Administration of Computer Systems

Report Topic: ACUNETIX

Member

Đặng Hoàng Phúc ID: BA9-050

Tables of Contents:

I. INTRODUCTION TO ACUNETIX:

1. Why You Need To Secure Your Web Applications:

- Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.

- Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits.

- The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and are used to propagate and facilitate further hacking.

- Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.

- If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber-attacks are done at the web application level.

- Why are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.

- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.

- Web applications often have direct access to backend data such as customer databases.

- Most web applications are custom-made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.

- Various high-profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised, hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.

- Network security defense provides no protection against web application attacks since these are launched on port 80 which has to remain open to allow regular operation of the business. It is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

2. The need for automated web application security scanning:

- Manual vulnerability auditing of all your web applications is complex and time-consuming, since it generally involves processing a large volume of data. It also demands a high level of expertise and the ability to keep track of considerable volumes of code used in a web application. In addition, hackers are constantly finding new ways to exploit your web application, which means that you would have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them.

- Automated vulnerability scanning allows you to focus on the already challenging task of building a web application. An automated web application scanner is always on the lookout for new attack paths that hackers can use to access your web application or the data behind it.

- Within minutes, an automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components.

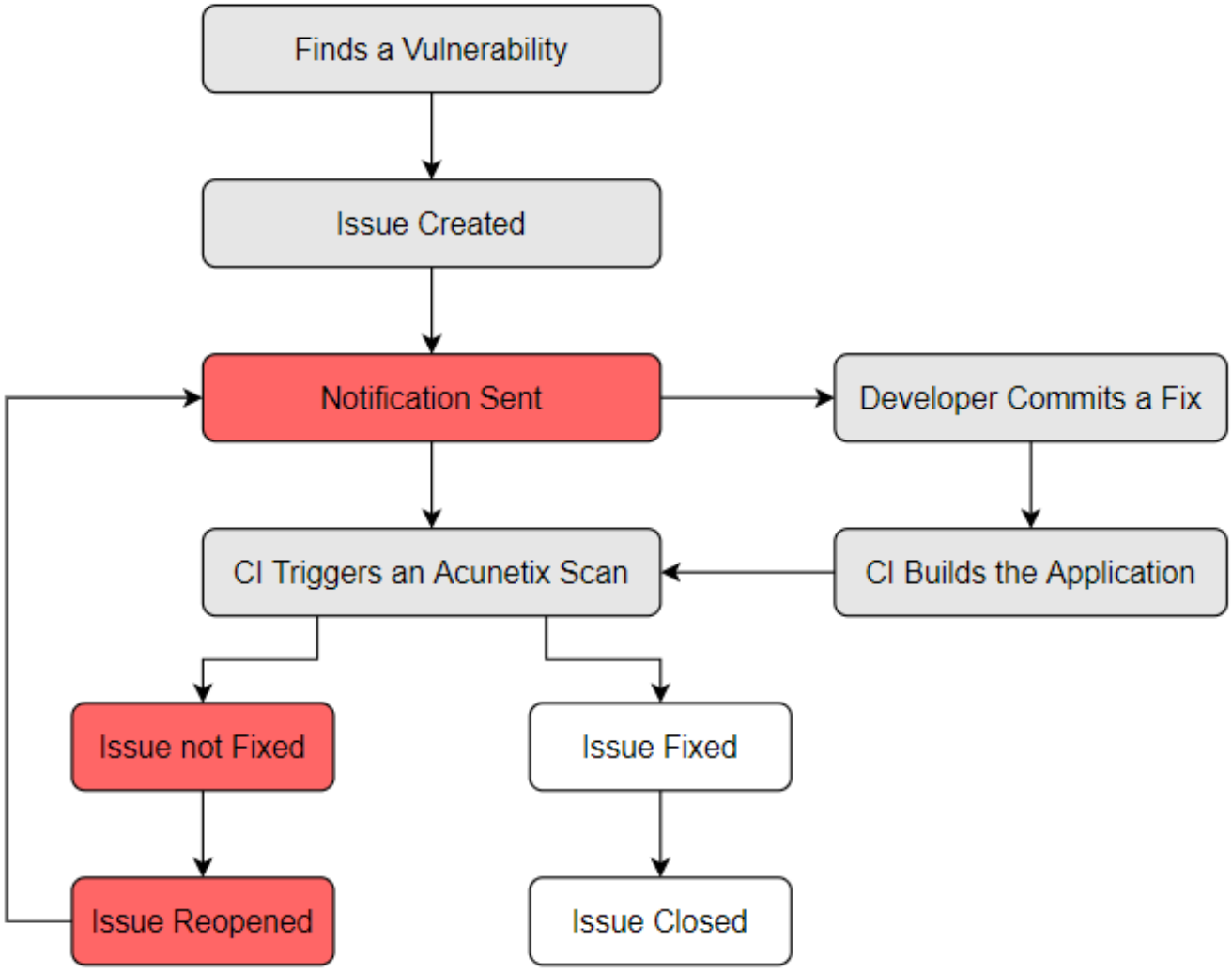
- In addition, an automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited.

3. Acunetix Vulnerability Management:

- Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

- Acunetix offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

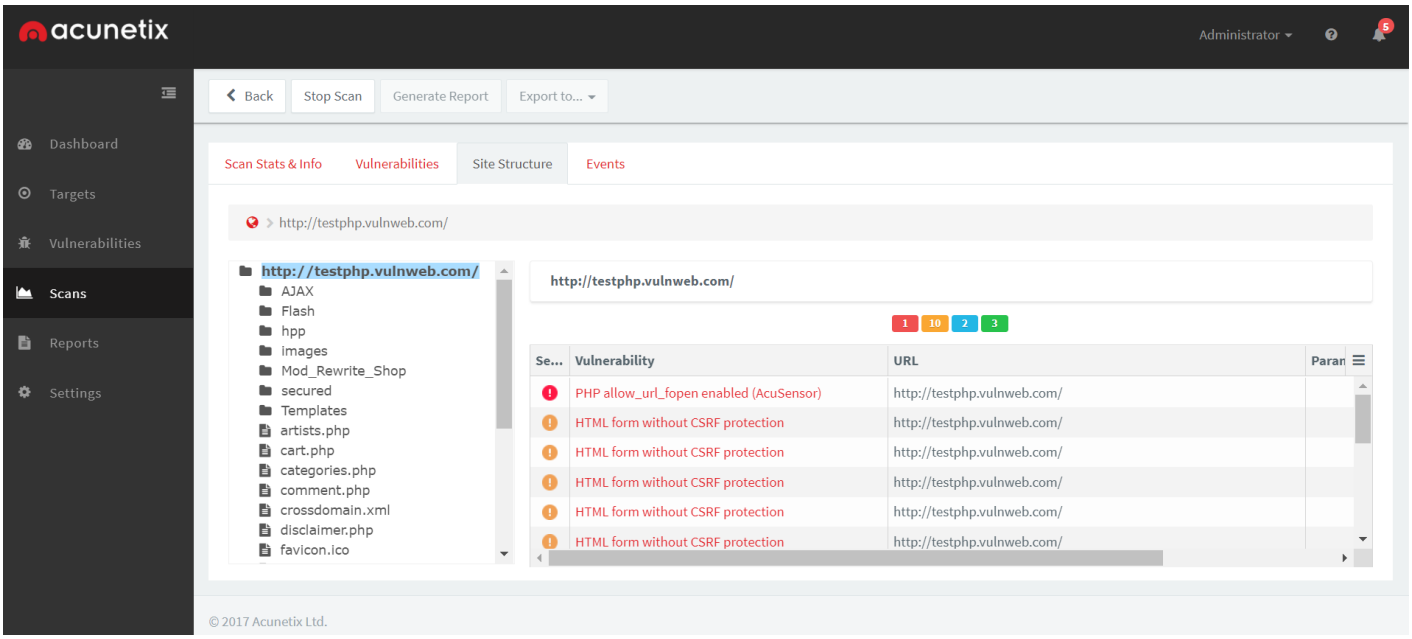
4. Diagram of acunetix:



5. How Acunetix Works:

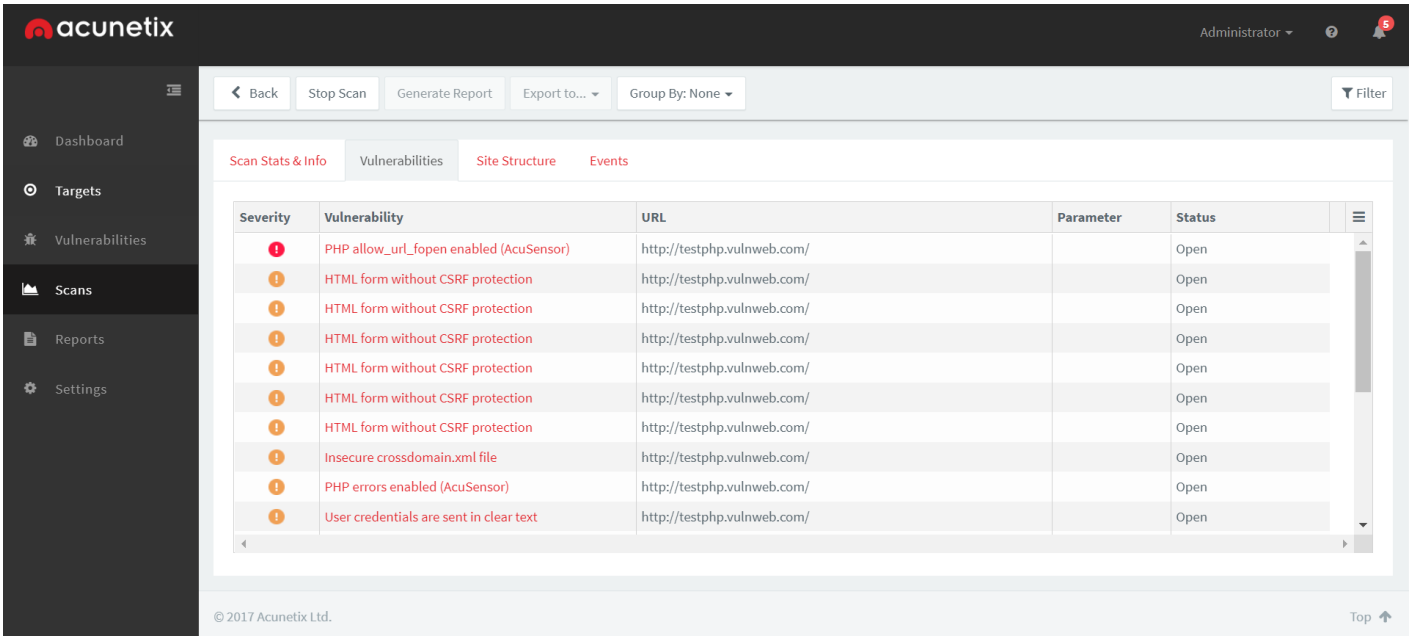
- Acunetix works in the following manner:

+ Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix will use to launch targeted checks against each part of the site.



+ If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and add the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website. Acunetix AcuSensor also analyses files which are not accessible from the internet, such as web.config.

+ After the crawling process, the scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Acunetix also analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage. If the AcuSensor Technology is enabled, a series of additional vulnerability checks are launched against the website. More information about AcuSensor is provided in the following section.



+ The vulnerabilities identified are shown in the Scan Results. Each vulnerability alert contains information about the vulnerability such as POST data used, affected item, HTTP response of the server and more.

+ If AcuSensor Technology is used, details such as source code line number, stack trace or affected SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.

+ Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI DSS or ISO 270001.

6. Acunetix AcuSensor Technology:

- Acunetix' unique AcuSensor Technology allows you to identify more vulnerabilities than other Web Application Scanners, whilst generating less false positives. Acunetix AcuSensor indicates exactly where in your code the vulnerability is and reports additional debug information.

- The increased accuracy, available for PHP, .NET and JAVA web applications, is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. AcuSensor technology combines both techniques to achieve significantly better results than using source code analyzers and black box scanning independently.

- AcuSensor can be installed in .NET, PHP and JAVA code transparently.

- AcuSensor can be installed into pre-compiled .NET and JAVA assemblies, even if they are signed (strong-named), therefore, neither .NET or JAVA source code, nor a compiler (or any other dependencies) are required. In case of PHP web applications, the source is readily available. To date, Acunetix is the only web vulnerability security solution to implement this technology.

7. Advantages of using AcuSensor Technology:

- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.

- Significantly reduces false positives when scanning a website because it understands the behavior of the web application better.

- Alerts you to web application configuration problems which can result in a security misconfiguration, or expose sensitive information. E.g. If 'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.

- Advises you how to better secure your web server settings, e.g. if write access is enabled on the web server.

- Detects more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported, whereas now the source code can be analyzed for improved detection.

- Ability to detect SQL injection vulnerabilities in all SQL statements, including in SQL INSERT statements. Using a black box scanner such SQL injection vulnerabilities cannot be found. This significantly increases the ability for Acunetix to find vulnerabilities.

- Scans run using AcuSensor run a back-end crawl, presenting all files accessible through the web server to the scanner; even if these files are not linked through the front-end application. This ensures 100% coverage of the application, and alerts users of any backdoor files that might have been maliciously uploaded by an attacker.

- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and test them.

- Ability to test for arbitrary file creation and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.

8. Network Vulnerability Scanning:

- As part of a website audit, the online version of Acunetix will execute a network security audit of the server hosting the website. This network security scan will identify any services running on the scanned server by running a port scan on the system. Acunetix will report the operating system and the software hosting the services detected. This process will also identify Trojans which might be lurking on the server.

- The network vulnerability scan assesses the security of popular protocols such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet. Apart from testing for weak or default passwords, Acunetix will also check for misconfiguration in the services detected which could lead to a security breach. Acunetix will also check that any other servers running on the machine are not using any deprecated protocols. All these lead to an insecure system, which would allow an intruder to damage your web site and your reputation.

- Acunetix Online also integrates the popular OpenVAS network scanner to check for over 50,000 network vulnerabilities. During a network scan, Acunetix makes use of various port probing and OS fingerprinting techniques to identify a vast number of devices, Operating Systems and server products. Numerous security checks are then launched against the products identified running on the scanned server, allowing you to detect all the vulnerabilities that exist on your perimeter servers.

II. HOW DOES ACUNETIX PERFORM AN AUTOMATED SCAN AND DETECT VULNERABILITIES?

As an automated black-box web application security scanner, Acunetix performs a series of tasks to identify web application vulnerabilities as outlined below.

1. Target Identification:

- Acunetix checks if the Target in question is reachable and running a web server, and therefore serving requests over the HTTP protocol.

- Acunetix fingerprints the web server to identify popular technologies that the web server might be using. This allows the scanner to identify the type of web server (e.g. Apache HTTP Server, Nginx, IIS…), the server-side language being used (e.g. PHP, ASP.NET, Java/J2EE, Python, NodeJS…) as well as the operating system the web server is running on. This information allows the scanner to automatically tune itself to the Target to be scanned – for example, certain vulnerabilities will only exist on Windows servers, or specific versions of PHP.

2. Site crawling and structure mapping:

- The index file is requested from the web server. This is determined by the start URL (e.g. http://www.example.com/ will load index.html).

- Once a response is received, DeepScan is launched, executing any JavaScript present on the web page.

- The Crawler, hand-in-hand with DeepScan will follow links, map input fields and parameters. This contributes to building a list of directories and files within the site.

- Crawling with AcuSensor: If AcuSensor technology is used a list of files will be accurately retrieved directly from the server via a back-end crawl.

3. Security analysis performed against the site structure:

- Acunetix launches a number of security tests against the target website.

- As Acunetix discovers vulnerabilities, alerts are reported in real-time. Each alert produces detailed information about the vulnerability, recommendations on how to fix it, as well as several links through which the user can learn more about the reported vulnerability and how to fix it.

- Scanning with AcuSensor: If AcuSensor is enabled, debug information will also be reported, like the SQL query vulnerable to SQL injection and the line of vulnerable code responsible for the exploit.

- After a scan is completed, scan results may be exported to an XML format, submitted to an Issue Tracker, exported to a WAF for virtual patching, or used to generate a variety of reports.

III. INSTALLING ACUNETIX

1. Minimum System Requirements

- Supported Operating systems

+ Microsoft Windows 8.1 or Windows 2012 R2 and later

+ MacOS Catalina and MacOS Big Sur

+ Ubuntu Desktop/Server 18.0.4 LTS or higher

+ Suse Linux Enterprise Server 15

+ openSUSE Leap 15.0 and 15.1

+ Kali Linux versions 2019.1 and 2020.1

+ CentOS 8 and CentOS Stream Server and Workstation (with SELinux disabled)

+ RedHat 8 (with SELinux disabled)

+ We are actively testing other Linux distributions. Please let us know if you have requests for specific distros.

- CPU: 64 bit processor

- System memory: minimum of 2 GB RAM

- Storage: 1 GB of available hard-disk space.

- This does not include the storage required to save the scan results - this will depend on the level of usage of Acunetix.

2. Supported Browsers

- The Acunetix User Interface is delivered through a web server. The supported browsers are:

+ Firefox

+ Chrome

+ Edge

+ Safari

- If you encounter browser-related issues, please first ensure that you are running the latest version of one of the supported browsers before contacting support.

3. Networking PreRequisites

- Following installation, you will need to configure settings for the AcuSensor Bridge. Before deploying AcuSensor, you need to give some attention to the networking information that Acunetix will use for incoming AcuSensor data. Check the AcuSensor Bridge information here.

4. Installation on Windows

- Download the latest Windows version of Acunetix from the download location provided when you purchased the license.

- Double click the installation file to launch the Acunetix installation wizard and click Next when prompted.

- Review and accept the License Agreement.

- Provide credentials for the Administrative user account. These will be used to access and configure Acunetix.

- Configure how the Acunetix Web UI is accessed, and if remote UI access is allowed.

- Review the installation tasks, and click Install to start the installation.

- Setup will now copy all files and install the Acunetix services.

- Click Finish when ready.

5. Installation on Linux

- Download the latest Linux version of Acunetix from the download location provided when you purchased the license.

- Open a Terminal Window

- Use chmod to add executable permissions on the installation file E.g. chmod +x acunetix_13.0.200205121_x64.sh

- Run the installation

- E.g. sudo ./acunetix_13.0.200205121_x64.sh

- In case there are dependencies missing see the Notes section

- Review and accept the License Agreement.

- Configure the hostname which will be used to access the Acunetix UI

- Provide credentials for the Administrative user account. These will be used to access and configure Acunetix.

- Proceed with the installation.

IV. UPGRADING ACUNETIX

1. Upgrading Acunetix for Windows

- To upgrade from a previous MAJOR version of Acunetix:

+ Close all instances of Acunetix

+ Optionally backup the Acunetix data folder which includes the Acunetix database and other settings. These are all found in <C:\ProgramData\Acunetix>

+ You can run the latest Acunetix installation directly on the machine running the previous version of Acunetix. The installation will detect the older version, and will proceed with upgrading it to the latest version. All your settings will be retained.

2. Upgrading Acunetix for Linux

- To upgrade from a previous MAJOR version of Acunetix:

+ Close all instances of Acunetix

+ Optionally backup the Acunetix data folder which includes the Acunetix database and other settings. These are all found in /home/acunetix/.acunetix

+ You can run the latest Acunetix installation directly on the machine running the previous version of Acunetix. The installation will detect the older version, and will proceed with upgrading it to the latest version. All your settings will be retained.

3. Upgrading Acunetix for MacOS

+ Close all instances of Acunetix

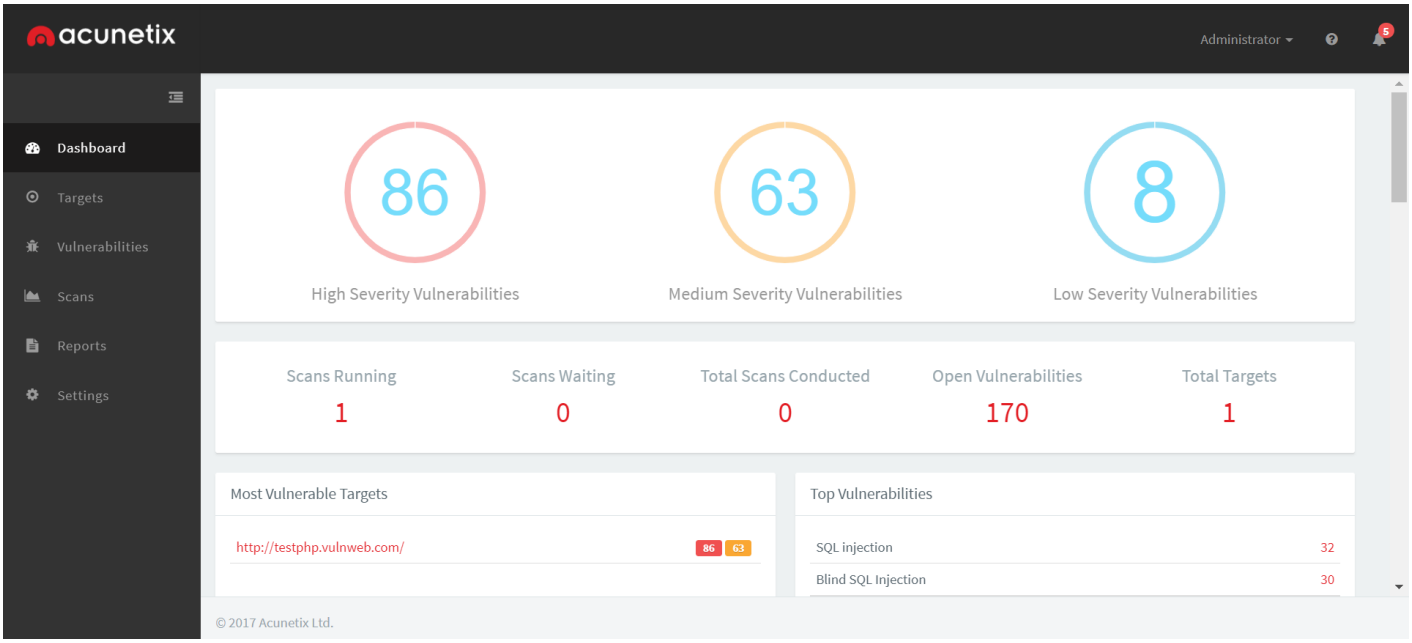
+ Optionally backup the Acunetix data folder which includes the Acunetix database and other settings. These are all found in /Applications/Acunetix.app/Contents/Resources

+ You can run the latest Acunetix installation directly on the machine running the previous version of Acunetix. The installation will detect the older version, and will proceed with upgrading it to the latest version. All your settings will be retained.

V. OVERVIEW AND USAGE OF ACUNETIX

1. Acunetix Overview

- Acunetix allows you to secure your websites and web applications quickly and efficiently, while making it easy to manage the vulnerabilities detected. It consists of the following components:



2. Acunetix Web Interface

- Acunetix ships with an easy to use web interface, allowing multiple users to use Acunetix from a standard web browser. After logging in, users are taken to the Dashboard which provides a bird's-eye view of the security of the organisation’s assets.

- The Dashboard provides a summary view of the security statistics of your web assets, including:

+ totals of unfixed vulnerabilities, split by severity level

+ total number of defined Targets

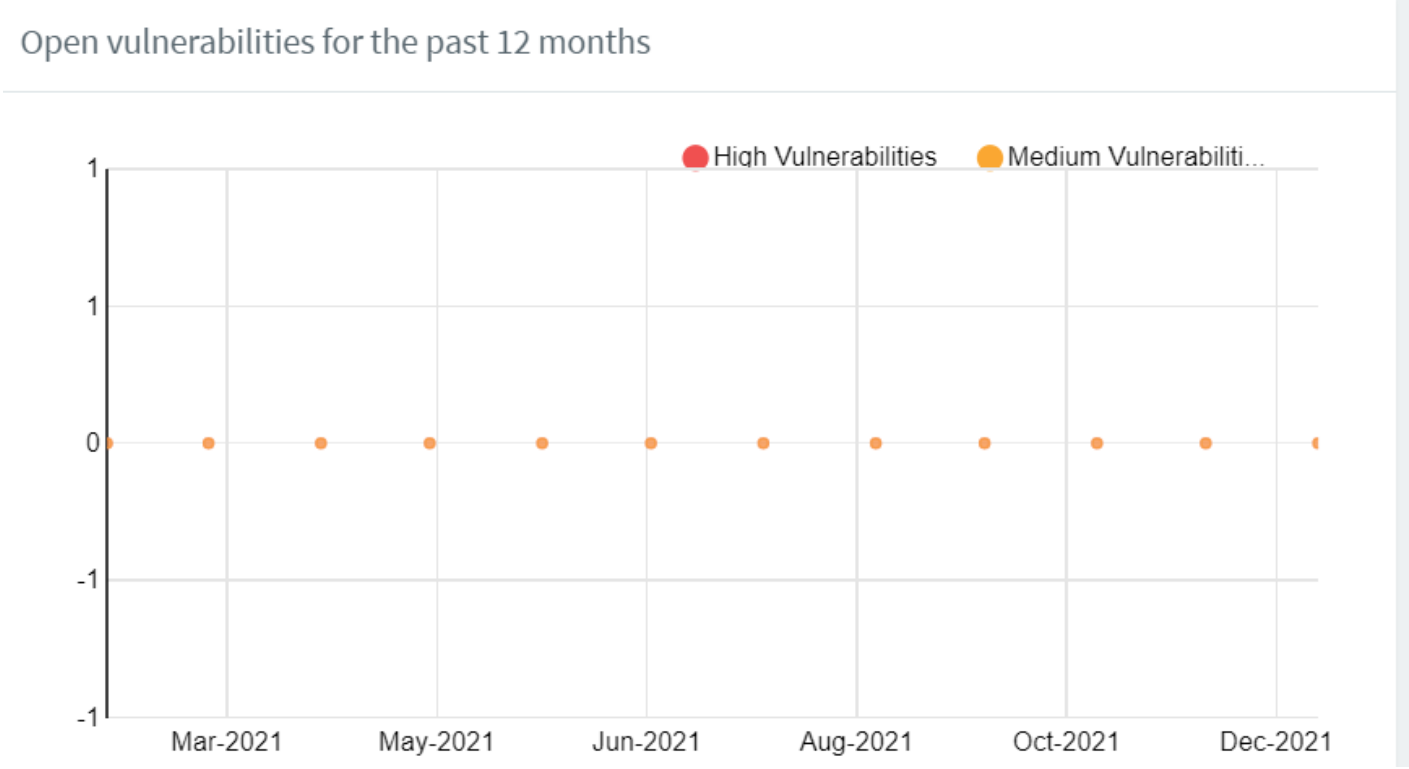
+ total number of Scans completed; total number of Scans in progress; total number of Scans queued

