ACUNETIX WEB VULNERABILITY SCANNER

A REAL WORLD REVIEW

MSI::Labs

May, 2006

Table of Contents

What is the Acunetix Web Vulnerability Scanner?

Acunetix web vulnerability scanner is a tool designed to discover security holes in your web applications that an attacker would likely abuse to gain illicit access to your systems and data. It looks for multiple vulnerabilities including SQL injection, cross site scripting, and weak passwords.

The application can be used to perform scanning for web and application vulnerabilities and to perform penetration testing against the identified issues. Mitigation suggestions are then provided for each weakness and can be used to increase the security of the web server or application being tested.

About this Review

MicroSolved, Inc used Acunetix in real world tests. Testing occurred during an actual vulnerability assessment and penetration test.

Testing was performed by a panel of technicians with extensive penetration testing experience and knowledge of numerous commercial and open source web and application scanning tools. During the testing, multiple websites were assessed. Only the scans from these websites and this penetration test were used as input during this review. Each feature of the Acunetix web vulnerability scanner was rated on a scale of 1-5, with 5 being the best possible score.

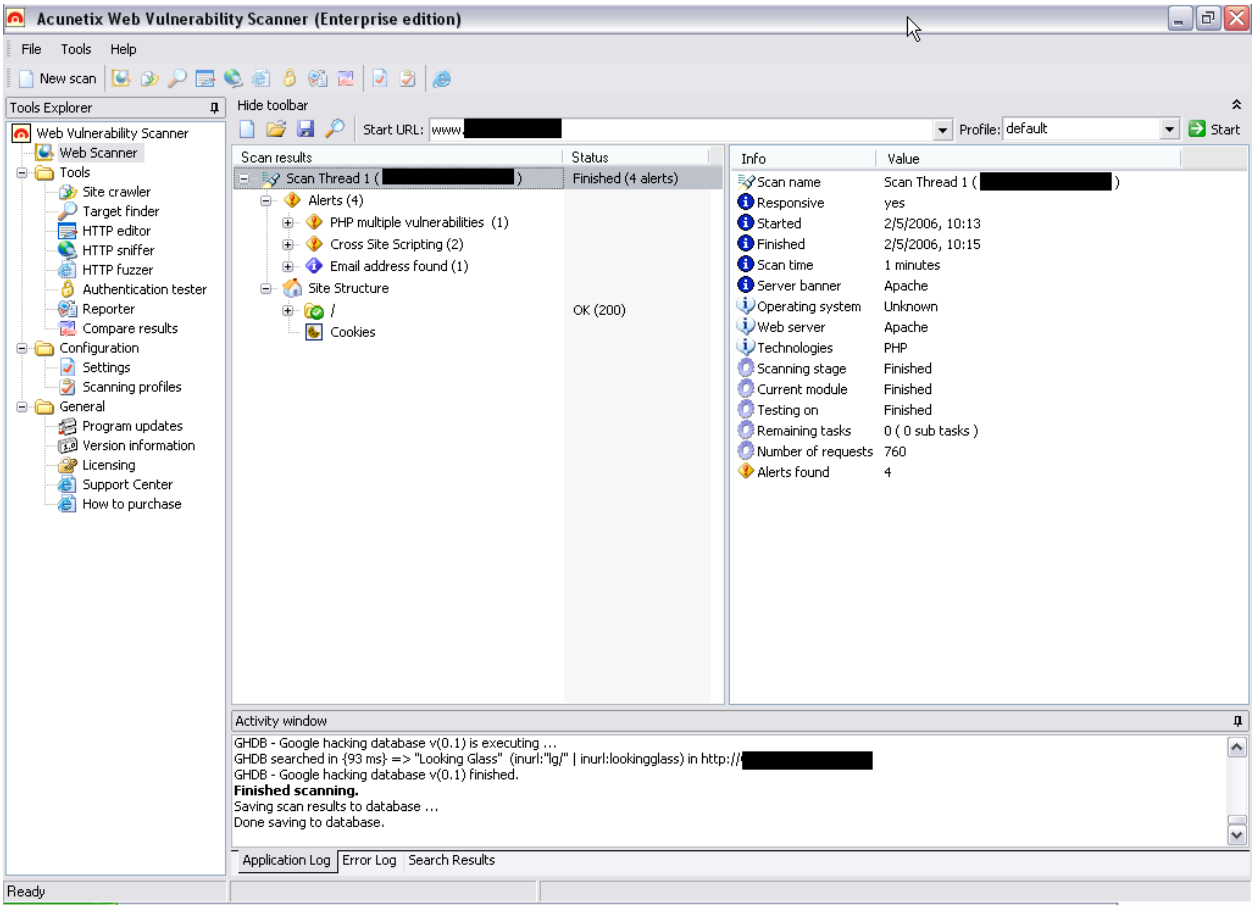
Installation and Updating Mechanisms

Installation is straight forward. An executable with a typical Windows installation procedure is provided. The only input required for the install is the license that was issued. The program provides a built in update mechanism. Acunetix is capable of updating itself without requiring a restart of the program. Acunetix has the option of checking for updates at start, or you may set it to only check when you manually use the update feature.

