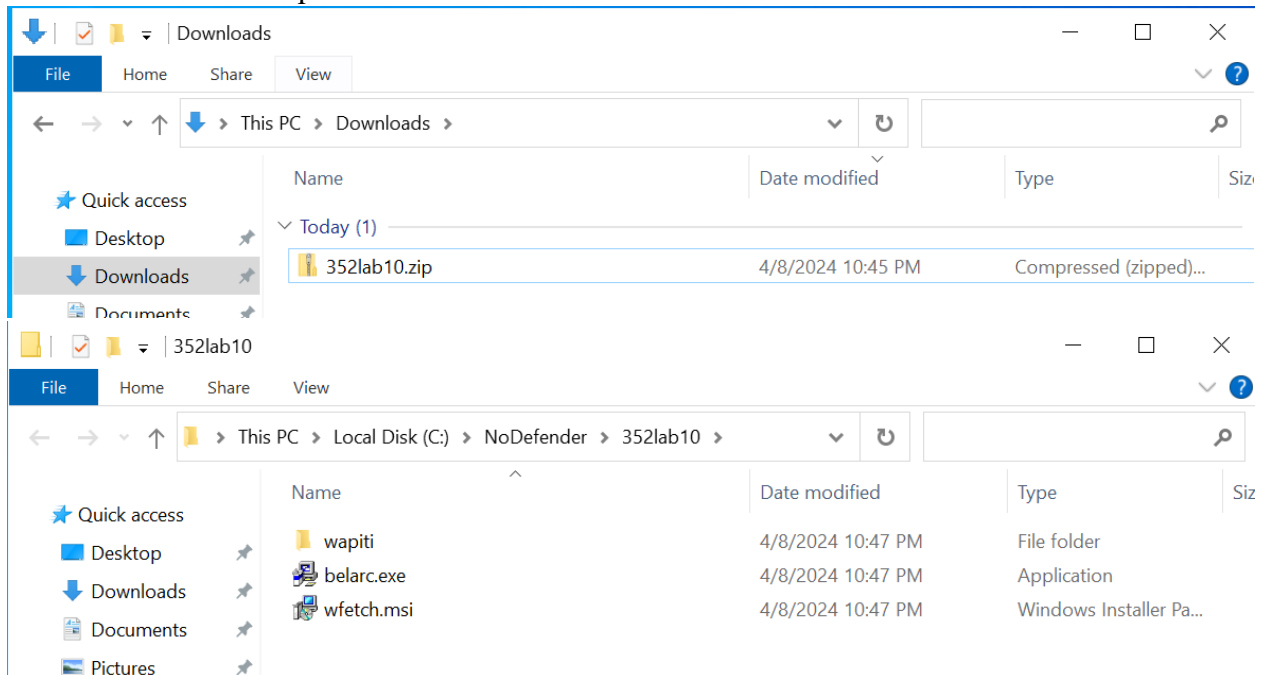
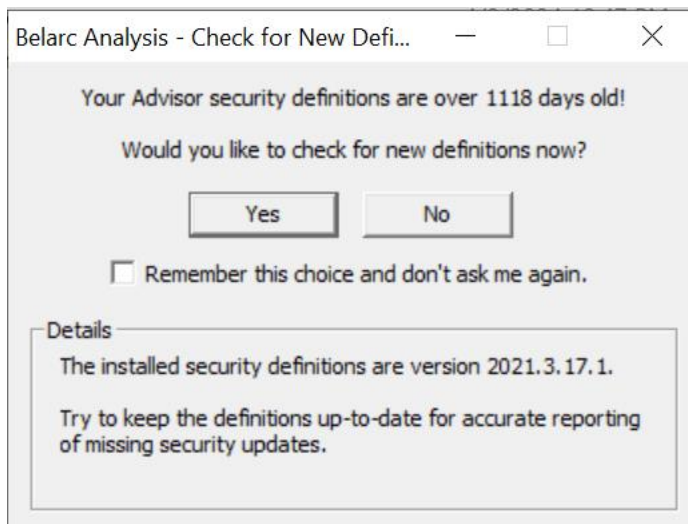


CYBR 352 Week 10 Lab


- Download 352lab10.zip file and extract it to 352lab10 folder in the NoDefender folder.