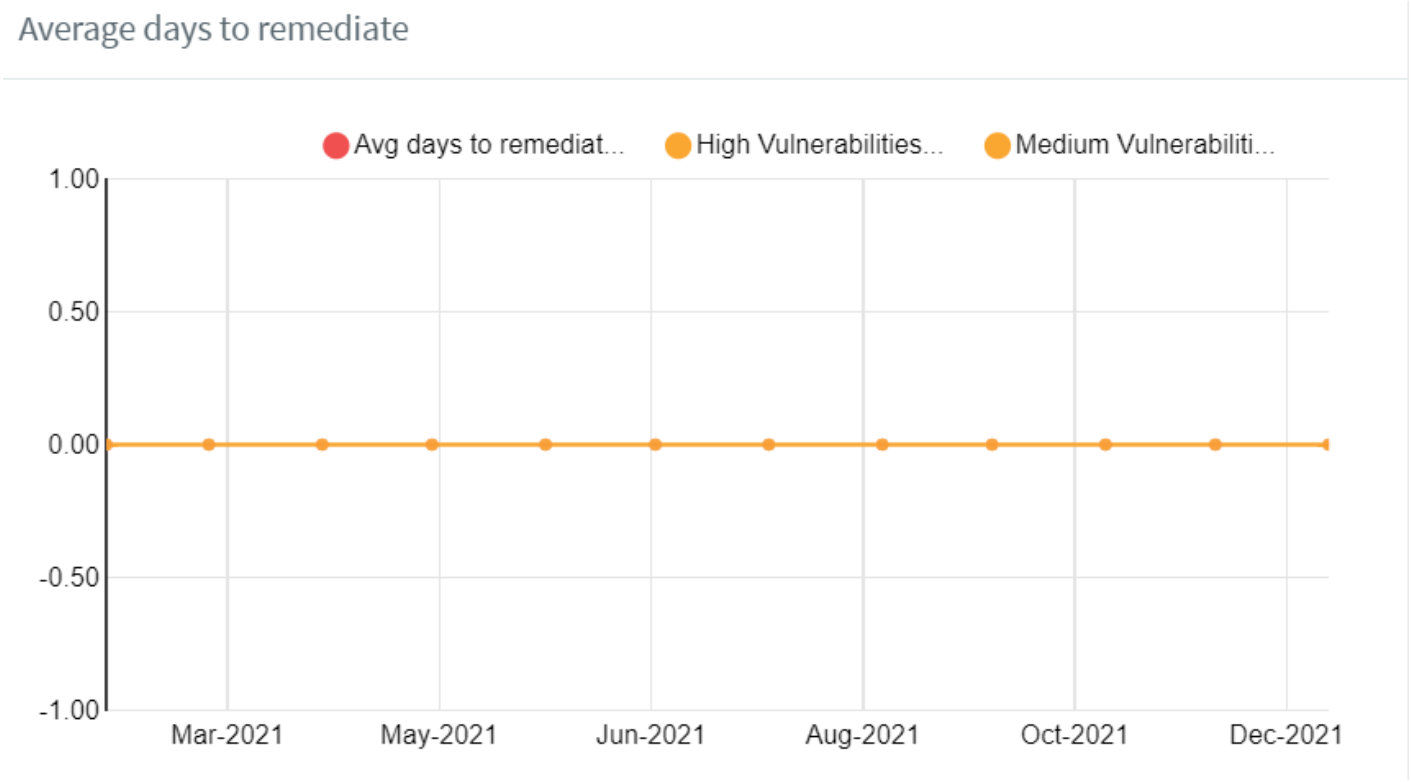
+ top 5 most vulnerable Targets

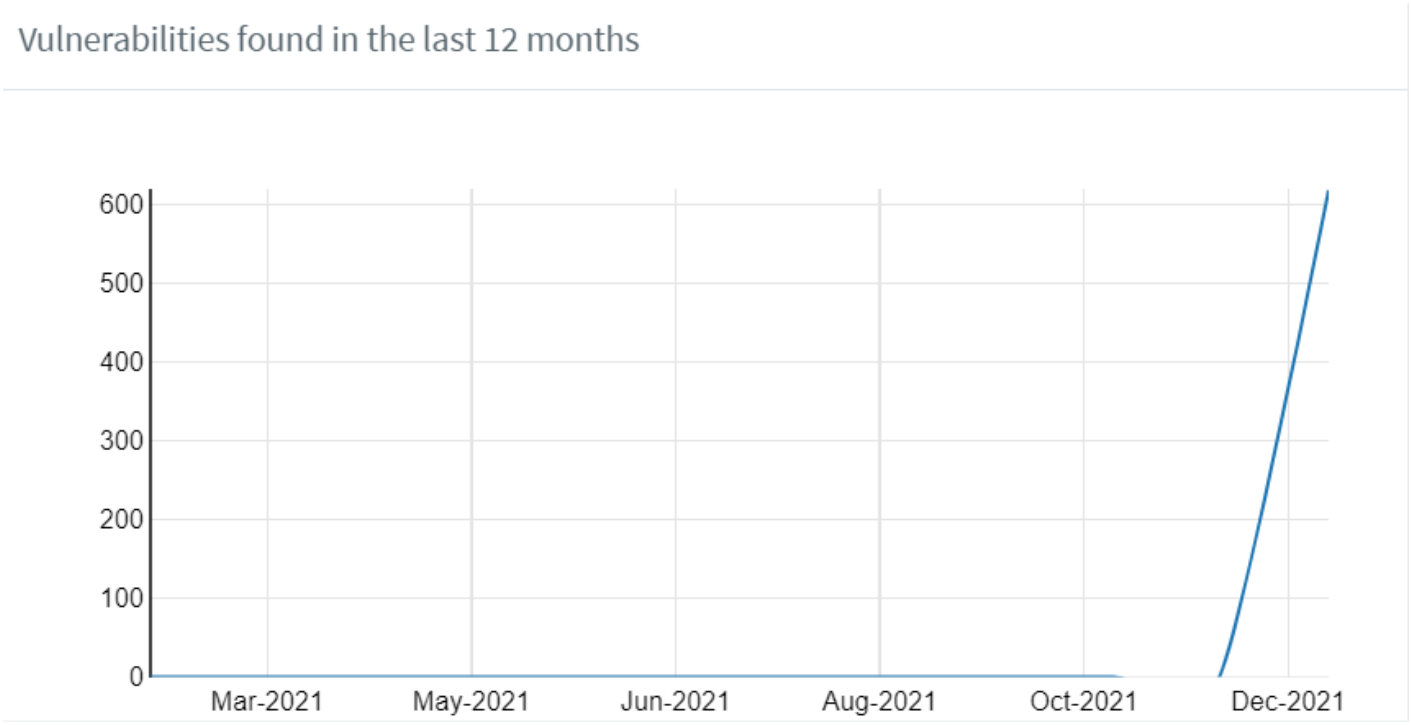
+ top 5 most reported vulnerabilities

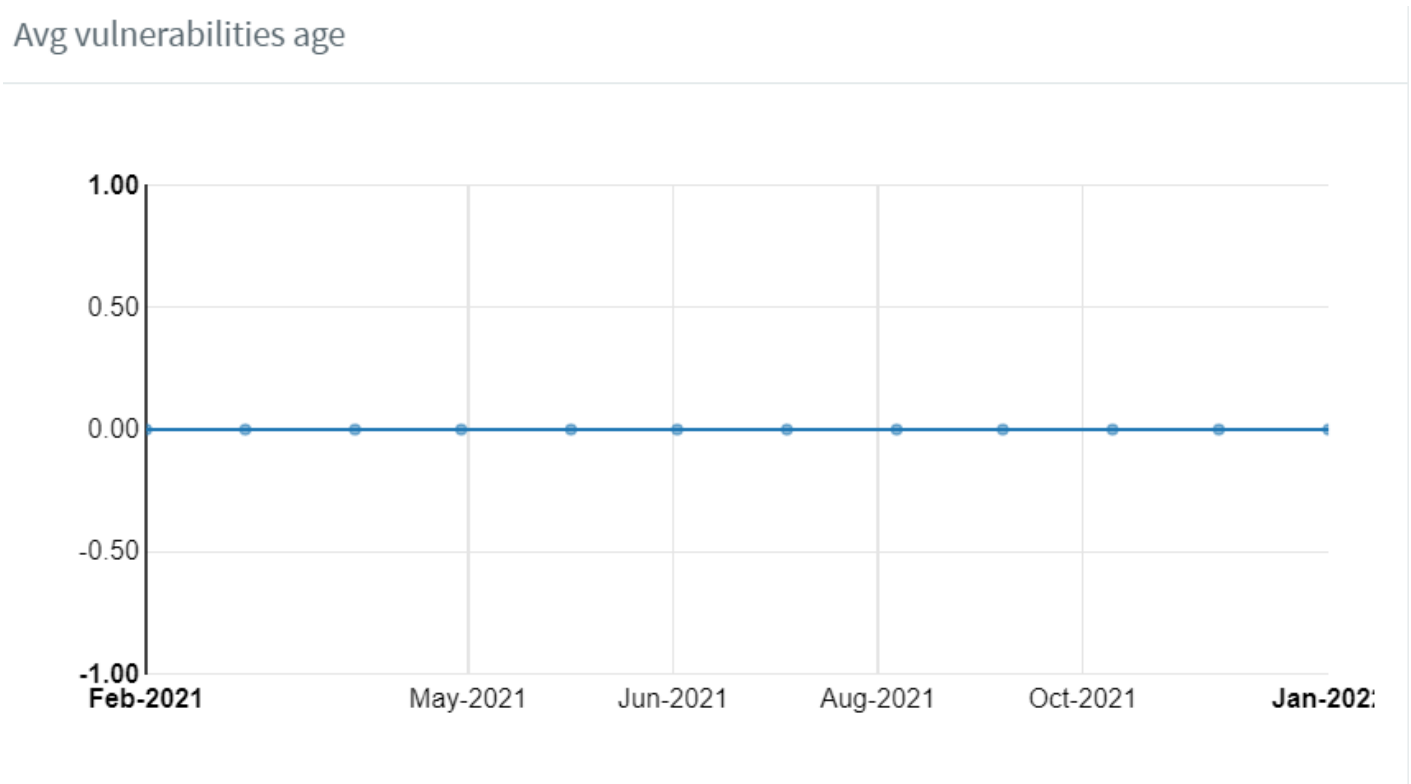
+ trend charts showing month-on-month trends for the last 12 months for:

- number of open vulnerabilities
- average number of days to remediate vulnerabilities
- number of vulnerabilities found
- average vulnerabilities age in days



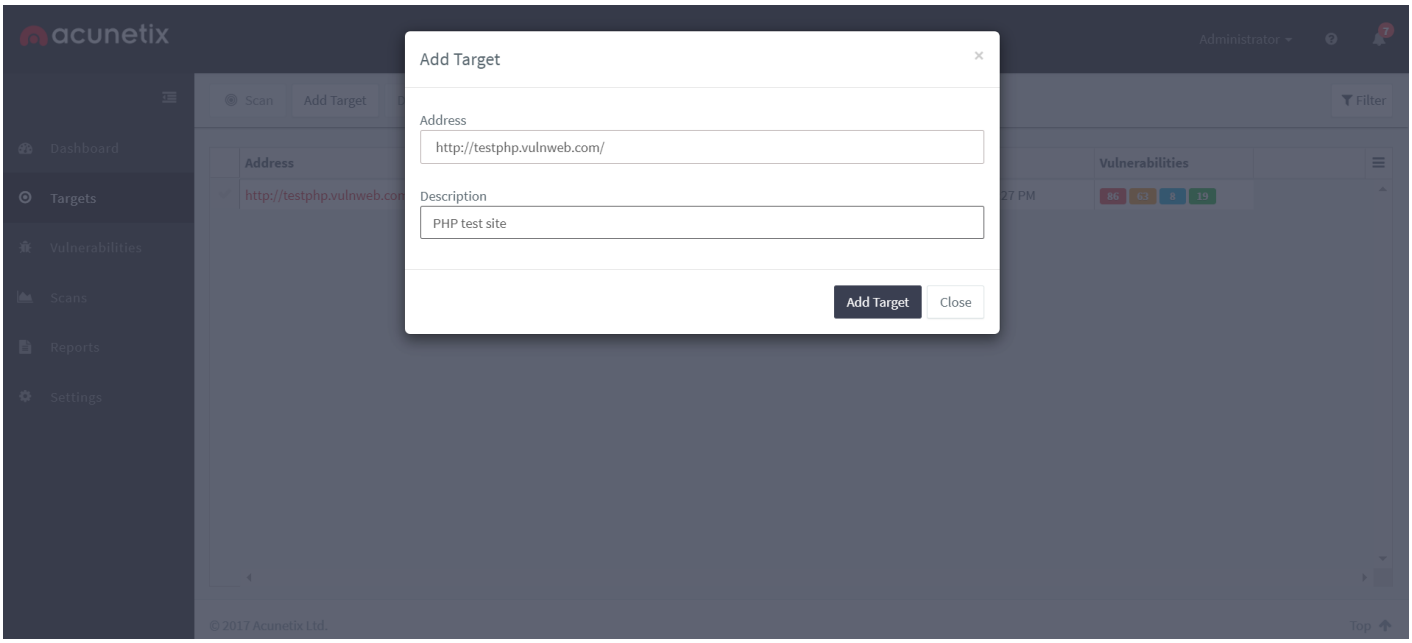






3. Change to the Targets page to configure a new website to scan:

a. From the Targets' page, select 'Add Target'.



b. Provide the address of the asset to scan

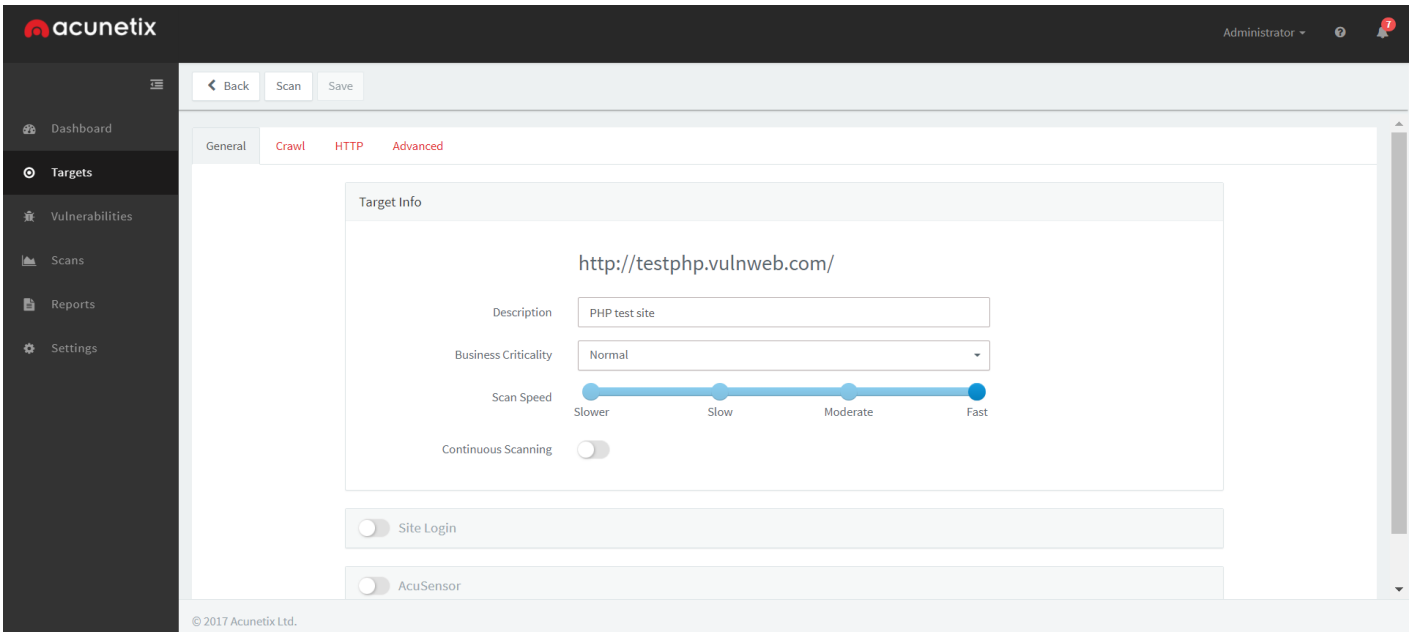
c. Optionally, enter a short description that will allow you to easily identify this target.

d. Click ‘Add Target’ when done.

e. You will be taken to the Target’s options, where you can configure other options if

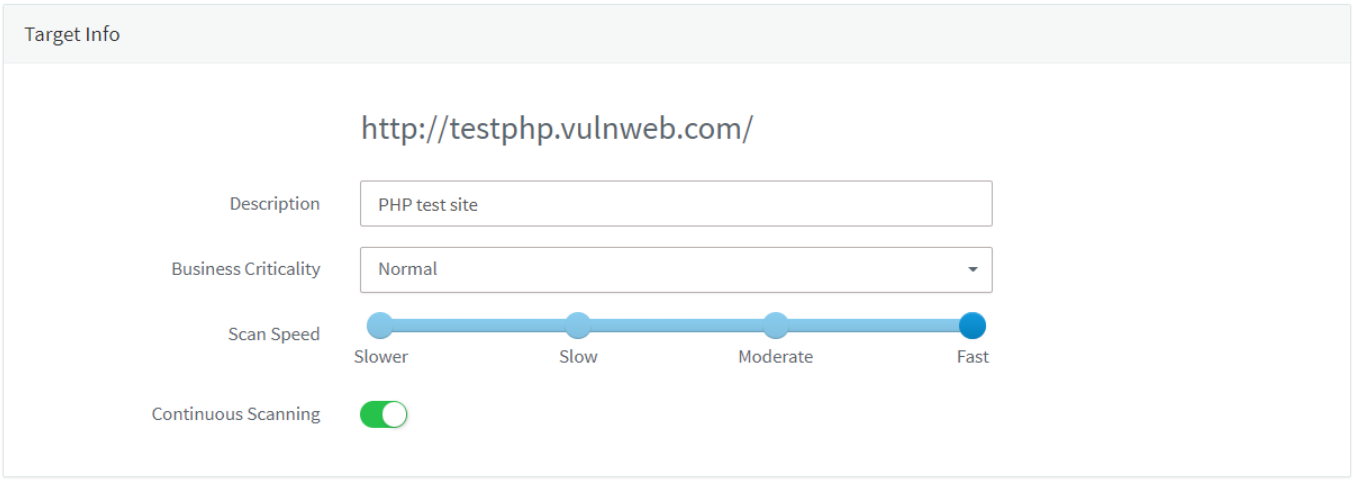
f. needed.

4. From within the Target’s settings



- Continuous Scanning

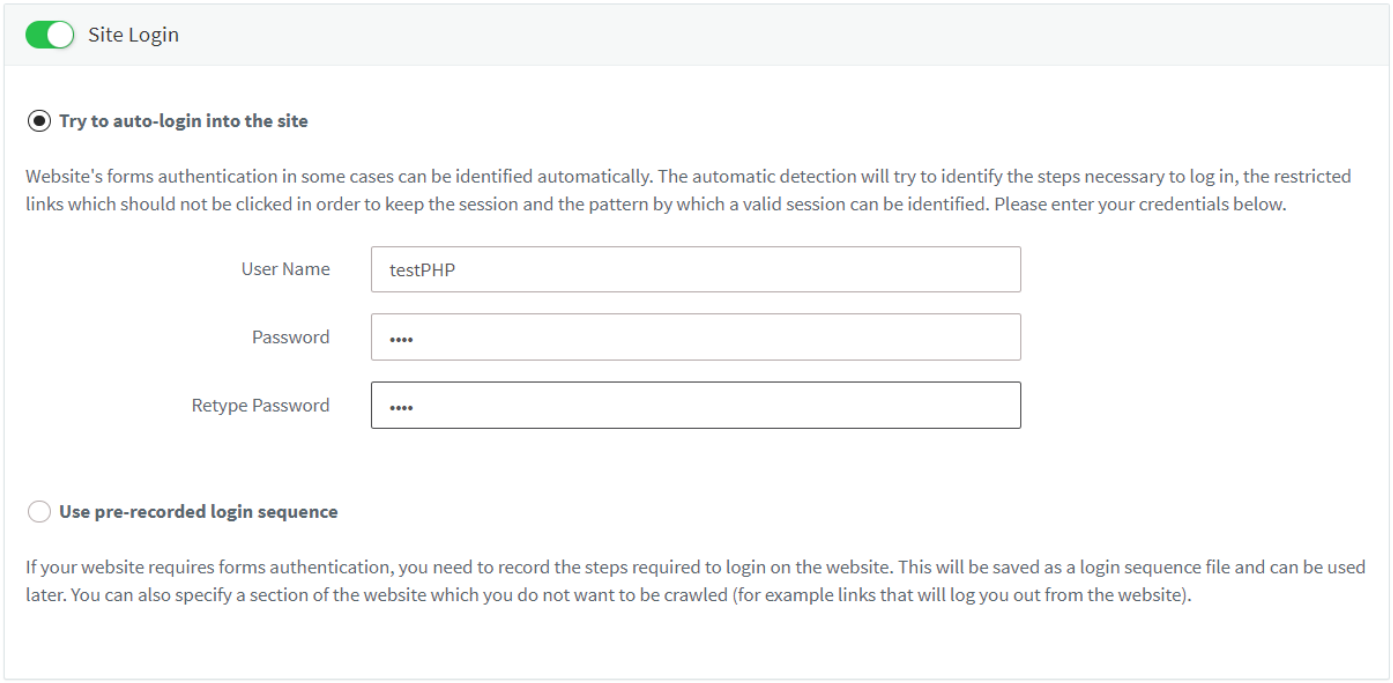
+ After running the initial scan, identifying and fixing the vulnerabilities detected, and making sure that your Targets do not contain vulnerabilities, you need to ensure that they remain secure. Enable Continuous Scanning on a Target to have Acunetix scan the Target on a daily basis and report back any new vulnerabilities immediately. New vulnerabilities can be introduced by web developers making updates to the site or by administrators making changes the web server's configuration. In addition, Acunetix is often updated to detect new vulnerabilties.



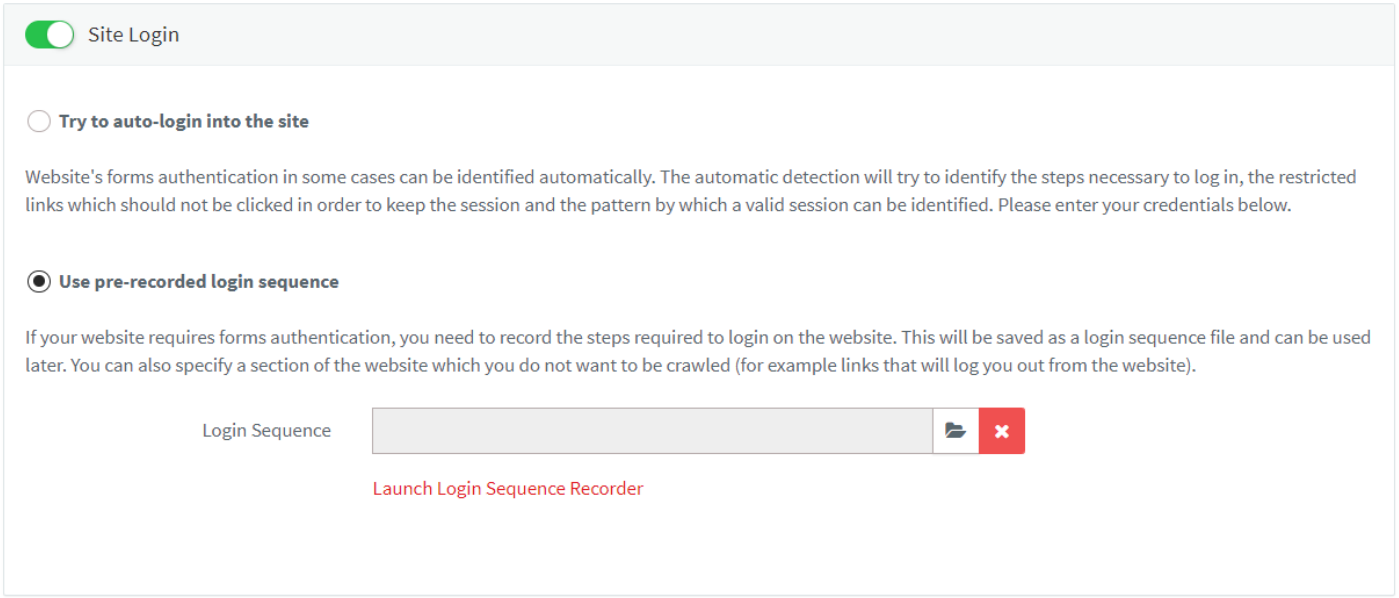
+ Continuous Scanning performs a full scan once a week. This scan is augmented by a daily quick scan, which only scans for critical vulnerabilities. Continuous scans updates the vulnerabilities for the Target, and these can be accessed from the Vulnerabilities page. You will be notified by email and in the notification area when new vulnerabilities are identified.

- Configuring Site Login

+ You may need to scan restricted areas within the web application configured as a Target in Acunetix. The information used to access the restricted area can be configured from the Site Login options found in the General Settings within the Target's configuration.



+ In most cases, you can select to have Acunetix try to auto-login into the site. This will work for most web applications which use a simple login process. You need to provide the Username and Password to access the restricted area. The scanner will automatically detect the login link, the logout link and the mechanism used to maintain the session active.

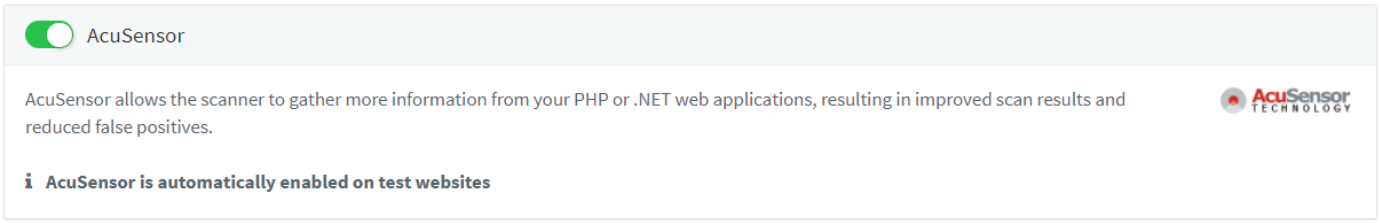


+ For more complex web applications, which might be using a more elaborate login mechanism, you would need to Launch the Login Sequence Recorder and record a login sequence (*.lsr file), which can then be uploaded and saved with your Target settings. Information on how to use the Login Sequence Recorder can be found at

http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/

- Generating and Installing AcuSensor

+ AcuSensor improves the scan results provided by Acunetix by being able to identify all the pages on your website, increases the information about the vulnerabilities detected and decreases false positives.



- click the Scan Now button

5. From the Scans page, click on New Scan. You will be asked to select the Targets to Scan

- After choosing the Target(s) to scan, configure the scan options to be used for the Scan.

+ **Scan Type** - Choose between Full Scan or a scanning profile which will scan for specific vulnerabilities, such as High Risk Vulnerabilities only. The Scan Types are described below

+ **Report** - You can request that a report is automatically generated after the scan is completed. Here is a description of all the Reports

+ **Schedule** - Select if the scan should start instantly, or if the scan should be scheduled for a future date / time. You can also configure to have a recurrent scan.

- Scan Types

The Scan Types is a logical grouping of checks that Acunetix performs to scan for a specific category of vulnerabilities (such as Cross-Site Scripting, SQL Injection, etc.). Below is a list of scanning types available in Acunetix with a short description about each:

+ Full Scan - Use the Full Scan profile to launch a scan using all the checks available in Acunetix.

+ High Risk Vulnerabilities - The High Risk Alerts scanning profile will only check for the most dangerous web vulnerabilities.

