CIS 700/002 : Special Topics : NIKTO

Swathi G Nayak

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

2017/03/03

NIKTO

“Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.”

https://cirt.net/Nikto2

Web server vulnerability

- Password stored in web code, e.g. cookies
- Allow traverse within directories
- Ability to execute programs or scripts
- Ability to bypass URL checking
- Improperly patched and configured web servers

Cookies and Session ID

- Cookies: A set of key-value pairs that a web site can store in your browser
- Browser sends the cookie in all subsequent requests to the same web site until it expires
- Session ID: Maintained on the client or server or both
- Commonly stored in Cookies or browser URL requests

A. Haeberlen, Z. Ives: CIS 455/555 Internet and Web systems

Cookies and Session ID

- **Vulnerabilities**:
- Session ID exposed in URL
- Session ID not invalidated on Logout
- Same Session ID for every session created
- Session Timeouts are not implemented correctly

Secure Directory

- Vulnerability due to exposure of a reference to an internal object
- Example: file, directory, database key as in URL or as a FORM parameter

Improperly Configured

- Points of concern: application, frameworks, application server, web server, database server, and platform

URL Checking

- Applications need to perform access control checks each time pages are accessed.
- Attacker could gain access to unauthorized URLs, without logging in and exploit the vulnerability

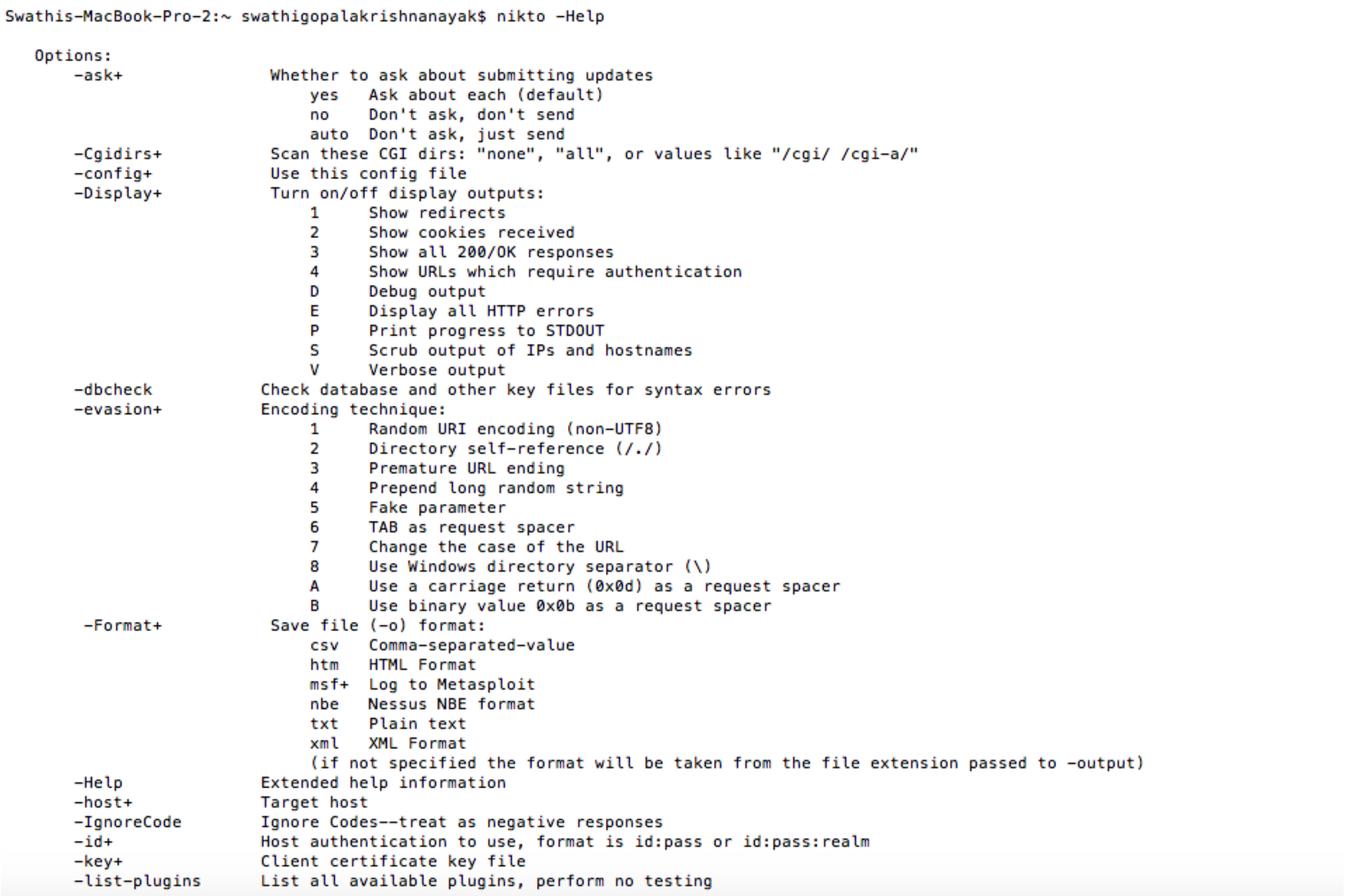
Using Nikto

- Examine a web server to identify security problems proactively, and fixing them
- Information gathered: Web server, Vulnerable web applications, Information leaking pages etc
- Osvdb numbers of the issues for further analysis

How Nikto Works

- Nikto uses a database of URL's for its scan requests
- Detection technique is far from stealthy
- Examines the full response from servers

Options Supported



```
Swathis-MacBook-Pro-2:~ swathigopalakrishnanayak$ nikto -Help

   Options:
       -ask+                   Whether to ask about submitting updates
                                   yes   Ask about each (default)
                                   no    Don't ask, don't send
                                   auto  Don't ask, just send
       -Cgidirs+               Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+                Use this config file
       -Display+               Turn on/off display outputs:
                                   1     Show redirects
                                   2     Show cookies received
                                   3     Show all 200/OK responses
                                   4     Show URLs which require authentication
                                   D     Debug output
                                   E     Display all HTTP errors
                                   P     Print progress to STDOUT
                                   S     Scrub output of IPs and hostnames
                                   V     Verbose output