Scanning Tools Review:

The interface for the scanner divides the tasks up by function. While data can be shared, copied and pasted between the tools, the interface creates a logical and efficient way of handling the tasks associated with performing web and application assessment. Each specific tool and function is detailed below:

Web Scanner:



When starting the scan Acunetix takes a quick look at the server to determine what technologies are used. So if it determines that PHP is being used, it will only check for PHP vulnerabilities. You may also manually choose the technologies present as well as limit the vulnerabilities that Acunetix checks for. Scans are relatively fast, even when scanning large sites.

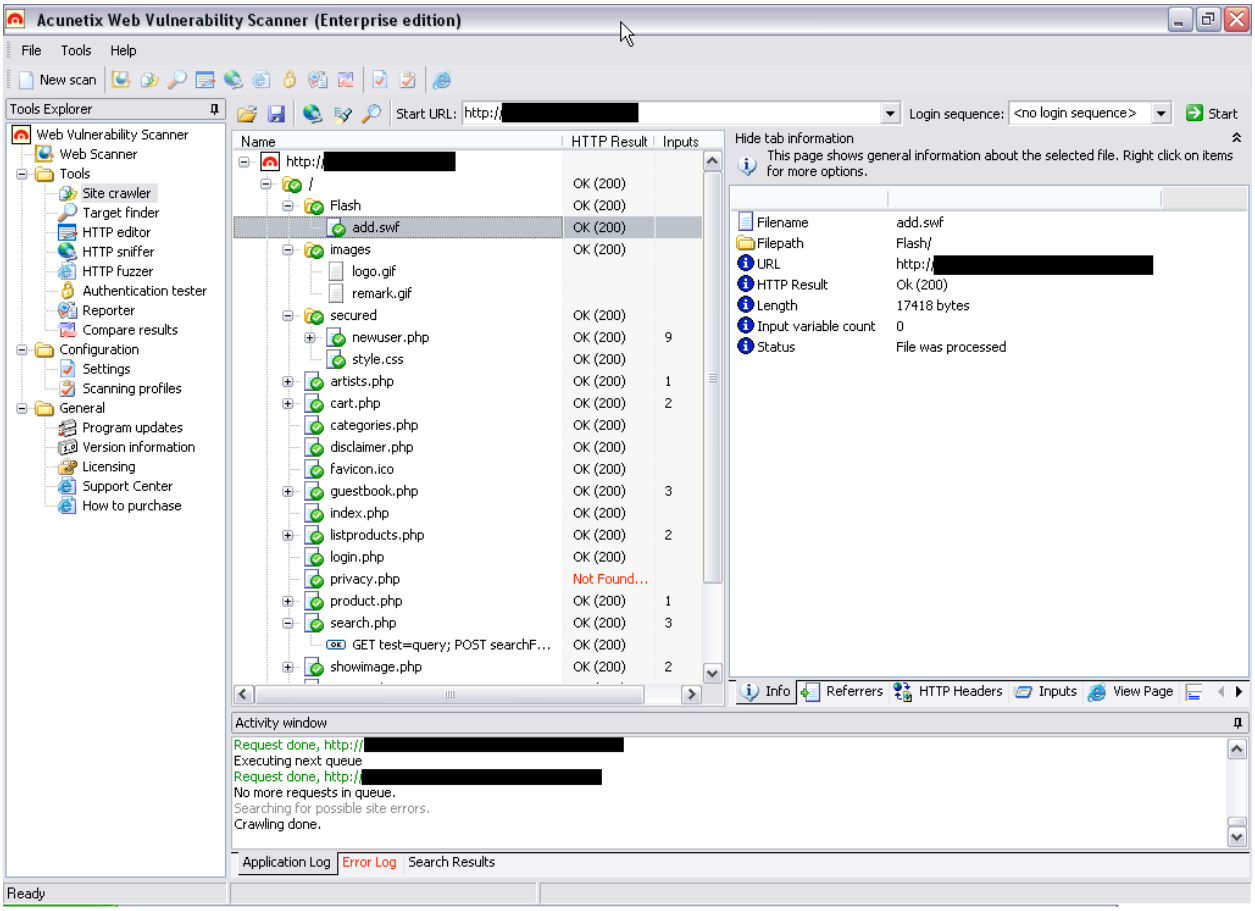
The scanner checks for SQL injection exploits, cross site scripting vulnerabilities, common default files (ex. manuals, "test" files), and server misconfigurations (ex. TRACK or TRACE enabled). Acunetix's scanner performed as well and in some cases better than scanners that are commonly used during our tests. Twice Acunetix found files and pages that were not identified by other scanners. Acunetix was able to identify SQL injections and cross site scripting errors as well as the best tools.