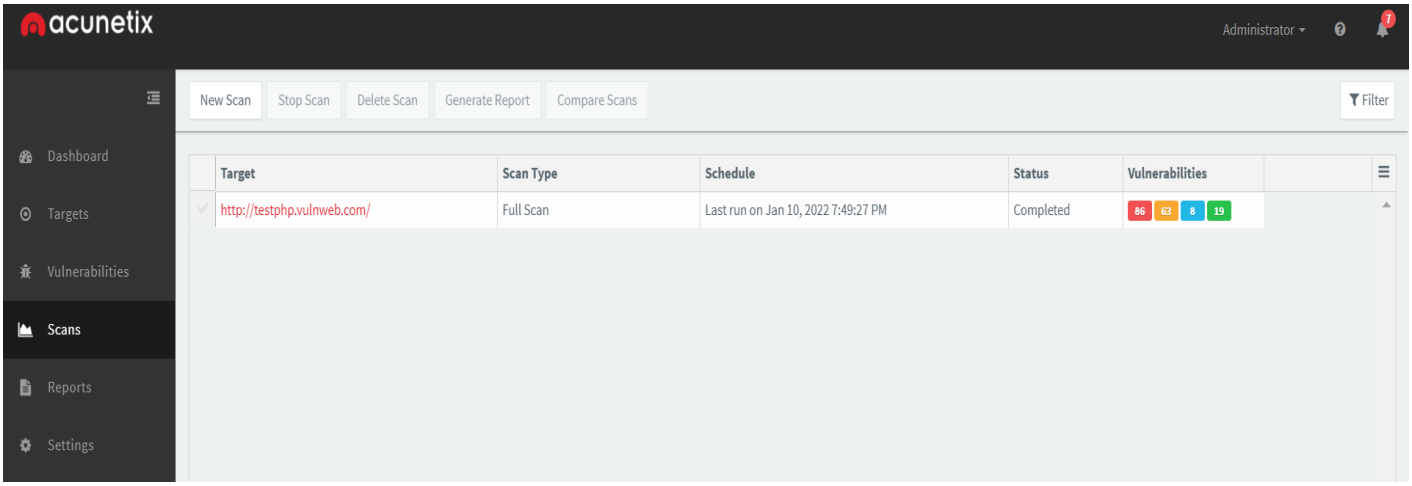
+ Cross-Site Scripting (XSS) - The XSS scanning profile will only check for Cross-Site Scripting vulnerabilities.

+ SQL Injection - The SQL Injection scanning profile will only check for SQL Injection vulnerabilities.

+ Weak Passwords - The Weak Passwords Scanning profile will identify forms which accept a username and password and will attack these forms.

+ Crawl Only - The crawl only scan will only crawl the site and builds the structure of the site without running any vulnerability checks.

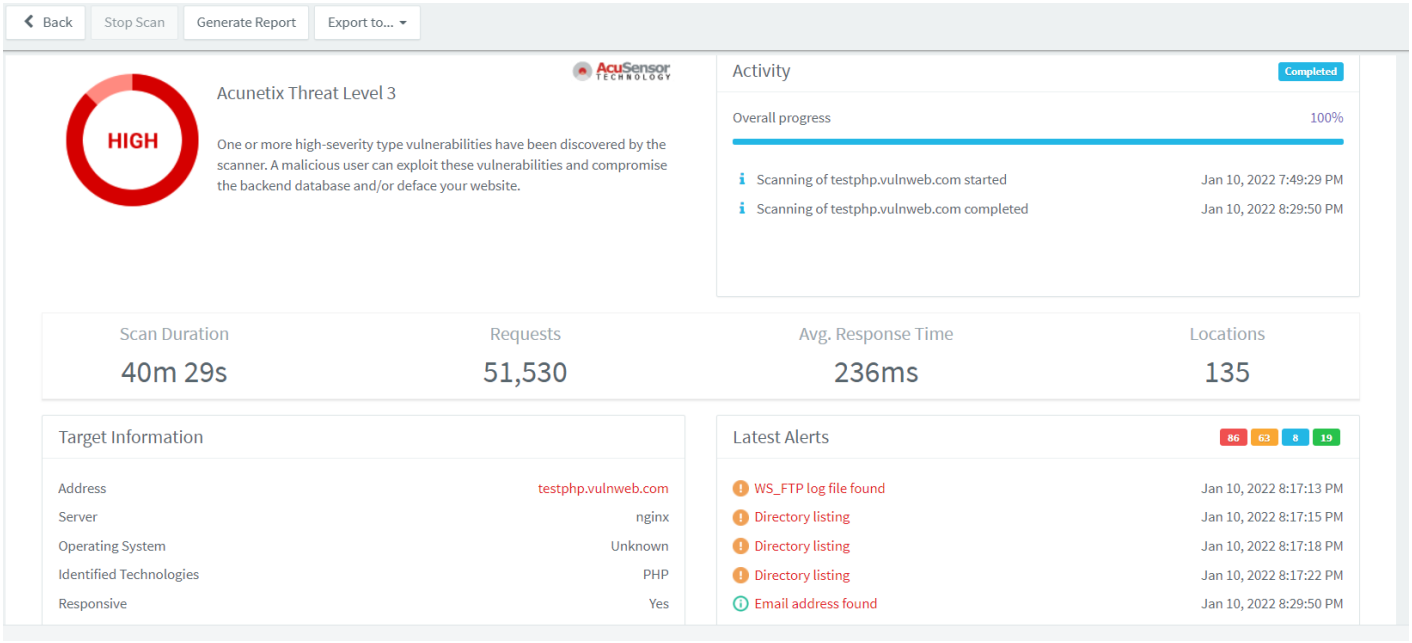
6. Review Scan Results



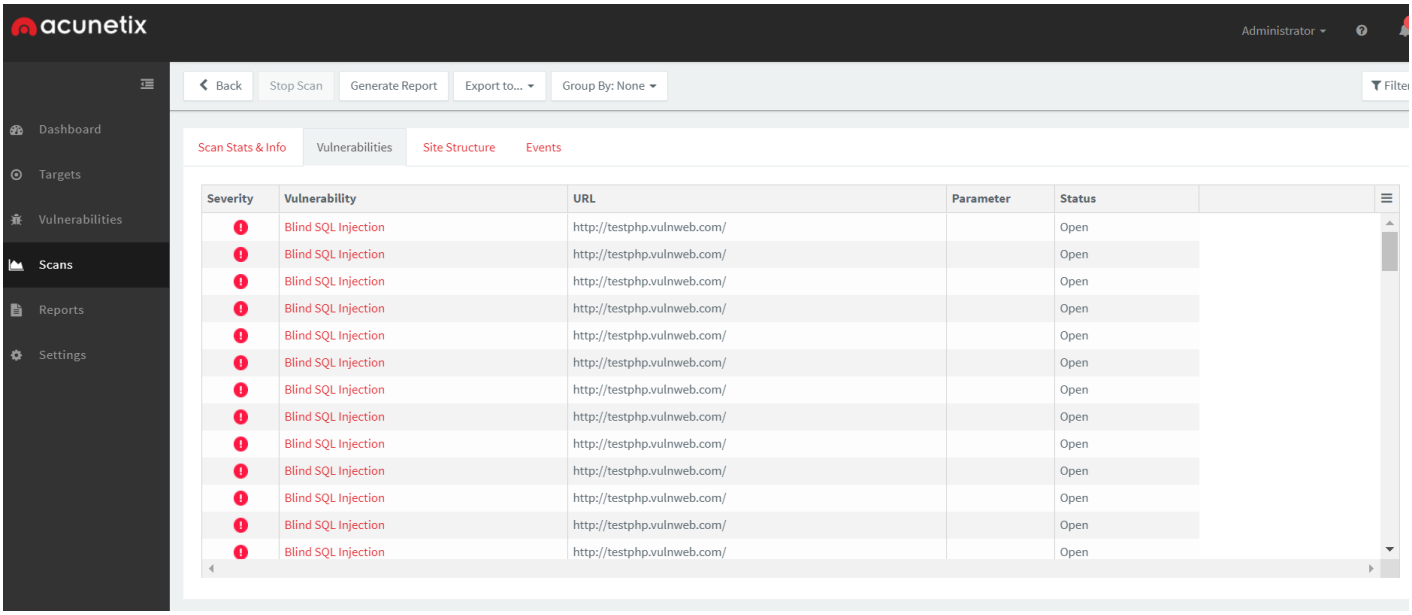
- Once the scan has finished, Acunetix will send you an email with a summary of the results and a link allowing you to access the scan results directly. The scan results show the start and end date of the scan, the duration of the scan and all the alerts that have been identified during the scan. The AcuSensor logo is also displayed when the scan detects and makes use of AcuSensor during a web scan.

- The scan results consists of 4 sections:

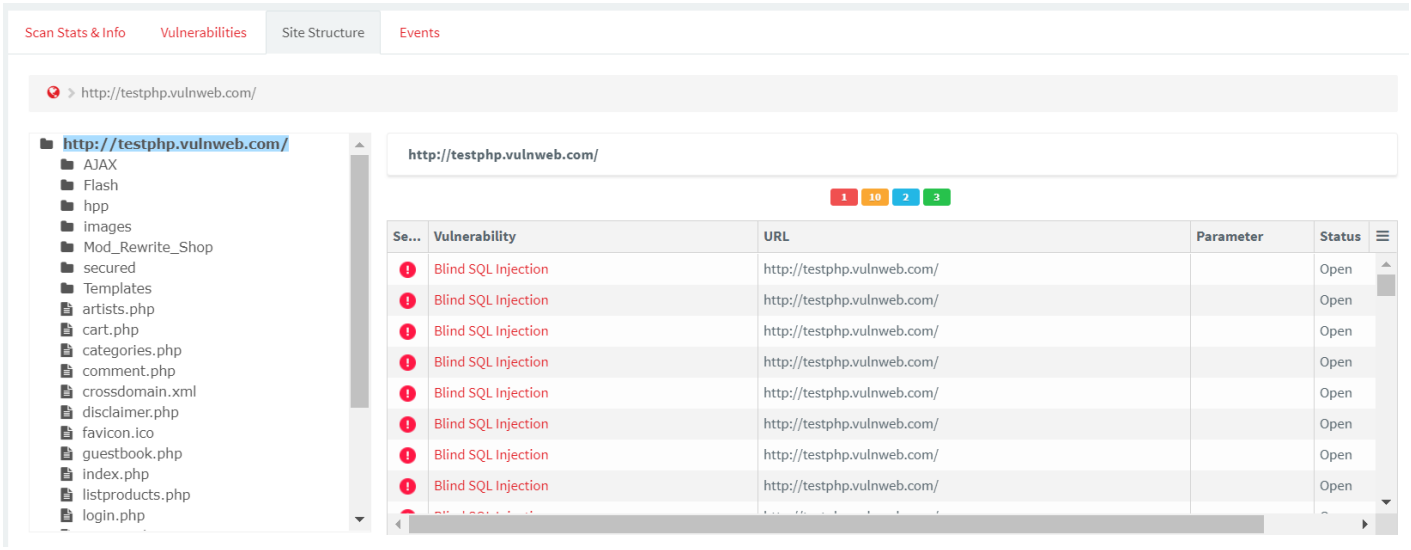
+ Scan Stats & Info - this provides an overview of the Target as detected by the scan, and information about the Scan, such as scan duration, average response time and the number of files scanned.



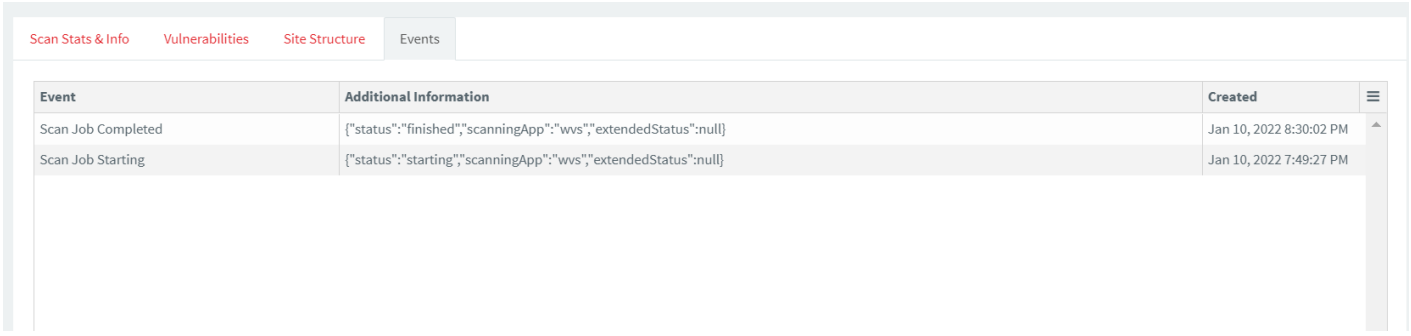
+ Vulnerabilities - This is the list of vulnerabilities detected ordered by severity



+ Site Structure - You can use the site structure to ensure that Acunetix has covered all the site, and to identify vulnerabilities affecting a specific file or folder of the site scanned. Click on the folder icon to expand the site structure tree.



+ Events - A list of events related to scan. This will show when the scan started and finished, and if any errors have been encountered during the scan.



- Alerts (vulnerabilities) discovered

+ One of the key components of the scan results is the list of all vulnerabilities found in the scan target during the scan. Depending on the type of scan, these can be either Web Alerts or Network Alerts, and the alerts are categorized according to 4 severity levels:

● **High Risk Alert Level 3** – Vulnerabilities categorized as the most dangerous, which put the scan target at maximum risk for hacking and data theft.

● **Medium Risk Alert Level 2** – Vulnerabilities caused by server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.

● **Low Risk Alert Level 1** – Vulnerabilities derived from lack of encryption of data traffic or directory path disclosures.

● **Informational Alert** – These are items which have been discovered during a scan and which are deemed to be of interest, e.g. the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database, or information on a service that has been discovered during the scan.

+ Depending on the type of vulnerability, additional information about the vulnerability is shown when you click on an alert category node:

● **Vulnerability description** - A description of the discovered vulnerability.

● **Affected items** - The list of files or components which are affected by the alert.

● **The impact of this vulnerability** – Level of impact on the website, web server or perimeter server if this vulnerability is exploited.

● **Attack details** - Details about the parameters and variables used to test for this vulnerability. E.g. for a Cross Site Scripting alert, the name of the exploited input variable and the string it was set to will be displayed. You can also find the HTTP request sent to the web server and the response sent back by the web server (including the HTML response).

● How to fix this vulnerability - Guidance on how to fix the vulnerability.

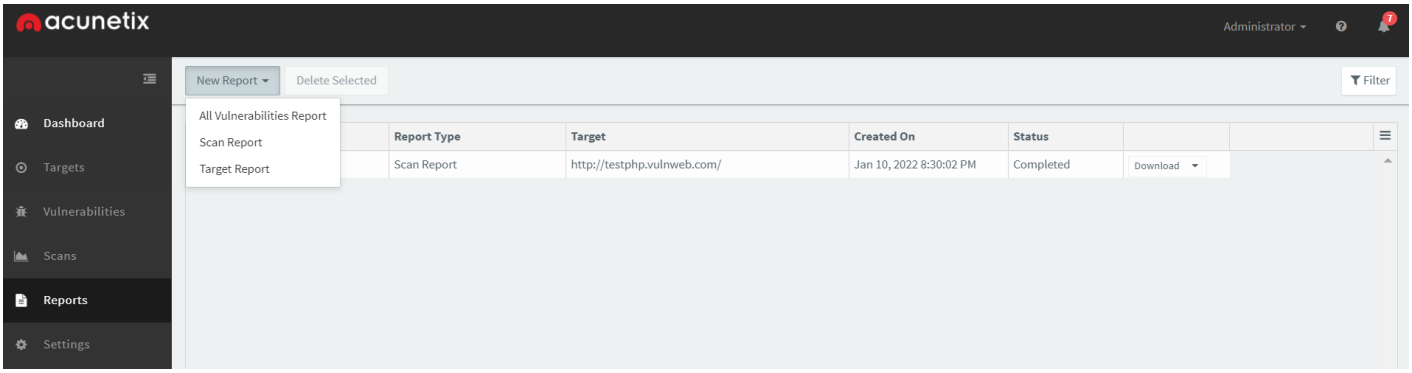
● **Classification** - Apart from the Acunetix classification, this section provides classification by CVSS (v2 and v3) score and CWE enumeration id.

● **Detailed information** - More information on what is causing the reported vulnerability, with examples where applicable.

● **Web references** - A list of web links to external sources providing more information on the vulnerability to help you understand and fix it.

7. Report page:

- **Generating Reports**



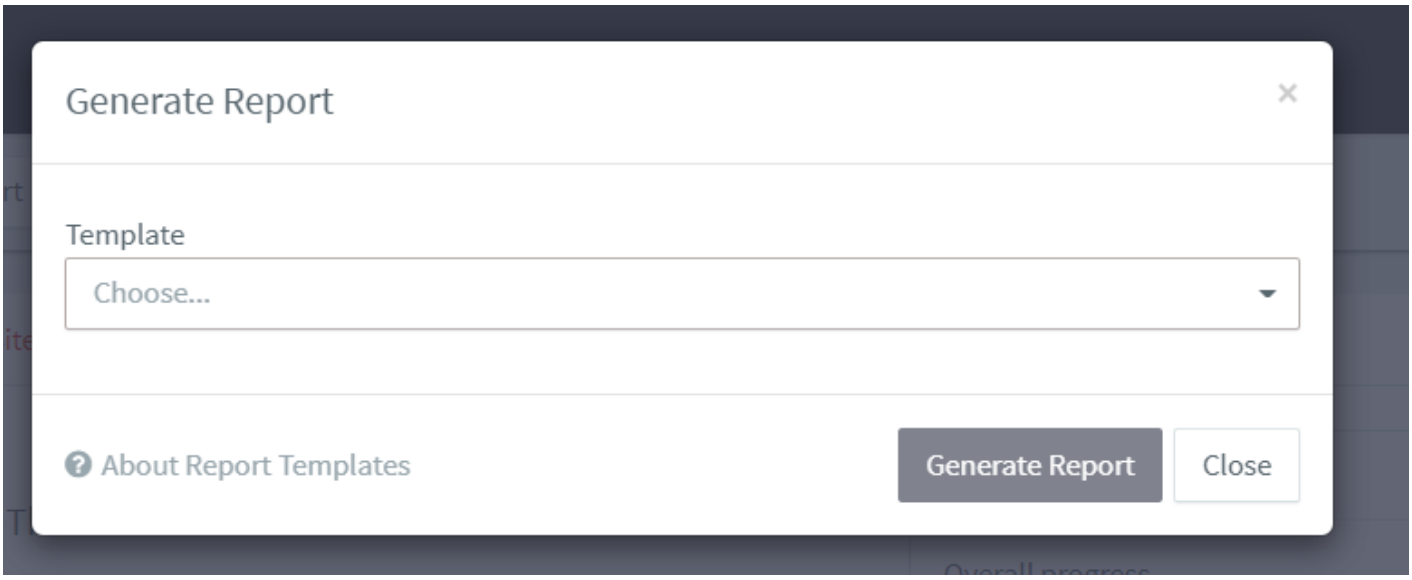
+ From the Reports page, there are 3 types of reports that can be generated:

● **All Vulnerabilities report** - report on all the vulnerabilities detected on all the Targets configured in Acunetix

● **Scan Report** - report on the vulnerabilities detected by one or multiple scans. When 2 scans for the same Target are selected, you will be given the option to compare the scans when generating the report (by selecting the Scan Comparison report template)

● **Target Report** - report on all the vulnerabilities detected on one or multiple Targets taking into consideration all the scans done on the target(s).

+ Reports can also be generated directly from the Targets page, the Vulnerabilities page or the Scans page.



+ After choosing what to report on, you will need to choose a report template. The format of the report, the detail included, and the grouping used in the report are determined by the report template. Report templates are described in the next section.

+ After choosing to generate the report, you will then be taken to the Saved Reports. The report might take a few seconds to generate. The PDF or HTML report can be downloaded by clicking on the Download link, which becomes available when Acunetix has finished generating the report.

- **Acunetix Reports**

+ The following is a list of the reports that can be generated in Acunetix:

● **Affected Items Report:** The Affected Items report shows the files and locations where vulnerabilities have been detected during a scan. The report shows the severity of the vulnerability detected, together with other details about how the vulnerability has been detected.

● **Developer Report**: The Developer Report is targeted to developers who need to work on the website in order to address the vulnerabilities discovered by Acunetix. The report provides information on the files which have a long response time, a list of external links,

email addresses, client scripts and external hosts, together with remediation examples and best practice recommendations for fixing the vulnerabilities.

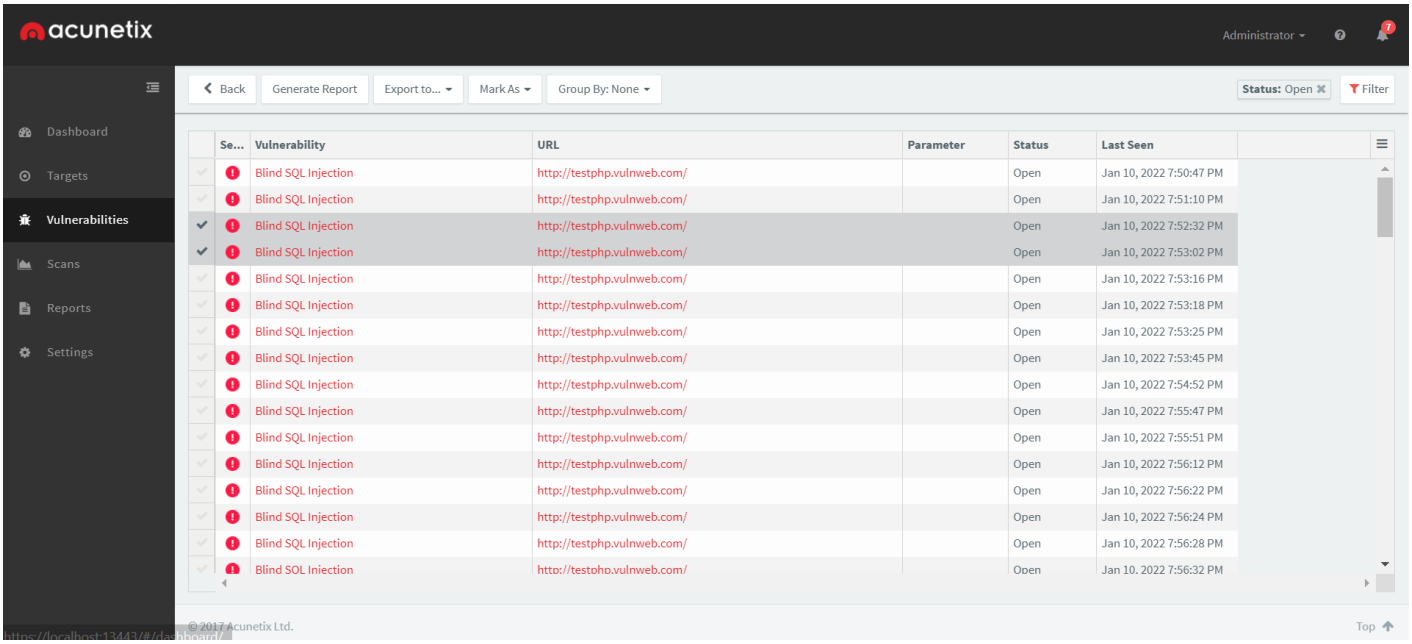
● **Executive Report:** The Executive Report summarizes the vulnerabilities detected in a website and gives a clear overview of the severity level of vulnerabilities found in the website.

● **Quick Report:** The Quick Report provides a detailed listing of all the vulnerabilities discovered during the scan

● **Scan Comparison:** The Scan Comparison report allows you to compare two scans on the same Target, highlighting the differences between the scans. This report template will only become available when 2 scans for the same Target are selected.

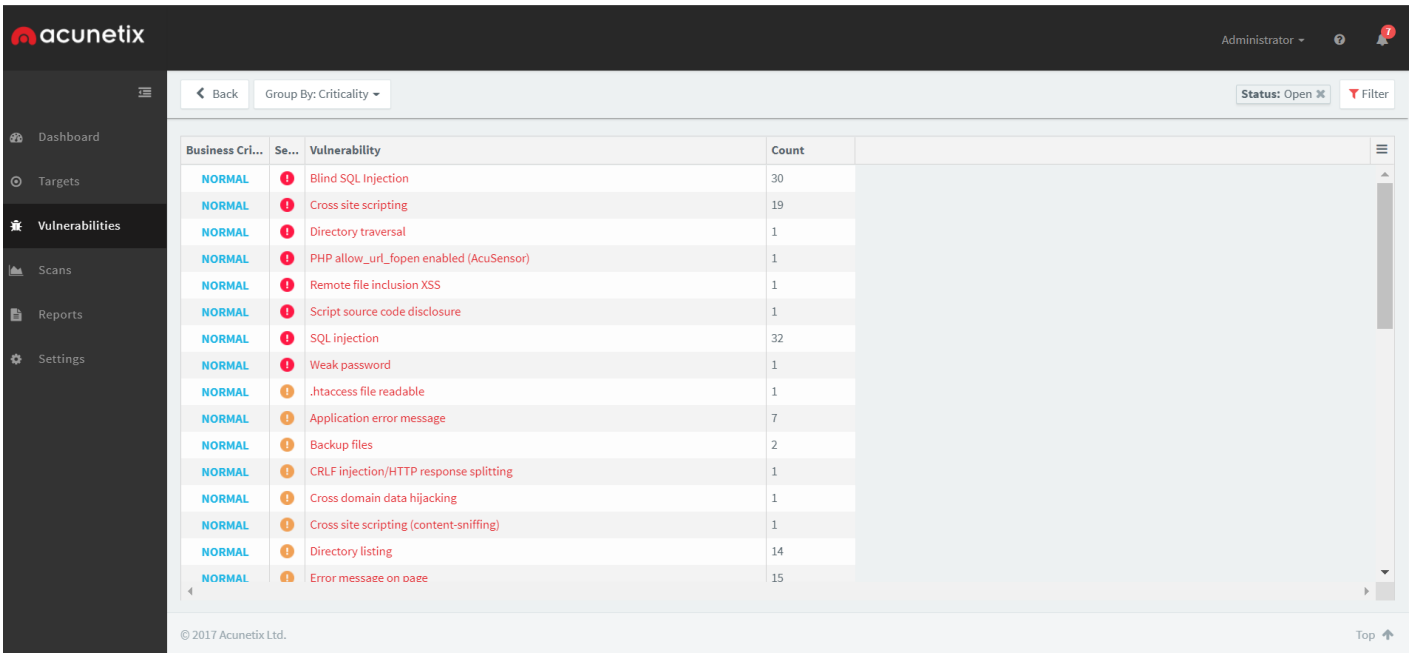
8. Managing Vulnerabilities

- The detection of vulnerabilities is the first step to securing your web applications. The vulnerabilities detected need to be managed and eventually fixed. Acunetix provides the means to help you prioritise and manage vulnerabilities.



- The Vulnerabilities page provides a list of all the vulnerabilities detected by Acunetix. By default, the vulnerabilities are sorted by Business Criticality of the target the vulnerability was detected on, and the severity assigned to the vulnerability by Acunetix. This will help you focus on the most important vulnerabilities, without losing sight of the less important ones.