- Install Belarc Advisor and use Belarc Advisor to build a system profile.



Belarc Advisor

 Your Advisor security definitions have been updated.
(Version 2021.3.17.1 was updated to 2024.4.8.1)

OK



File | C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(WIN-S9N14MKS36J).html

The license associated with the Belarc Advisor product allows for **free personal home use only**. Use on computers in a corporate, educational, military or government installation is prohibited. See the [license agreement](#) for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. [Click here for more info.](#)

Belarc Advisor

Commercial and Government Products
Belarc SaaS Offering
Your Privacy
About Belarc

Scroll to section:
Software Licenses
Software Versions and Usage
Missing Updates
USB Storage Use
Hosted Virtual Machines
Network Map
Installed Hotfixes
Back to Top

	SECURITY BENCHMARK SCORE	VIRUS PROTECTION	SECURITY UPDATES
System Security Status	Unavailable	 Up-to-date	 2 missing

Computer Profile Summary

Computer Name: WIN-S9N14MKS36J (in WORKGROUP)
Profile Date: Monday, April 8, 2024 10:53:52 PM
Advisor Version: 9.7
Windows Logon: Administrator


Try BelManage, the Enterprise version of the Belarc Advisor

Operating System	System Model
Windows Server 2022 Datacenter (Evaluation Installation) Version 2009 (build 20348.587) Install Language: English (United States) System Locale: English (United States) Installed: 2/12/2024 8:29:07 PM Servicing Branch: Current Branch (CB) Boot Mode: UEFI with Secure Boot disabled	VMware, Inc. VMWare7.1 System Serial Number: VMWare-56 4d dc 73 b8 83 73 ce-37 d9 99 35 51 91 2a 4e Enclosure Type: Other

Copyright 2000-2020, Belarc, Inc. All rights reserved.
Legal notice. U.S. Patents 8473607, 6085229, 5665951 and Patents pending.

- Install Wfetch and use Wfetch to query Web servers:

WFetch 1.4 (x86) Setup

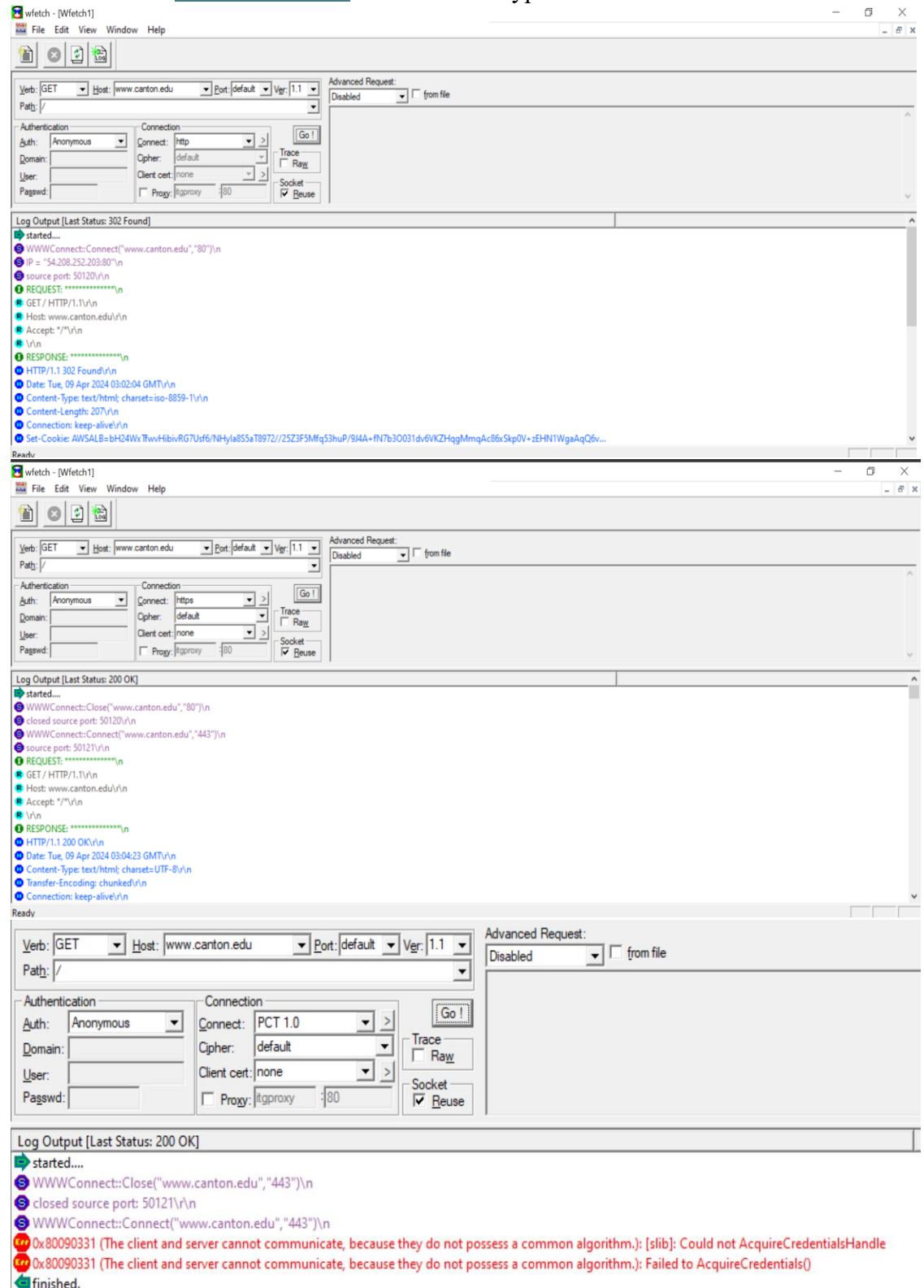


Completing the WFetch 1.4 (x86) Setup Wizard

Click the Finish button to exit the Setup Wizard.

< Back Finish Cancel

- Run Wfetch on www.canton.edu with different types of connections.



Verb: GET Host: www.canton.edu Port: default Ver: 1.1		Advanced Request: Disabled <input type="checkbox"/> from file	
Path: /			
Authentication Auth: Anonymous Domain: User: Passwd:		Connection Connect: SSL 2.0 Cipher: default Client cert: none <input type="checkbox"/> Proxy: httpproxy :80	
		Go ! Trace <input type="checkbox"/> Raw Socket <input checked="" type="checkbox"/> Reuse	
Log Output [Last Status: 200 OK]			
<p>started....</p> <p>WWWConnect::Connect("www.canton.edu", "443")\n</p> <p>0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): [slib]: Could not AcquireCredentialsHandle</p> <p>0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): Failed to AcquireCredentials()</p> <p>finished.</p>			

Verb: GET Host: www.canton.edu Port: default Ver: 1.1		Advanced Request: Disabled <input type="checkbox"/> from file	
Path: /			
Authentication Auth: Anonymous Domain: User: Passwd:		Connection Connect: SSL 3.0 Cipher: default Client cert: none <input type="checkbox"/> Proxy: httpproxy :80	
		Go ! Trace <input type="checkbox"/> Raw Socket <input checked="" type="checkbox"/> Reuse	
Log Output [Last Status: 200 OK]			
<p>started....</p> <p>WWWConnect::Connect("www.canton.edu", "443")\n</p> <p>0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): [slib]: Could not AcquireCredentialsHandle</p> <p>0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): Failed to AcquireCredentials()</p> <p>finished.</p>			

