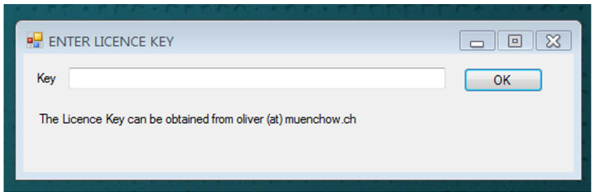
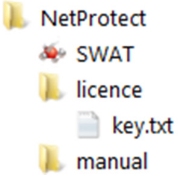
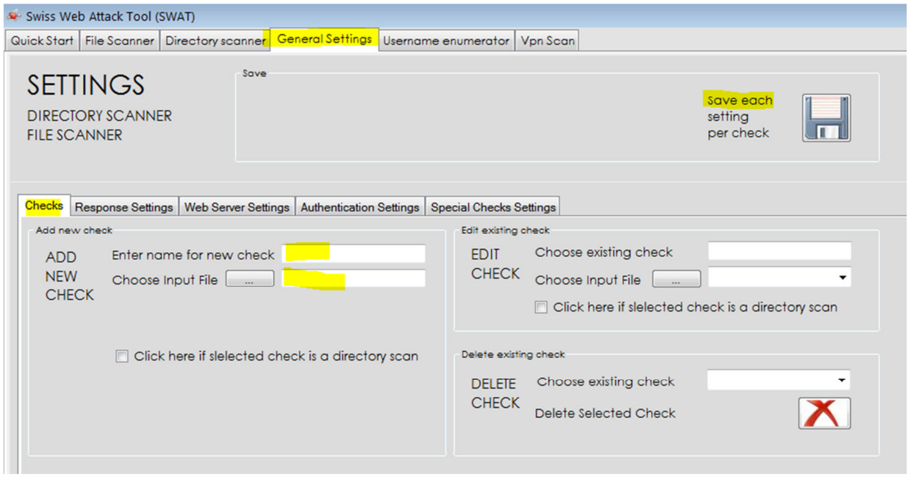
SWAT MANUAL

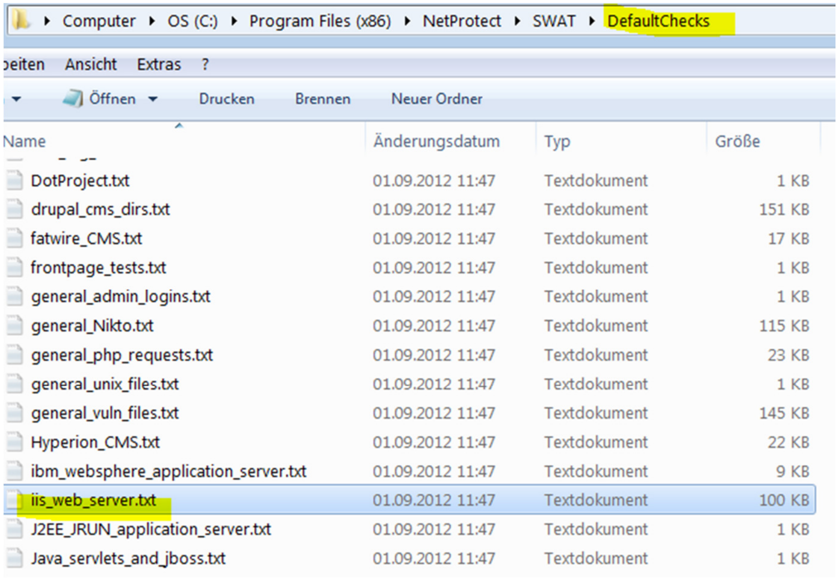
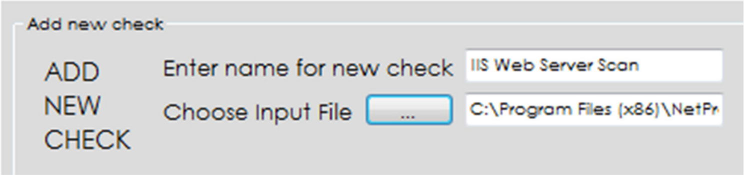
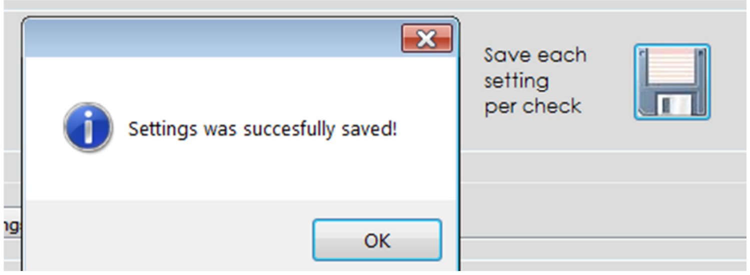
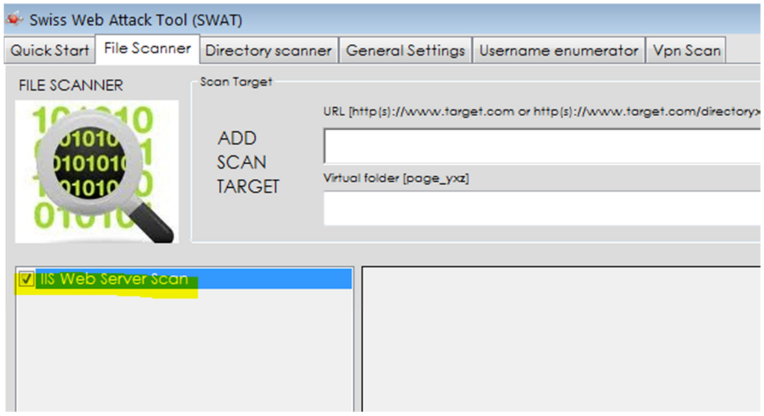
LICENCE KEY