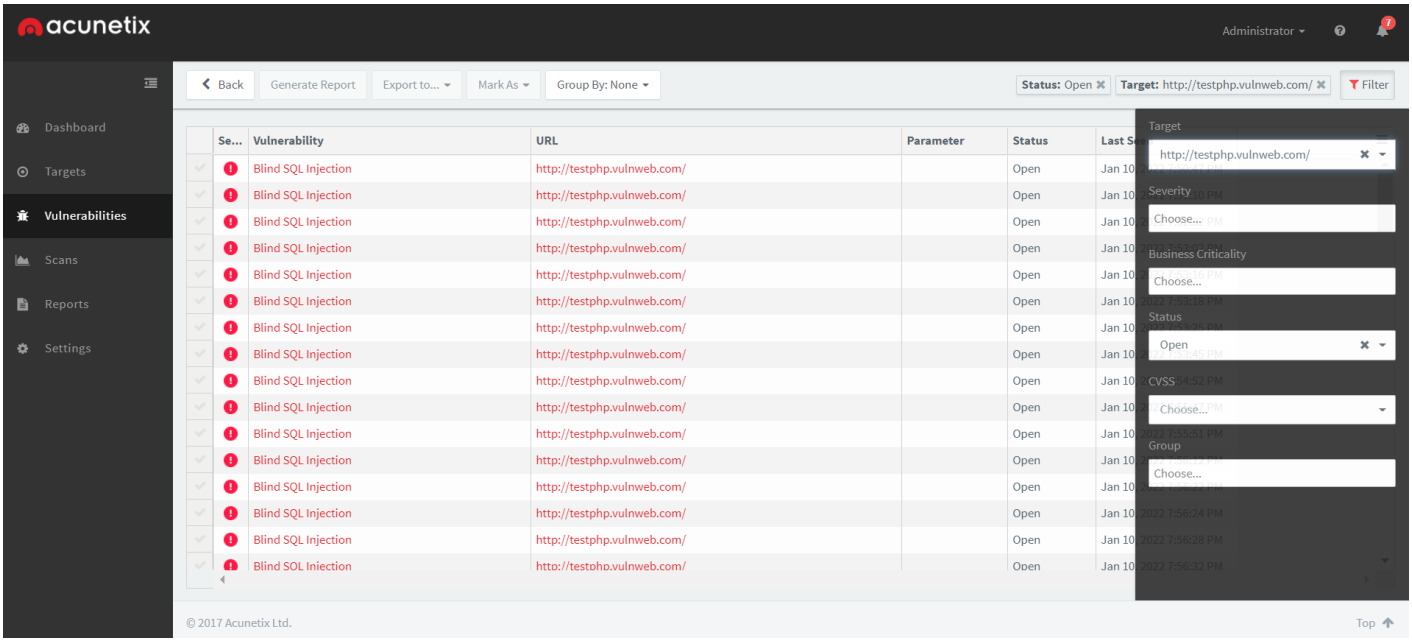
- **Grouping and Filtering Vulnerabilities**



+ As the amount of vulnerabilities detected increases, the list of vulnerabilities can become cumbersome to manage. For this reason, the vulnerabilities can be grouped or filtered

+ Vulnerabilities can be grouped either by Business Criticality or by Vulnerability Type. Grouping by Business Criticality gives priority the vulnerabilities occurring on web applications which are of higher importance to the organisation. Grouping by Vulnerability Type prioritises the vulnerabilities using the severity assigned by Acunetix.

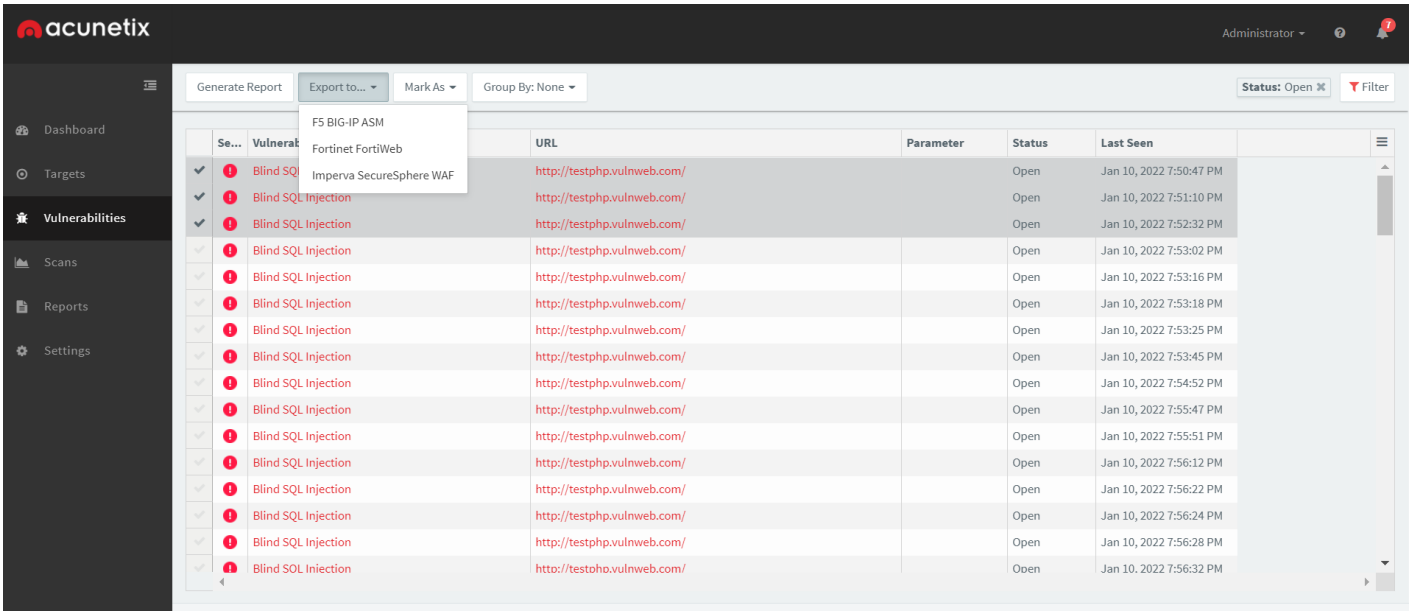
+ Vulnerabilities can be filtered by Target, Severity, Target's Business Criticality, Status, CVSS, and Target Group. The list allows for multiple flexible filters, e.g. show all the high severity Vulnerabilities, identified on a specific Target, which are still open.



- **Import vulnerabilities into your Web Application Firewall (WAF)**

+ Ideally, vulnerabilities are fixed as soon as possible. Unfortunately, it often takes months to fix a vulnerability. If you make use of a Web Application Firewall (WAF) supported by Acunetix, you can export vulnerabilities from Acunetix and import them into your WAF. Your WAF will be able to provide virtual patching for the vulnerability.

+ Acunetix supports exporting vulnerabilities for F5 BIG-IP ASM, Fortinet FortiWeb and Imperva SecureSphere WAF.



- **Sending Vulnerabilities to an Issue Tracker**

+ For a developer, vulnerabilities are considered as bugs in the web application. Acunetix provides to means to send the vulnerabilities to the issue tracker used by the organisation, allowing for better tracking of vulnerabilities by the development team.

+ You will first need to configure the issue tracker in the Acunetix settings, and assign the Issue Tracker to the Target. You will then be able to send vulnerabilities detected for the specific Target to the Issue Tracker

+ Acunetix supports GitHub, Jira and Microsoft TFS issue trackers

- **Retesting Vulnerabilities**

+ When a vulnerability has been fixed, you can have Acunetix confirm the fix by selecting the vulnerability and clicking on the Retest option. This will create a new scan using a custom scanning profile restricted to the specific vulnerability.

- **Closing Vulnerabilities**

+ Vulnerabilities detected by Acunetix remain in the vulnerabilities list until they are marked as not open. You can remove vulnerabilities from the list of open vulnerabilities by marking them as:

+ **Fixed** - This status is given to vulnerabilities that are fixed by the developers. If the vulnerability is found again by Acunetix, the vulnerability will be re-opened, and marked as Rediscovered

+ **False Positive** - There are situations where a vulnerability is incorrectly detected by Acunetix. The vulnerability will not be reported again in future scans.

+ **Ignored** - This status can be used for vulnerabilities which are not False Positives, but which for some reason should be ignored in future scans.

+ Vulnerabilities marked as False Positives or Ignored can be re-opened manually at any time

VI. DEMO

A. Setup dvwa, apache2, mysql, php:

1) Setup Web server (Install Apache)

To install Apache, Open your Terminal and type the following:

sudo apt install apache2

Once done, type **127.0.0.1** in the browser and you will see the default Apache 2 web page, similar to this:

2) Download DVWA

We need to download the archive of DVWA from Github.

To install Git, type following command:

sudo apt-get install git

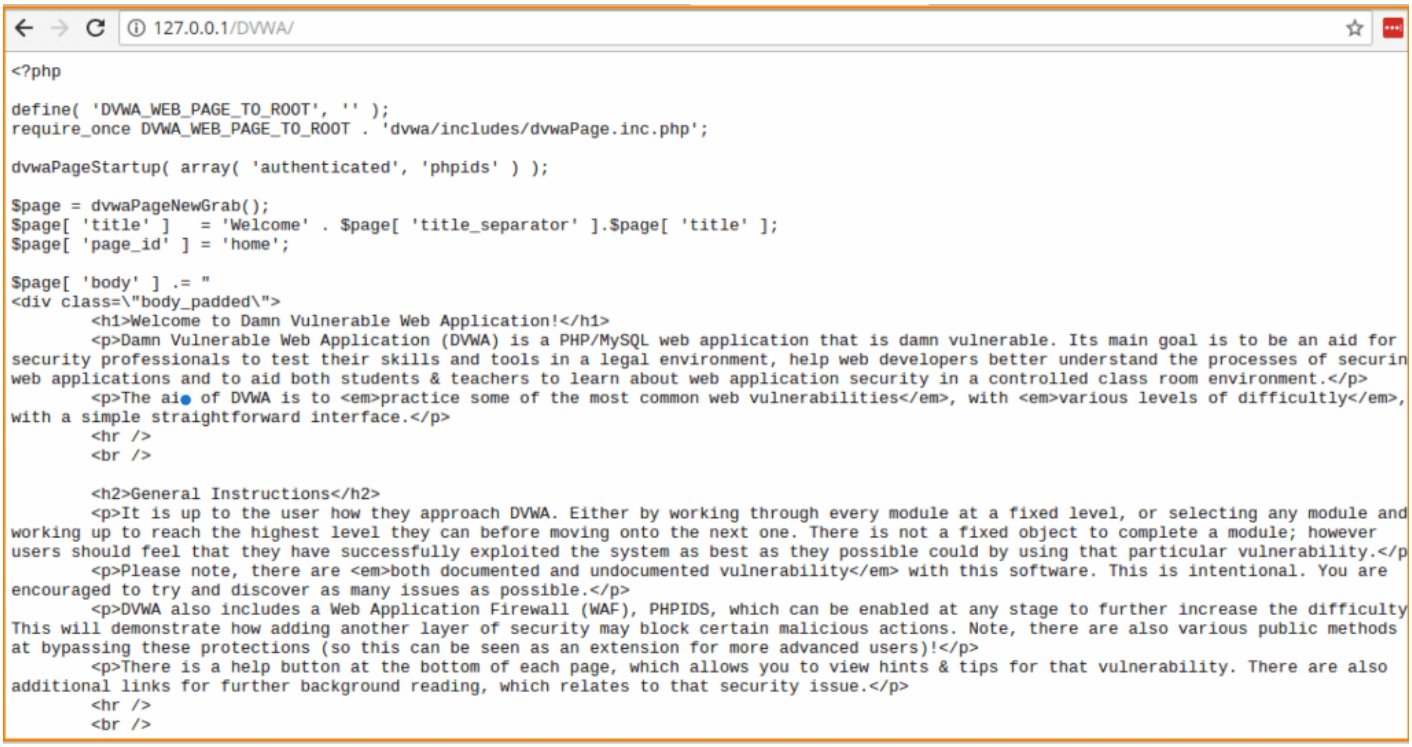
Go to the **apache2** folder.

cd /var/www/html/

Clone **DVWA** from **Github**, type the following command:

sudo git clone https://github.com/ethicalhack3r/DVWA.git

Once done, type **127.0.0.1/DVWA/** in the browser and you will see the DVWA page, similar to this:



Change permissions for DVWA

sudo chmod -R 777 /var/www/html/DVWA/

3) Install MySQL

The next component for Setting up DVWA is Installing **MySQL**.

- To install **MySQL,** type the following:

sudo apt install mysql-server

Note that the installation routine may ask you to create a new password for the **root** MySQL user. Once you have completed all of the required steps, your MySQL installation should be completed. Let's double-check that our new MySQL server is running. Type this command:

mysql -u root -p

Enter the root password you created for MySQL when you installed the software package. Once in, the following to get the server status, version information and more:

status

This is a good way to ensure that you've installed MySQL and are ready for further configuration.

- Restart **Apache** Server

sudo service apache2 restart

- **Create Database and User**

To create a MySQL **database** and user, follow these steps:

At the command line, type the following:

mysql -u root -p

- Type the MySQL root password, and then press Enter.
- To create a database, type the following command:

CREATE DATABASE **dvwadb**;

- To create a database user, type the following command. Replace ***dvwausr*** with the user you want to create, and replace **dvwa@123** with the user's password:

CREATE USER 'dvwausr'@'127.0.0.1' IDENTIFIED BY 'dvwar@123';

- Grant permission, type the following command:

GRANT ALL PRIVILEGES ON dvwadb.* TO '**dvwausr'@'localhost**' IDENTIFIED BY '**dvwa@123**';

- Once done, exit the application by typing either of the following commands:

\q

(or)

Exit

4) Install PHP5

For our last component in **DVWA** Installation, we will set up and install PHP. Installing this on your VM is quite easy.

- To install PHP, simply type the following command:

sudo apt install php5

or

sudo apt install php5.6

Agree to the installation and **PHP 5** will be installed on your Server.

- Restart **Apache** Server

sudo service apache2 restart

Now, let's take a moment to test the PHP software that you just installed. Move into your public web directory:

cd /var/www/html

Once there, use the text editor to create a file named info.php by typing the following command:

sudo vim info.php

This command will use the command line editor vim to open a new blank file with this name. Inside this file, type the following:

Inside this file, copy paste the following:

<?php phpinfo(); ?>

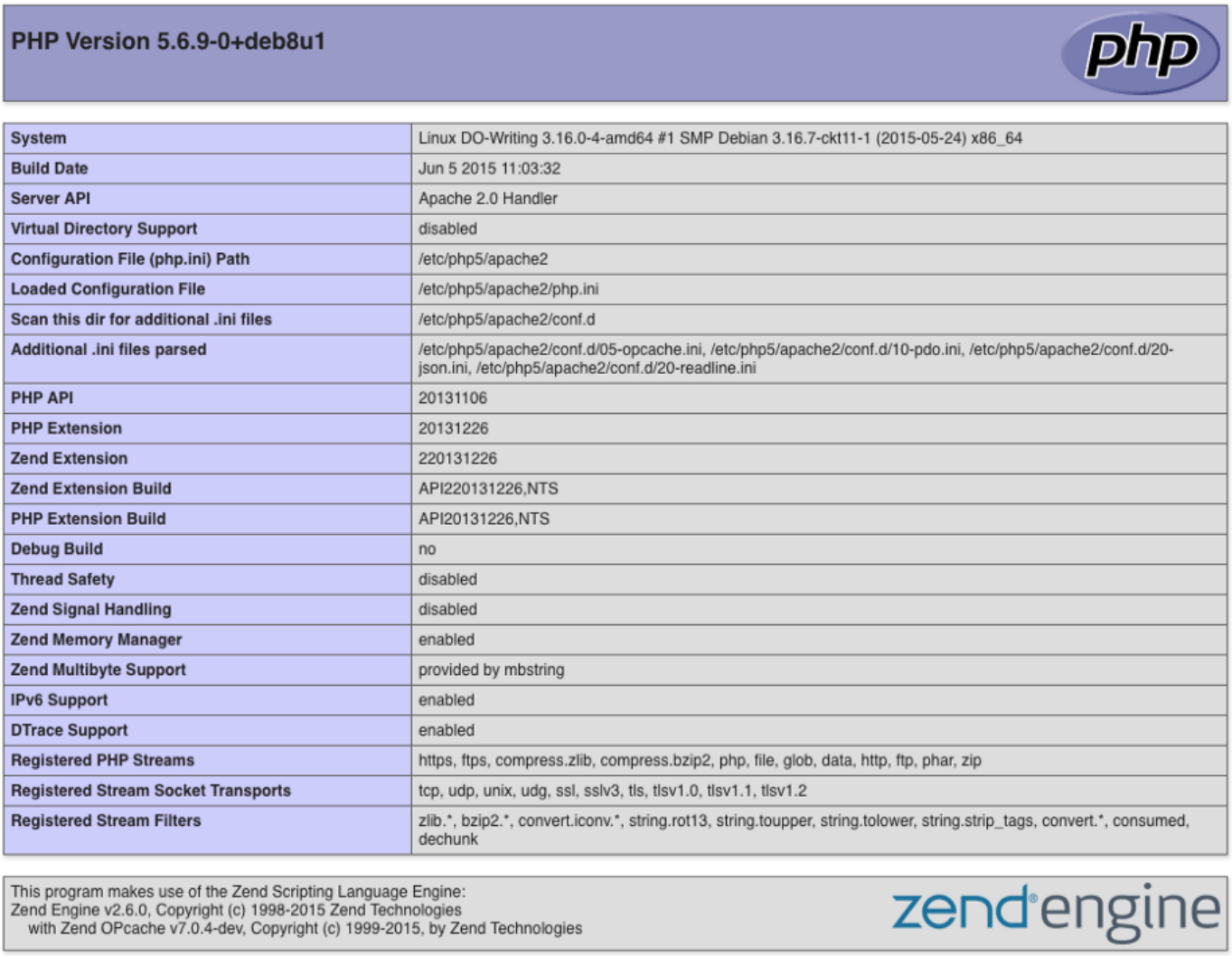
Save your changes by entering:

:wq!

Once done, open your web browser and type your localhost **IP address** in the browser.

http://127.0.0.1/info.php

You will see the default PHP information page, similar to this:



PHP Version 5.6.9-0+deb8u1

System	Linux DO-Writing 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt11-1 (2015-05-24) x86_64
Build Date	Jun 5 2015 11:03:32
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2015 Zend Technologies
with Zend OPcache v7.0.4-dev, Copyright (c) 1999-2015, by Zend Technologies

When you are done looking at this test **PHP** page, you can remove this file if you want by typing the following command:

sudo rm /var/www/html/info.php

- Install **MySQL** Extension for **PHP.**

To Install **MySQL** Extension for PHP Support, type the following:

sudo apt install php5-mysql

Once done, you have completed the PHP installation required for DVWA.

- Install **PHP-GD**

DVWA requires a module for php which is not installed into Kali Linux or elementaryOS. So we need to add a Debian source for APT.

sudo add-apt-repository 'http://ftp.de.debian.org/debian sid main'

sudo apt update

sudo apt install php5-gd

Once done, you have completed the PHP installation for DVWA.

5) Configure DVWA

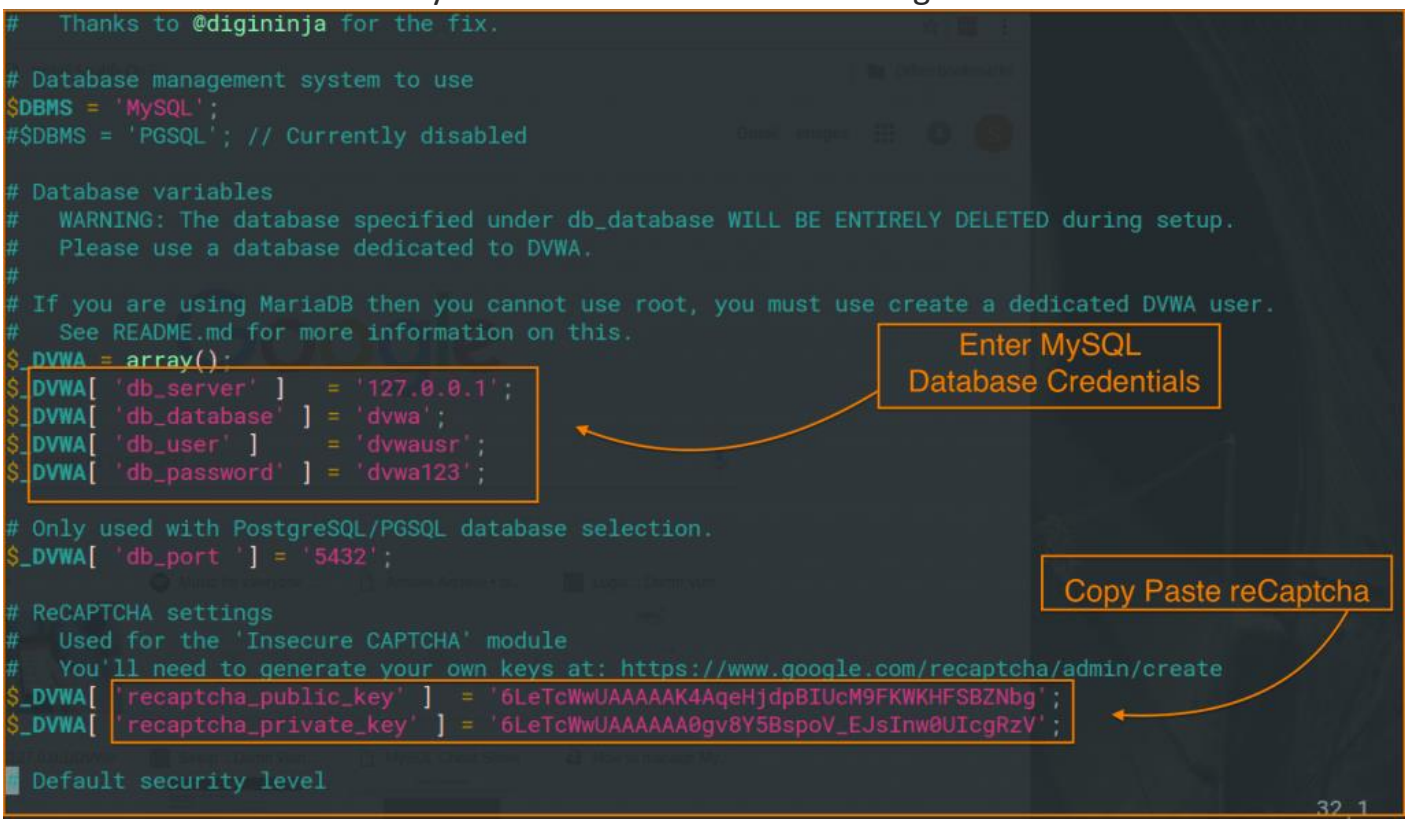
Now we are ready to edit the source of php config files to make sure your web application connects to the database and has got a working captcha. You can obtain reCaptcha keys from your Google Account by clicking here.

We will use the text editor to edit the configuration typing the following command:

sudo vim /var/www/html/dvwa/config/config.inc.php.dist

- Add the database **name**, **user**, and **password** of the mysql database.
- Enter **reCaptcha** keys.

Here's a screenshot on how your file needs to be after editing.



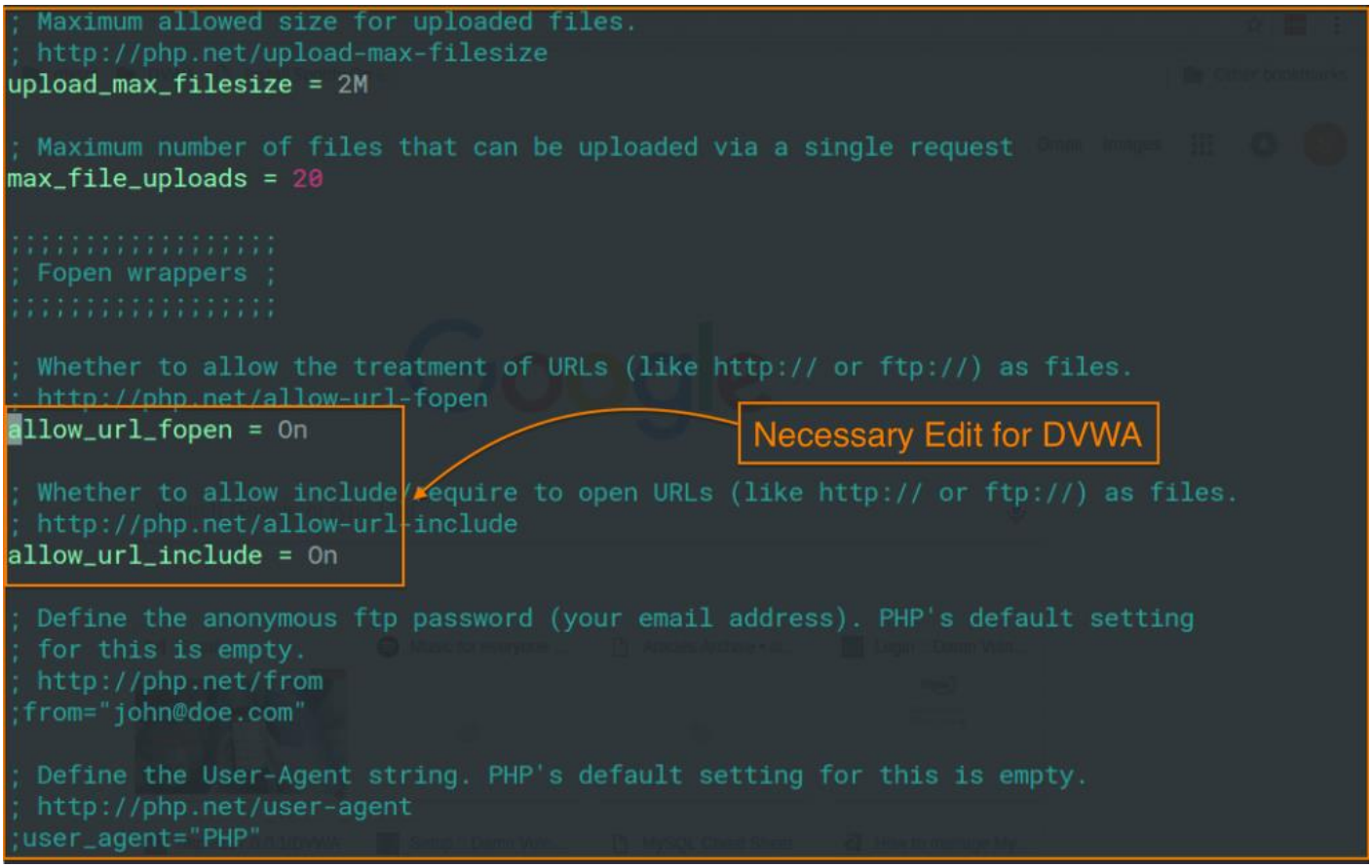
Enter Database credentials and reCaptcha

Once done, we need to edit the main config (***php.ini***) file for apache2, which is not correctly overridden for **DVWA** by default.

sudo vim /etc/php5/apache2/php.ini

- Enable Allow_url_fopen
- Enable Allow_url_include

This is necessary to exploit the file upload vulnerability. Here's a screenshot for ***php.ini*** after making changes.



Jump to line 821 in php.ini

After saving changes for ***php.ini***, we need to follow a few more steps.

