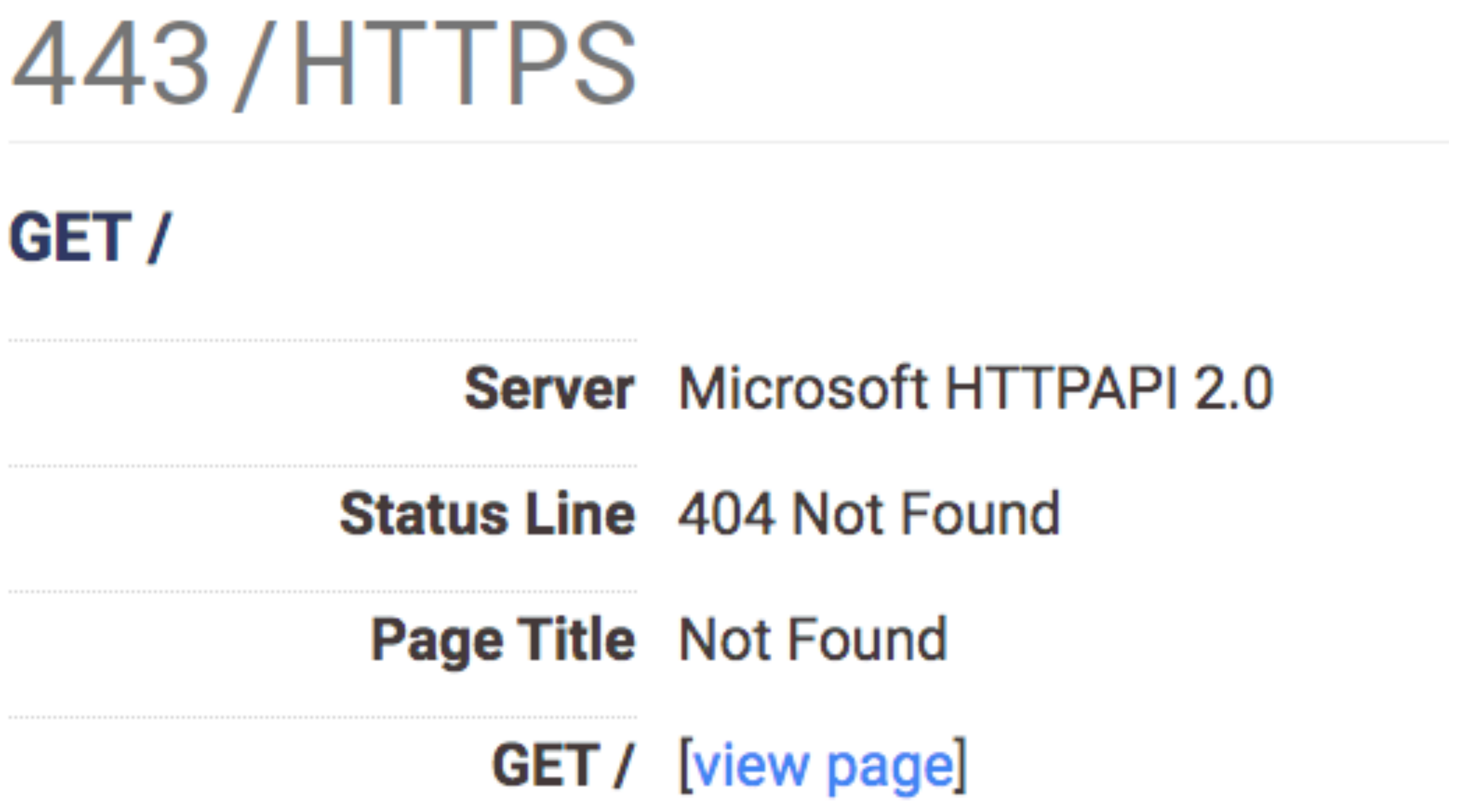
Dealing with HTTPAPI 2.0 Assets

ASSETNOTE

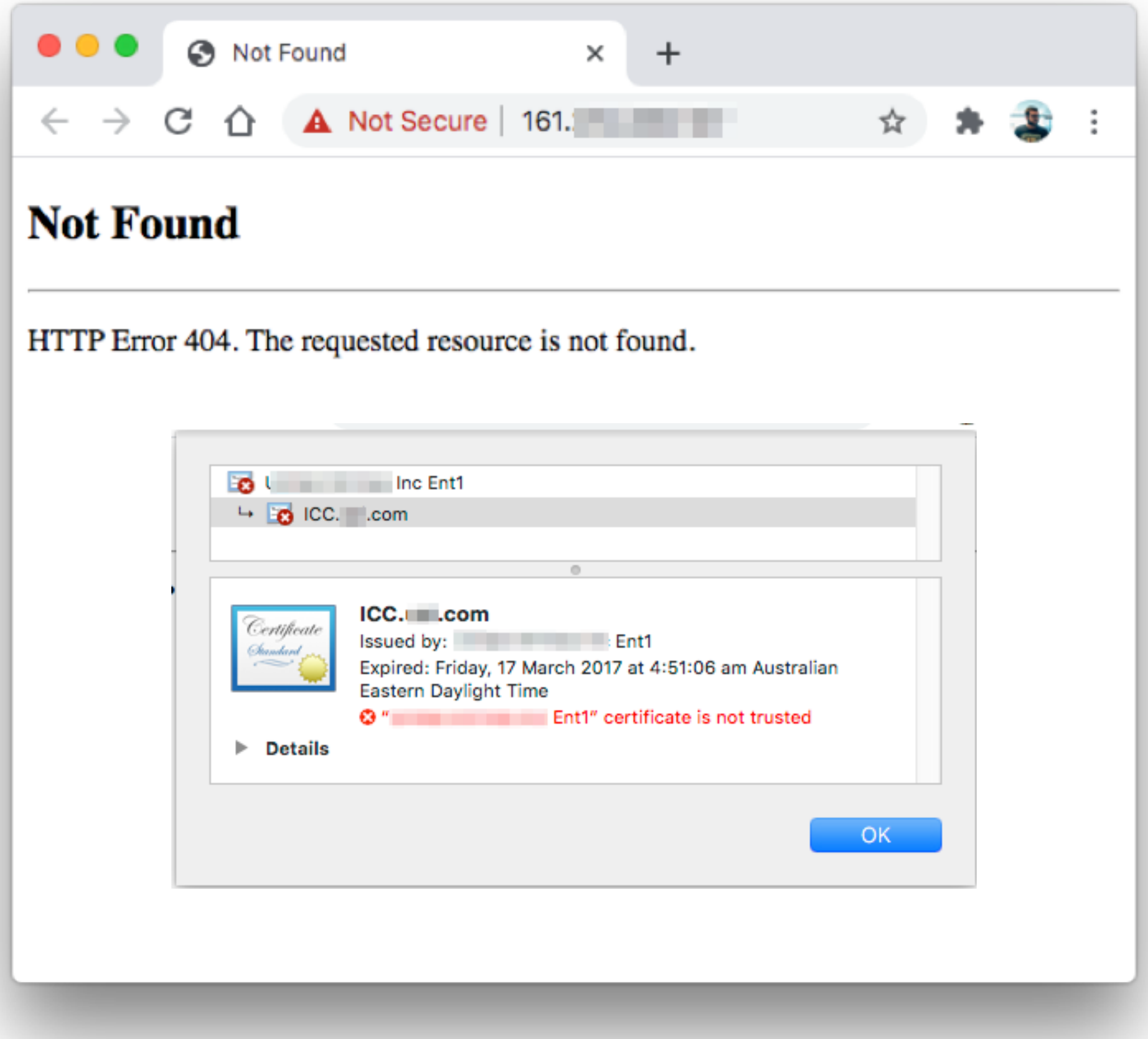
Have you seen this before?



443 / HTTPS

GET /

Server	Microsoft HTTPAPI 2.0
Status Line	404 Not Found
Page Title	Not Found
GET /	[view page]



Not Found

HTTP Error 404. The requested resource is not found.