Verb: GET Host: www.canton.edu Port: default Ver: 1.1				Advanced Request: Disabled <input type="checkbox"/> from file	
Path: /					
Authentication		Connection		Go !	
Auth: Anonymous		Connect: TLS 3.1	>	Trace <input type="checkbox"/> Raw	
Domain:		Cipher: default		Socket <input checked="" type="checkbox"/> Reuse	
User:		Client cert: none	>		
Passwd:		<input type="checkbox"/> Proxy: itgproxy :80			
Log Output [Last Status: 200 OK]					
<pre>\t</div>\n </footer>\r\n \r\n \r\n </div>\r\n <script>\r\n var navigation1 = responsiveNav(".nav-1");\r\n \r\n \t var navigation2 = responsiveNav(".nav-2", {\r\n insert: "before",\r\n \t\tlabel: "Q"\r\n });\r\n </script>\r\n </body>\r\n </html>\r\n finished.</pre>					

- Run Wfetch on zero.webappsecurity.com with different types of connections.

The screenshot shows the Wfetch application window. At the top, the 'Verb' is set to 'GET', 'Host' is 'zero.webappsecurity.com', 'Port' is 'default', and 'Ver' is '1.1'. The 'Path' is '/'. Below this, the 'Authentication' section has 'Auth' set to 'Anonymous', with empty fields for 'Domain', 'User', and 'Passwd'. The 'Connection' section has 'Connect' set to 'http', 'Cipher' set to 'default', and 'Client cert' set to 'none'. There is a checkbox for 'Proxy' set to 'itgproxy' on port '80'. To the right, there is a 'Go !' button, a 'Trace' checkbox, and a 'Socket Reuse' checkbox which is checked. On the far right, there is a tab labeled 'Advanced' and a button labeled 'Disabled'. Below the configuration fields is a 'Log Output [Last Status: 200 OK]' section. The log output shows a series of JavaScript code snippets being fetched, each preceded by a 'D' icon. The final line of the log is 'finished.' with a green arrow icon.

Verb: GET Host: zero.webappsecurity.com Port: default Ver: 1.1 Path: /

Authentication: Auth: Anonymous Domain: User: Passwd:

Connection: Connect: http Cipher: default Client cert: none Proxy: itgproxy :80

Go ! Trace Raw Socket Reuse

Log Output [Last Status: 200 OK]

```
D \r\n
D $.each(footerLinks, function(linkId, link) {\r\n
D   attachClickHandler('span[id="" + linkId + "']", function(event) {\r\n
D     event.preventDefault();\r\n
D     if (link.absolute) {\r\n
D       window.location.href = link.page;\r\n
D     } else {\r\n
D       window.location.href = path + link.page + ".html";\r\n
D     }\r\n
D   });\r\n
D });\r\n
D </script>\r\n
D </body>\r\n
D </html>\r\n
D finished.
```

Verb: GET Host: zero.webappsecurity.com Port: default Ver: 1.1 Path: /

Authentication: Auth: Anonymous Domain: User: Passwd:

Connection: Connect: https Cipher: default Client cert: none Proxy: ffigproxy :80

Advanced Request: Disabled from fi

Go !

Trace ☐ Raw

Socket ☒ Reuse

Log Output [Last Status: 200 OK]

```
R Host: zero.webappsecurity.com\r\n
R Accept: */*\r\n
R \r\n
I RESPONSE: *****\n
H HTTP/1.1 200 OK\r\n
H Date: Tue, 09 Apr 2024 03:16:05 GMT\r\n
H Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40\r\n
H Access-Control-Allow-Origin: *\r\n
H Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT\r\n
H ETag: "24c22-2c-44adde00"\r\n
H Accept-Ranges: bytes\r\n
H Content-Length: 44\r\n
H Content-Type: text/html\r\n
H \r\n
D <html><body><h1>It works!</h1></body></html>
finished.
```

Verb: GET Host: zero.webappsecurity.com Port: default Ver: 1.1 Path: /

Authentication: Auth: Anonymous Domain: User: Passwd:

Connection: Connect: PCT 1.0 Cipher: default Client cert: none Proxy: ffigproxy :80

Advanced Request: Disabled from file

Go !