- Install **Iceweasel**

sudo apt install iceweasel

- Restart **Apache**

sudo /etc/init.d/apache2 restart

- Restart **MySQL** Service

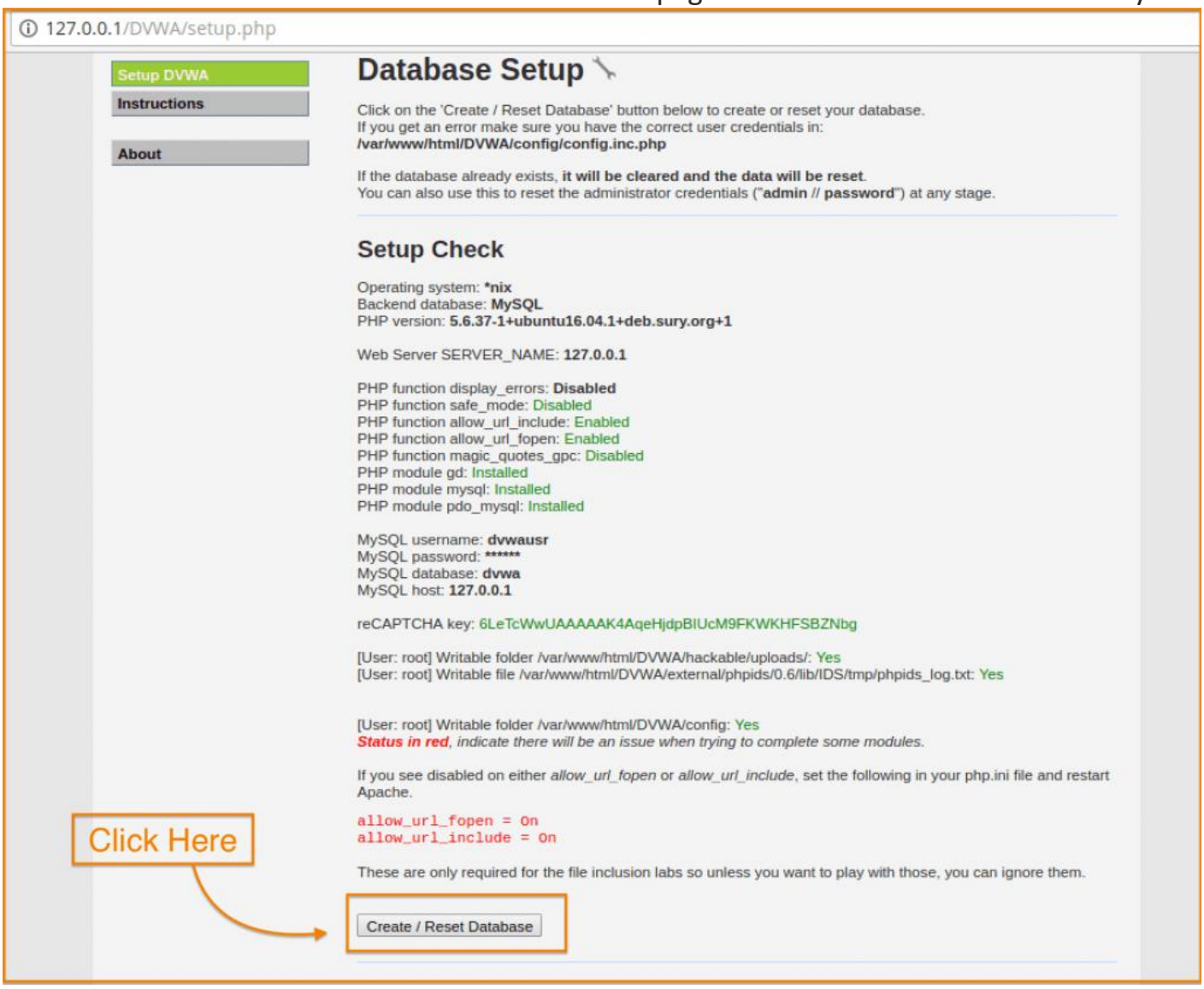
sudo /etc/init.d/mysql restart

Once done, you have completed the required configuration for DVWA.

- Test **DVWA** Installation

iceweasel http://127.0.0.1/DVWA/setup.php

You will be redirected to the web browser and the page similar to this will be in front of you.



DVWA Setup Check

When you are done looking at this DVWA Setup page, you can click on Create / Reset Database button. You will be redirected to the login page.

- Use MySQL User and Password to Login

Insert the default credentials (***admin/password***) and log into the panel.

Now, login to change the strength of vulnerabilities by clicking on “DVWA Security”.

Low Level: Low-Level Security gives you the freedom to exploit all known vulnerabilities means there will be no security in a given framework and hence you can try all attacks if you are using it first Time.

Medium Level: Medium security will have all entry-level validations and filtration which can stop any script kiddie to get the benefit of available vulnerabilities.

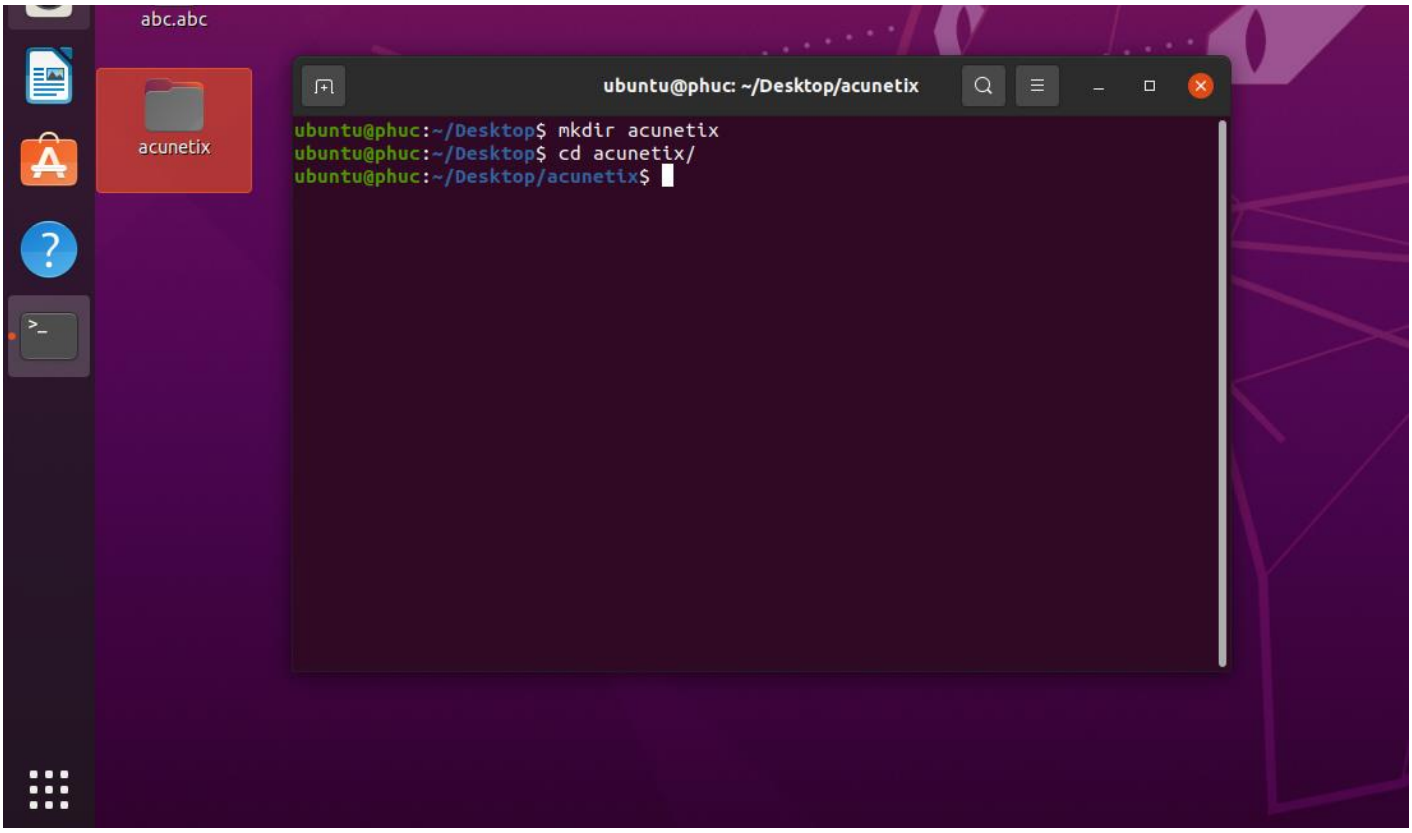
High Level: High Level is kind of Zero Day environment and if you can breach it then that means you are on the right track to becoming a VAPT Expert.

B. Install acunetix:

Create a directory to download acunetix files:

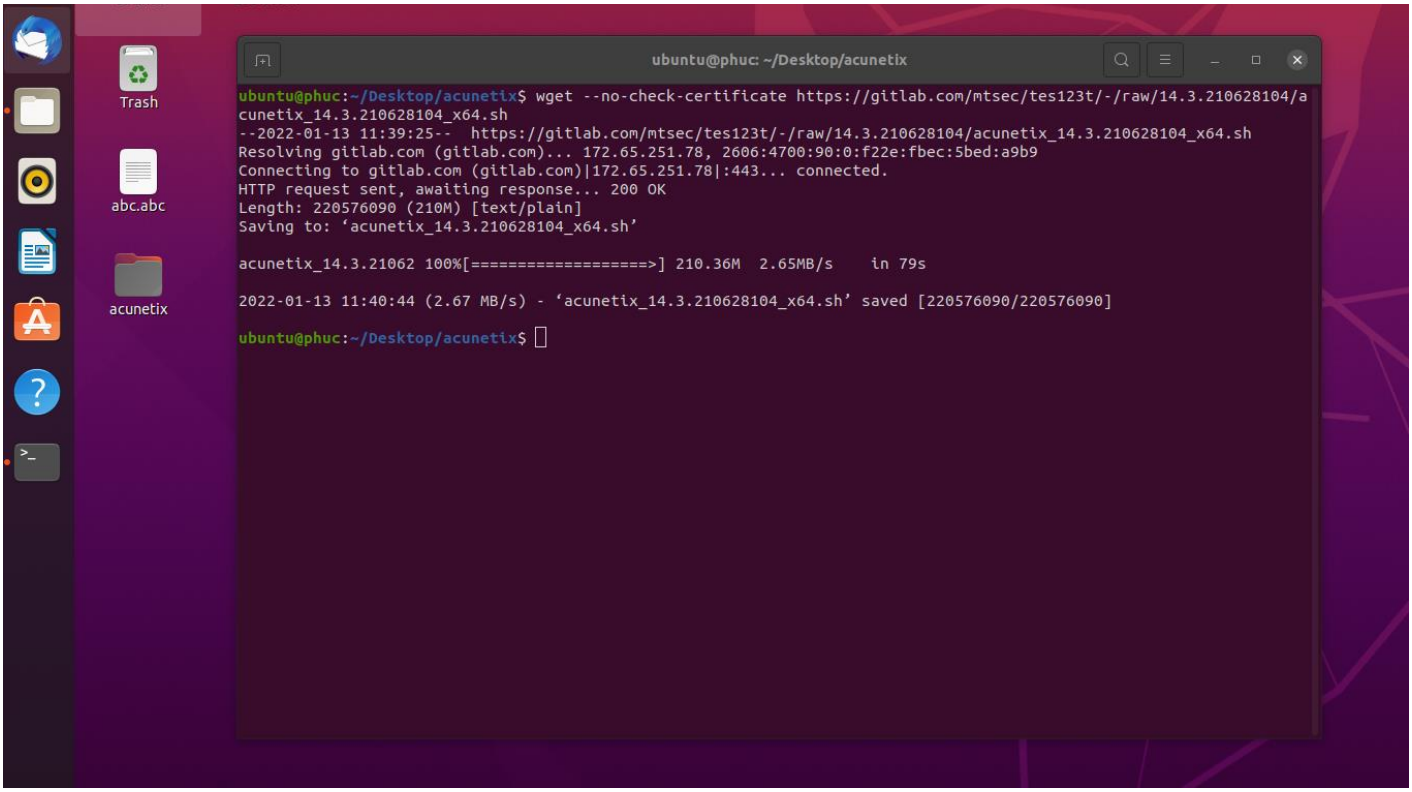
$ mkdir acunetix

$ cd acunetix/



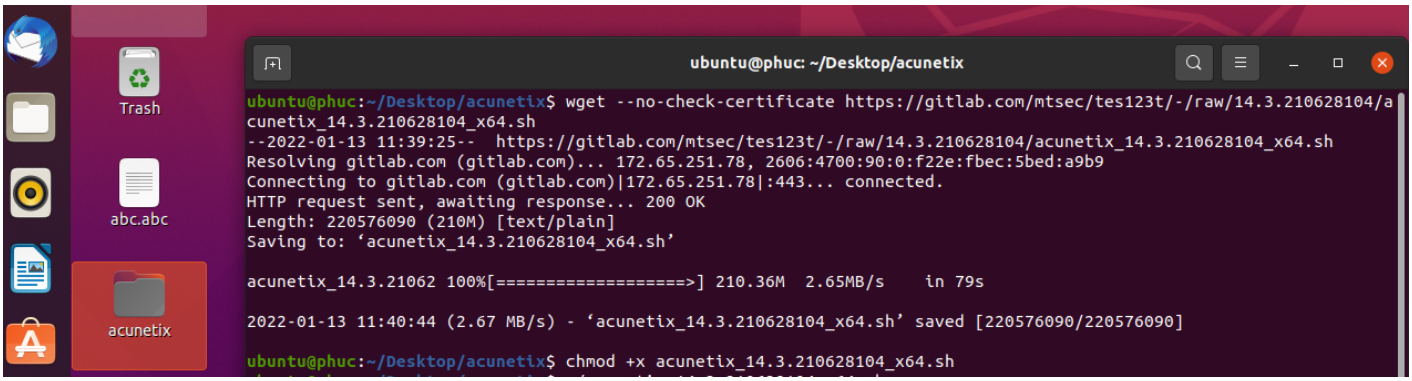
go to the directory that was created, and download.

$ wget --no-check-certificate https://gitlab.com/mtsec/tes123t/-/raw/14.3.210628104/acunetix_14.3.210628104_x64.sh



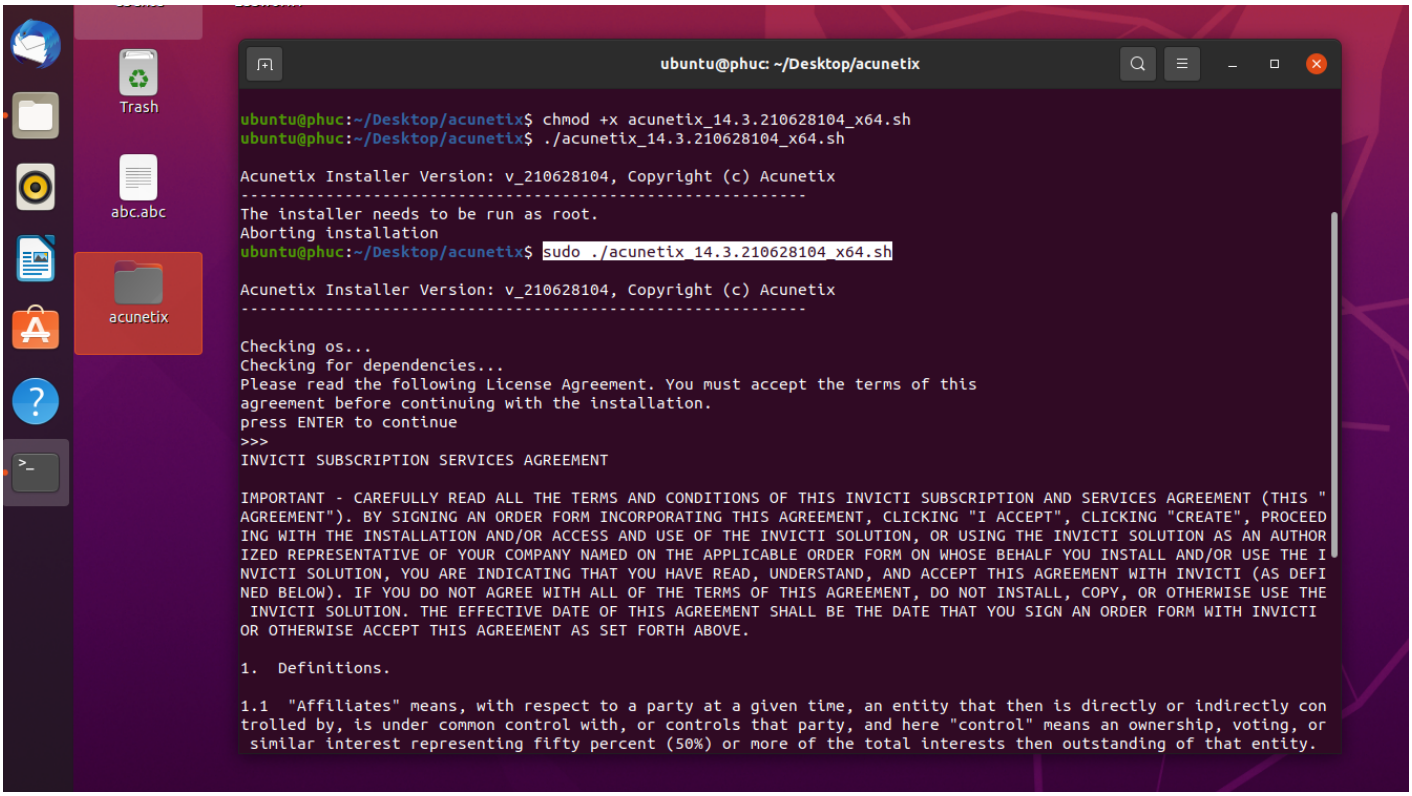
After download, create access permissions using chmod

$ chmod +x acunetix_14.3.210628104_x64.sh

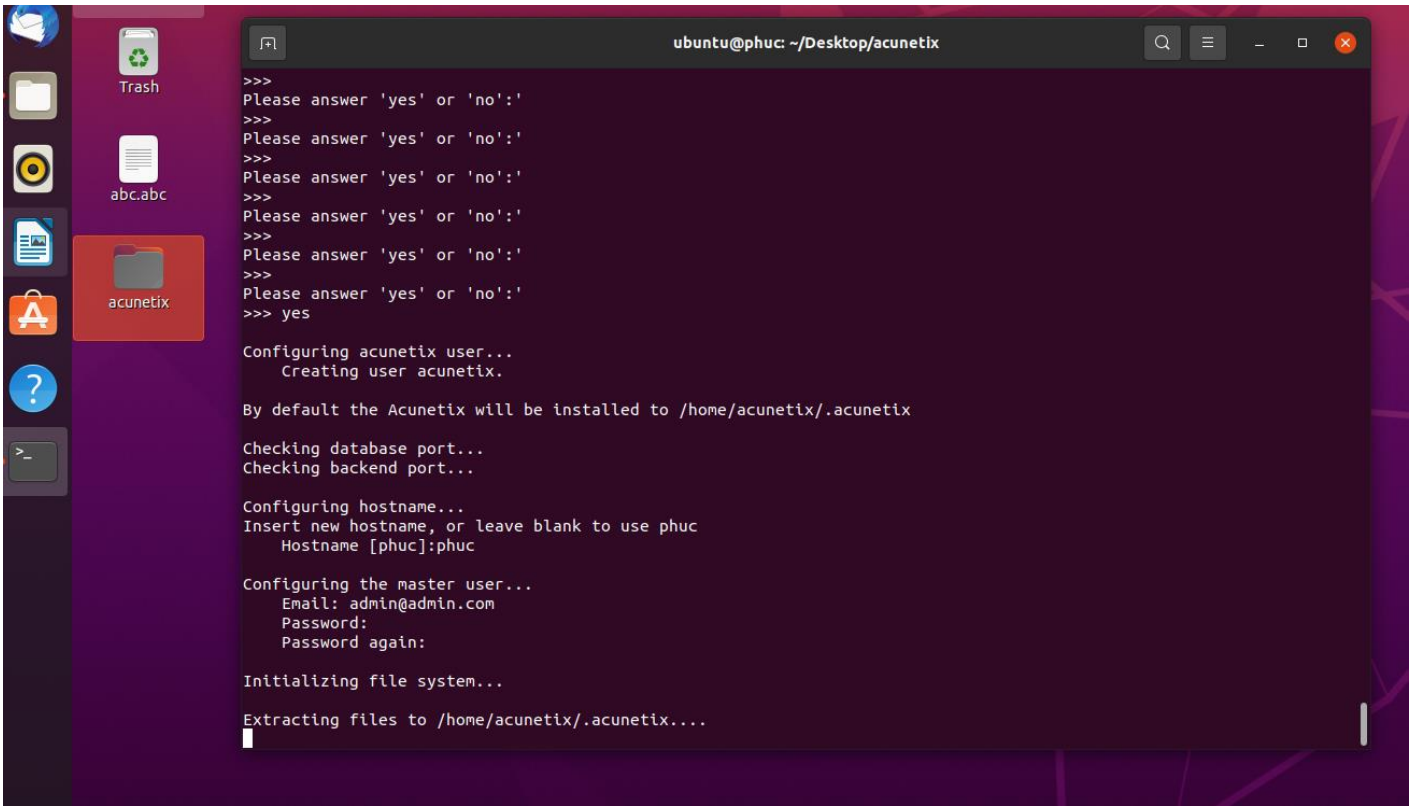


run the installation

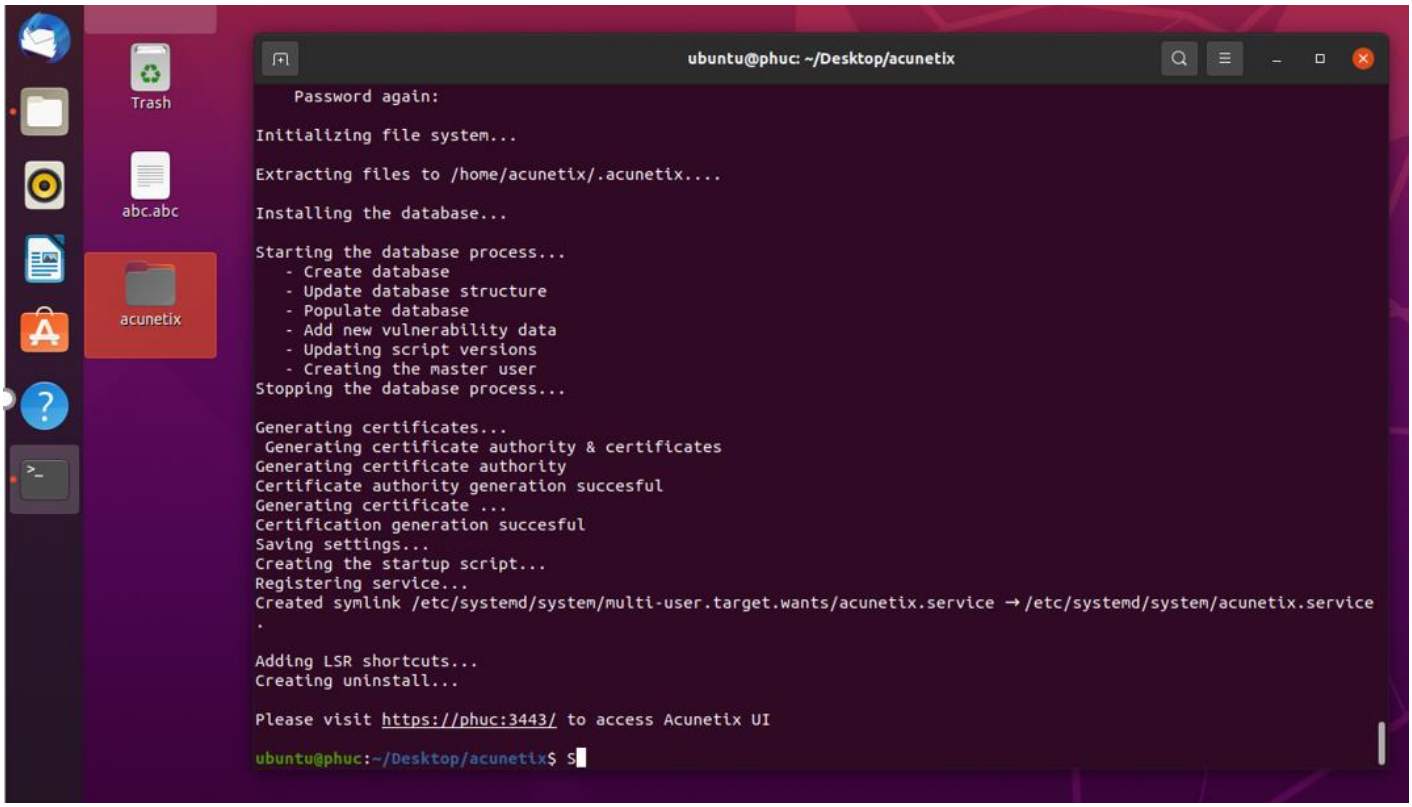
sudo ./acunetix_14.3.210628104_x64.sh



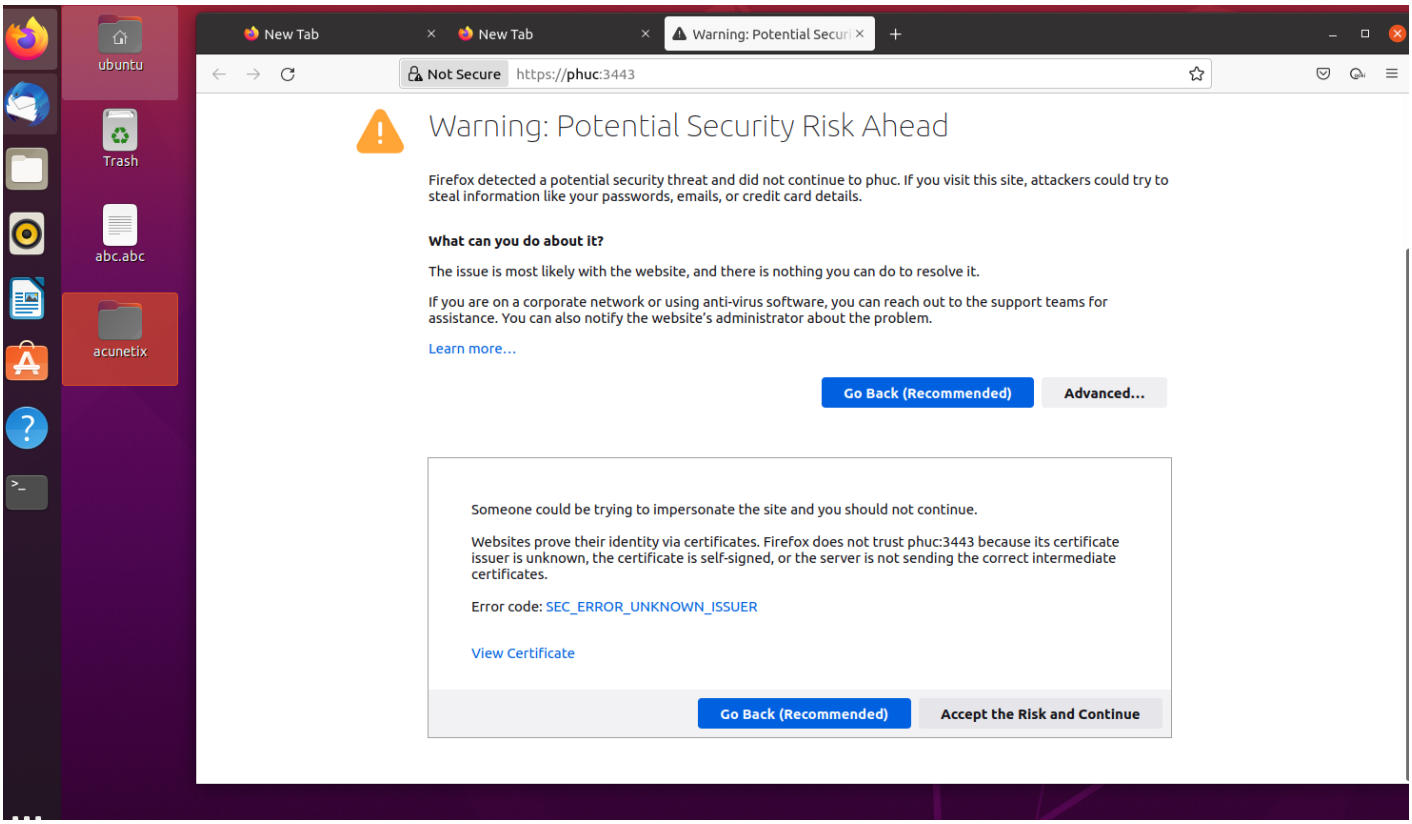
Next: enter hostname, email and password