[redacted] Inc Ent1

ICC.[redacted].com

ICC.[redacted].com

Issued by: [redacted] Ent1

Expired: Friday, 17 March 2017 at 4:51:06 am Australian Eastern Daylight Time

“[redacted] Ent1” certificate is not trusted

- Either, you’re missing the subdomain associated with the IP address (No SSL certificate)
- Or the subdomain doesn’t resolve but you can obtain a full/partial subdomain from the SSL certificate

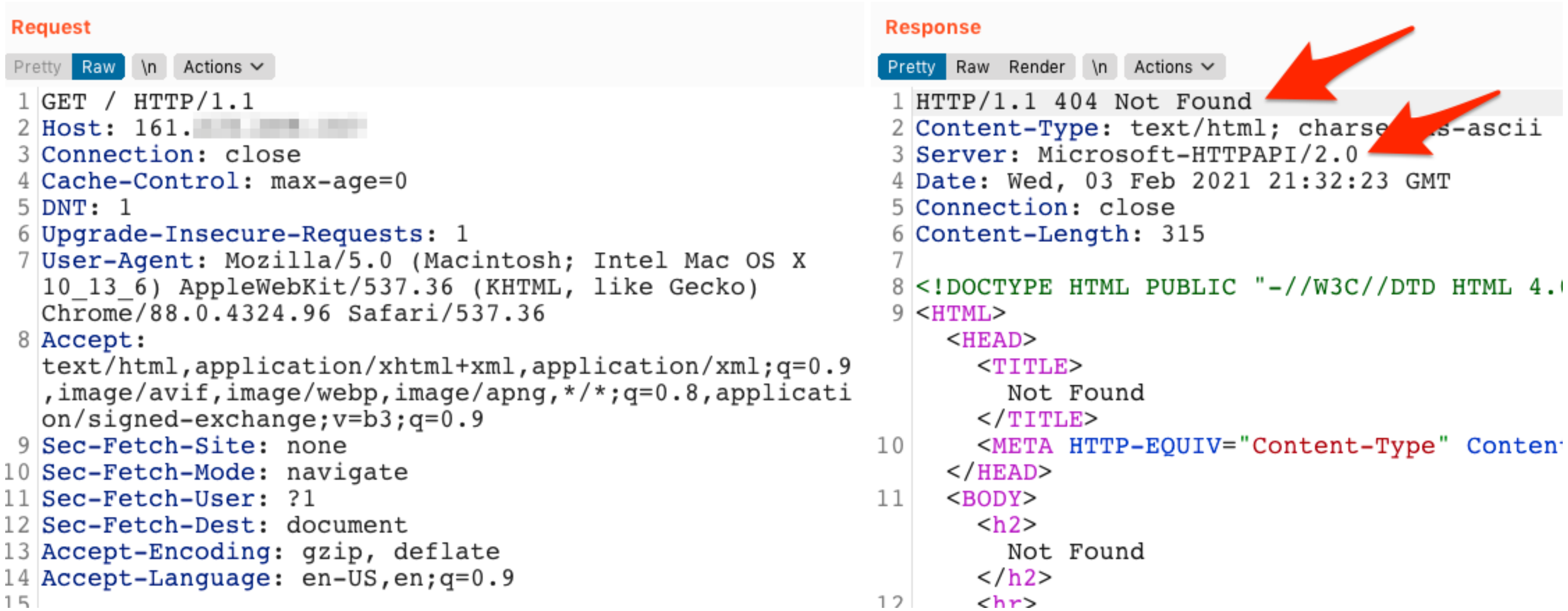
Resolving the HTTPAPI 2.0 404 Error

- This is super simple, but often people skip assets when they see the HTTPAPI 2.0 404 error. This error usually means that the asset needs the correct host header to route to the application.

- You're not always fortunate enough to have the full subdomain provided to you via the SSL certificate.

- If you know the hostname, simply provide the hostname in the HTTP Host header.