Trace ☐ Raw

Socket ☒ Reuse

Log Output [Last Status: 200 OK]

```
started....
WWWConnect::Close("zero.webappsecurity.com","443")\n
closed source port: 50164\n
WWWConnect::Connect("zero.webappsecurity.com","443")\n
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): [slib]: Could not AcquireCredentialsHandle
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): Failed to AcquireCredentials()
finished.
```

Verb: GET	Host: zero.webappsecurity.com	Port: default	Ver: 1.1	Advanced Request: Disabled <input type="checkbox"/> from file	
Path: /					
Authentication		Connection			
Auth: Anonymous	Connect: SSL 2.0			Go !	
Domain:	Cipher: default			Trace <input type="checkbox"/> Raw	
User:	Client cert: none			Socket <input checked="" type="checkbox"/> Reuse	
Passwd:	<input type="checkbox"/> Proxy: itgproxy :80				

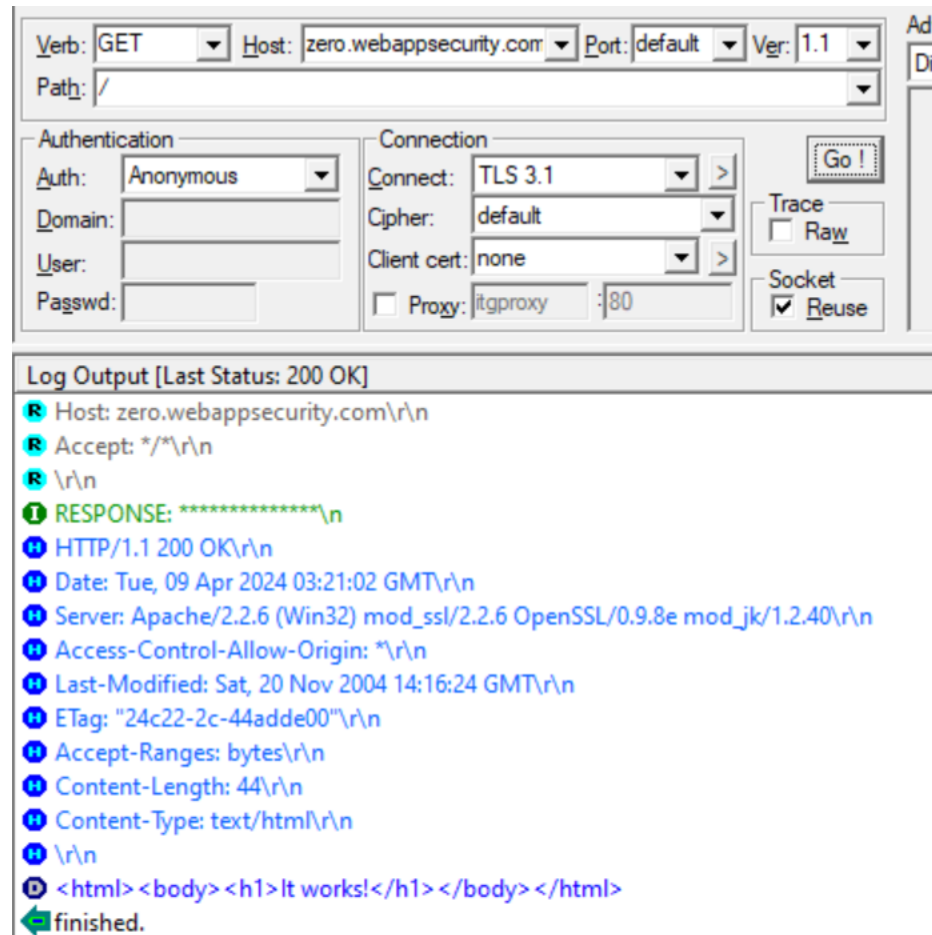
Log Output [Last Status: 200 OK]

```
started....
WWWConnect::Connect("zero.webappsecurity.com", "443")\n
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): [slib]: Could not AcquireCredentialsHandle
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): Failed to AcquireCredentials()
finished.
```

