

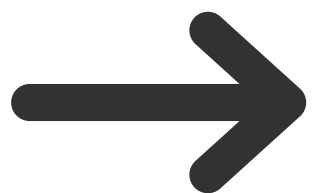
<https://certifications.tcm-sec.com/>

WEB APPLICATION PENETRATION TESTING TOOLS

A NON-DEFINITIVE GUIDE



**TCM
SECURITY
TEAM**





<https://certifications.tcm-sec.com/>



BURP SUITE PRO

No Web App pentester can go without Burp Suite - made all the more powerful with an array of freely available plug-ins. You can customize it as you need to in order to get the most from it.



Get it here:

<https://portswigger.net/burp>

<https://portswigger.net/bappstore>

<https://certifications.tcm-sec.com/>



CAIDO

Similar to Burp Suite, but free and open source. Use this lightweight tool to test and audit web apps.



Get it here:

<https://caido.io/download>

<https://certifications.tcm-sec.com/>



NMAP

Another freely available open source tool, you can use Nmap for network discovery and security auditing.



NMAP

Get it here:

<https://nmap.org/>



<https://certifications.tcm-sec.com/>



NESSUS VULNERABILITY SCANNER

This tool is a little more on the expensive side, but its power makes it worth the price tag. (P.S. - You can try it for free.)



Get it here:

<https://www.tenable.com/products/nessus>



<https://certifications.tcm-sec.com/>



NIKTO

Use nikto - a Perl-based pluggable web server & CGI scanner - to perform fast security or informational checks!

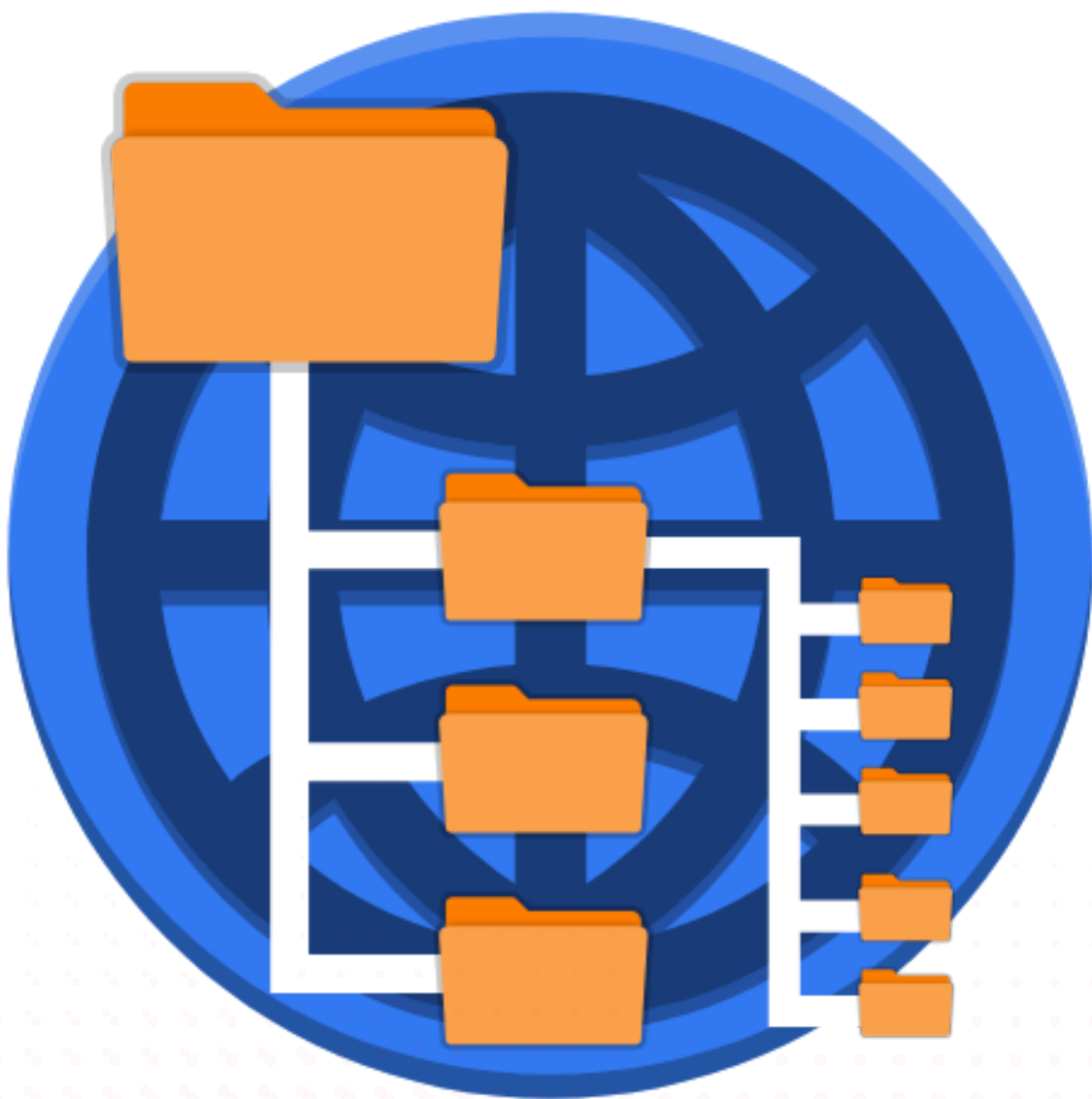


Get it here:

<https://www.kali.org/tools/dirbuster/>

DIRBUSTER

This one is a lot of fun! DirBuster is incredibly useful as a tool for brute-forcing directories and file names on servers.

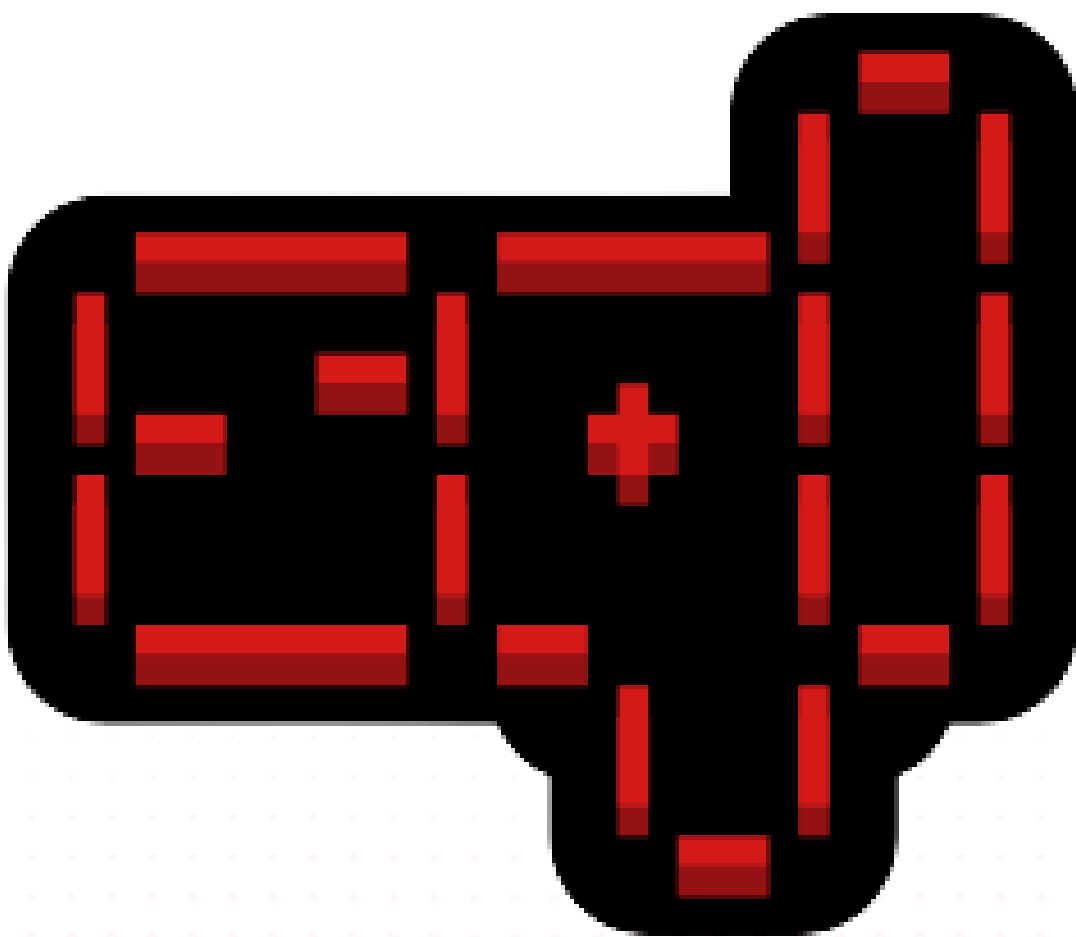


Get it here:

<https://www.kali.org/tools/dirbuster/>

SQLMAP

Just as its name suggests, sqlmap allows you to automate the process of finding and exploiting SQL injection (always a helpful vulnerability to come across.)



Get it here:
<https://sqlmap.org/>



<https://certifications.tcm-sec.com/>



METASPLOIT

For over 20 years, penetration testers have depended on Metasploit for vulnerability scanning, exploit development and execution, payload generation, and more.



Metasploit

Get it here:

<https://www.metasploit.com/>





<https://certifications.tcm-sec.com/>



QUALYS SSL SCANNER

This one is simple yet effective. The Qualys SSL Scanner analyzes the configuration of any publicly available web server.



Get it here:

<https://www.ssllabs.com/ssltest/>





<https://certifications.tcm-sec.com/>



BUILTWITH

This tool can help you see what a website is made out of - quickly and easily! Simply enter the domain you want to look at, and that's really it!

**built
with®**

Get it here:

<https://builtwith.com/>



WHATWEB

Finally, this last tool is also intended for domain analysis. It operates in a similar way to BuiltWith, and can help you identify SQL errors, web framework errors, and more!



INTRO TO WEB APP HACKING.



[HTTPS://CERTIFICATIONS.TCM-
SEC.COM/LIVE-
TRAINING/INTRODUCTION-TO-
WEB-APP-HACKING/](https://certifications.tcm-sec.com/live-training/introduction-to-web-app-hacking/)