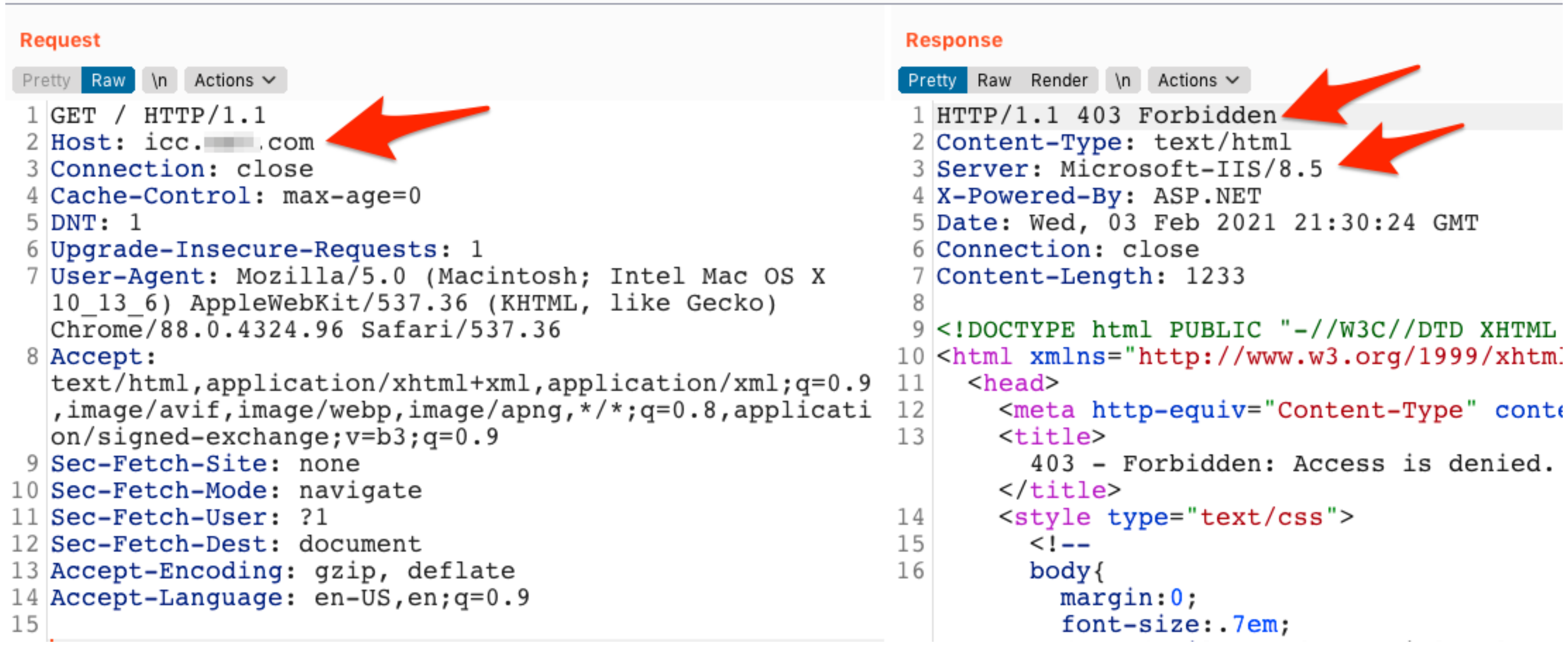
- Sometimes you have to bruteforce VHosts until you can access the application.



```
GET / HTTP/1.1
Host: 161.[redacted]
Connection: close
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4324.96 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charse  s-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 03 Feb 2021 21:32:23 GMT
Connection: close
Content-Length: 315

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.
<HTML>
  <HEAD>
    <TITLE>
      Not Found
    </TITLE>
    <META HTTP-EQUIV="Content-Type" Conten
  </HEAD>
  <BODY>
    <h2>
      Not Found
    </h2>
    <hr>
```



```
GET / HTTP/1.1
Host: icc.[redacted].com
Connection: close
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4324.96 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 03 Feb 2021 21:30:24 GMT
Connection: close
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML
<html xmlns="http://www.w3.org/1999/xhtm
  <head>
    <meta http-equiv="Content-Type" conte
    <title>
      403 - Forbidden: Access is denied.
    </title>
    <style type="text/css">
      <!--
      body{
        margin:0;
        font-size:.7em;
```

After fixing the host header

- Add a line to your /etc/hosts file to map the correct host name to the IP address of the asset.
- **Run all of your scanning again, including your enumeration through IIS shortname scanner.**
- Perform VHost enumeration/bruteforcing to see if there are any other applications that are present on the host.
- Find all other assets that respond with HTTPAPI 2.0 404 errors and apply the same workflow (rinse and repeat).

VHost Hopping

ASSETNOTE

Accessing an internal admin panel via VHost Hopping ($1900)

- Came across an asset that looked something like apply.company.com running IIS.

- Used a large subdomain wordlist to bruteforce VHosts using Burp Intruder (%bruteforce%.company.com).