       -dbcheck               Check database and other key files for syntax errors
       -evasion+              Encoding technique:
                                   1     Random URI encoding (non-UTF8)
                                   2     Directory self-reference (/./)
                                   3     Premature URL ending
                                   4     Prepend long random string
                                   5     Fake parameter
                                   6     TAB as request spacer
                                   7     Change the case of the URL
                                   8     Use Windows directory separator (\)
                                   A     Use a carriage return (0x0d) as a request spacer
                                   B     Use binary value 0x0b as a request spacer
        -Format+               Save file (-o) format:
                                   csv   Comma-separated-value
                                   htm   HTML Format
                                   msf+  Log to Metasploit
                                   nbe   Nessus NBE format
                                   txt   Plain text
                                   xml   XML Format
                                   (if not specified the format will be taken from the file extension passed to -output)
       -Help                  Extended help information
       -host+                 Target host
       -IgnoreCode            Ignore Codes--treat as negative responses
       -id+                   Host authentication to use, format is id:pass or id:pass:realm
       -key+                  Client certificate key file
       -list-plugins          List all available plugins, perform no testing
```

Demo

Two different Servers

- Application 1: Custom built using python+flask
- Application 2: Open source web application with vulnerabilities

Web application

- https://github.com/nswathi/Nikto-demo

Install Nikto

- Mac Users: ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)" < /dev/null 2> /dev/null
- Ubuntu users:

  Download Nikto from https://cirt.net/nikto2/
  Unzip folder: go to Programs
  Command Line: perl nikto.pl

Status Codes

- 200: Status ok
- 400: bad Request
- 405: Method not supported(often arise with the POST method)
- 403: Forbidden
- 404: File not Found

Assignment

- Capture errors due to SQL injection on mutillidae
- Capture the complete set of response received but disable nikto attempting to guess a 404 page
- Analyze one of the Authentication Bypass Error
- Generate one custom test case

Thank you

1. https://github.com/nswathi/Nikto-demo/
2. https://cirt.net/Nikto2
3. http://126kr.com/article/lii75sdq1
4. http://searchsecurity.techtarget.com/video/How-to-use-Nikto-to-scan-for-Web-server-vulnerabilities
5. http://www.binarytides.com/nikto-hacking-tutorial-beginners/
6. http://blog.pusheax.com/2012/01/nikto-web-vulnerability-scanner.html
7. https://www.madirish.net/547
8. http://www.guru99.com/web-security-vulnerabilities.html#3