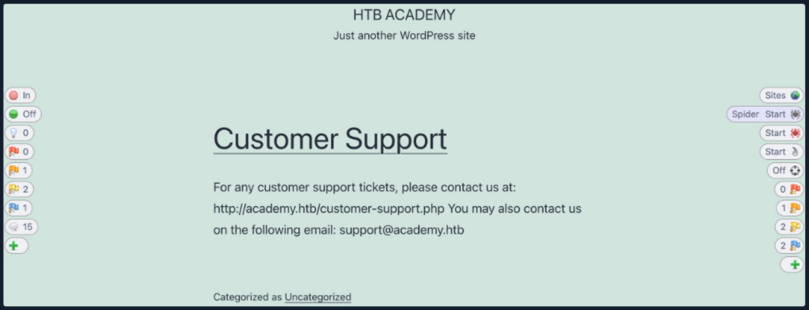
ZAP Scanner

ZAP also comes bundled with a Web Scanner similar to Burp Scanner. ZAP Scanner is capable of building site maps using ZAP Spider and performing both passive and active scans to look for various types of vulnerabilities.

Spider

Let's start with `ZAP Spider`, which is similar to the Crawler feature in Burp. To start a Spider scan on any website, we can locate a request from our History tab and select (`Attack>Spider`) from the right-click menu. Another option is to use the HUD in the pre-configured browser. Once we visit the page or website we want to start our Spider scan on, we can click on the second button on the right pane (`Spider Start`), which would prompt us to start the scan:



HTB ACADEMY
Just another WordPress site

Customer Support

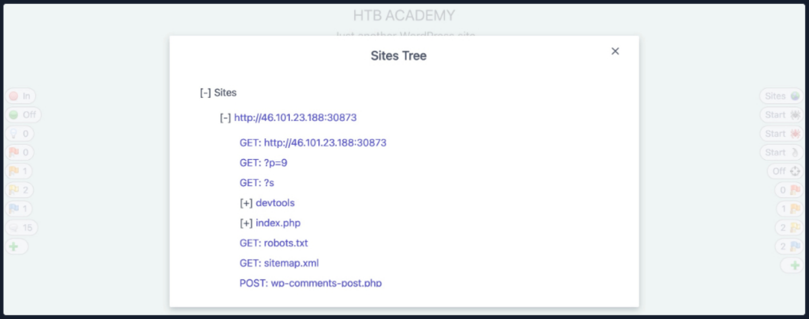
For any customer support tickets, please contact us at: http://academy.htb/customer-support.php You may also contact us on the following email: support@academy.htb

Categorized as Uncategorized

Note: When we click on the Spider button, ZAP may tell us that the current website is not in our scope, and will ask us to automatically add it to the scope before starting the scan, to which we can say 'Yes'. The Scope is the set of URLs ZAP will test if we start a generic scan, and it can be customized by us to scan multiple websites and URLs. Try to add multiple targets to the scope to see how the scan would run differently.

Note: In some versions of browsers, the ZAP's HUD might not work as intended.

Once we click on `Start` on the pop-up window, our Spider scan should start spidering the website by looking for links and validating them, very similar to how Burp Crawler works. We can see the progress of the spider scan both in the HUD on the `Spider` button or in the main ZAP UI, which should automatically switch to the current Spider tab to show the progress and sent requests. When our scan is complete, we can check the Sites tab on the main ZAP UI, or we can click on the first button on the right pane (`Sites Tree`), which should show us an expandable tree-list view of all identified websites and their sub-directories:



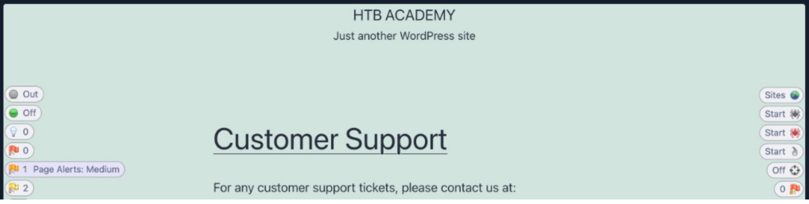
Sites Tree

```
[-] Sites
    [-] http://46.101.23.188:30873
        GET: http://46.101.23.188:30873
        GET: ?p=9
        GET: ?s
        [+] devtools
        [+] index.php
        GET: robots.txt
        GET: sitemap.xml
        POST: wp-comments-post.php
```

Tip: ZAP also has a different type of Spider called `Ajax Spider`, which can be started from the third button on the right pane. The difference between this and the normal scanner is that Ajax Spider also tries to identify links requested through JavaScript AJAX requests, which may be running on the page even after it loads. Try running it after the normal Spider finishes its scan, as this may give a better output and add a few links the normal Spider may have missed, though it may take a little bit longer to finish.