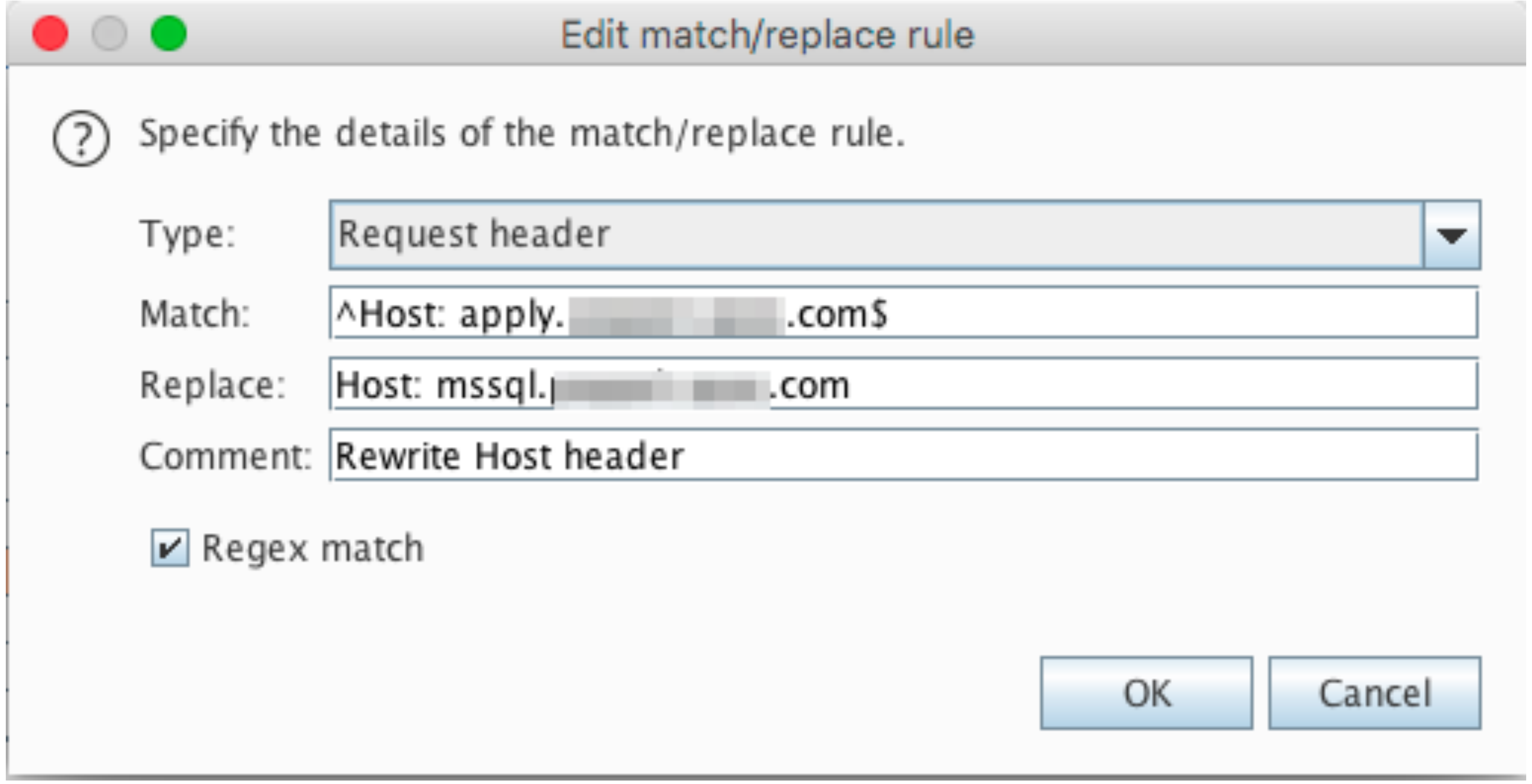
- Large and different response returned for mssql.company.com which was not accessible externally, only accessible through “VHost Hopping”.

- This was running a MSSQL database manager/explorer (https://sourceforge.net/projects/asp-ent-man/).

Accessing the VHost

- Often, on IIS servers, there may be internal applications running under a different host name. Host name bruteforcing / VHost hopping is very effective in IIS environments.

- A simple match and replace rule to facilitate the access:



Edit match/replace rule

Specify the details of the match/replace rule.