Verb: GET	Host: zero.webappsecurity.com	Port: default	Ver: 1.1	Advanced Request: Disabled <input type="checkbox"/> from file	
Path: /					
Authentication		Connection			
Auth: Anonymous	Connect: SSL 3.0			Go !	
Domain:	Cipher: default			Trace <input type="checkbox"/> Raw	
User:	Client cert: none			Socket <input checked="" type="checkbox"/> Reuse	
Passwd:	<input type="checkbox"/> Proxy: itgproxy :80				

Log Output [Last Status: 200 OK]

```
started....
WWWConnect::Connect("zero.webappsecurity.com", "443")\n
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): [slib]: Could not AcquireCredentialsHandle
0x80090331 (The client and server cannot communicate, because they do not possess a common algorithm.): Failed to AcquireCredentials()
finished.
```

- Use Wapiti to attempt Web application vulnerability scans:
 - o Wapiti www.testfire.net -m "-all,xss"

Administrator: C:\Windows\System32\cmd.exe

```
C:\NoDefender\352lab10\wapiti>wapiti www.testfire.net -m "-all,xss"
Wapiti-2.3.0 (wapiti.sourceforge.net)

Note
=====
This scan has been saved in the file C:\Users\Administrator\wapiti\scans\www.testfire.net.xml
You can use it to perform attacks without scanning again the web site with the "-k" parameter
[*] Loading modules:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentxss, mod_nikto
Problem with local nikto database.
Downloading from the web...

[+] Launching module xss
XSS vulnerability in http://www.testfire.net/search.jsp via injection in the parameter query
    Evil url: http://www.testfire.net/search.jsp?query=%3Cscript%3Ealert%28%27w10ccvr4ja%27%29%3C%2Fscript%3E
XSS vulnerability in http://www.testfire.net/util/serverStatusCheckService.jsp via injection in the parameter HostName
    Evil url: http://www.testfire.net/util/serverStatusCheckService.jsp?HostName=%3Cscript%3Ealert%28%27w5ufqirykz%27%29%3C%2Fscript%3E
XSS vulnerability in http://www.testfire.net/sendFeedback via injection in the parameter name
Evil request:
POST /sendFeedback HTTP/1.1
Host: www.testfire.net
Referer: http://www.testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded

cfile=comments.txt&name=%3Cscript%3Ealert%28%27we4sirzayr%27%29%3C%2Fscript%3E&email_addr=default&subject=default&comments=on&submit=%20Submit%20
```

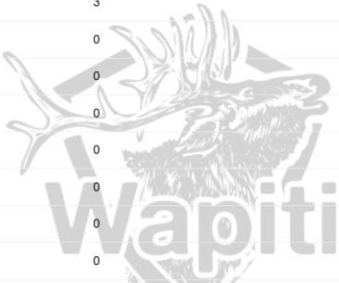
← ↻ ⓘ File | C:/Users/Administrator/wapiti/generated_report/index.html

Wapiti vulnerability report for www.testfire.net

Date of the scan: Tue, 09 Apr 2024 03:31:13 +0000. Scope of the web scanner : folder

Summary

Category	Number of vulnerabilities found
Cross Site Scripting	3
Htaccess Bypass	0
Backup file	0
SQL Injection	0
Blind SQL Injection	0
File Handling	0
Potentially dangerous file	0
CRLF Injection	0



- Wapiti www.canton.edu

```
Administrator: C:\Windows\System32\cmd.exe

C:\NoDefender\352lab10\wapiti>wapiti www.canton.edu
Wapiti-2.3.0 (wapiti.sourceforge.net)

Note
=====
This scan has been saved in the file C:\Users\Administrator\.wapiti\scans\www.canton.edu.xml
You can use it to perform attacks without scanning again the web site with the "-k" parameter
[*] Loading modules:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentxss, mod_n
ikto

[+] Launching module exec
[+] Launching module file
[+] Launching module sql
[+] Launching module xss
[+] Launching module blindsql
[+] Launching module permanentxss

Report
-----
A report has been generated in the file C:\Users\Administrator\.wapiti\generated_report
Open C:\Users\Administrator\.wapiti\generated_report\index.html with a browser to see this report.

C:\NoDefender\352lab10\wapiti>
```

