Sparty : A Frontpage and Sharepoint Auditing Tool

Aditya K Sood (@AdityaKSood)
BlackHat Arsenal USA - 2013
SecNiche Security Labs

About Me

- Senior Security Practitioner – IOActive
- PhD Candidate at Michigan State University
  - Worked for Armorize, COSEINC, KPMG and others.
  - Active Speaker at Security conferences
    - » DEFCON, RSA, SANS, HackInTheBox, OWASP AppSec, BruCon and others
  - LinkedIn - http ***://www.linkedin.com/in/adityaks***
  - ***Twitter: @AdityaKSood***
  - Website: ***http://www.secniche.org***

Sparty Overview !

- Open source tool written in python
- Assist penetration testers in routine jobs
- Written in python 2.6
- Libraries support
  - import urllib2
  - import re
  - import os, sys
  - import optparse
  - import httplib
- Use Sparty with Back Track for penetration testing purposes
  - Works on other flavors also

Frontpage Overview !

- Frontpage Flavors
  - Microsoft IIS (.dll)
  - Unix (.exe)

- Frontpage Access File Settings
  - service.pwd → frontpage passwords
  - service.grp → list of groups
  - administrators.pwd → passwords for administrators
  - authors.pwd → authors password
  - users.pwd for → users password

Frontpage Overview (cont.) !

- Frontpage DLLs
  - _vti_bin/_vti_adm/admin.dll → administrative tasks
  - _vti_bin/_vti_aut/author.dll → authoring FrontPage webs
  - _vti_bin/shtml.dll → browsing component

- Frontpage virtual directories
  - vti_bin
  - _vti_bin_vti_aut
  - _vti_bin_vti_adm
  - _vti_pvt
  - _vti_cnf
  - _vti_txt
  - _vti_log.

```
/document root
   /_vti_bin
      shtml.dll
      /_vti_adm
         admin.dll
      /_vti_aut
         author.dll
```

Frontpage Configuration Flaws !

- RPC service querying
- Command execution using author.dll via RPC
- File uploading through RPC interface
- Information disclosure in _vti_pvt, _vti_bin, etc.
- Information disclosure in HTTP Response Headers
- Directory indexing
- Exposed password files in the web directories

Sparty helps the penetration tester to gather information and to perform manual analysis later on !

Sharepoint Configuration Flaws !

- Exposed services on the Internet
- Excessive user Access [admin.asmx, permissions.asmx]
- Information disclosure in HTTP Response Headers
- Publicly available insecure deployments [GOOGLE/SHODAN]
- Directory indexing
- Some of the manual tests:
  - Third-party plugin checks
  - Inappropriate deployment of sharepoint services

Sparty helps the penetration tester to gather information and to perform manual analysis later on !

Sparty Functionalities !

- Sharepoint and Frontpage Version Detection
- Dumping Password from Exposed Configuration Files
- Exposed Sharepoint/Frontpage Services Scan
- Exposed Directory Check
- Installed File and Access Rights Check
- RPC Service Querying
- File Enumeration
- File Uploading Check

Sparty Options!

```
# python sparty_beta_v_0.1.py -h
        ------------------------------------------------------------------

         _|_|_|    _|_|_|     _|_|    _|_|_|    _|_|_|_|_|  _|      _|
        _|        _|    _|  _|    _|  _|    _|      _|        _|  _|
          _|_|    _|_|_|    _|_|_|_|  _|_|_|        _|          _|
              _|  _|        _|    _|  _|    _|      _|          _|
        _|_|_|    _|        _|    _|  _|    _|      _|          _|

        SPARTY : Sharepoint/Frontpage Security Auditing Tool!
        Authored by: Aditya K Sood |{0kn0ck}@secniche.org  | 2013
        Twitter:     @AdityaKSood
        Powered by: IOActive Labs !

        ------------------------------------------------------------
Usage: sparty_beta_v_0.1.py [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit

  Frontpage::
    -f FRONTPAGE, --frontpage=FRONTPAGE
                        <FRONTPAGE = pvt | bin> -- to check acces
                        on frontpage standard files in vti or bin

  Sharepoint::
    -s SHAREPOINT, --sharepoint=SHAREPOINT
                        <SHAREPOINT = forms | layouts | catalog>
                        access permissions on sharepoint standard
                        forms or layouts or catalog directory!

  Mandatory::
    -u URL, --url=URL   target url to scan with proper structure

Information Gathering and Exploit::
  -v FINGERPRINT, --http_fingerprint=FINGERPRINT
                        <FINGERPRINT = ms_sharepoint | ms_frontpage> --
                        fingerprint sharepoint or frontpage based on HTTP
                        headers!
  -d DUMP, --dump=DUMP
                        <DUMP = dump | extract> -- dump credentials from
                        default sharepoint and frontpage files (configuration
                        errors and exposed entries)!
  -l DIRECTORY, --list=DIRECTORY
                        <DIRECTORY = list | index> -- check directory listing
                        and permissions!
  -e EXPLOIT, --exploit=EXPLOIT
                        EXPLOIT = <rpc_version_check | rpc_service_listing |
                        rpc_file_upload | author_config_check |
                        author_remove_folder> -- exploit vulnerable
                        installations by checking RPC querying, service
                        listing and file uploading
  -i SERVICES, --services=SERVICES
                        SERVICES = <serv | services> -- checking exposed
                        services !

General::
  -x EXAMPLES, --examples=EXAMPLES
                        running usage examples !
```