Type: Request header

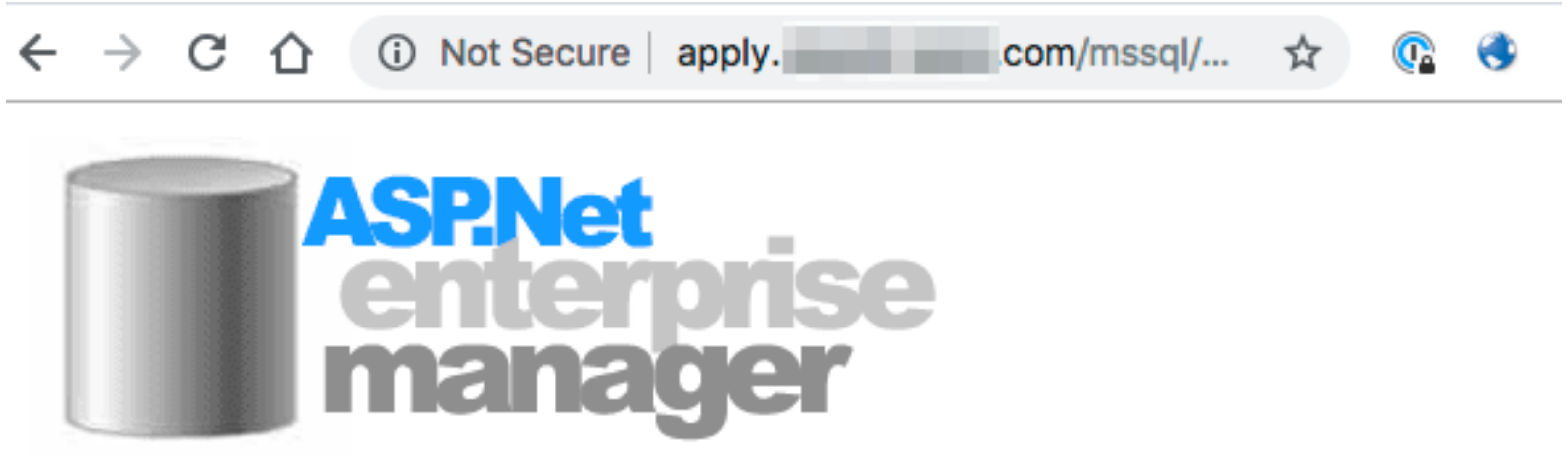
Match: ^Host: apply.[redacted].com$

Replace: Host: mssql.[redacted].com

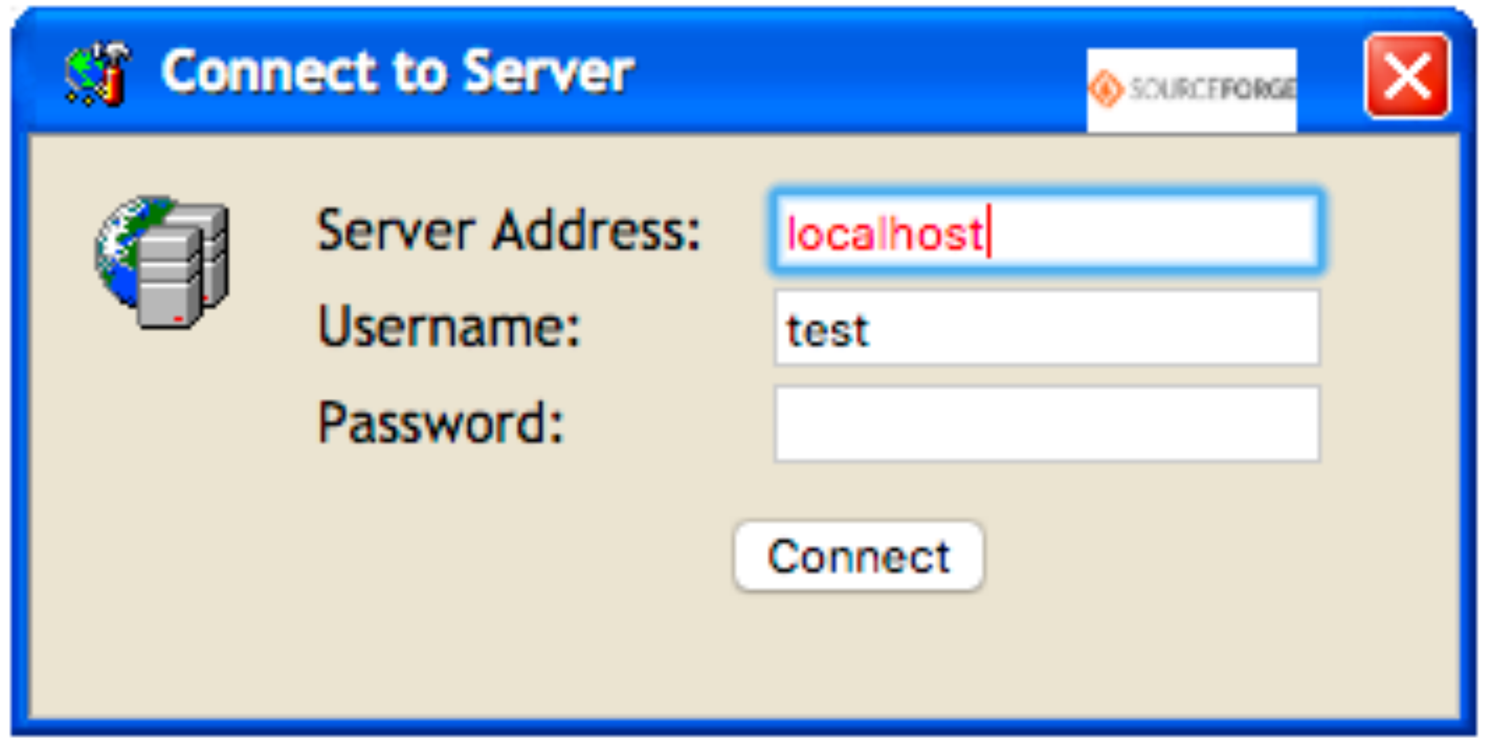
Comment: Rewrite Host header

☑ Regex match

Reap the benefits