False positives can be reduced through a feature that lets you specify custom error pages. This is a great feature that some other tools are lacking. The scanner also found and cataloged other information such as email addresses and broken links. We found the email address gathering to be useful as we commonly pull those from web pages during penetration testing.

The scanner is thorough and quick and has some features not found in other scanners.

Rating: 4.5

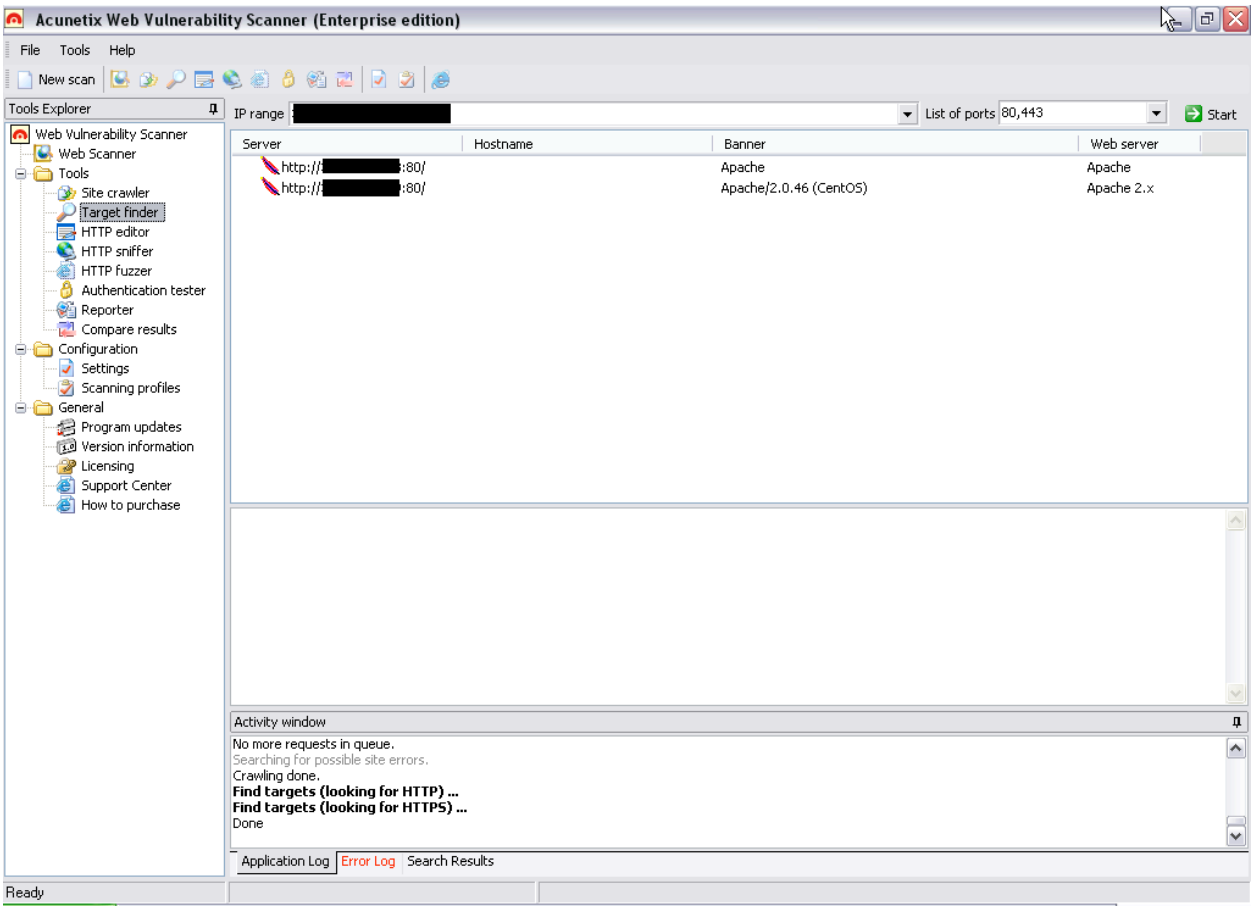
Web Crawler:



The spider feature crawls a website and displays hierarchal view of the site structure. Additionally, the spider collects information such as referrer pages, headers, and variables within the pages. By default, it will spider your whole site, but you can limit the extensions that are spidered if you desire. We found the spider to be quick, and the way it is displayed helps to understand the layout of the site. However, the spider was stuck in a loop on one of the sites we tested. We spidered the site with several other applications to determine the fault and all but one of them also got stuck in an infinite loop. Unfortunately, we were not able to determine why this happened, and why one application crawled the site with no problems. With no lacking major features, excellent display, and quick crawling we give the spider 4.5 stars.