Description	Screenshot
Before starting you will be asked to enter a licence key.	 ENTER LICENCE KEY Key OK The Licence Key can be obtained from oliver (at) muenchow.ch
The key file can be found within your installation folder or when you browse to the start menu → programs → netprotect → licence.	 NetProtect SWAT licence key.txt manual

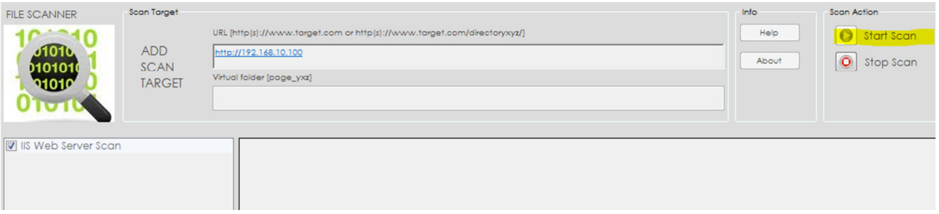
START FILE SCAN

The file scanner is looking for specific files (f.ex. /iissamples/sdk/asp/docs/CodeBrws.asp is looking for the file CodeBrws.asp in a given directory).

Description	Screenshot
To set up a new file scan template go to general settings, then within "Checks" choose a name for the new check and browse to the file.	 Swiss Web Attack Tool (SWAT) Quick Start | File Scanner | Directory scanner | General Settings | Username enumerator | Vpn Scan SETTINGS DIRECTORY SCANNER FILE SCANNER Save Save each setting per check Checks | Response Settings | Web Server Settings | Authentication Settings | Special Checks Settings Add new check ADD NEW CHECK Enter name for new check Choose Input File ... □ Click here if selelected check is a directory scan Edit existing check EDIT CHECK Choose existing check Choose Input File ... □ Click here if selelected check is a directory scan Delete existing check DELETE CHECK Choose existing check Delete Selected Check

Description	Screenshot
Assuming you want to test a IIS web server choose the iis_web_server.txt as the input file. This can be found in the default installation directory (f.ex. C:\Program Files (x86)\NetProtect \SWAT\DefaultChecks). Then give the check a name and save it (the save button can be used for all other settings as well).	 Computer ▸ OS (C:) ▸ Program Files (x86) ▸ NetProtect ▸ SWAT ▸ DefaultChecks beiten Ansicht Extras ? Öffnen Drucken Brennen Neuer Ordner Name · Änderungsdatum · Typ · Größe DotProject.txt · 01.09.2012 11:47 · Textdokument · 1 KB drupal_cms_dirs.txt · 01.09.2012 11:47 · Textdokument · 151 KB fatwire_CMS.txt · 01.09.2012 11:47 · Textdokument · 17 KB frontpage_tests.txt · 01.09.2012 11:47 · Textdokument · 1 KB general_admin_logins.txt · 01.09.2012 11:47 · Textdokument · 1 KB general_Nikto.txt · 01.09.2012 11:47 · Textdokument · 115 KB general_php_requests.txt · 01.09.2012 11:47 · Textdokument · 23 KB general_unix_files.txt · 01.09.2012 11:47 · Textdokument · 1 KB general_vuln_files.txt · 01.09.2012 11:47 · Textdokument · 145 KB Hyperion_CMS.txt · 01.09.2012 11:47 · Textdokument · 22 KB ibm_websphere_application_server.txt · 01.09.2012 11:47 · Textdokument · 9 KB iis_web_server.txt · 01.09.2012 11:47 · Textdokument · 100 KB J2EE_JRUN_application_server.txt · 01.09.2012 11:47 · Textdokument · 1 KB Java_servlets_and_jboss.txt · 01.09.2012 11:47 · Textdokument · 1 KB  Add new check ADD NEW CHECK Enter name for new check: IIS Web Server Scan Choose Input File ... C:\Program Files (x86)\NetPr  Settings was succesfully saved!
After the scan is saved It will later appear in the file scanner menu.	 Swiss Web Attack Tool (SWAT) Quick Start File Scanner Directory scanner General Settings Username enumerator Vpn Scan FILE SCANNER Scan Target ADD SCAN TARGET URL [http(s)://www.target.com or http(s)://www.target.com/directory Virtual folder [page_yxz] ☑ IIS Web Server Scan

<table>
<tr><th>Description</th><th>Screenshot</th></tr>
<tr><td>Let’s assume you want to scan a website https://www.target.com you just have to enter that website in the target section and then select the scan you want to start.</td><td>



FILE SCANNER

Scan Target

ADD SCAN TARGET

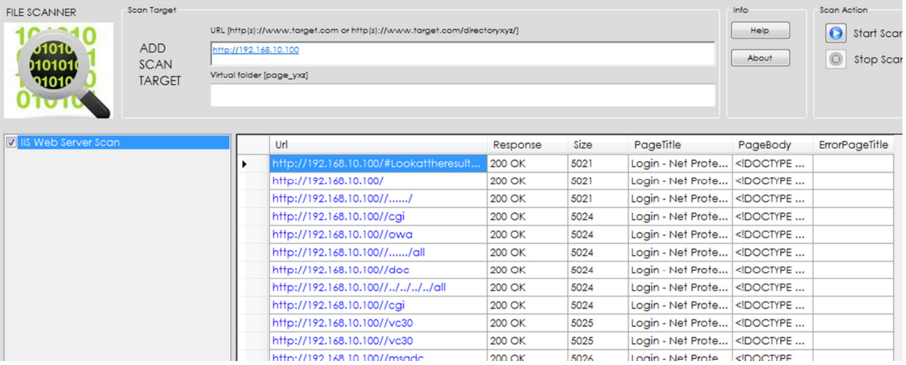
URL [http(s)://www.target.com or http(s)://www.target.com/directoryxyz/]

http://192.168.10.100

Virtual folder [page_yxz]

☑ IIS Web Server Scan

</td></tr>
<tr><td>By default the scanner will only display the 200 OK answers from the web server. In the result window you will also have the page size, title and body. All fields are sortable.</td><td>



FILE SCANNER

Scan Target

ADD SCAN TARGET

URL [http(s)://www.target.com or http(s)://www.target.com/directoryxyz/]

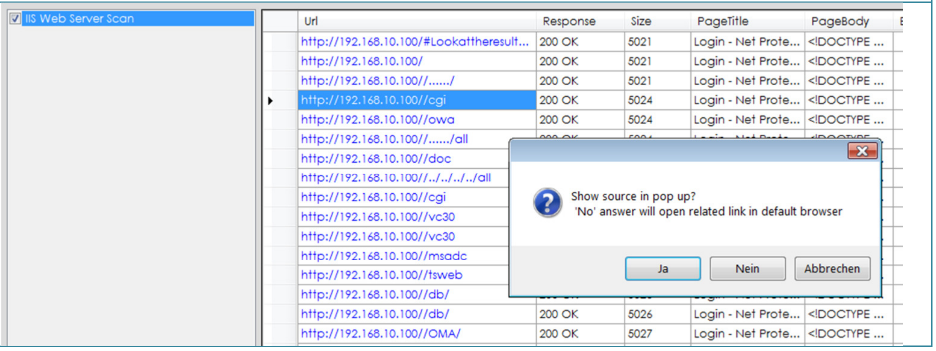
http://192.168.10.100

Virtual folder [page_yxz]

☑ IIS Web Server Scan

<table>
<tr><th>Url</th><th>Response</th><th>Size</th><th>PageTitle</th><th>PageBody</th><th>ErrorPageTitle</th></tr>
<tr><td>http://192.168.10.100/#Lookattheresult...</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100/</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//....../</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//cgi</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//owa</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//....../all</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//doc</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//../../../../all</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//cgi</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//vc30</td><td>200 OK</td><td>5025</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//vc30</td><td>200 OK</td><td>5025</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td><td></td></tr>
<tr><td>http://192.168.10.100//msadc</td><td>200 OK</td><td>5026</td><td>Login - Net Prote</td><td>&lt;!DOCTYPE</td><td></td></tr>
</table>

</td></tr>
<tr><td>If you want to look at the result you can either open it in the browser (press “no” or a pop up.</td><td>



☑ IIS Web Server Scan

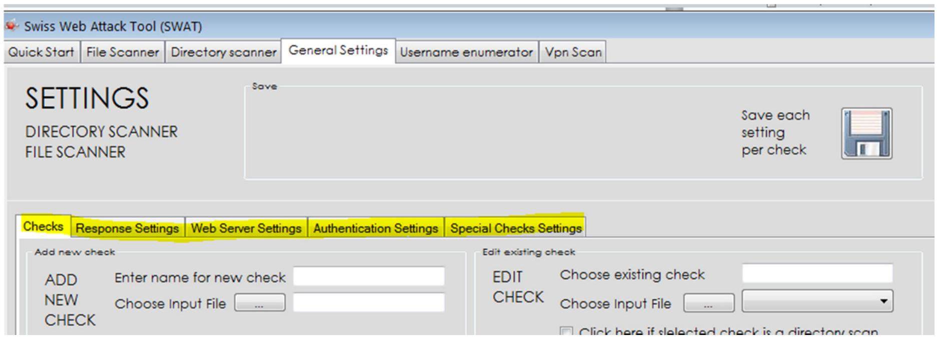
<table>
<tr><th>Url</th><th>Response</th><th>Size</th><th>PageTitle</th><th>PageBody</th></tr>
<tr><td>http://192.168.10.100/#Lookattheresult...</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100/</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100//....../</td><td>200 OK</td><td>5021</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100//cgi</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100//owa</td><td>200 OK</td><td>5024</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100//....../all</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//doc</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//../../../../all</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//cgi</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//vc30</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//vc30</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//msadc</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//tsweb</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//db/</td><td></td><td></td><td></td><td></td></tr>
<tr><td>http://192.168.10.100//db/</td><td>200 OK</td><td>5026</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
<tr><td>http://192.168.10.100//OMA/</td><td>200 OK</td><td>5027</td><td>Login - Net Prote...</td><td>&lt;!DOCTYPE ...</td></tr>
</table>

Show source in pop up?
'No' answer will open related link in default browser

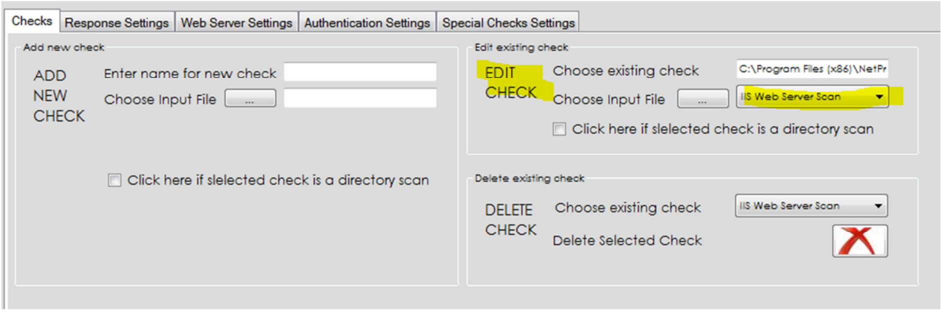
</td></tr>
</table>

FILE SCAN OPTIONS – Response Settings

All settings have to saved per Check – they don't apply in general. So you might have a separate setting for each check. By default the scanner will only look for the 200 OK message, make a request on port 80 or 443 (depends if you enter http or https in the target URL) and make all reuests with the GET method.

Description	Screenshot
As mentioned before the Web File scanner will only look for 200 OK answers from the webserver to determine if a file exists or not. But you have a lot of extra options that you can configure.	

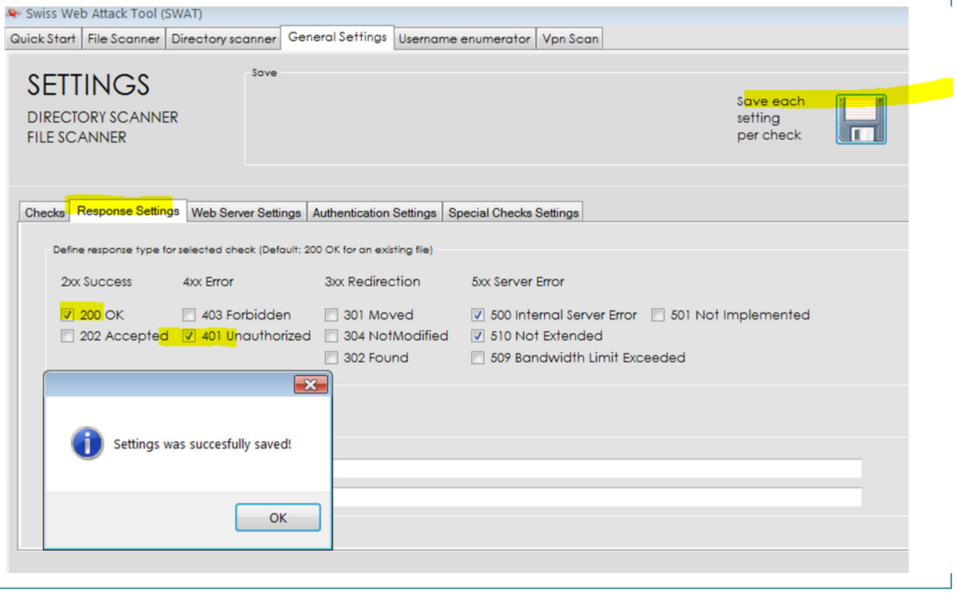
Set different Status Codes

Description	Screenshot
Lets assume you want to also look for other answers from the IIS web server. You have to select "edit check" and select the check you want to edit.	

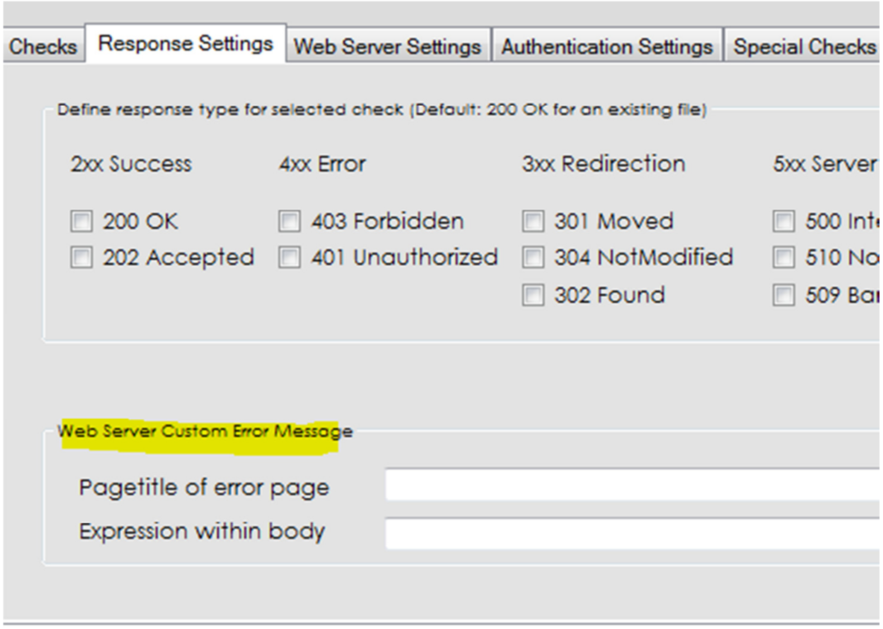
C:\Program Files (x86)\NetPr

IIS Web Server Scan

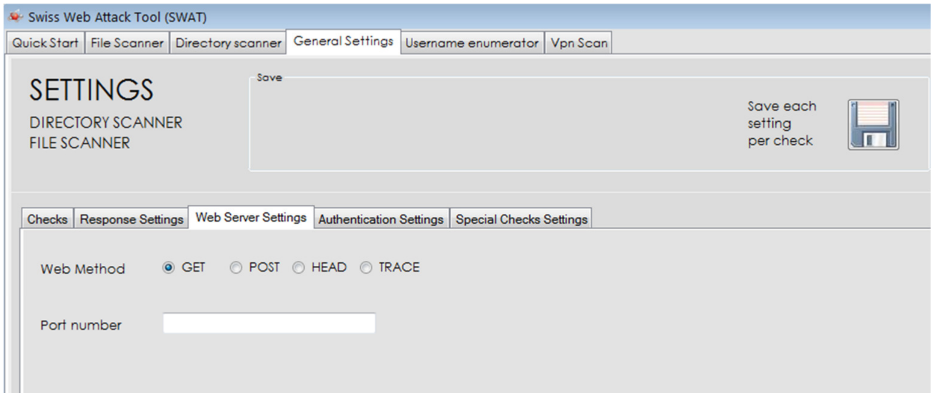
IIS Web Server Scan

Description	Screenshot
Next you click on the response settings tab and select the response code you wanna look for. Use then the save button to save the check again.	 Swiss Web Attack Tool (SWAT) Quick Start | File Scanner | Directory scanner | General Settings | Username enumerator | Vpn Scan SETTINGS DIRECTORY SCANNER FILE SCANNER Save Save each setting per check Checks | Response Settings | Web Server Settings | Authentication Settings | Special Checks Settings Define response type for selected check (Default: 200 OK for an existing file) 2xx Success: ☑ 200 OK, ☐ 202 Accepted 4xx Error: ☐ 403 Forbidden, ☑ 401 Unauthorized 3xx Redirection: ☐ 301 Moved, ☐ 304 NotModified, ☐ 302 Found 5xx Server Error: ☑ 500 Internal Server Error, ☐ 501 Not Implemented, ☑ 510 Not Extended, ☐ 509 Bandwidth Limit Exceeded Settings was succesfully saved! OK

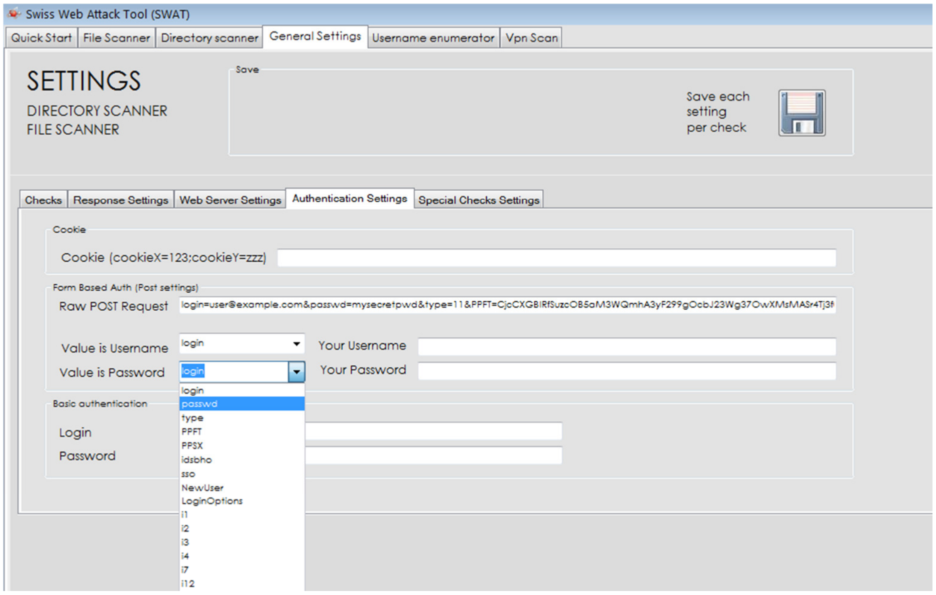
Catch custom error pages

Description	Screenshot
Some web servers will give you a 200 OK error message with some custom text. This page you want to ignore. To do that you need to tell the scanner some part of the custom error page title **or** some text from the page itself (like "we are sorry but this page does not exist")	 Checks | Response Settings | Web Server Settings | Authentication Settings | Special Checks Define response type for selected check (Default: 200 OK for an existing file) 2xx Success: ☐ 200 OK, ☐ 202 Accepted 4xx Error: ☐ 403 Forbidden, ☐ 401 Unauthorized 3xx Redirection: ☐ 301 Moved, ☐ 304 NotModified, ☐ 302 Found 5xx Server: ☐ 500 Int, ☐ 510 No, ☐ 509 Ba Web Server Custom Error Message Pagetitle of error page Expression within body

FILE SCAN OPTIONS – Set the Port and the Web Method

Description	Screenshot
If you want to scan a different port or select a different method for each request you can specify this here.	 Swiss Web Attack Tool (SWAT) Quick Start File Scanner Directory scanner General Settings Username enumerator Vpn Scan Save Checks Response Settings Web Server Settings Authentication Settings Special Checks Settings SETTINGS DIRECTORY SCANNER FILE SCANNER Save each setting per check Web Method ● GET ○ POST ○ HEAD ○ TRACE Port number

FILE SCAN OPTIONS – Authentication Settings

Description	Screenshot
You can set form based authentication values, basic auth values or just send the "authenticated" session cookie with each request. To use the form based authentication just paste the body from the raw HTTP POST or GET request in the marked field and then the SWAT which value is the username or the password. Then set your username/password.	 Swiss Web Attack Tool (SWAT) Quick Start File Scanner Directory scanner General Settings Username enumerator Vpn Scan Save Checks Response Settings Web Server Settings Authentication Settings Special Checks Settings login passwd type PPFT PPSX idsbho sso NewUser LoginOptions i1 i2 i3 i4 i7 i12 SETTINGS DIRECTORY SCANNER FILE SCANNER Save each setting per check Cookie Cookie (cookieX=123;cookieY=zzz) Form Based Auth (Post settings) Raw POST Request login=user@example.com&passwd=mysecretpwd&type=11&PPFT=CjcCXGBIRfSuzcOB5aM3WQmhA3yF299gOcbJ23Wg37OwXMsMASr4Tj3f Value is Username login Your Username Value is Password login Your Password Basic authentication Login Password

START DIRECTORY SCAN

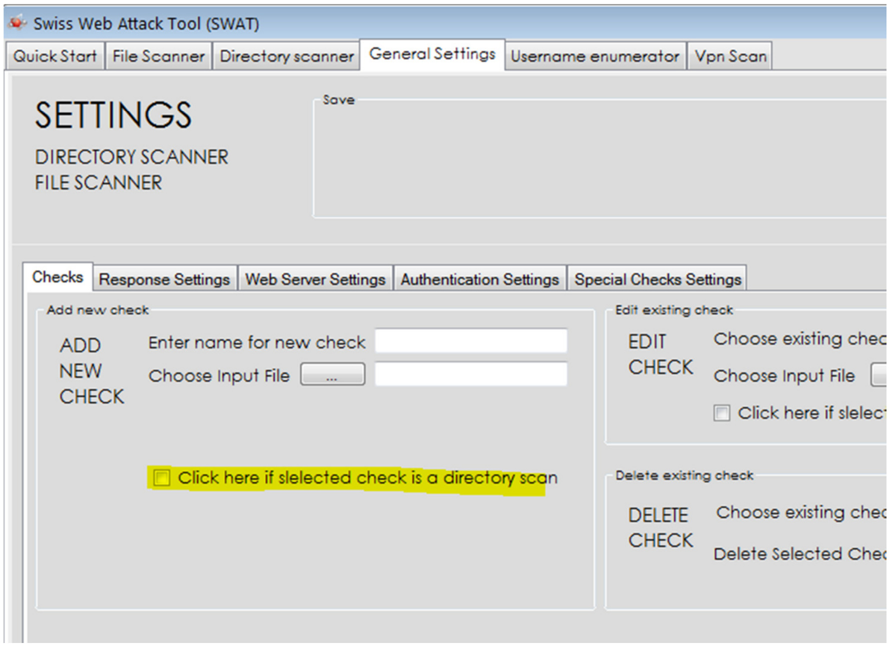
The directory scanner is looking for specific directories – not files (f.ex. /iissamples/sdk/asp/docs/).

<table>
<tr><th>Description</th><th>Screenshot</th></tr>
<tr><td>

To set up a new Dir scan template go to general settings, then within "Checks" choose a name for the new check and browse to the file.

The only difference to the web file scanner is that a 403 (forbidden) error message is indicating that the directory exists. So if you choose "click here if selected check is a directory scan" the scanner will only look for 403 messages by default.

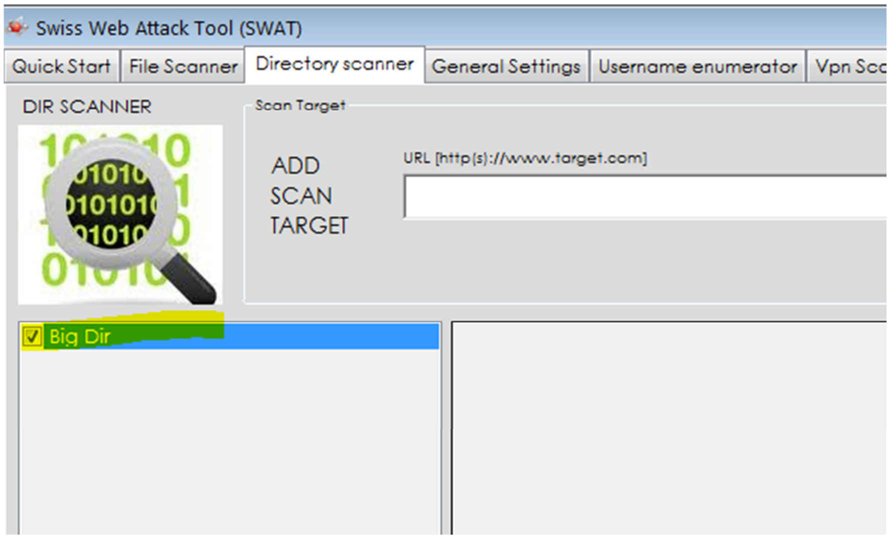
</td><td>



</td></tr>
<tr><td>

After selecting the option, that the check is a directory scan you will find the check within the directory scanner tab.

</td><td>



</td></tr>
</table>

USERNAME SCANNER

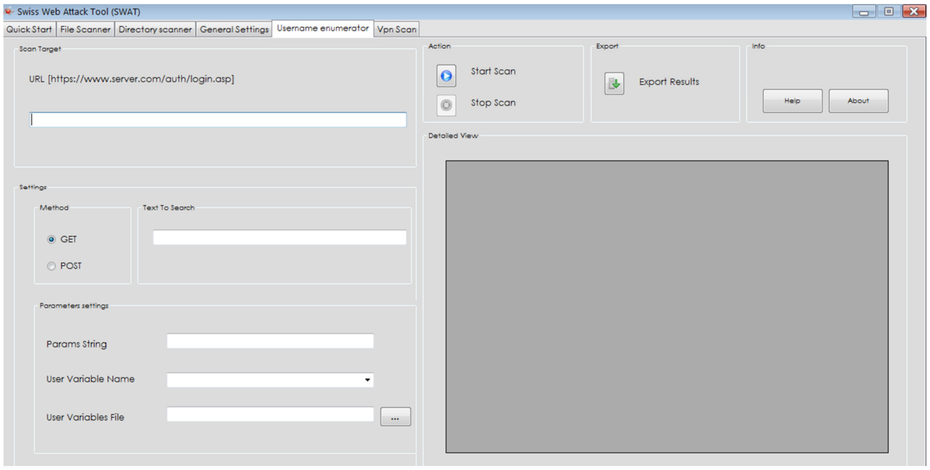
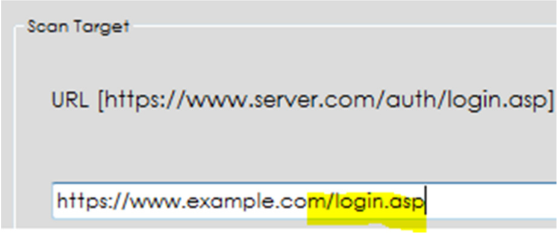
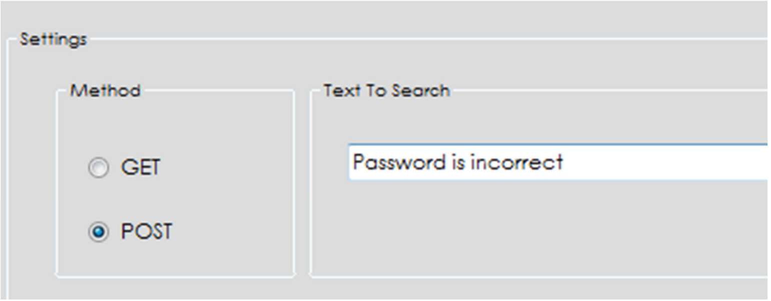
This tool is used to catch error messages when you login to a server and determine possible usernames. Let's assume you have an incorrect user/pwd you might get the following error:

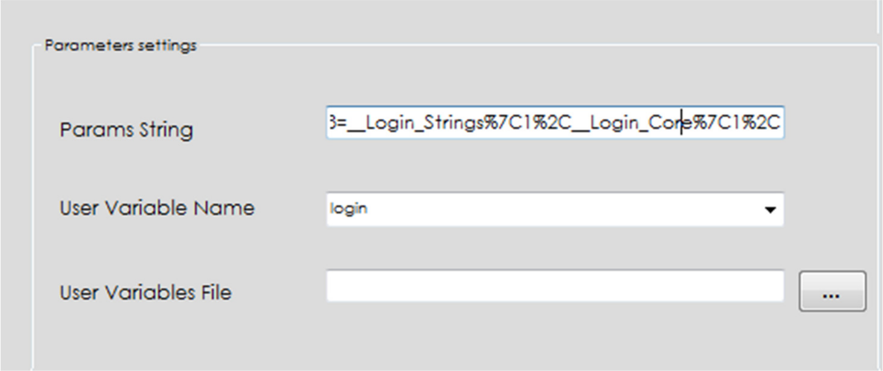
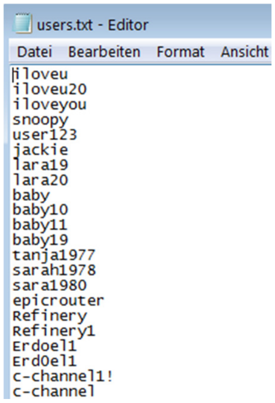
```
Incorrect login
```

Let's assume you have a correct user but an invalid password you might get this error:

```
Password is incorrect
```

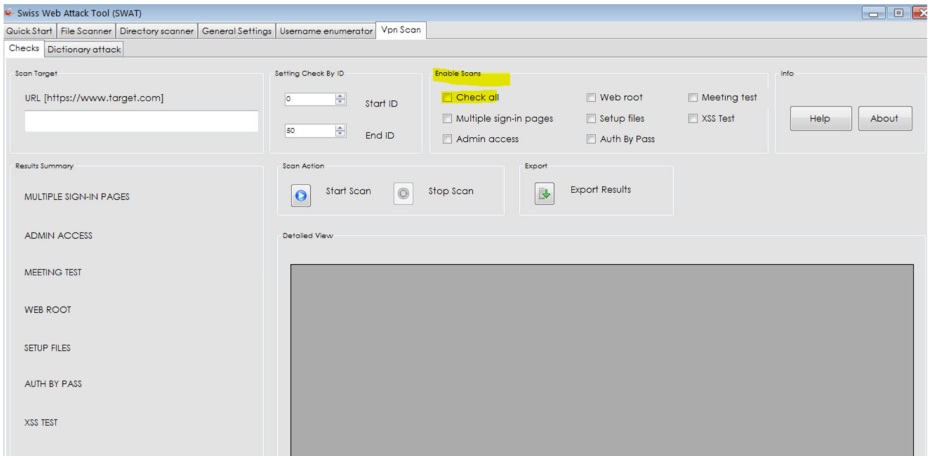
You know then that the username is correct.

Description	Screenshot
To get started open the username scanner tab.	 Swiss Web Attack Tool (SWAT) Quick Start File Scanner Directory scanner General Settings Username enumerator Vpn Scan Scan Target URL [https://www.server.com/auth/login.asp] Action Start Scan Stop Scan Export Export Results Info Help About Detailed View Settings Method Text To Search Parameters settings Params String User Variable Name User Variables File ... ● GET ○ POST
Then enter the URL of the target .	 https://www.example.com/login.asp
Next enter the text from the error message that appears, when the user exists but the password is wrong.	 ○ GET ● POST Password is incorrect

Description	Screenshot
Next you have to paste the POST request (just the body) in the field and select from the dropdown menu the variable, which is represents the user name.	 Parameters settings Params String: 3=__Login_Strings%7C1%2C__Login_Core%7C1%2C User Variable Name: login User Variables File:
Within the user variable file you can choose a list of possible usernames. SWAT comes with a user input file that you can use.	 iloveu iloveu20 iloveyou snoopy user123 jackie lara19 lara20 baby baby10 baby11 baby19 tanja1977 sarah1978 sara1980 epicrouter Refinery Refinery1 Erdoel1 Erd0el1 c-channel1! c-channel

VPN SCANNER

This tool targets multiple vulnerabilities and misconfiguration issues within a JUNIPER VPN web service.

Description	Screenshot
The easiest way to get started is choosing all tests and just enter the URL of the target.	 Swiss Web Attack Tool (SWAT) Quick Start File Scanner Directory scanner General Settings Username enumerator Vpn Scan Checks Dictionary attack Scan Target URL [https://www.target.com] Setting Check By ID Start ID End ID Enable Scans Info Help About Results Summary MULTIPLE SIGN-IN PAGES ADMIN ACCESS MEETING TEST WEB ROOT SETUP FILES AUTH BY PASS XSS TEST Scan Action Start Scan Stop Scan Export Export Results Detailed View Start ID: 0 End ID: 50 □ Check all □ Multiple sign-in pages □ Admin access □ Web root □ Setup files □ Auth By Pass □ Meeting test □ XSS Test