Not Secure | apply.[redacted]com/mssql/...

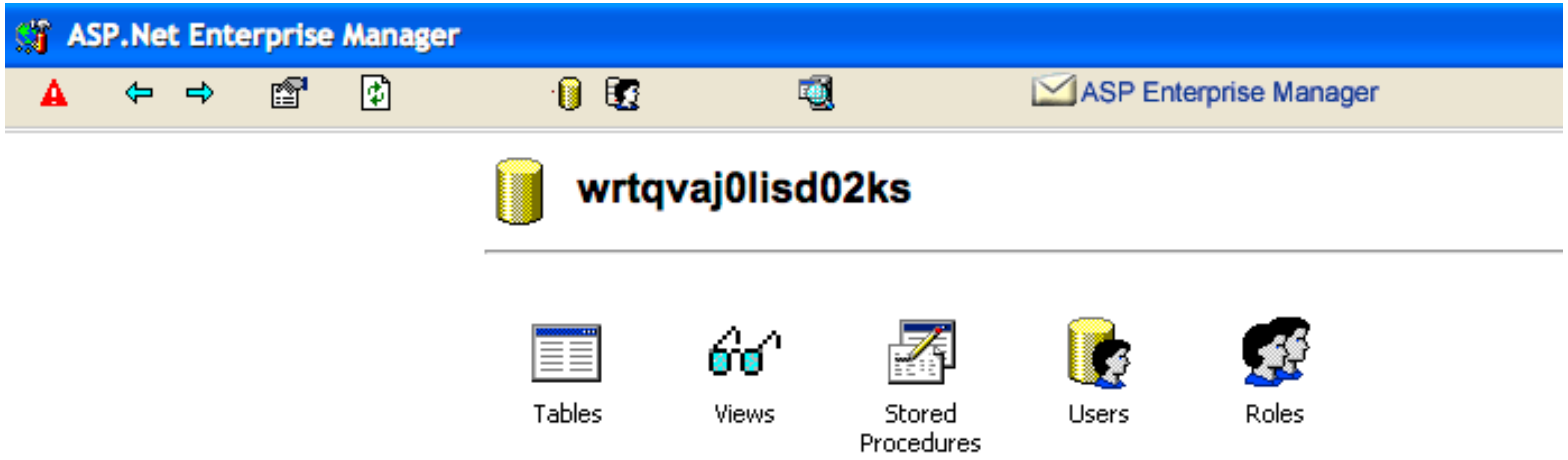


Server Address: localhost

Username: test

Password:

Reap the benefits


ASP.Net Enterprise Manager
ASP Enterprise Manager
wrtqvaj0lisd02ks
Tables
Views
Stored Procedures
Users
Roles