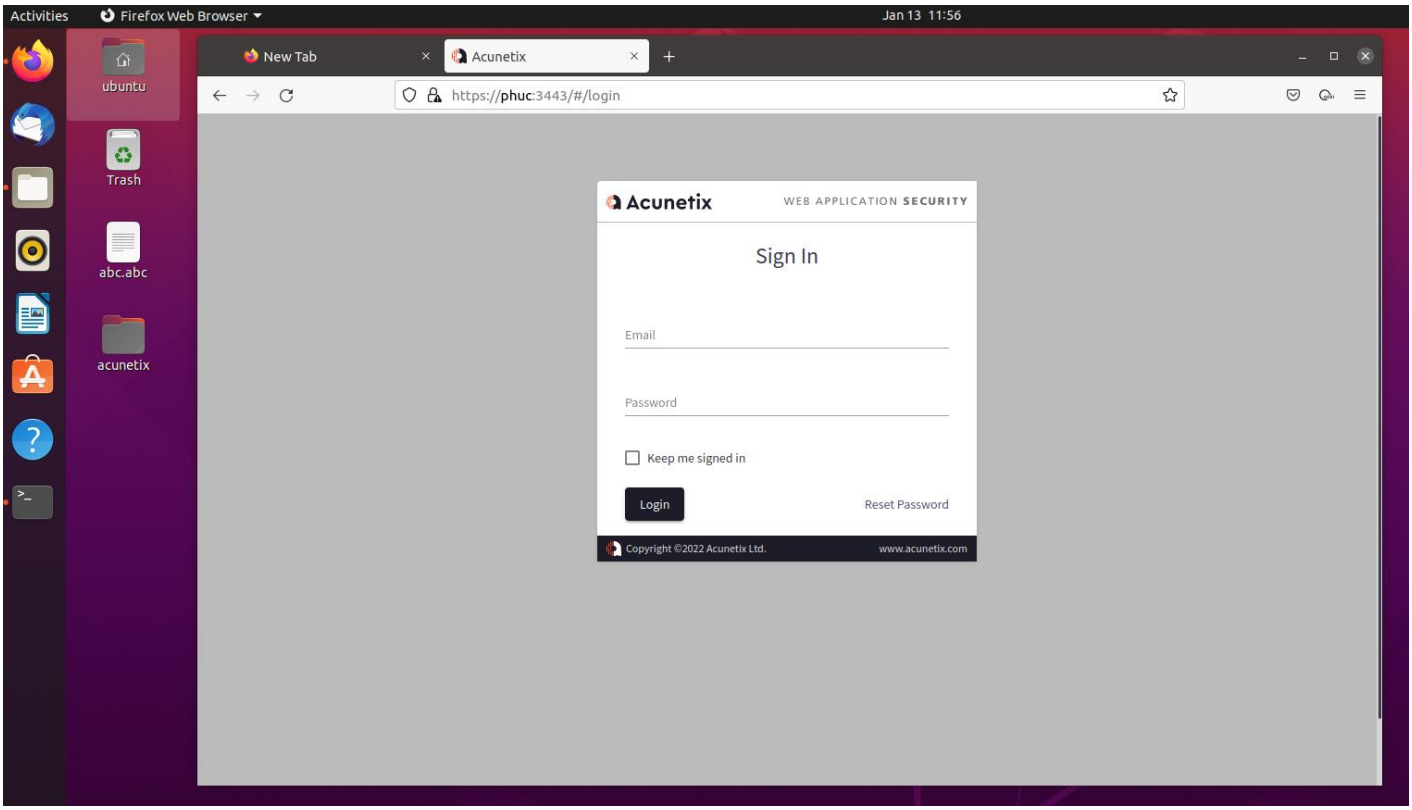
Click to the link to open Acunetix in the browser and use port 3443 and don't forget to also use https



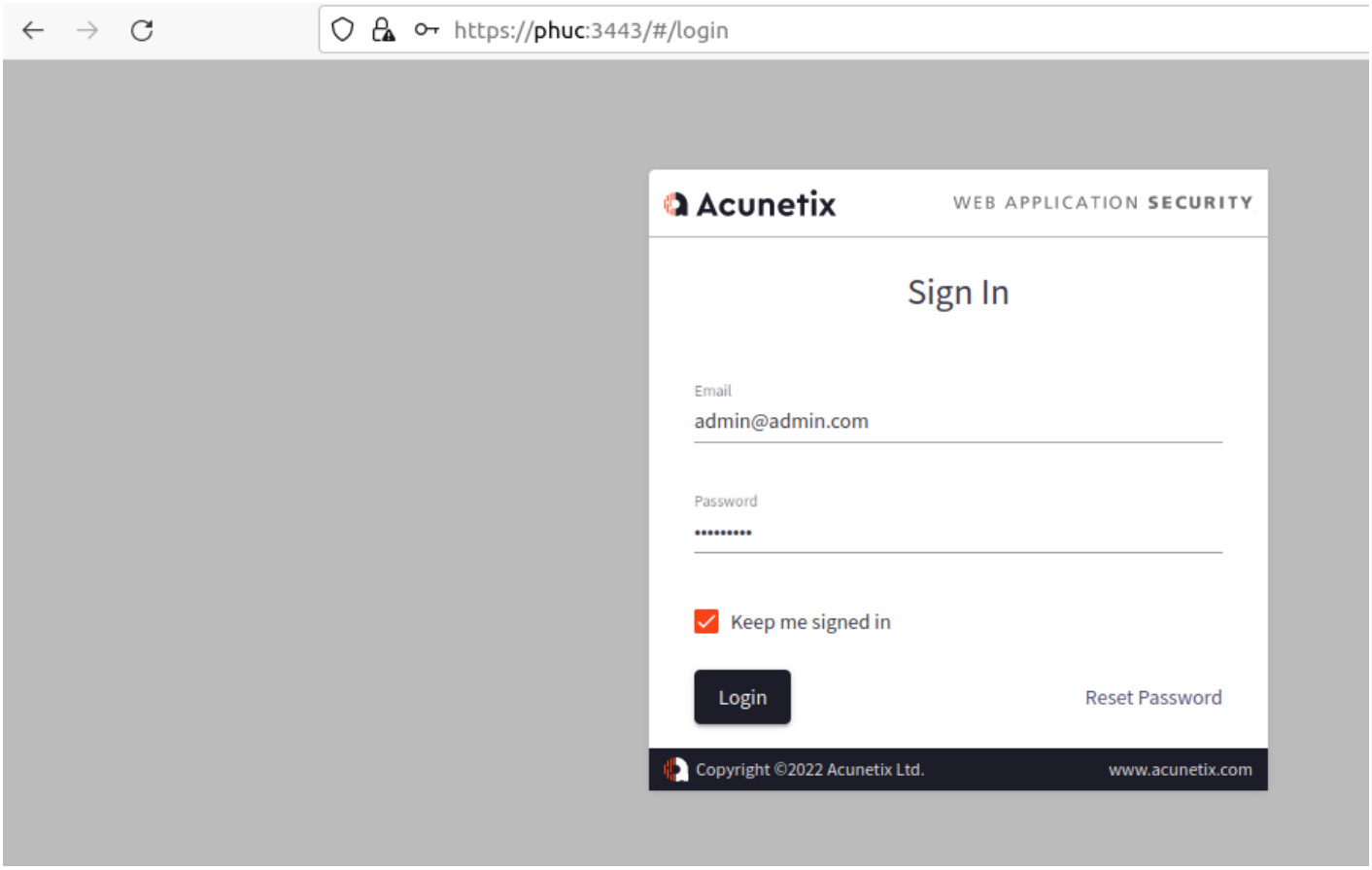
After that, click to “accept the Risk and continue”



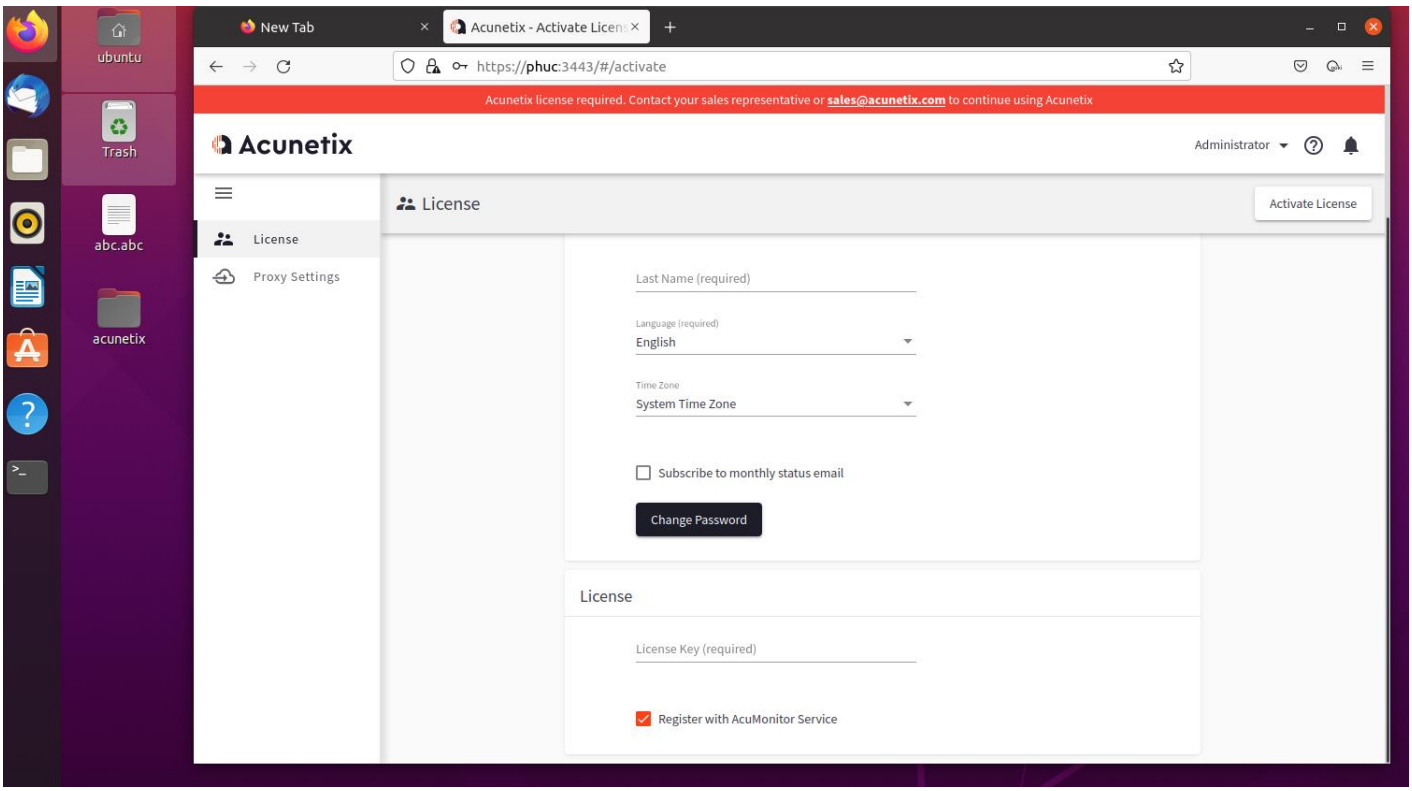
It will move to website login



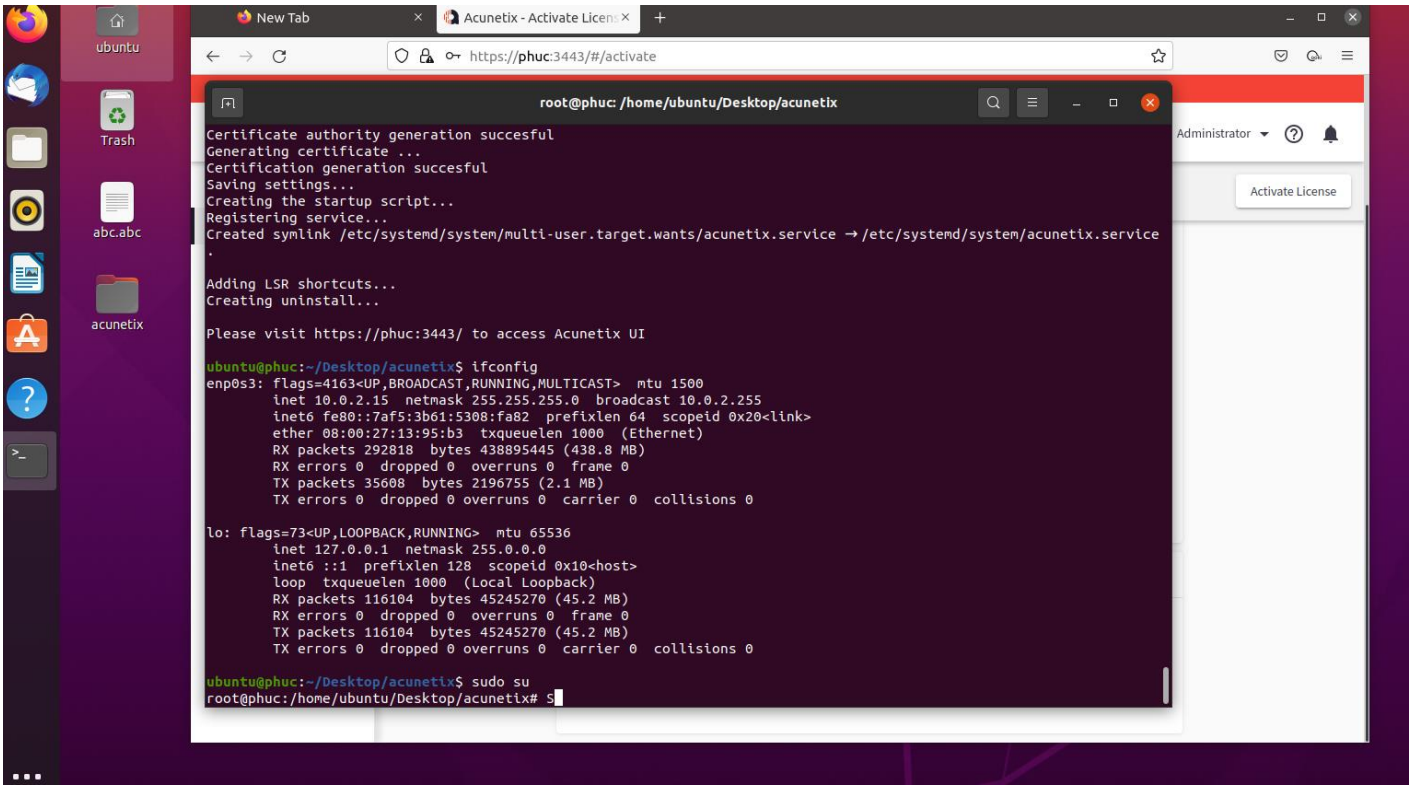
Enter email and password create before to login account



Because the acunetix don’t active license so now we will active it.

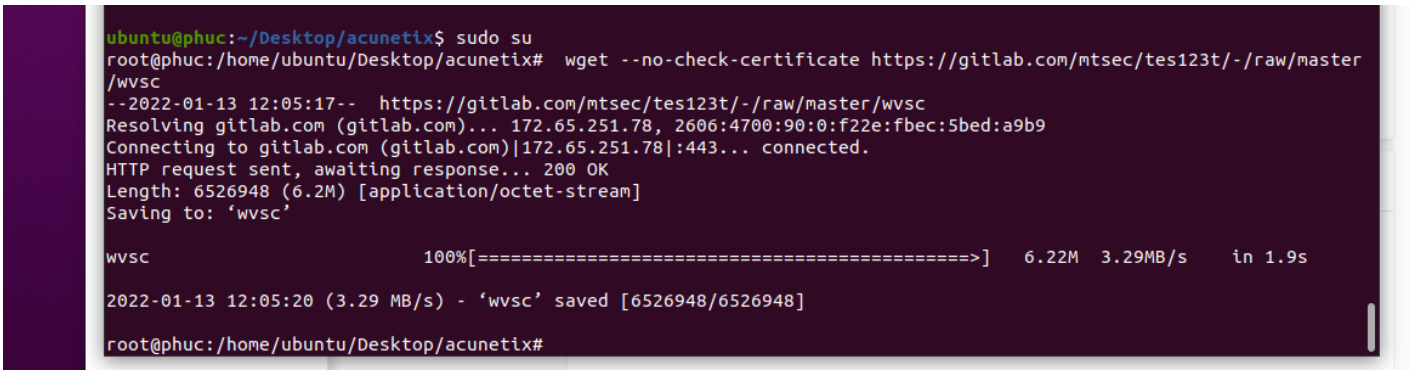


Now root ubuntu



Enter and run 4 code to active license key

$ wget --no-check-certificate https://gitlab.com/mtsec/tes123t/-/raw/master/wvsc



$ cp wvsc /home/acunetix/.acunetix/v_210628104/scanner/

$ wget --no-check-certificate https://gitlab.com/mtsec/tes123t/-/raw/master/license_info.json

$ cp license_info.json /home/acunetix/.acunetix/data/license/

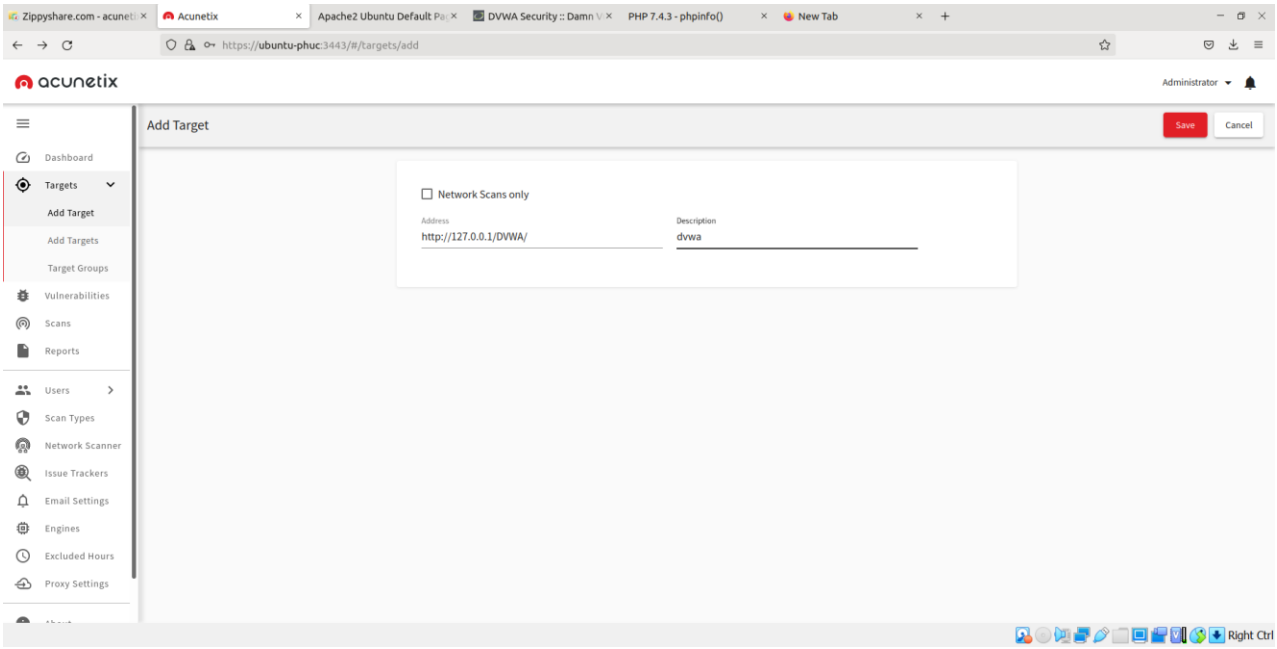
```
root@phuc:/home/ubuntu/Desktop/acunetix# cp wvsc /home/acunetix/.acunetix/v_210628104/scanner/
root@phuc:/home/ubuntu/Desktop/acunetix# wget --no-check-certificate https://gitlab.com/mtsec/tes123t/-/raw/master/
license_info.json
--2022-01-13 12:09:14--  https://gitlab.com/mtsec/tes123t/-/raw/master/license_info.json
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 799 [text/plain]
Saving to: 'license_info.json'

license_info.json           100%[=======================================>]     799  --.-KB/s    in 0s

2022-01-13 12:09:14 (3.80 MB/s) - 'license_info.json' saved [799/799]

root@phuc:/home/ubuntu/Desktop/acunetix# cp license_info.json /home/acunetix/.acunetix/data/license/
root@phuc:/home/ubuntu/Desktop/acunetix#
```

It's cracked, open again Acunetix in the browser and use port 3443 and use https.

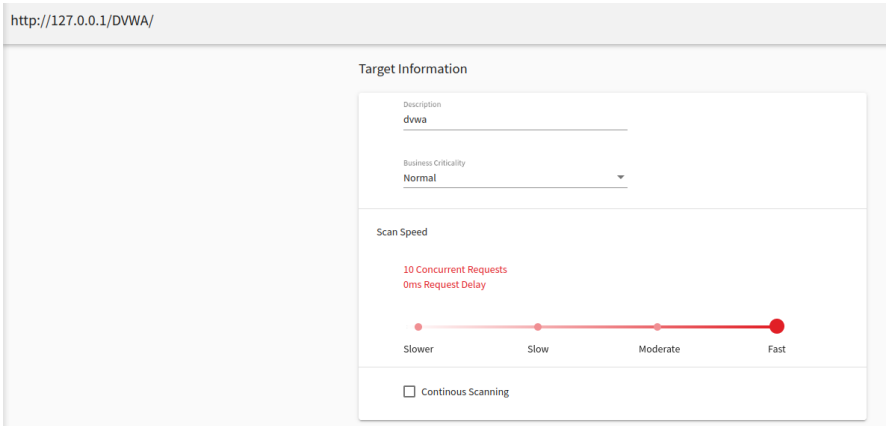
C. Run acunetix to scan DVWA:

Now I will test acunetix on my dvwa I create:

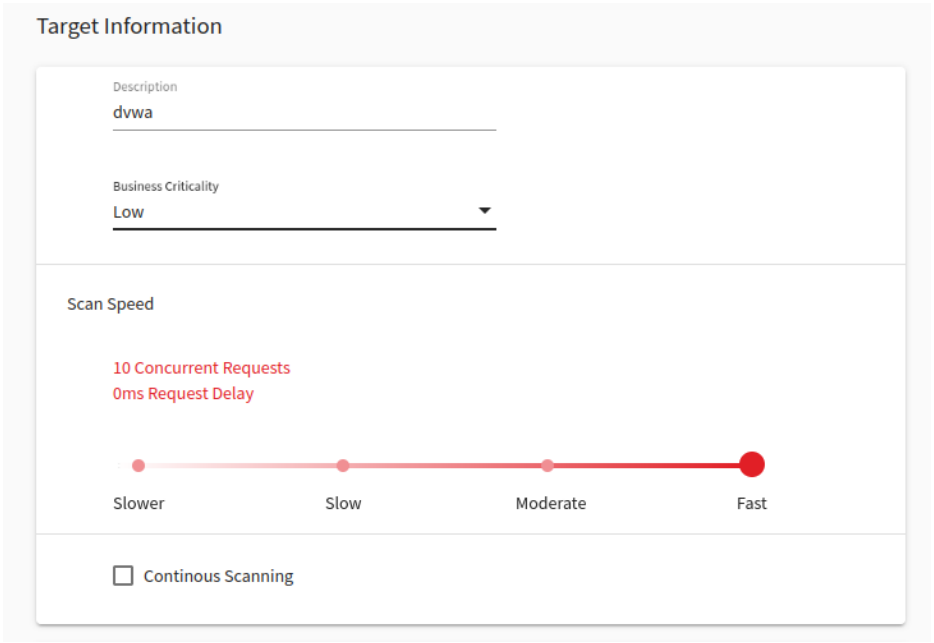
1) Add DVWA as a target in Acunetix. Click on the Targets menu on the left and then click on the Add Target option in the Targets menu. Enter your DVWA URL in the Address field.



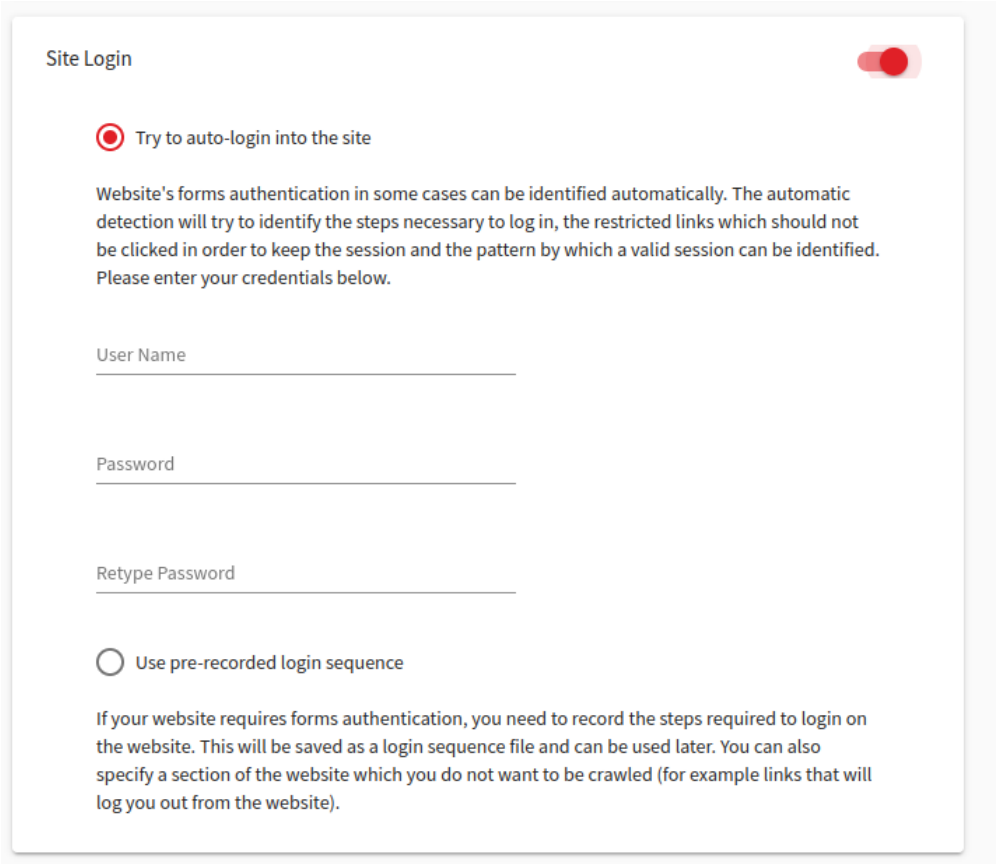
2) Click on the Targets menu on the left and click on the http://127.0.0.1/DVWA/ target.