Passive Scanner

As ZAP Spider runs and makes requests to various end-points, it is automatically running its passive scanner on each response to see if it can identify potential issues from the source code, like missing security headers or DOM-based XSS vulnerabilities. This is why even before running the Active Scanner, we may see the alerts button start to get populated with a few identified issues. The alerts on the left pane shows us issues identified in the current page we are visiting, while the right pane shows us the overall alerts on this web application, which includes alerts found on other pages:



HTB ACADEMY
Just another WordPress site

Customer Support

For any customer support tickets, please contact us at:

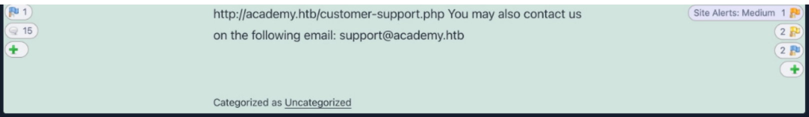
Cheat Sheet
Go to Questions

Table of Contents

My Workstation

OFFLINE

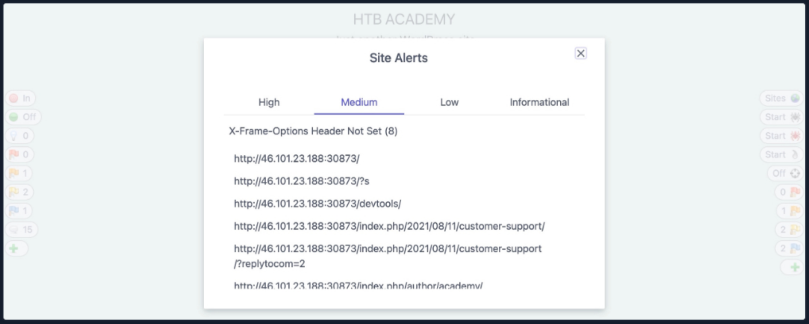
Start Instance
∞ / 1 spawns left



http://academy.htb/customer-support.php You may also contact us on the following email: support@academy.htb

Categorized as Uncategorized

We can also check the `Alerts` tab on the main ZAP UI to see all identified issues. If we click on any alert, ZAP will show us its details and the pages it was found on:

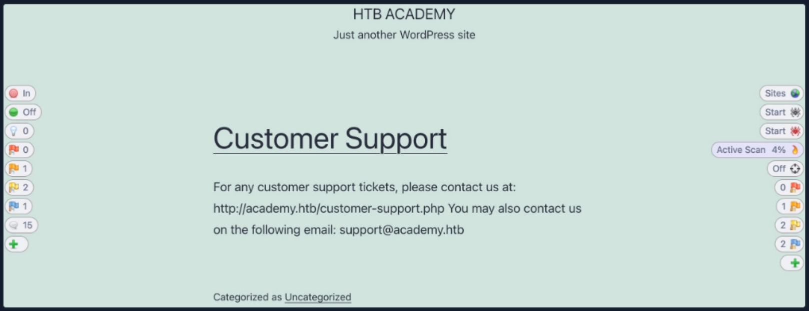


X-Frame-Options Header Not Set (8)

http://46.101.23.188:30873/
http://46.101.23.188:30873/?s
http://46.101.23.188:30873/devtools/
http://46.101.23.188:30873/index.php/2021/08/11/customer-support/
http://46.101.23.188:30873/index.php/2021/08/11/customer-support/?replytocom=2
http://46.101.23.188:30873/index.php/author/academy/

Active Scanner

Once our site's tree is populated, we can click on the `Active Scan` button on the right pane to start an active scan on all identified pages. If we have not yet run a Spider Scan on the web application, ZAP will automatically run it to build a site tree as a scan target. Once the Active Scan starts, we can see its progress similarly to how we did with the Spider Scan:



HTB ACADEMY

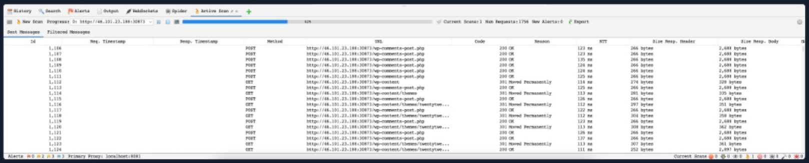
Just another WordPress site

Customer Support

For any customer support tickets, please contact us at: http://academy.htb/customer-support.php You may also contact us on the following email: support@academy.htb