Rating: 4.5

Target Finder:

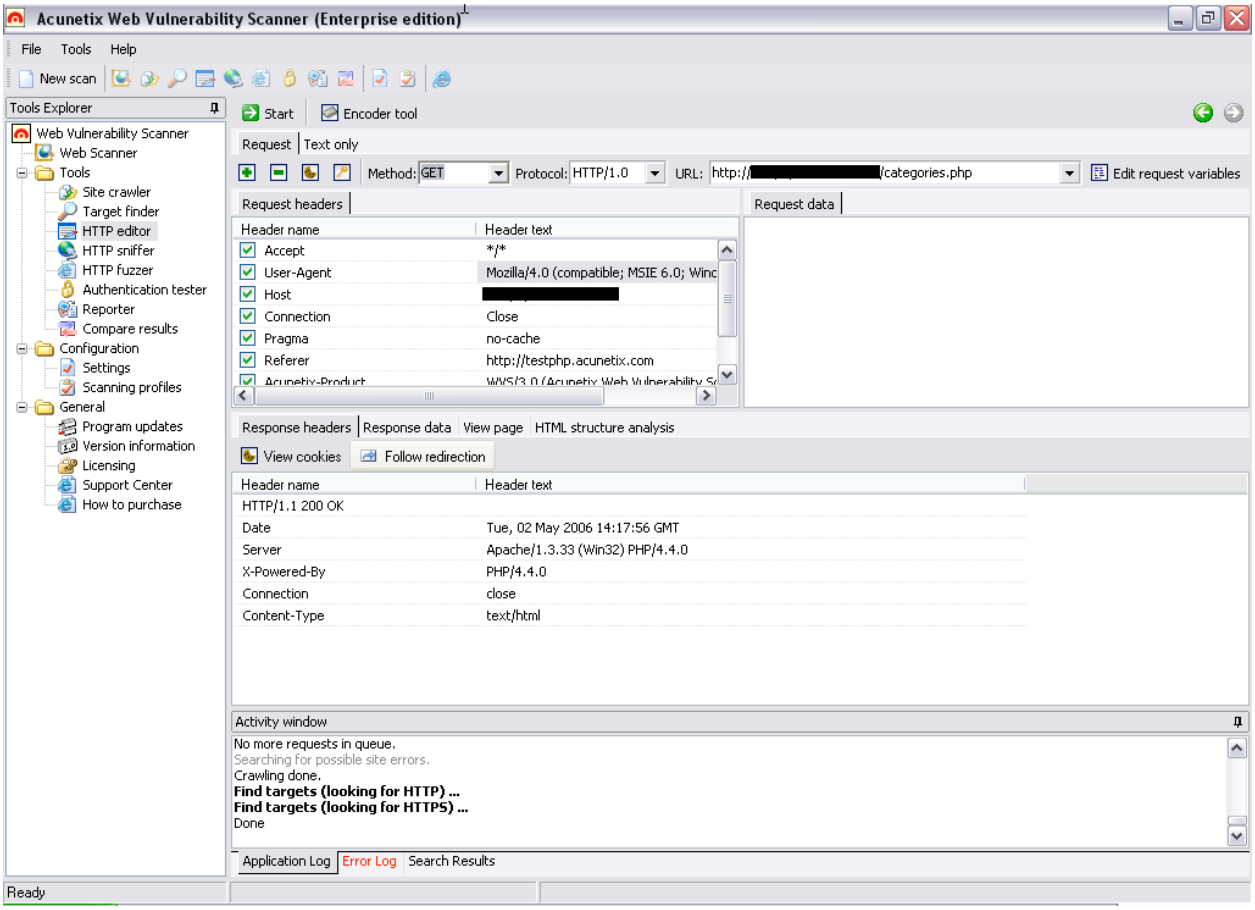


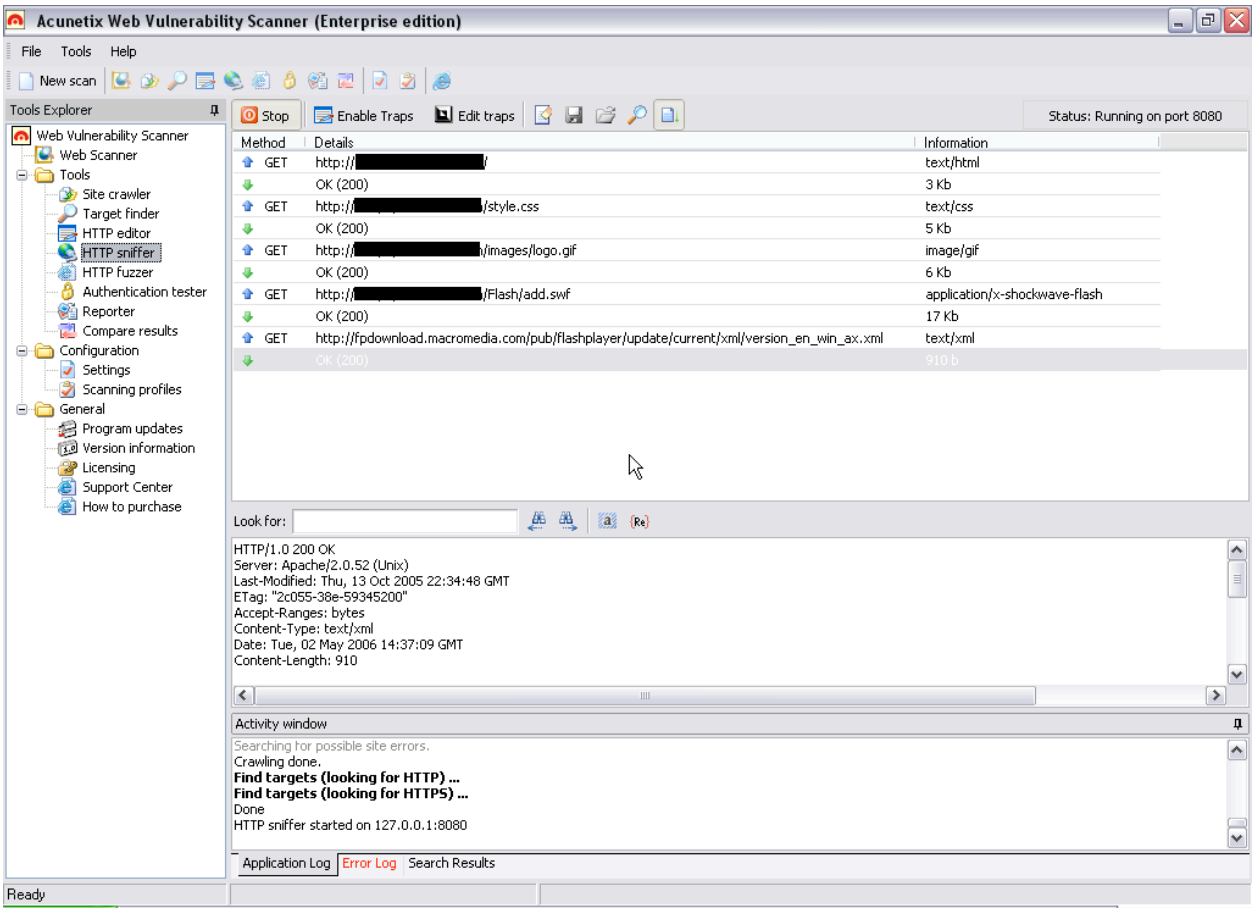
The target finder is a simple port scanner that is designed to find websites running in a range of given addresses. The range of addresses is not limited and you can specify which ports to look on in order to discover websites on non-standard ports. It will also attempt to identify the type of web server running.

We did experience some awkward issues with this feature. When we gave it a half class C address space to scan, it identified no web servers, even though we knew they existed. If the address space was reduced, it accurately identified existing servers. Due to the fact that it was not able to work with large address ranges we are giving it 2 stars.

Rating: 2

HTTP Editor and Sniffer:

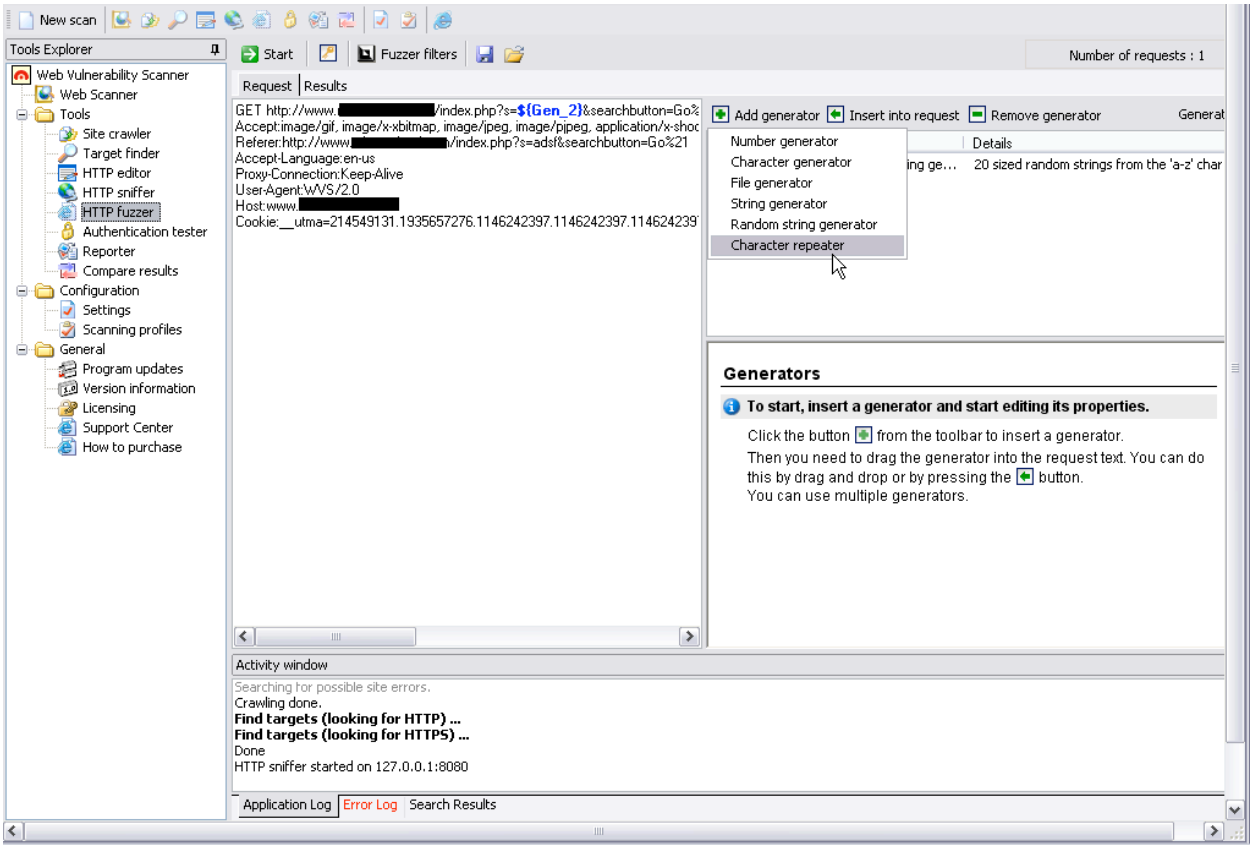




These tools allow you to view, edit, or create HTTP requests. This is designed to allow the penetration tester to analyze the traffic between the server and the client. With this information, it's possible to construct custom attacks against SQL and cross site scripting vulnerabilities. The sniffer also allows interception and changing of data before sending it to the server or receiving it, allowing bypassing of client side validation. These tools enable digging deeply into the application where it's hard for a scanner to automate. Definitely, this is a valuable feature that we're pleased to see in the product. The interface could be streamlined a little, but otherwise this is another top notch feature.

Rating: 4

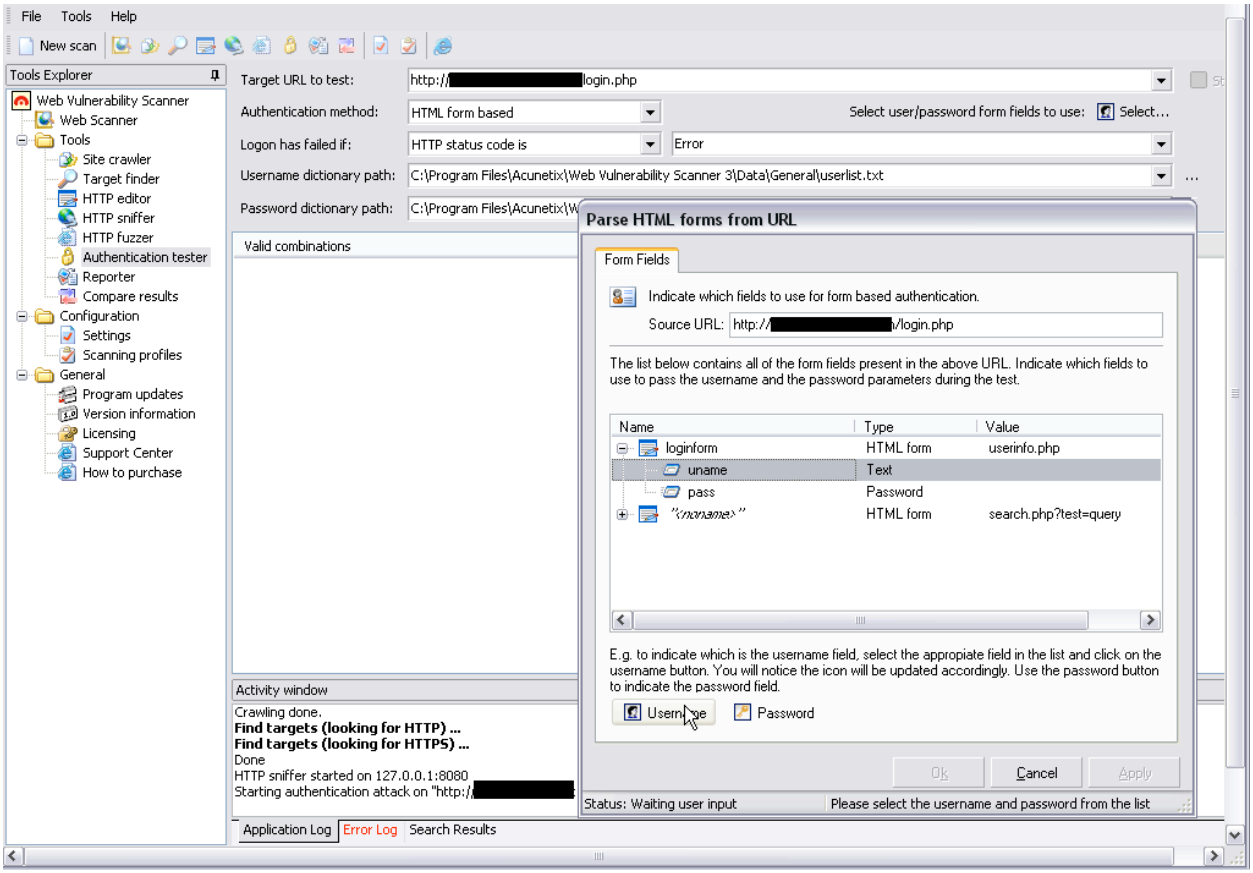
HTTP Fuzzer:



HTTP fuzzer is related to the editor and sniffer. However, the fuzzer automates injecting characters into variables, instead of doing it manually. Fuzzing enables a quick and easy way to brute force test applications for buffer overflows. The options for the fuzzer are extensive, allowing you to generate numerous types of strings and characters witch to fuzz. The interface may be a little confusing for a person that has never tried automated fuzzing, but a short tutorial is included in the manual. Along with the editor and sniffer, this is another great feature that deserves some credit.

Rating: 4

Authentication Tester:



We were surprised by this feature. Not only because there are not many good web site authentication brute forcers, but because it just works well. The authentication tester can test both HTTP authentication (the pop up box type) and HTML forms.

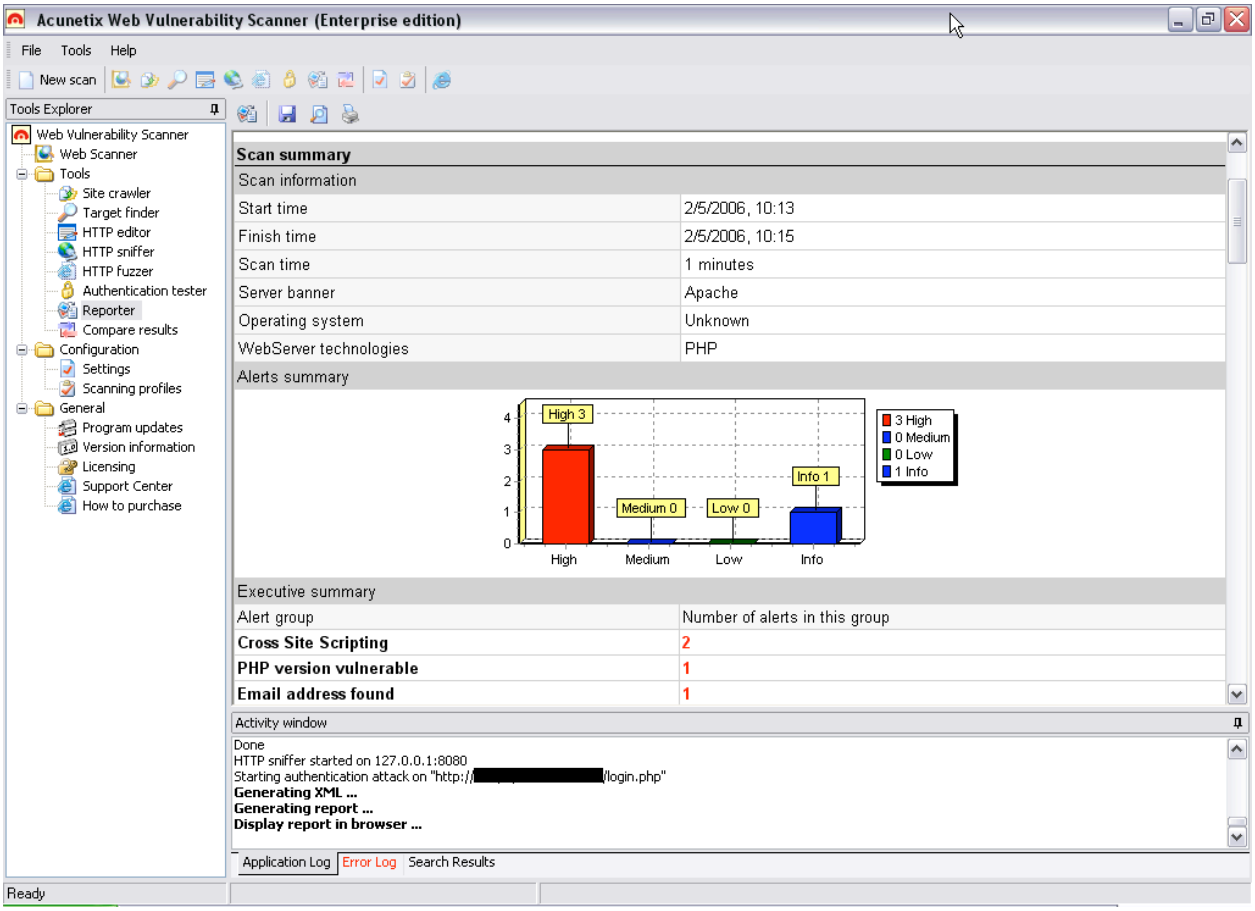
When testing HTTP authentication, it's rather straight forward. You choose the user name list, password list and also the error returned upon authentication failure. This last option is important as it allows you to test sites that give a non standard response instead of just giving you a false positive.