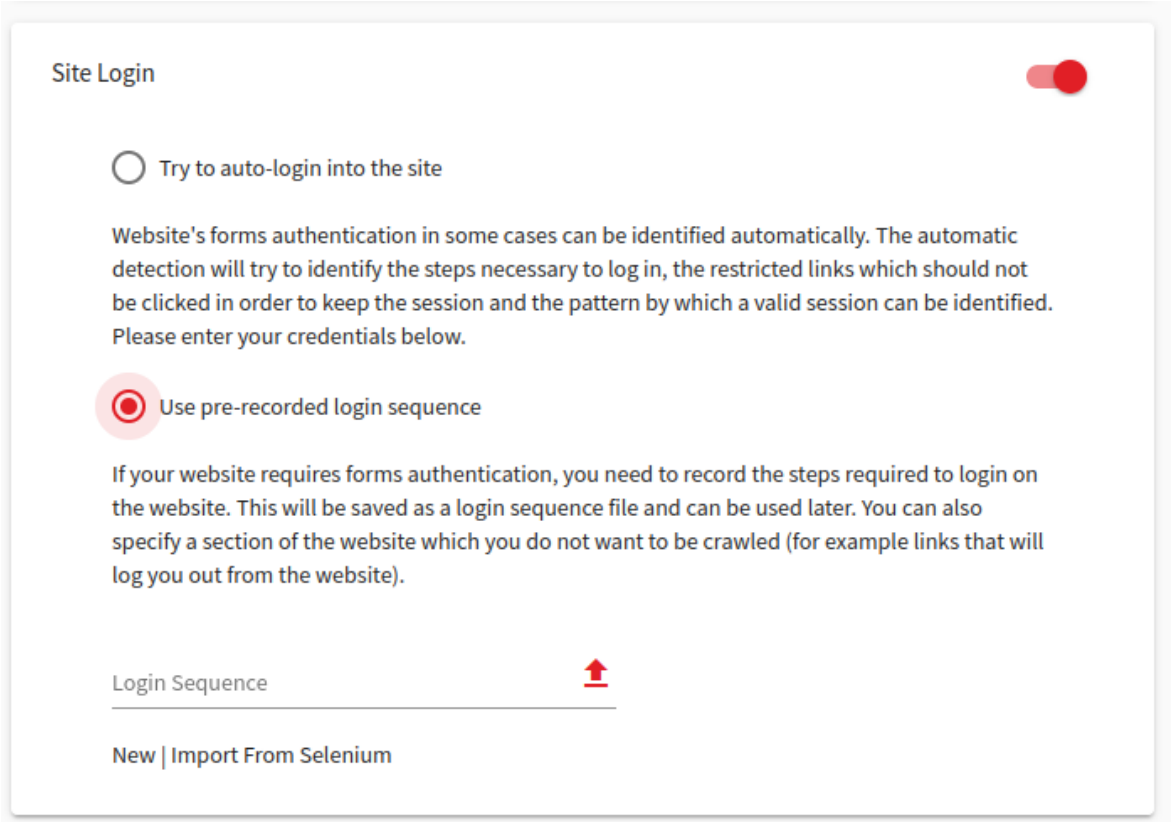
3) Set the Business Criticality to Low to signify that scanning this application will not have any effect on the performance of your organization.



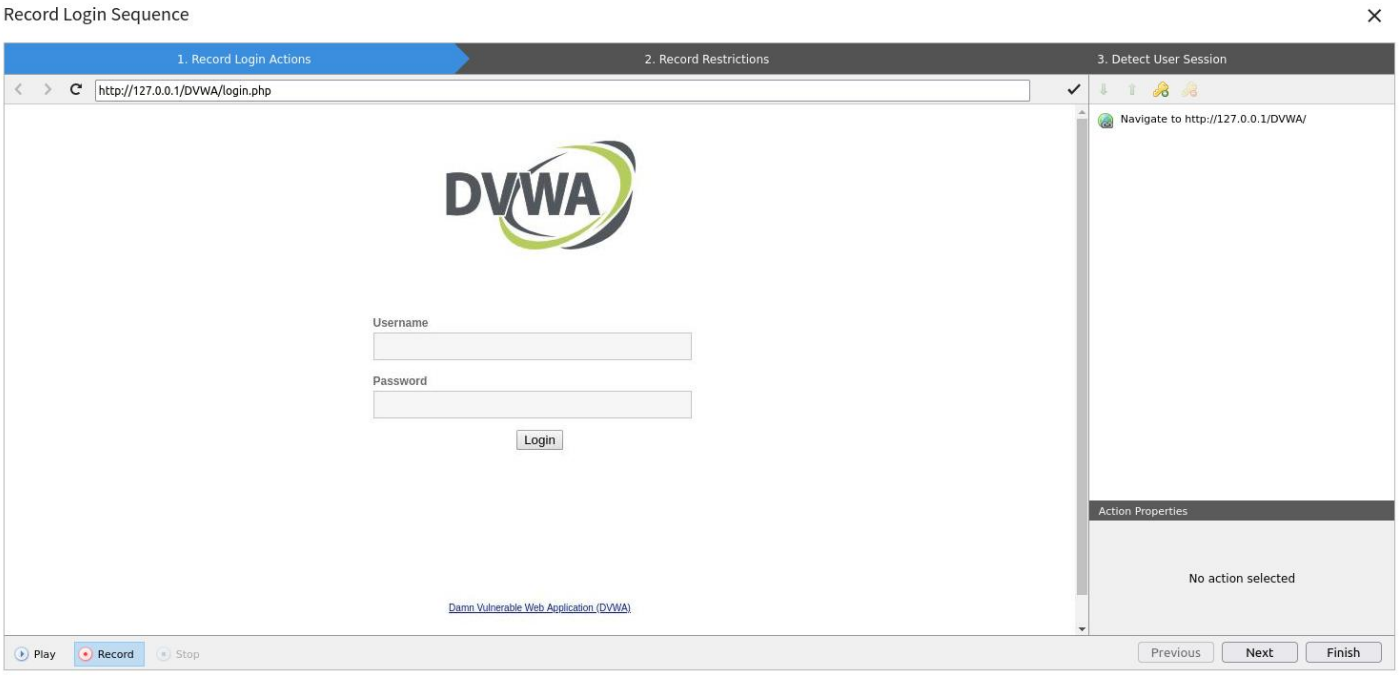
4) Click on the Site Login option to open the Site Login section.



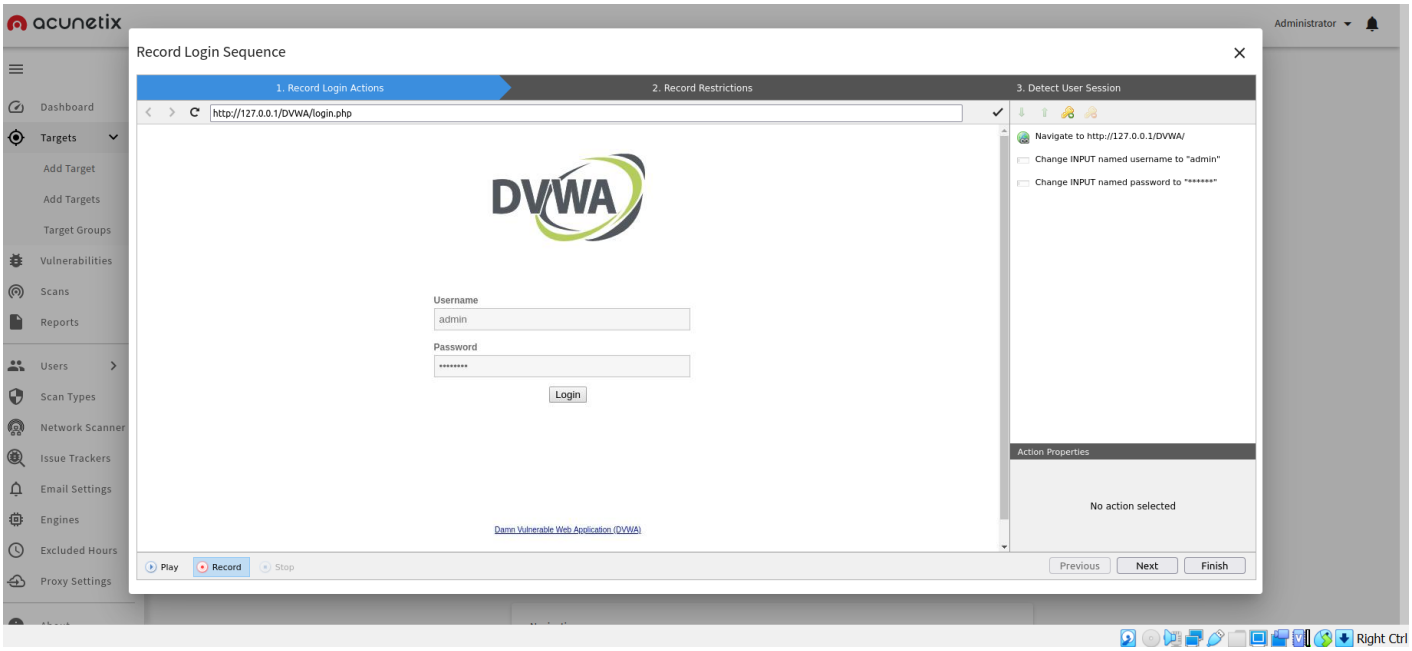
5) Click on the Use pre-recorded login sequence option.

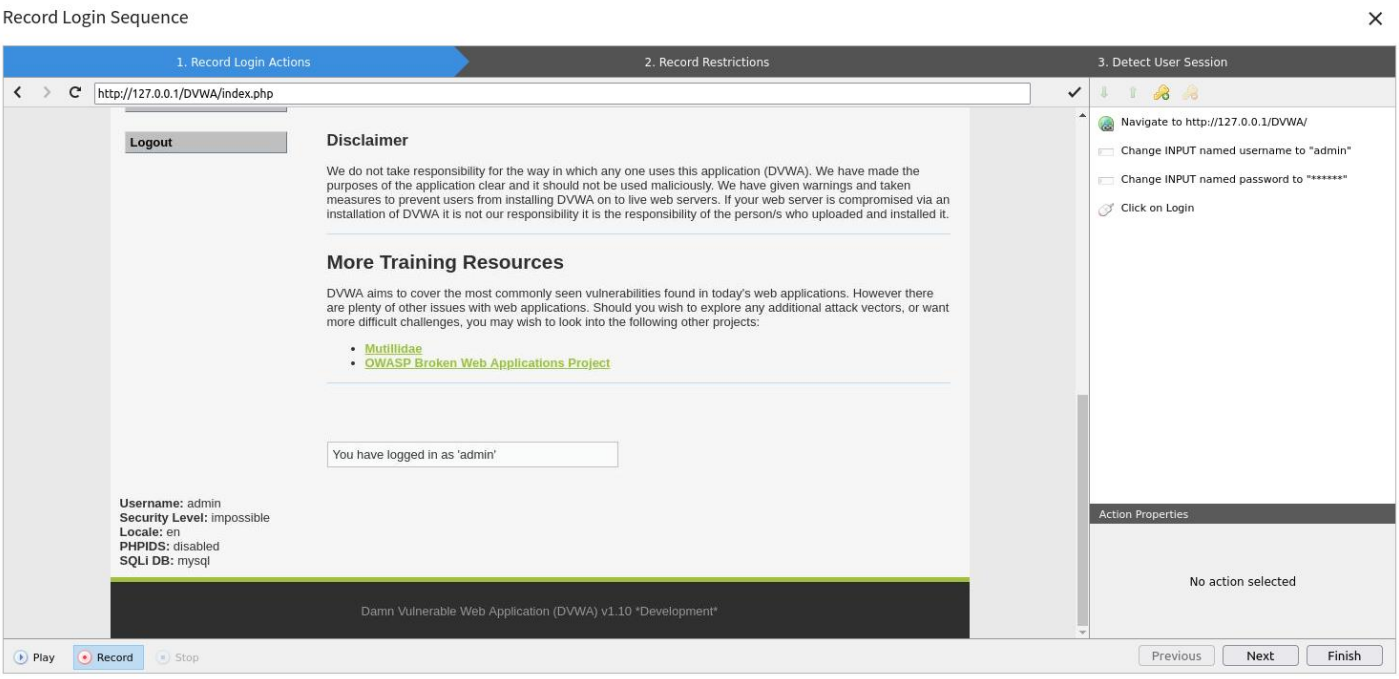


6) Click on the New link below the Login Sequence field to open the Login Sequence Recorder (LSR). The DVWA login screen will be displayed.

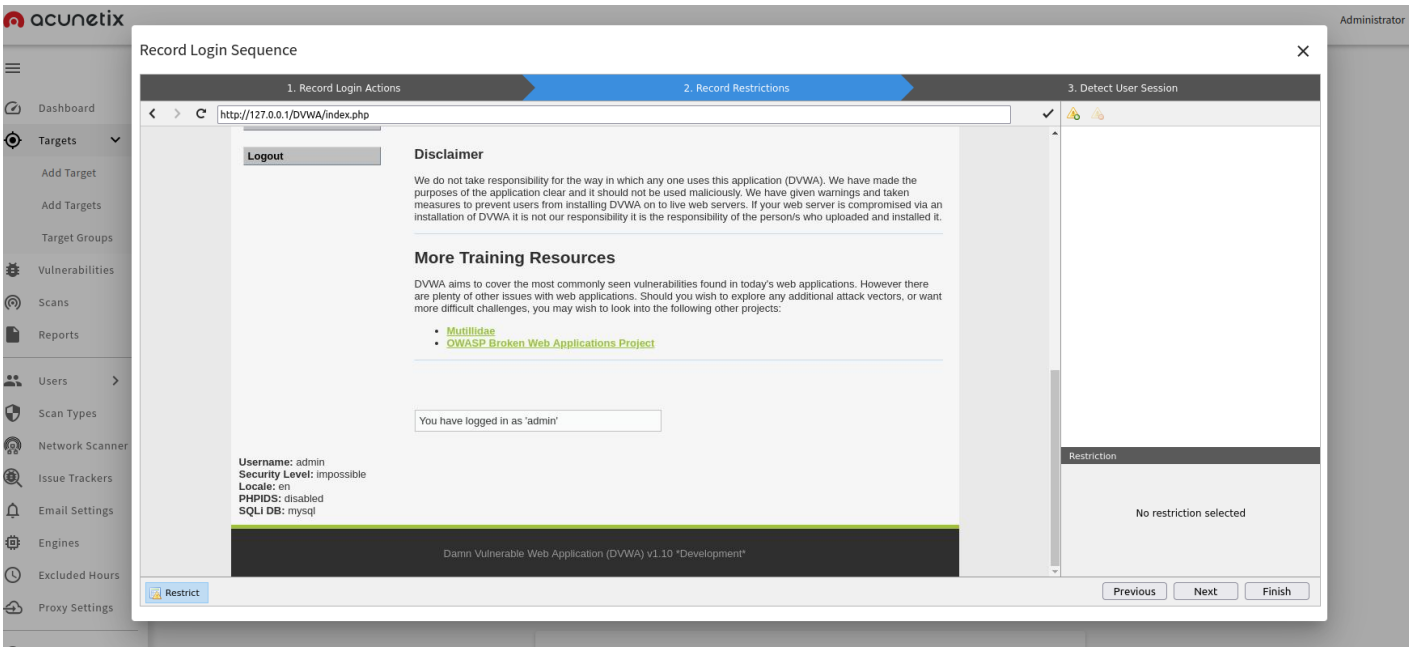


7) Enter the DVWA credentials in the LSR (admin/password).

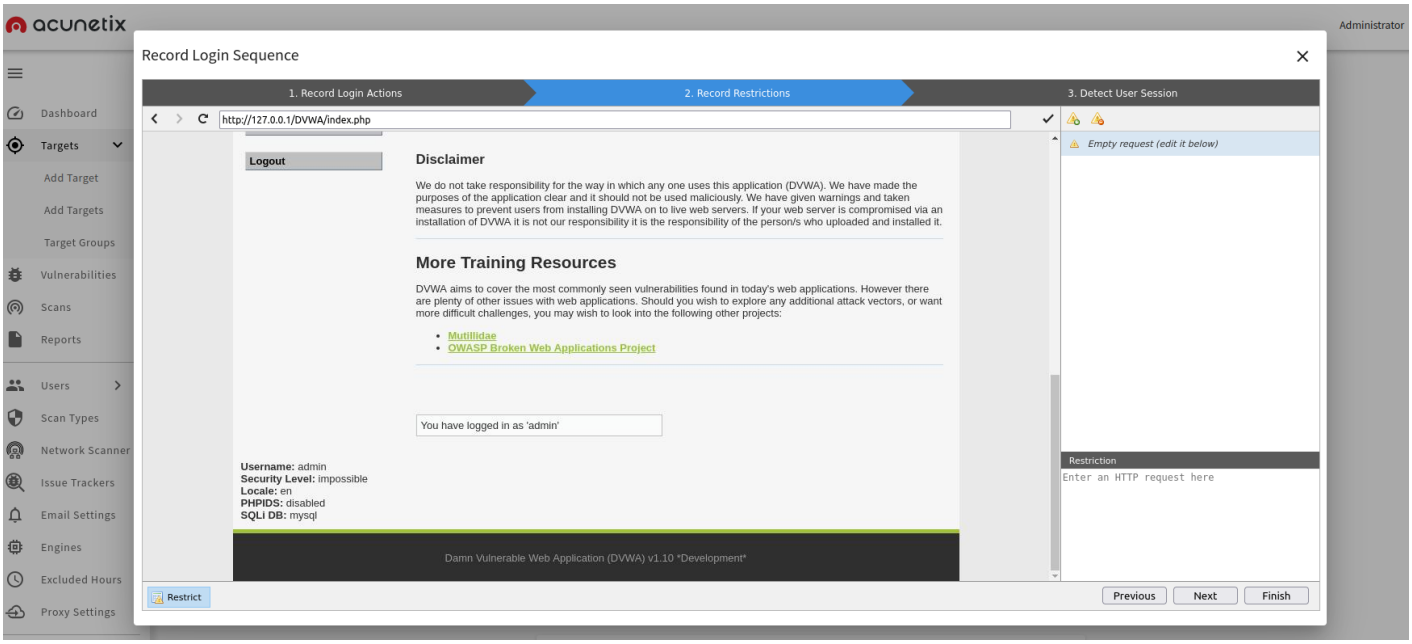




8) Click on the Next button to proceed to configure restrictions.

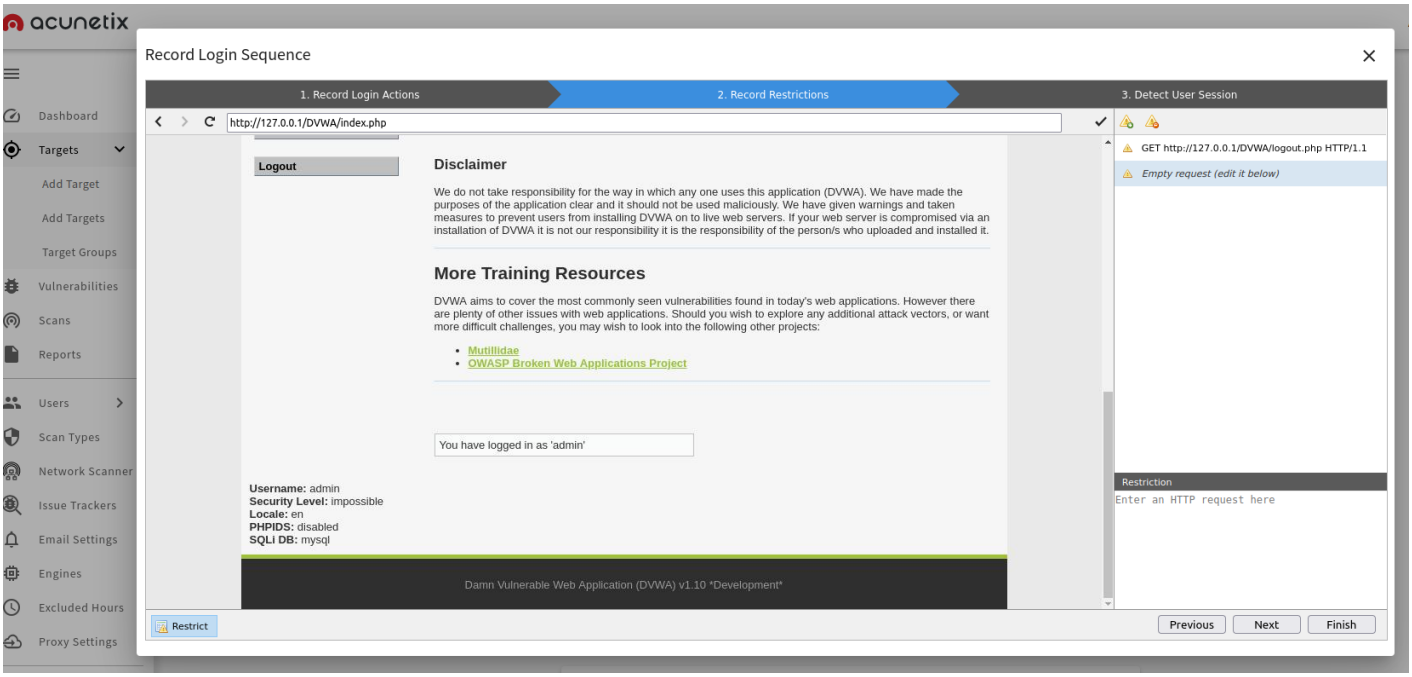


9) Click on the LSR exclamation mark icon icon above the right panel.



10) Enter the following in the Restriction field below:

GET http://127.0.0.1/DVWA/logout.php HTTP/1.1



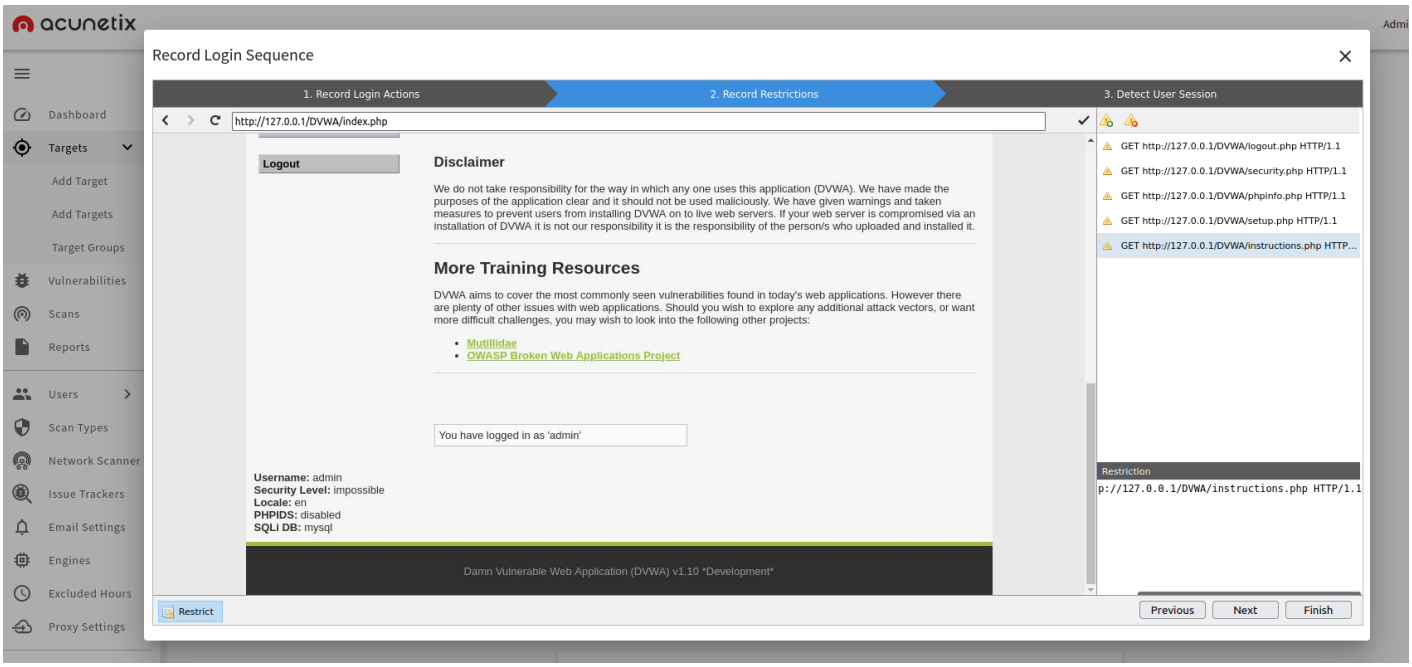
11) Repeat steps 8 and 9 for the following four values:

GET http://127.0.0.1/DVWA/security.php HTTP/1.1

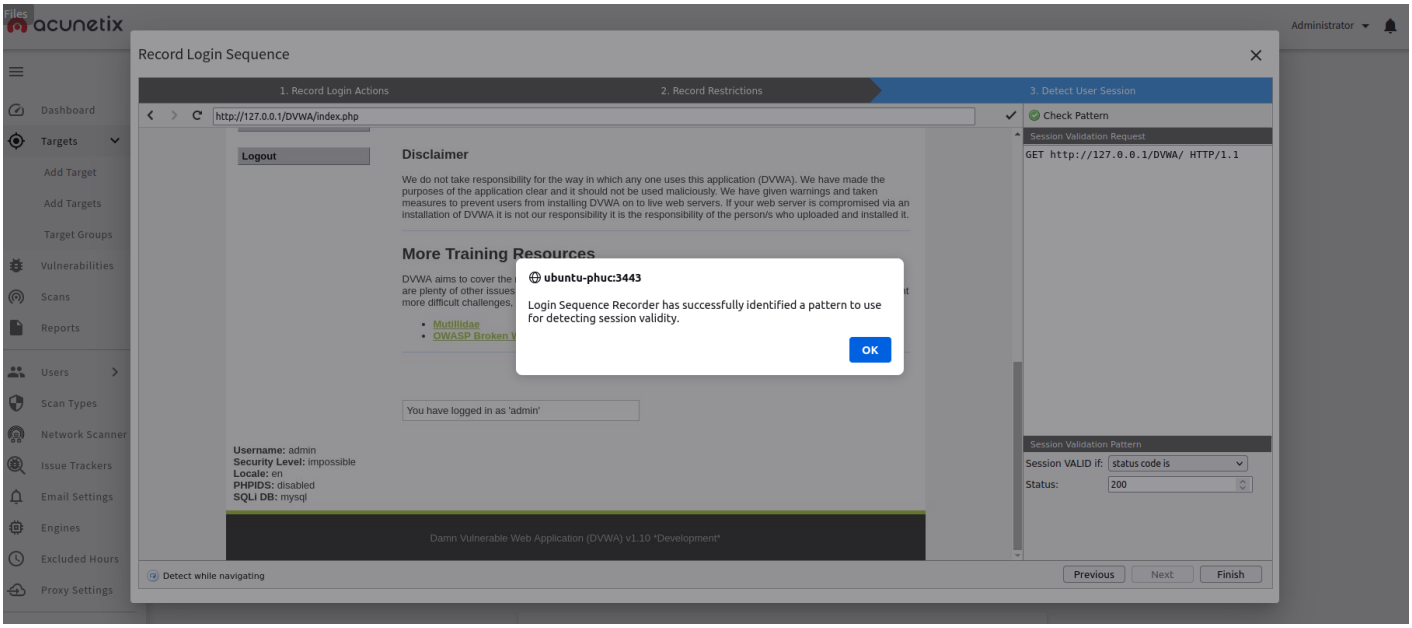
GET http://127.0.0.1/DVWA/phpinfo.php HTTP/1.1

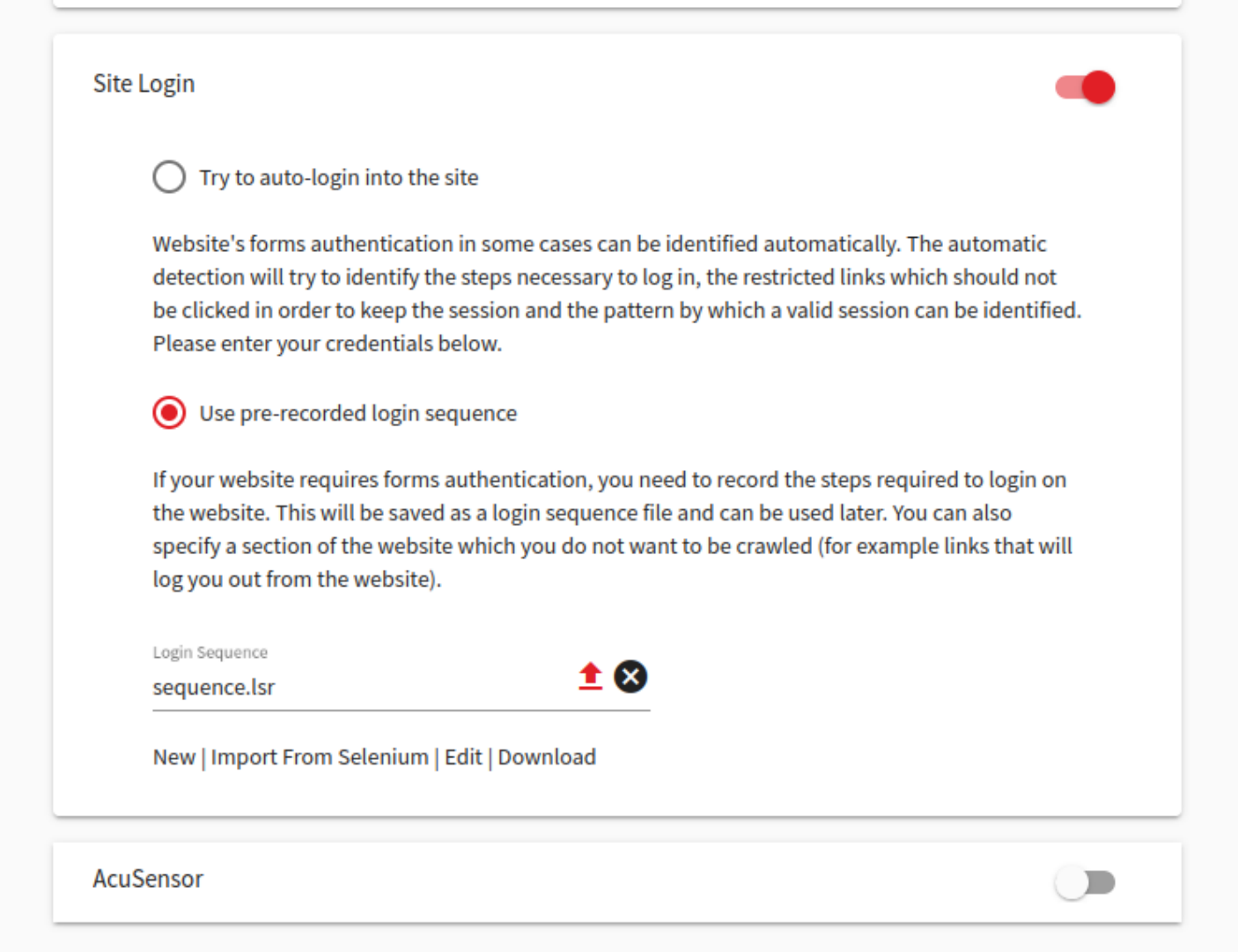
GET http://127.0.0.1/DVWA/setup.php HTTP/1.1

GET http://127.0.0.1/DVWA/instructions.php HTTP/1.1



12) Click on the Next button to have LSR identify the session and click on the Finish button when identification is complete.





