

WhiteHat Arsenal 1.06 Beta Released

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/secprog/2002-05/0002.html>

From: Jeremiah Grossman (jeremiah@whitehatsec.com)

Date: 05/21/02

Date: Mon, 20 May 2002 16:33:38 -0700

From: Jeremiah Grossman <jeremiah@whitehatsec.com>

To: secprog@securityfocus.com

WhiteHat Arsenal 1.06 Beta Release

Free download available from:

<http://community.whitehatsec.com/>

What's new in WhiteHat Arsenal:

Four weeks have passed since the last release of WhiteHat Arsenal. WhiteHat has spent that time killing various bugs and upgrading features. WHArsenal 1.06 Beta, is now faster, easier to use, and contains some new feature enhancements.

Among the several minor changes, you'll notice Forced Browsing has been fitted with an HTTP Response Code lookup utility. This utility allows the user to look up the meaning of any HTTP Response code found in the HTTP/1.1 RFC. Encoding/Encrypting encoding has its own string manipulation field. You'll also notice a new HTTP Fix-up option to help with HTTP compliance. Also worth noting is an integrated Bug and Feedback submission form. This allows bug and feedback notification to happen easier. Remember we need all the feedback we can get to make WHArsenal the best web application security product available. Documentation on WHArsenal usage is also now part of the package.

New Screen shots available.

Quick Update:

- HTTP Response Code Lookup
- Interface Changes
- Encoding/Encryption entry fields.
- HTTP Fix Option.
- Feedback and Bug Fix forms.
- Faster Spider. The last releases of Spider had a "sleep 2" in the code. This has now been removed so expect a 2 second improvement per request while spidering.
- Documentation now included within WHArsenal.

* See changelog in the package for more detailed information.

WhiteHat Arsenal is designed to be the next generation of professional web application security audit software. Architected from the ground up to be a generic web application security productivity tool, WhiteHat Arsenal provides security professionals and web application developers access to the tools they need to make the job of securing web applications faster and easier than ever before.

Currently, for even the most experienced security professionals, it is cumbersome if not impossible to quickly and efficiently execute most known web application attacks without resorting to quickly written custom utilities. Writing custom utilities during a penetration test or formal security review is a waste of time; a security professional's time should be focused on actually identifying vulnerabilities and resolving them. Unfortunately, penetration testers and web application developers alike lack effective tools to test common, let alone hard to find, security weaknesses. As a result, many mission critical web applications are inadequately protected against the increasingly prevalent threat of malicious attacks.

Many experienced information security professionals agree that currently available web security scanners, which scan only for known vulnerabilities, achieve only limited success at best. Furthermore, these types of tools often result in an enormous overflow of false positives resulting in wasted time and effort. WhiteHat Security understands these frustrating shortcomings of the existing tools and the increased need for securing the Internet's web applications. WhiteHat Arsenal is poised to revolutionize the manner in which web applications are penetration tested and secured.

WhiteHat Arsenal possesses a powerful suite of GUI–Browser based web security tools. These endowments make WhiteHat Arsenal capable of completing painstaking web security penetration test work faster and more effectively than any tool currently available. Imagine having the ability to quickly customize and execute just about any web security attack, and having those penetration attempts logged in XML format for later reporting or analysis.

WhiteHat Arsenal makes it possible to quickly focus attention on HTML forms, to easily view their inputs, (even the hidden fields), and modify them in seconds. It can be utilized to rapidly uncover a vast a number of vulnerabilities in any web application by providing the ability to perform any of the following attacks faster than ever before:

Perform the following attacks:

- Cross–Site Scripting (XSS)
- Parameter Tampering
- Cookie Poisoning
- URL Manipulation
- CGI Directory Traversal
- Direct OS Commanding
- Meta Character Injection

SecurityFocus SecProg: WhiteHat Arsenal 1.06 Beta Released

SQL Command Injection
HTTP Request Header Manipulation
HTTP Request Method Manipulation
Protocol Manipulation

and many more variants and combinations...

WhiteHat Arsenal is about increasing the effectiveness of web application security testing and audits, saving huge amounts of time in the process. WhiteHat Security is on a mission to improve the way in which people build, secure and penetration test web applications.

The WhiteHat Arsenal download is available from:

<http://community.whitehatsec.com/>

Users must be registered to download (takes 30 seconds).

WhiteHat Arsenal Features

Session Manager:

WhiteHat Arsenal logs all HTTP Request activities in either XML or HTML format. This allows for the presentation of log data to be easier to understand, analyze and report on. The Session Manager keeps log files organized with an easy to use Session Management system. Create, Edit, Delete sessions as well as individual log files. Session Manager makes web security easier by allowing organization of multiple independent tasks.

Spidering:

- Page Characteristics Logging XML Logging
- Web Application Description XML Logging
- Session Based
- Spider Continuation
- Results Limiter
- Image Counter

*Full HTTP Support

*Enhanced Features

Ripper:

- Allows on-the-fly editing of HTML Forms.
- Request/Response header viewing and editing.
- Request/Response Display HTTP Headers ON|OFF Support
- Advanced control over HTTP requests.
- HTTP Request XML Logging
- Session Based
- 302/301 Support w/ Auto Interface Update
- WH HTML Proxy

*Full HTTP Support

*Enhanced Features

SecurityFocus SecProg: WhiteHat Arsenal 1.06 Beta Released

Forced Browsing:

Find hidden directories, log files, and backup files which may contain useful information quickly, easily and efficiently.

- Common Directory forcing
- Common Logfile Forcing
- Backup file suffix forcing
- Session Based
- Response String Searching Support
- Response Code Look up integration.

*Full HTTP Support

*Enhanced Features

Response Codes:

Look up the meaning of a particular HTTP Response Code or view a list of all HTTP response codes according to the HTTP/1.1 RFC.

Utilities:

Quickly encode or decode strings, authentication credentials or anything else, to reverse engineer applications, perform various discovery methodologies, or pervasive attacks.

- URL Encode/Decode
- Base64 Encode/Decode
- ROT13
- MD4
- MD5
- SHA-1

*Full HTTP Support

(Ability to modify and manipulate just about every aspect of an HTTP Request.)

- Path
- Protocol
- Port
- Content
- Method
- Version
- Web Auth
- Request Headers
- HTTP Fixup Feature
- Browser Mimic

Enhanced Features:

- Easy to use Web-GUI Interface.

(Only a recent web browser is required to use everything in WhiteHat Arsenal.)

SecurityFocus SecProg: WhiteHat Arsenal 1.06 Beta Released

- Browser Mimicking
(Mimic the HTTP Request behavior of a standard web browser.)
- WH Proxy
(Remain within WhiteHat Arsenal, having the ability to traverse web sites while modifying HTTP requests).
- HTTP Fix
Use libwhisker to "fix" an HTTP Request before the request is sent. The fix includes things such as adding a "Host" header, "Content-Length" header, etc. Helpful for HTTP compliance.

Support:

- Web Authentication
- SSL

WebAppSec Community

<http://community.whitehatsec.com/>

WhiteHat Security has created a new web application security information portal and web security community. A place for people to read related news, access up-to-date information, and talk web app sec stuff. The archives are full of web application security presentations, whitepapers, news, etc.

WhiteHat Security is asking all those interested to submit news and other related information (please be specific to web app sec). Also if you know any good web app sec white paper's and/or PPT material, please post those submissions as well.

-
- **Previous message:** [Steve: "Call For Papers – Canadian Security & Intelligence Conference \(CSIC\)"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)