Version Fingerprinting !

```
# python sparty.py -v ms_frontpage -u http://www.target-front.com

[+] extracting frontpage version from default file : (['"4.0.2.2717"']):

[+] frontpage fingerprinting module completed !

# python sparty.py -v ms_sharepoint -u https://www.target-share.com

[+] configured sharepoint version is  : (12.0.0.6211)
[-] sharepoint load balancing ability could not be determined using HTTP header : X-SharepointHealthScore !
[-] sharepoint diagnostics ability could not be determined using HTTP header : SPRequestGuid !

[+] sharepoint fingerprinting module completed !
```

Dumping Passwords !

```
# python sparty.py -d dump -u http://www.target-front.com

[+]-------------------------------------------------------------------------------------------------!
[+] dumping (service.pwd | authors.pwd | administrators.pwd | ws_ftp.log) files if possible!
[+]-------------------------------------------------------------------------------------------------!

[+] dumping contents of file located at : (http://www.target-front.com/_vti_pvt/service.pwd)

[+] dumping contents of file located at : (http://www.target-front.com/_vti_pvt/administrators.pwd)

[+] dumping contents of file located at : (http://www.target-front.com/_vti_pvt/authors.pwd)

[+] check the (__dump__.txt) file if generated !


[+] check for HTTP codes (200) for active list of accessible files or directories! (404) - Not exists | (403) - Forbidden !

[+] (password dumping) - module executed successfully !

# cat   dump _.txt
# -FrontPage-
target-front:Tagzan9yidZnI

# -FrontPage-
target-front:c/qfc.CTmiCAY

# -FrontPage-
target-front:c/qfc.CTmiCAY
```

Directories Check!

```
# python sparty.py -l list -u http://www.target-front.com

[+]-------------------------------------------------------------------------!
[+] auditing frontpage directory permissions (forbidden | index | not exist)!
[+]-------------------------------------------------------------------------!

[+] (http://www.target-front.com/_vti_pvt/) - (200)
[+] (http://www.target-front.com/_vti_bin/) - (200)
[+] (http://www.target-front.com/_vti_log/) - (200)
[+] (http://www.target-front.com/_vti_cnf/) - (200)
[-] (http://www.target-front.com/_vti_bot) - (404)
[+] (http://www.target-front.com/_vti_bin/_vti_adm) - (200)
[+] (http://www.target-front.com/_vti_bin/_vti_aut) - (200)
[+] (http://www.target-front.com/_vti_txt/) - (200)

[+] check for HTTP codes (200) for active list of accessible files or directories!

[+] (directory check) - module executed successfully !
```

Scanning Access Permissions (1) !

```
# python sparty_beta_v_0.1.py -f pvt -u http://www.target-front.com

        ----------------------------------------------------------------
[+] fetching information from the given target : (http://www.target-front.com)
[+] target responded with HTTP code: (200)
[+] target is running server: (YTS/1.20.28)

[+]-------------------------------------------------------------!
[+] auditing '/_vti_pvt/' directory for sensitive information !
[+]-------------------------------------------------------------!

[+] (http://www.target-front.com/_vti_pvt/authors.pwd) - (200)
[+] (http://www.target-front.com/_vti_pvt/administrators.pwd) - (200)
[+] (http://www.target-front.com/_vti_pvt/users.pwd) - (200)
[+] (http://www.target-front.com/_vti_pvt/service.pwd) - (200)
[+] (http://www.target-front.com/_vti_pvt/service.grp) - (200)
[+] (http://www.target-front.com/_vti_pvt/bots.cnf) - (200)
[+] (http://www.target-front.com/_vti_pvt/service.cnf) - (200)
[+] (http://www.target-front.com/_vti_pvt/access.cnf) - (200)
[+] (http://www.target-front.com/_vti_pvt/writeto.cnf) - (200)
[-] (http://www.target-front.com/_vti_pvt/botsinf.cnf) - (404)
[+] (http://www.target-front.com/_vti_pvt/doctodep.btr) - (200)
[+] (http://www.target-front.com/_vti_pvt/deptodoc.btr) - (200)
[+] (http://www.target-front.com/_vti_pvt/linkinfo.cnf) - (200)
[-] (http://www.target-front.com/_vti_pvt/services.org) - (404)
[-] (http://www.target-front.com/_vti_pvt/structure.cnf) - (404)
[+] (http://www.target-front.com/_vti_pvt/svcacl.cnf) - (200)
[-] (http://www.target-front.com/_vti_pvt/uniqperm.cnf) - (404)
[-] (http://www.target-front.com/_vti_pvt/service/lck) - (404)
[+] (http://www.target-front.com/_vti_pvt/frontpg.lck) - (200)

[+] check for HTTP codes (200) for active list of accessible files or directories! (404)

[+] (pvt file access) - module executed successfully !
```

Scanning Access Permissions (2) !

```
# python sparty.py -s layouts -u http://www.target-share.com

[+]----------------------------------------------------------------!
[+] auditing sharepoint '/_layouts/' directory for access permissions !
[+]----------------------------------------------------------------!

[+] (http://www.target-share.com/_layouts/aclinv.aspx) - (200)
[+] (http://www.target-share.com/_layouts/addrole.aspx) - (200)
[+] (http://www.target-share.com/_layouts/AdminRecycleBin.aspx) - (200)
[+] (http://www.target-share.com/_layouts/AreaNavigationSettings.aspx) - (200)
[+] (http://www.target-share.com/_Layouts/AreaTemplateSettings.aspx) - (200)
[+] (http://www.target-share.com/_Layouts/AreaWelcomePage.aspx) - (200)
[+] (http://www.target-share.com/_layouts/associatedgroups.aspx) - (200)
[+] (http://www.target-share.com/_layouts/bpcf.aspx) - (200)
[+] (http://www.target-share.com/_Layouts/ChangeSiteMasterPage.aspx) - (200)
[+] (http://www.target-share.com/_layouts/create.aspx) - (200)
[+] (http://www.target-share.com/_layouts/editgrp.aspx) - (200)
[+] (http://www.target-share.com/_layouts/editprms.aspx) - (200)
[+] (http://www.target-share.com/_layouts/groups.aspx) - (200)
[+] (http://www.target-share.com/_layouts/help.aspx) - (200)
[-] (http://www.target-share.com/_layouts/images/) - (403)
[+] (http://www.target-share.com/_layouts/listedit.aspx) - (200)
[+] (http://www.target-share.com/_layouts/ManageFeatures.aspx) - (200)
[+] (http://www.target-share.com/_layouts/ManageFeatures.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mcontent.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mngctype.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mngfield.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mngsiteadmin.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mngsubwebs.aspx) - (200)
[+] (http://www.target-share.com/_layouts/mngsubwebs.aspx?view=sites) - (200)
[+] (http://www.target-share.com/_layouts/mobile/mbllists.aspx) - (200)
[+] (http://www.target-share.com/_layouts/MyInfo.aspx) - (200)
[+] (http://www.target-share.com/_layouts/MyPage.aspx) - (200)
[+] (http://www.target-share.com/_layouts/MyTasks.aspx) - (200)
[+] (http://www.target-share.com/_layouts/navoptions.aspx) - (200)
```

Exposed Services Check !

```
# python sparty.py -i services -u https://www.target-share.com


[+]-------------------------------------------------------!
[+] checking exposed services in the frontpage/sharepoint  directory!
[+]-------------------------------------------------------!

[-] (https://www.target-share.com/_vti_bin/Admin.asmx) - (404)
[+] (https://www.target-share.com/_vti_bin/alerts.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/dspsts.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/forms.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/Lists.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/people.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/Permissions.asmx) - (200)
[-] (https://www.target-share.com/_vti_bin/search.asmx) - (404)
[+] (https://www.target-share.com/_vti_bin/UserGroup.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/versions.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/Views.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/webpartpages.asmx) - (200)
[+] (https://www.target-share.com/_vti_bin/webs.asmx) - (200)
[-] (https://www.target-share.com/_vti_bin/spsdisco.aspx) - (404)
[-] (https://www.target-share.com/_vti_bin/AreaService.asmx) - (404)
[-] (https://www.target-share.com/_vti_bin/BusinessDataCatalog.asmx) - (404)
[-] (https://www.target-share.com/_vti_bin/ExcelService.asmx) - (404)
[+] (https://www.target-share.com/_vti_bin/SharepointEmailWS.asmx) - (200)
[-] (https://www.target-share.com/_vti_bin/spscrawl.asmx) - (404)
[+] (https://www.target-share.com/_vti_bin/spsearch.asmx) - (200)
[-] (https://www.target-share.com/_vti_bin/UserProfileService.asmx) - (404)
[+] (https://www.target-share.com/_vti_bin/WebPartPages.asmx) - (200)

[+] check for HTTP codes (200) for active list of accessible files or directories!

[+] (exposed services check) - module executed successfully !
```

RPC Querying !

```
# python sparty.py -e rpc_version_check -u https://www.target-front.com

[+]-------------------------------------------------------------------------!
[+] auditing frontpage RPC service                                          !
[+]-------------------------------------------------------------------------!

[+] Sending HTTP GET request to - (https://www.target-front.com/_vti_bin/shtml.exe/_vti_rpc) for verifying whether RPC is listening !
[+] target is listening on frontpage RPC - (200) !

[+] Sending HTTP POST request to retrieve software version - (https://www.target-front.com/_vti_bin/shtml.exe/_vti_rpc)
[+] target accepts the request - (method= server version) | (200) !

<html><head><title>vermeer RPC packet</title></head>

<body>

<p>method= server version:5.0.2.2634

<p>status=

<ul>

<li>status=917506

<li>osstatus=0

<li>msg=The method ' server version' is not recognized.

<li>osmsg=

</ul>
```

RPC Service Listing !

```
# python sparty_beta_v_0.1.py -e rpc_service_listing -u http://www.target-front.com

        ------------------------------------------------------------
[+] fetching information from the given target : (http://www.target-front.com)
[+] target responded with HTTP code: (200)
[+] target is running server: (Apache/2.2.3 (Red Hat))

[+]-------------------------------------------------------------------------!
[+] auditing frontpage RPC service for fetching listing                      !
[+]-------------------------------------------------------------------------!

[+] Sending HTTP POST request to retrieve service listing  - (http://www.target-front.com/_vti_bin/shtml.exe/_vti_rpc)
[+] target accepts the request - (method=list+services:3.0.2.1076&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:3.0.2.1076&service_name=.html)

[+] target accepts the request - (method=list+services:4.0.2.471&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:4.0.2.471&service_name=.html)

[+] target accepts the request - (method=list+services:4.0.2.0000&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:4.0.2.0000&service_name=.html)

[+] target accepts the request - (method=list+services:5.0.2.4803&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:5.0.2.4803&service_name=.html)

[+] target accepts the request - (method=list+services:5.0.2.2623&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:5.0.2.2623&service_name=.html)

[+] target accepts the request - (method=list+services:6.0.2.5420&service_name=) | (200) !
[+] check file for contents - (__service-list__.txtmethod=list+services:6.0.2.5420&service_name=.html)

[*] ---------------------------------------------------------------------------------------
[+] Sending HTTP POST request to retrieve service listing  - (http://www.target-front.com/_vti_bin/shtml.dll/_vti_rpc)
[-] server responds with bad status !
[*] ---------------------------------------------------------------------------------------
```

Try Other Options of Your Own ☺

Sparty : Next Version !

- Integration of publicly available vulnerabilities
- Detection of more advanced payloads for checking admin.dll
- Additional checks and tests against author.dll
- Extended payloads

Project Details !

- Projects page: *http://sparty.secniche.org*
- Documentation: *http://sparty.secniche.org/usage.html*

Questions and Thanks !

- SecNiche Security Labs: *http://www.secniche.org*
- BlackHat USA Arsenal 2013 Team
- IOActive Inc.