13) Scroll down to the Crawling section of the target configuration page.

14) In the Excluded Paths field, enter the following regular expression:

```
^\/vulnerabilities/csrf/.*$
```

And click on the + button to add it

Crawling

Navigation

User Agent

Default

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Case Sensitive Paths

Auto

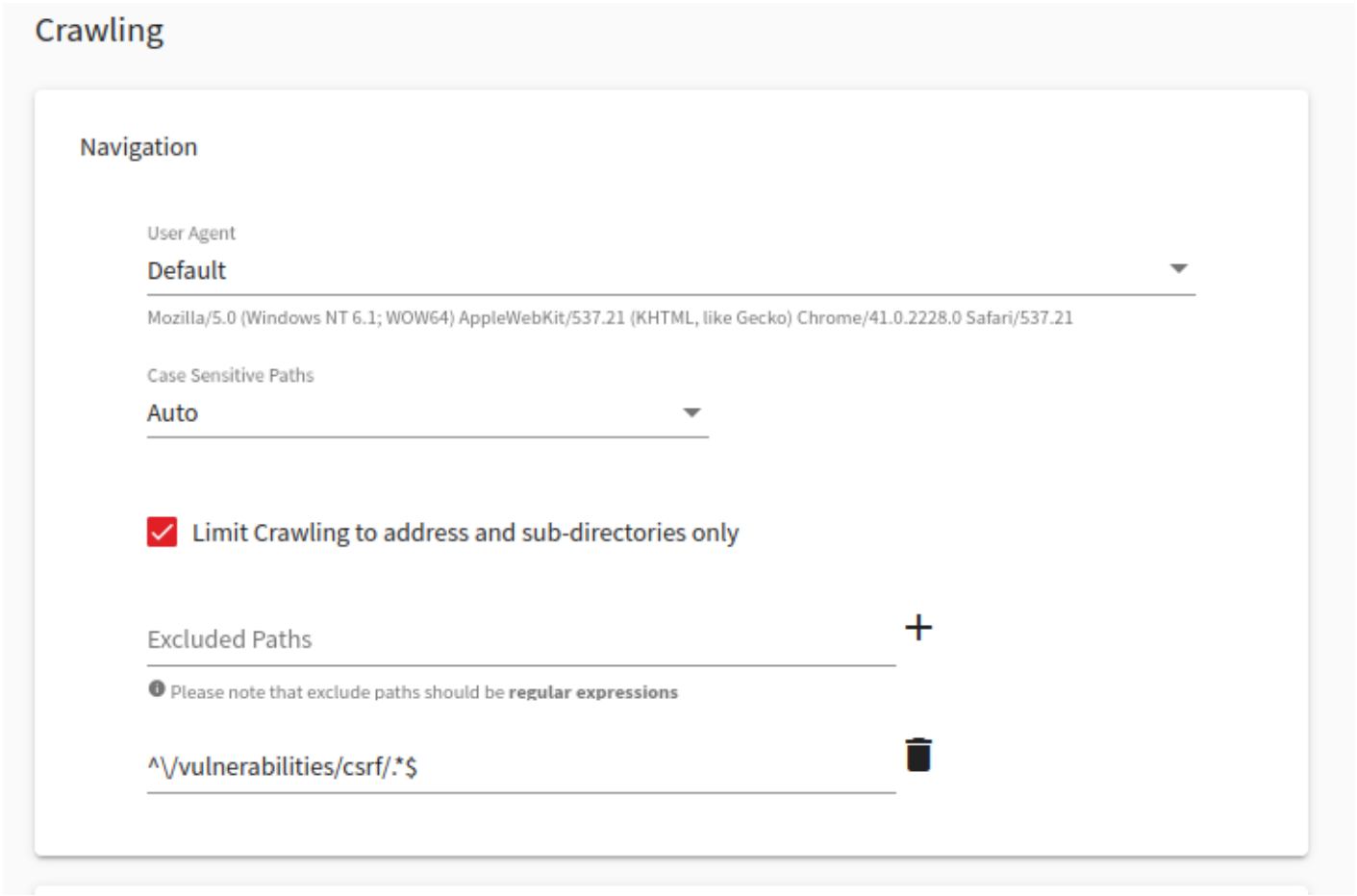
☑ Limit Crawling to address and sub-directories only

Excluded Paths +

Please note that exclude paths should be **regular expressions**

^\/vulnerabilities/csrf/.*$ 🗑

^\/vulnerabilities/captcha/.*$ 🗑



15) Repeat the previous step and add the following regular expression:

```
^\/vulnerabilities/captcha/.*$
```

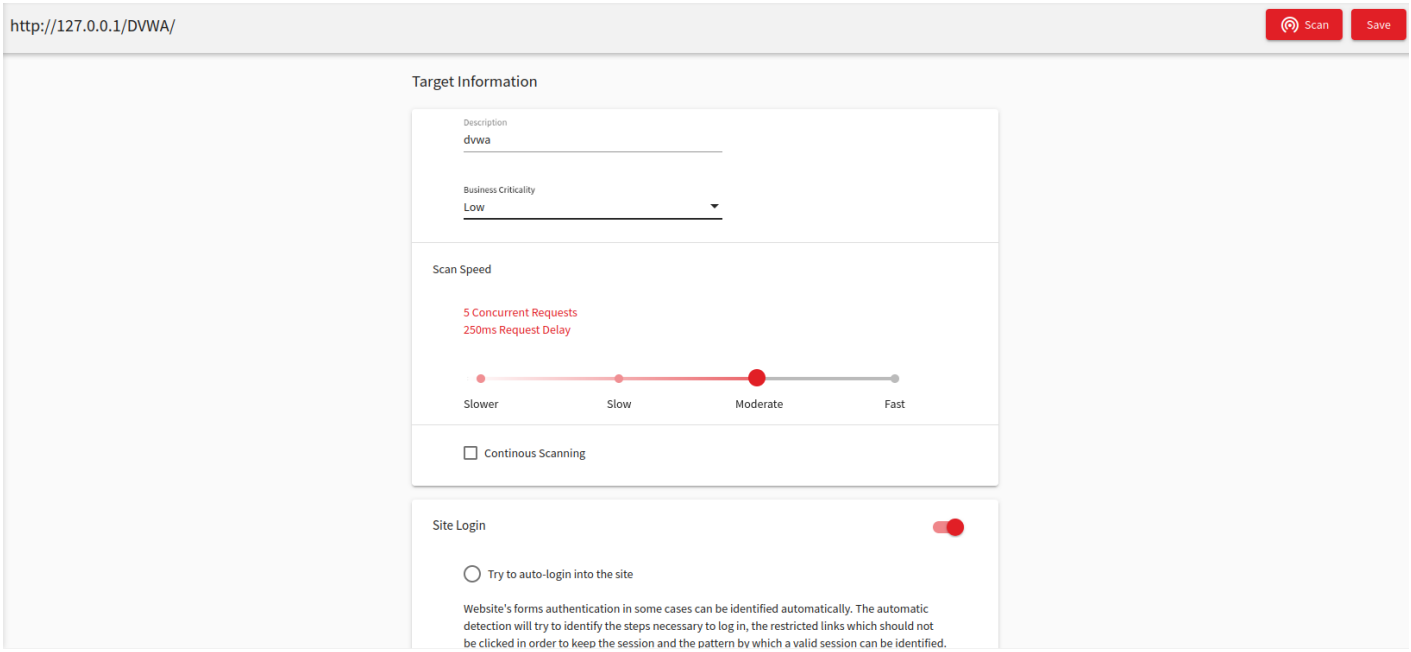
D. Scan the Target

Once the configuration is complete, you can scan the target. To identify all vulnerabilities, use the Full Scan type. We also recommend running this scan using *Moderate* scan speed to ensure that no requests are lost due to the target being flooded.

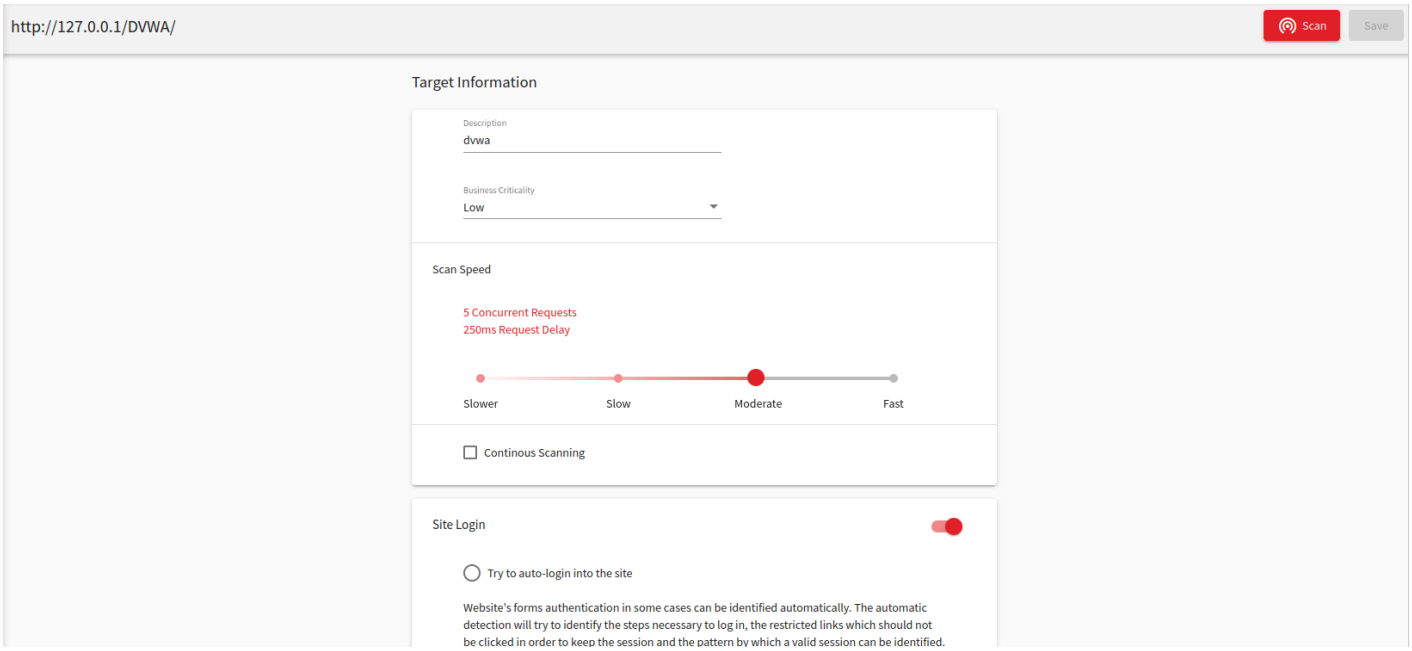
1) Click on the Targets menu on the left and click on

the http://acunetix.dvwa.com target.

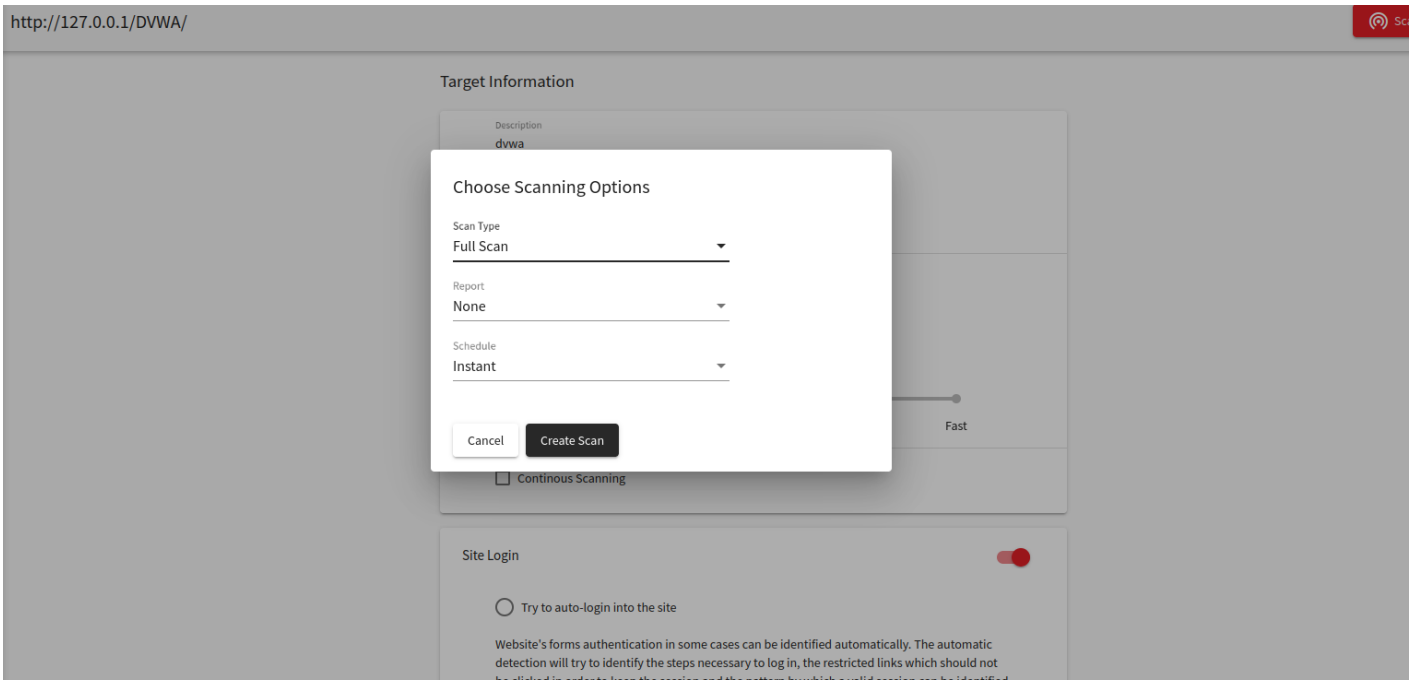
2) Set the Scan Speed to Moderate

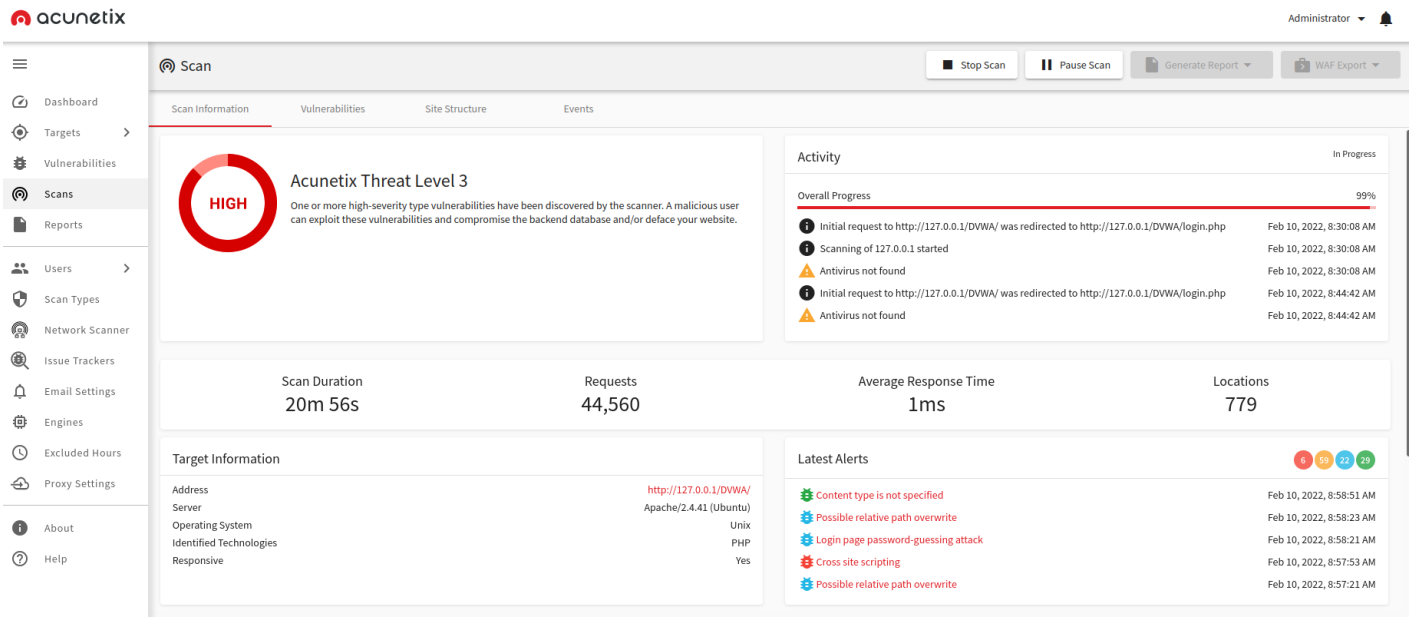


3) Click on the Save button in the top-right corner and then the Scan button to open the Choose Scanning Options box.

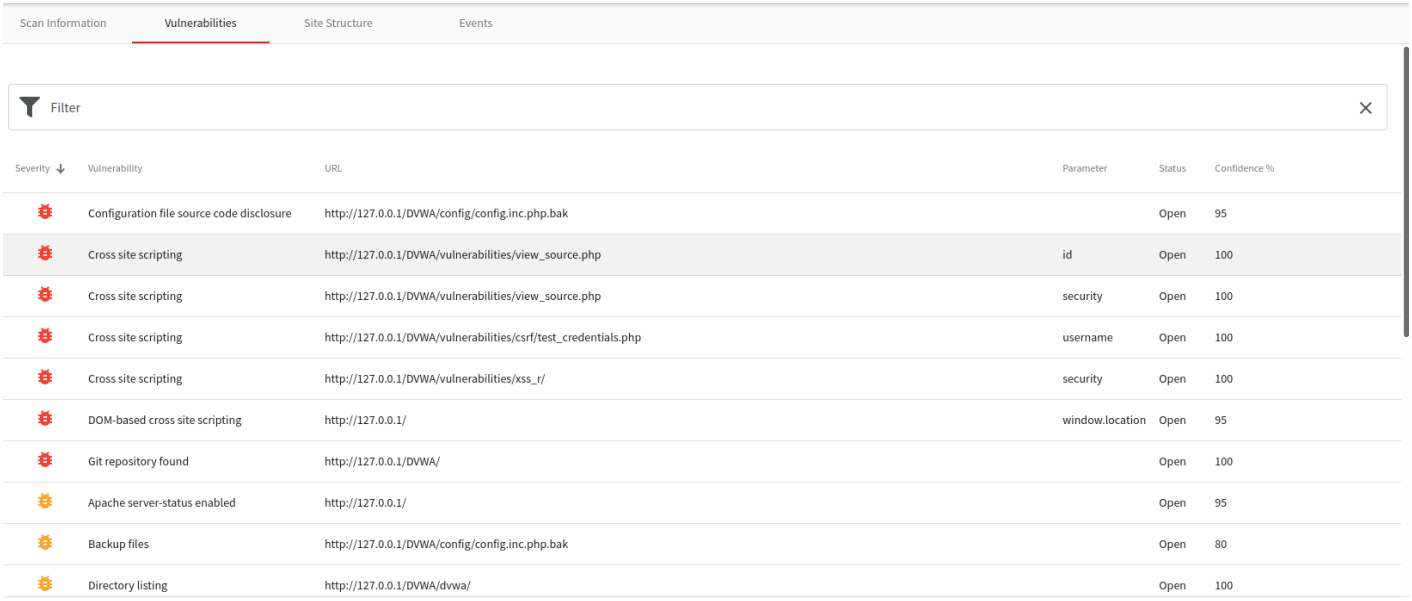


4) Make sure that Full Scan is selected in the Scan Type field and then click on the Create Scan button

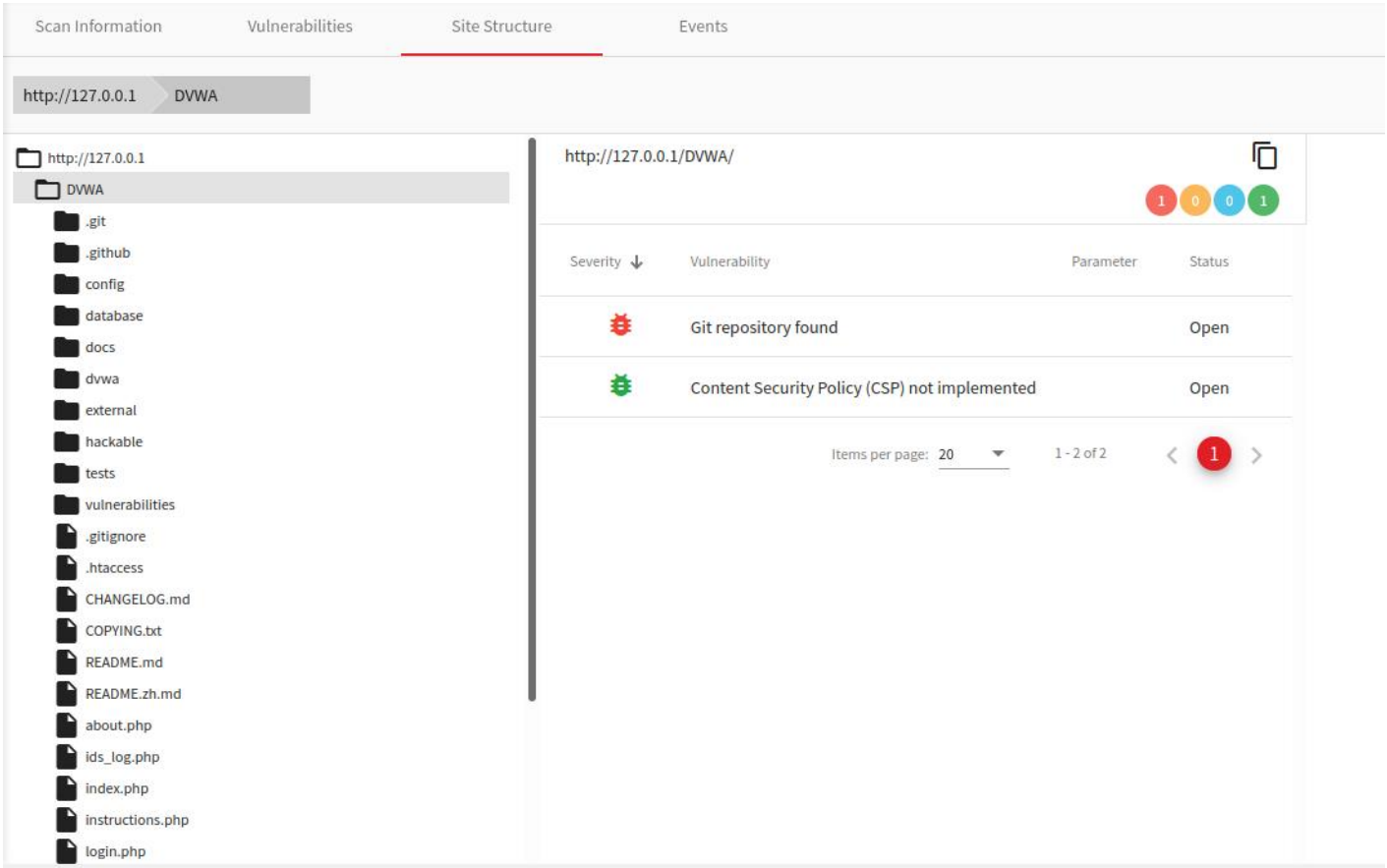




5) Some Vulnerability after some minutes scan:



6) Site structure:



7) Some event:

Scan Information | Vulnerabilities | Site Structure | Events

Event	Created	Additional Information

Scan Job Starting	Feb 10, 2022, 8:30:02 AM	{
		"status": "starting",
		"worker_id": "ffffffff-ffff-ffff-ffff-ffffffffffff",
		"scanning_app": "wvs",
		"extended_status": null
		}

Initial Request	Feb 10, 2022, 8:30:08 AM	{
		"data": "Initial request to http://127.0.0.1/DVWA/ was redirected to http://127.0.0.1/DVWA/login.php",
		"kind": "preflight_notification",
		"address": "127.0.0.1",
		"scan_id": "5b8c51df-276f-42e4-939a-381b1929aaf1",
		"target_id": "d4e01130-1b51-410c-b817-cf3619db4fd2",
		"scanning_app": "wvs"
		}

Scan Scanner Event	Feb 10, 2022, 8:30:08 AM	{
		"data": "",
		"kind": "antivirus_not_found",
		"address": null,
		"scan_id": "5b8c51df-276f-42e4-939a-381b1929aaf1",
		"target_id": null,
		"scanning_app": "wvs"
		}

Scan Paused	Feb 10, 2022, 8:36:47 AM	{
		"status": "paused",
		"scanning_app": "wvs",
		"extended_status": {
		"attachments": [
		{
		"url": "file:///home/acunetix/.acunetix/data/scans/c8c2bb08-1a4d-4613-b29d-2bdc7a9d8fc7.zip",
		"name": "output"
		}
		]
		}
		}

VII. CONCLUSION

- Find the vulnerabilities that put you at risk.
- Get actionable scan results in minutes.
- Resolve vulnerabilities fast.
- Easily scan in hard-to-reach places.
- Integrate web security into your development process.

VIII. Reference

https://www.acunetix.com/

https://www.acunetix.com/resources/wvsmanual.pdf

https://www.acunetix.com/support/docs/faqs/how-does-acunetix-perform-an-automated-scan-and-detect-vulnerabilities/

https://www.acunetix.com/support/docs/wvs/installing-acunetix-wvs/