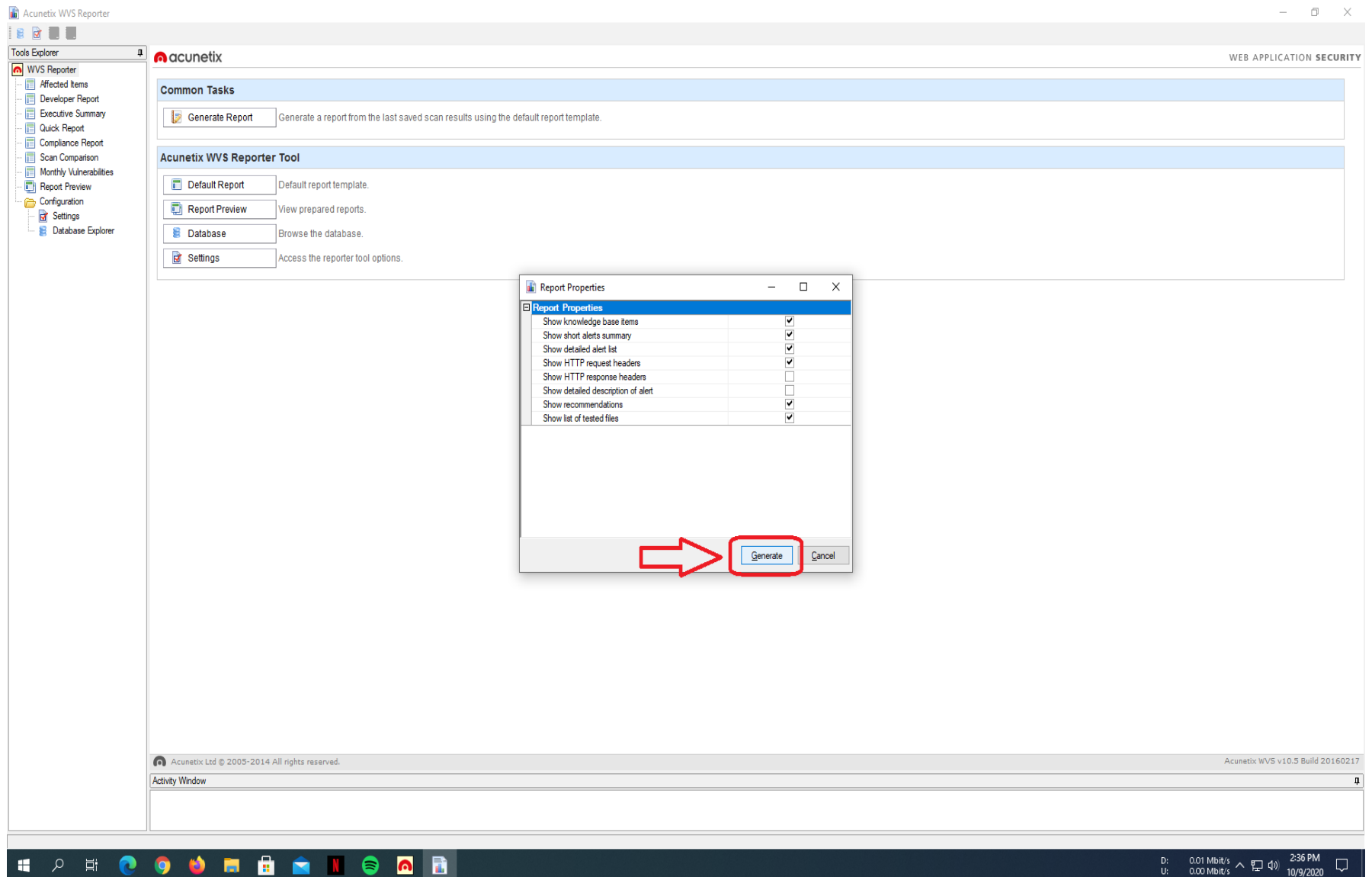
Ready

D: 0.00 Mbit/s U: 0.01 Mbit/s 2:35 PM 10/9/2020

Press “Generate Reports”.



Now create the report.



This is our report.

Acunetix WVS Reporter

Tools Explorer


- WVS Reporter
 - Affected Items
 - Developer Report
 - Executive Summary
 - Quick Report
 - Compliance Report
 - Scan Comparison
 - Monthly Vulnerabilities
 - Report Preview
- Configuration
 - Settings
 - Database Explorer

Scan details

- Knowledge base
- Alerts summary
 - Alerts details
 - Clickjacking
 - Cookie with
 - Cookie with
- Scanned items (cov

acunetix WEB APPLICATION SECURITY

Here is your Report



Acunetix Website Audit
9 October, 2020

Developer Report

1/8

Activity Window

D: 0.00 Mbit/s
U: 0.00 Mbit/s

2:36 PM
10/9/2020

Acunetix WVS Reporter

Tools Explorer

- WVS Reporter
 - Affected Items
 - Developer Report
 - Executive Summary
 - Quick Report
 - Compliance Report
 - Scan Comparison
 - Monthly Vulnerabilities
 - Report Preview
 - Configuration
 - Settings
 - Database Explorer
- Scan details
 - Knowledge base
 - Alerts summary
 - Alerts details
 - Clickjacking
 - Cookie with
 - Cookie with
 - Scanned items (cov

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-693

Affected items	Variation
Web Server	1

Acunetix Website Audit 3

Cookie without HttpOnly flag set

Classification

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Affected items	Variation
/	1

Cookie without Secure flag set

Classification

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Affected items	Variation
/	2

Activity Window

4/8

D: 0.00 Mbit/s
U: 0.00 Mbit/s
2:35 PM
10/9/2020

Acunetix WVS Reporter

Tools Explorer

WVS Reporter

Affected Items

Developer Report

Executive Summary

Quick Report

Compliance Report

Scan Comparison

Monthly Vulnerabilities

Report Preview

Configuration

Settings

Database Explorer

Scan details

Knowledge base

Alerts summary

Alerts details

Clickjacking

Cookie with

Cookie with

Scanned items (cov

the possible values for this header.

References

[Clickjacking Protection for Java EE](#)

[Frame Buster Buster](#)

[Defending with Content Security Policy frame-ancestors directive](#)

[OWASP Clickjacking](#)

[Clickjacking](#)

[The X-Frame-Options response header](#)

Affected items

Web Server

Details

No details are available.

Request headers

GET / HTTP/1.1

Cookie: _cfduid=d59316edd7ac62bbf86fa3c3435e0e7d11602232249; locale=en

Host: hikroy.com

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Accept: */*

Acunetix Website Audit

5

Cookie without HttpOnly flag set

Severity

Low

Type

Informational

Reported by module

Crawler

Activity Window

5/8

Windows Taskbar

0.00 Mbit/s

0.00 Mbit/s

2:36 PM

10/9/2020