HTML forms are a little different. Acunetix loads the page with the forms and you specify which fields are the user name and password. It's also possible to specify custom error pages. This can be done by telling Acunetix what error code is returned, or you can you can have Acunetix search for a string within the returned page. For example if the page says "Login Failed" on a failure, you would tell Acunetix this through a string match or regex. This greatly reduces false positives as more and more pages are using custom error messages.

Overall the authentication tester is an excellent addition to the product. There are a few features we would like to see implemented for this, but they are minor points.

Rating: 4

Reporting Capabilities



Reporting was found to be sufficient. The reports are clean, easy to read and Acunetix does not give inappropriate ratings for minor vulnerabilities. Overrating vulnerabilities seems to be a common practice among some other scanners, prompting irrational fears and actions. However, reports are only able to be saved in HTML type documents. Acunetix has no direct way of exporting to other formats, such as XML, or to input the data into other more extensive reporting tools. By default it does save all data to an MS Access database. If Microsoft Access is available, you are able to export to numerous types of formats. The reports are clean, but offer no direct way of exporting data to non-HTML formats which may be an issue for some users depending on their reporting needs.

Overall Package Rating

With the amount of features, ease of use, and speed, we give Acunetix an overall rating of 4 stars.

Pros:
+ Quick scanning
+ Specify custom error pages
+ Combines many tools into one application
+ High detection rate of vulnerabilities
+ Does not overrate minor vulnerabilities

Cons:
- Reporting is not robust
- Target identifier appeared to be buggy
- Could use some interface tweaks

Summary

Acunetix strives to be one application that contains a collection of comprehensive tools to give a complete look at the vulnerabilities of a website. Overall, Acunetix achieves this goal but could use some polish in its minor features to make the complete package shine like a diamond.

Suggestions for Future Enhancements

Acunetix is already a strong product, but with some minor additions could improve upon an already great product. We found a few minor things that could be included or changed. The interface could use a few tweaks, especially in the fuzzer. Although overall the interface is user friendly and easy to use. In the authentication tester, while doing HTML brute forcing, it was not able to only specify a password with no username. We have run across a few "administrative" web pages that only have input for a password. We could not find a way to brute force these pages. Additionally, a way to change the timeout period and multiple threads would be a welcome addition. These would provide a speed increase. In the spider, it would be beneficial to limit the depth of links that are crawled. This would provide a work around in the event of the spider getting stuck in an infinite loop.

About Acunetix (from www.acunetix.com)

Securing a company's web applications is today's most overlooked aspect of securing the enterprise. Web application hacking is on the rise with as many as 75% of cyber attacks done at web application level or via the web. Most corporations have secured their data at the network level, but have overlooked the crucial step of checking whether their web applications are vulnerable to attack. Web applications, which often have a direct line into the company's most valuable data assets, are online 24/7, completely unprotected by a firewall and therefore easy prey for attackers.

Acunetix was founded with this threat in mind. They realized the only way to combat web site hacking was to develop an automated tool that could help companies scan their web applications for vulnerabilities. In July 2005, Acunetix Web Vulnerability Scanner was released - a tool that crawls the website for vulnerabilities to SQL injection, cross-site scripting and other web attacks before hackers do.

The Acunetix development team consists of highly experienced security developers who have each spent years developing network security scanning software prior to starting development on Acunetix WVS. The management team is backed by years of experience in marketing and selling security software.

Acunetix is a privately held company with its offices in the US, Malta and the UK.

About MicroSolved, Inc.

MicroSolved, Inc. was founded in 1992 by L. Brent Huston. MSI was created to provide solutions that empower organizations to mitigate risks and create privacy while maintaining the practice of doing business in the online world. The projects MSI engages in range from managed security services to unique solutions crafted to answer complex security problems. Our work includes protecting the largest government and commercial networks in the world.

MSI's public work includes engagements on the Federal, State, and local level. Our work with the federal government includes protecting some of our nation's most sensitive networks, working to secure some of the largest HIPAA networking concerns, and working with federal auditing agencies to help them implement an auditing process that effects real world security. MSI has received accolades for its work for the U.S. government, and has even testified before congress.

MSI's work in the commercial sector includes a wide variety of vertical markets. MSI enjoys long-term relationships with some of the world's largest financial and telecom providers. Our work with various regulations including GLBA and HIPAA has made us an obvious choice for financial and healthcare organizations of all sizes. In the commercial sector our work ranges from the fortune 50 to working within the budget needs of small businesses.

What we're most proud of, however, is our work for the community. MSI has sponsored and contributed to various open source initiatives. We've contributed intellectual capital pro bono to various working groups and security organizations.

Our goal with each engagement is to preach security philosophy, transfer knowledge to client stakeholders, and to build a long-term relationship steeped in trust, understanding, and open communication.