Categorized as Uncategorized

The Active Scanner will try various types of attacks against all identified pages and HTTP parameters to identify as many vulnerabilities as it can. This is why the Active Scanner will take longer to complete. As the Active Scan runs, we will see the alerts button start to get populated with more alerts as ZAP uncovers more issues. Furthermore, we can check the main ZAP UI for more details on the running scan and can view the various requests sent by ZAP:

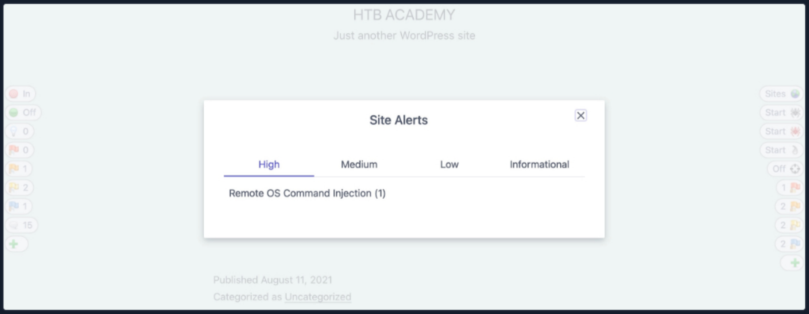


Progress: 0: http://46.101.23.188:30873 42% Current Scans:1 Num Requests:1756 New Alerts:0

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,106			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	123 ms	266 bytes	2,688 bytes
1,107			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	123 ms	266 bytes	2,688 bytes
1,108			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	135 ms	266 bytes	2,688 bytes
1,109			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	124 ms	266 bytes	2,688 bytes
1,110			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	124 ms	266 bytes	2,688 bytes
1,111			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	125 ms	266 bytes	2,688 bytes
1,112			GET	http://46.101.23.188:30873/wp-content	301	Moved Permanently	114 ms	274 bytes	328 bytes
1,113			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	125 ms	266 bytes	2,688 bytes
1,114			GET	http://46.101.23.188:30873/wp-content/themes	301	Moved Permanently	113 ms	281 bytes	335 bytes
1,115			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	126 ms	266 bytes	2,688 bytes
1,116			GET	http://46.101.23.188:30873/wp-content/themes/twentytwe...	301	Moved Permanently	112 ms	297 bytes	351 bytes
1,117			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	122 ms	266 bytes	2,688 bytes
1,118			GET	http://46.101.23.188:30873/wp-content/themes/twentytwe...	301	Moved Permanently	112 ms	304 bytes	358 bytes
1,119			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	123 ms	266 bytes	2,688 bytes
1,120			GET	http://46.101.23.188:30873/wp-content/themes/twentytwe...	301	Moved Permanently	113 ms	308 bytes	362 bytes
1,121			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	126 ms	266 bytes	2,688 bytes
1,122			POST	http://46.101.23.188:30873/wp-comments-post.php	200	OK	137 ms	266 bytes	2,688 bytes
1,123			GET	http://46.101.23.188:30873/wp-content/themes/twentytwe...	301	Moved Permanently	113 ms	307 bytes	361 bytes
1,124			GET	http://46.101.23.188:30873/wp-content/themes/twentytwe...	200	OK	111 ms	252 bytes	2,897 bytes

Alerts 0 2 3 3 Primary Proxy: localhost:8081

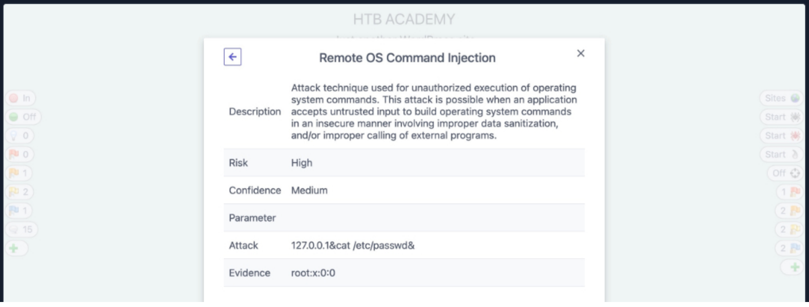
Once the Active Scan finishes, we can view the alerts to see which ones to follow up on. While all alerts should be reported and taken into consideration, the `High` alerts are the ones that usually lead to directly compromising the web application or the back-end server. If we click on the `High Alerts` button, it will show us the identified High Alert:



Remote OS Command Injection (1)

