



PROJECT

S3 STATIC WEBSITE HOSTING

Password Compromise Checker

PROJECT 1 | DAY 1

OVERVIEW

This project involves hosting a website that allows users to check whether their passwords have been compromised in previous data breaches using the Have I Been Pwned API. The website is hosted on AWS S3 as a static website.

WHAT IS S3?

Amazon S3 is a Simple Storage Service in AWS that stores files of different types like Photos, Audio, and Videos as Objects providing more scalability and security to. It allows the users to store and retrieve any amount of data at any point in time from anywhere on the web.

HOW TO:

1

Create Bucket

Your S3 bukcket name should be globally unique across all AWS accounts because S3 is a universal namespace.

The screenshot shows the AWS S3 'Create bucket' interface. On the left, there's a sidebar with 'Amazon S3' and 'General purpose buckets' options like Directory buckets, Table buckets, Access Grants, etc. The main area has a title 'Create bucket' with a 'Info' link. It says 'Buckets are containers for data stored in S3.' Below that is a 'General configuration' section with 'AWS Region' set to 'Canada (Central) ca-central-1'. The 'Bucket name' field contains 'mybucket', which is highlighted with a red border and has a tooltip 'Bucket with the same name already exists'. A note below says 'Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)'. There's also a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button and a note about copied settings.

2

Enable Static Website Hosting

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
 Disable
 Enable

Hosting type
 Host a static website
 Use the bucket endpoint as the web address. [Learn more](#)
 Redirect requests for an object
 Redirect requests to another bucket or domain. [Learn more](#)

Index document
Specify the home or default page of the website.
index.html

3

Add public bucket policy

Block public access (bucket settings)
Edit
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
⚠ Off
► Individual Block Public Access settings for this bucket

Bucket policy
Edit Delete
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

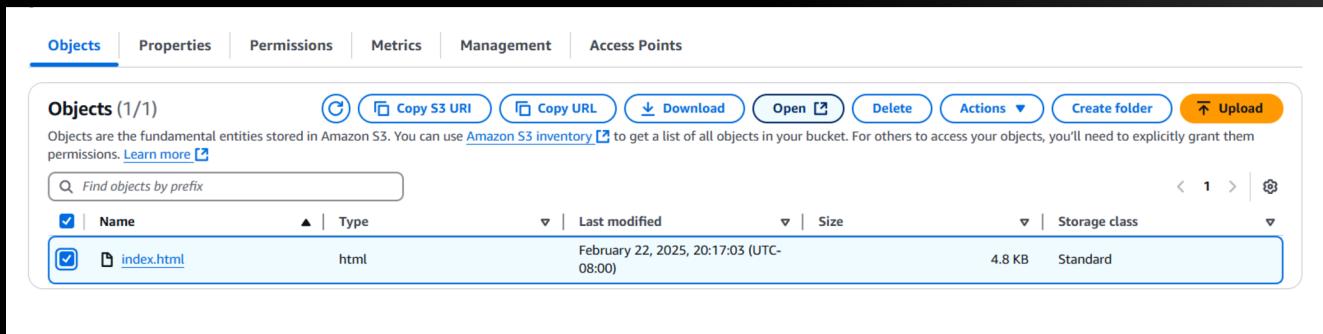
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::pwndwebsite/*"
    }
  ]
}
```

Copy

Key Takeaway: Public access settings only open the door, but a bucket policy controls who gets in and what they can do. Always use policies wisely to avoid security risks!

4 Configure index.html

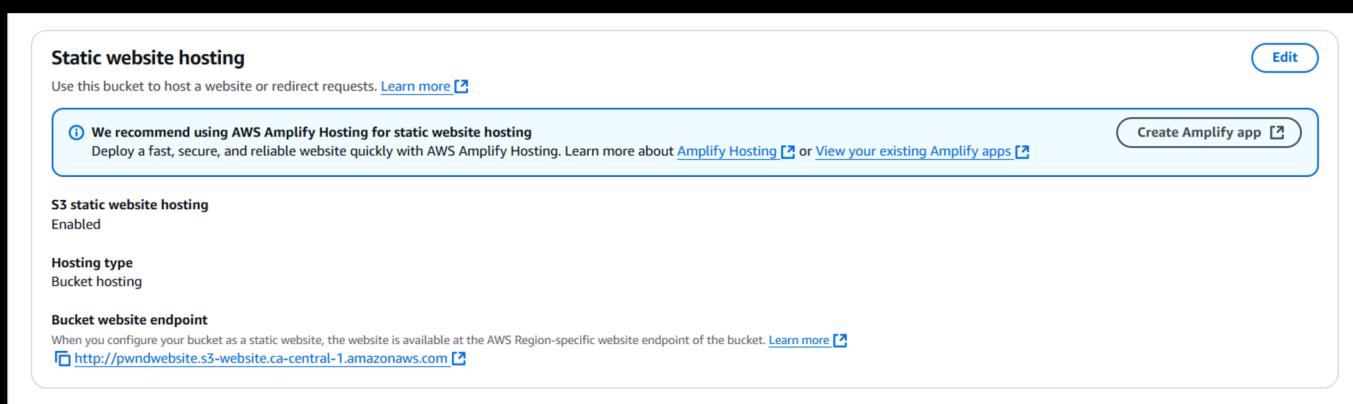
I've used git code for checking compromised passwords using haveibeenpwned API with GUI. You have check yours(at your own risk 😊)
Source: [Youtube- Have You Been Pwned? - Computerphile](#)



The screenshot shows the AWS S3 console with the 'Objects' tab selected. A single object, 'index.html', is listed. The details are as follows:

Name	Type	Last modified	Size	Storage class
index.html	html	February 22, 2025, 20:17:03 (UTC-08:00)	4.8 KB	Standard

5 Test Endpoints



The screenshot shows the 'Static website hosting' configuration for an S3 bucket. Key settings include:

- Bucket website endpoint:** <http://pwndwebsite.s3-website.ca-central-1.amazonaws.com>
- Hosting type:** Bucket hosting

Copy paste you link in web browser to test. 🤞😊

Only the first five characters of the hash of your password get send to haveibeenpwned.com

The password : passwordeasy

SHA1 Hash : 6BE1B6B82133925C37FE3BD7F7C3CB01CA8857BA

Was found **29** times!

6 Cleanup

Release the resources or let them be. Budget wisely

Key Notes:

- Configure access and policies carefully.
- Pretty easy to host simple websites for cheap.
- My Passwords have been breached, need to change them. 😊

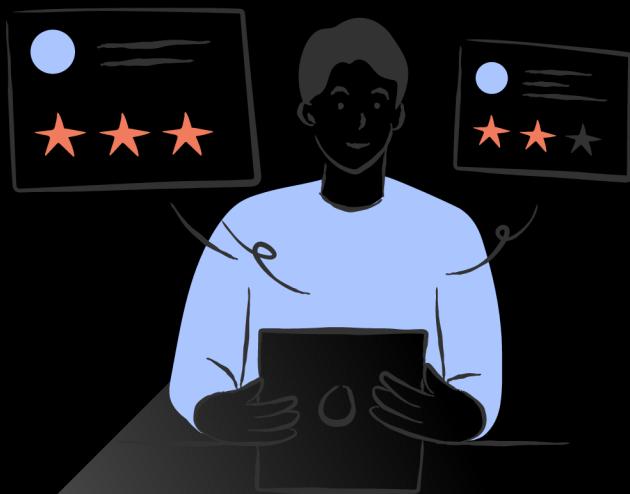
GET IN TOUCH



harshnehra33@gmail.com



/harshkumar444



@HARSHKUMAR444