Published August 11, 2021
Categorized as Uncategorized

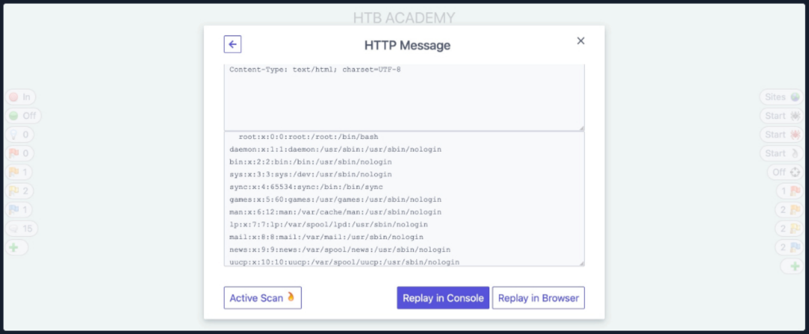
We can also click on it to see more details about it and see how we may replicate and patch this vulnerability:



Remote OS Command Injection

Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
Risk	High
Confidence	Medium
Parameter	
Attack	127.0.0.1&cat /etc/passwd&
Evidence	root:x:0:0

In the alert details window, we can also click on the URL to see the request and response details that ZAP used to identify this vulnerability, and we may also repeat the request through ZAP HUD or ZAP Request Editor:

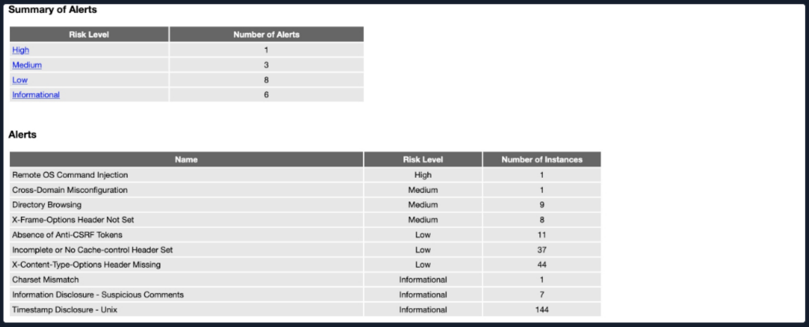


```
Content-Type: text/html; charset=UTF-8
```

```
  root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Reporting

Finally, we can generate a report with all of the findings identified by ZAP through its various scans. To do so, we can select (`Report>Generate HTML Report`) from the top bar, which would prompt us for the save location to save the report. We may also export the report in other formats like `XML` or `Markdown`. Once we generate our report, we can open it in any browser to view it:



Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	3
Low	8
Informational	6

Alerts

Name	Risk Level	Number of Instances
Remote OS Command Injection	High	1
Cross-Domain Misconfiguration	Medium	1
Directory Browsing	Medium	9
X-Frame-Options Header Not Set	Medium	8
Absence of Anti-CSRF Tokens	Low	11
Incomplete or No Cache-control Header Set	Low	37
X-Content-Type-Options Header Missing	Low	44
Charset Mismatch	Informational	1
Information Disclosure - Suspicious Comments	Informational	7
Timestamp Disclosure - Unix	Informational	144

As we can see, the report shows all identified details in an organized manner, which may be helpful to keep as a log for various web applications we run our scans on during a penetration test.

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 138ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

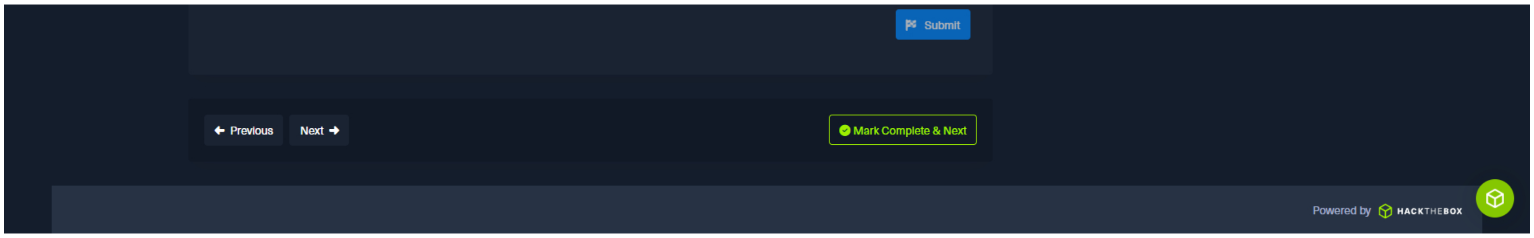
Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Target(s): Click here to spawn the target system!

+ 1 Run ZAP Scanner on the target above to identify directories and potential vulnerabilities. Once you find the high-level vulnerability, try to use it to read the flag at '/flag.txt'

HTB{5c4nn3r5_f1nd_vuln5_w3_m155}


Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX