

Forum:[Hack Forums](#)

Thread: [Getting error "Invalid CSRF" when trying HttpWebRequest Post data](#)

freesix - November 30, 2018, 6:06 am

Hi guys, have been struggling for more than 2 weeks now to solve this issue.
Can you please help me out?

I'm trying to post data and i'm getting {"status":403,"message":"Invalid CSRF"}.
I successfully logged in and set cookies on login and submitting page but when I try to submit the form (post httpwebrequest data) i'm getting {"status":403,"message":"Invalid CSRF"}.

I know that the web site has CSRF features for security, and I also use Fiddler to capture Http Traffic.

Any idea is welcomed.

Please see code below code from Fiddler but it doesn't work.

I'm using VB.Net with HttpWebRequest

Nikola ?esla - November 30, 2018, 9:56 am

As it clearly says Invalid CSRF so make sure you are grabbing it correctly and using it in right way.
Look at raw format in fiddler.

Zettabit - December 1, 2018, 2:53 am

There is most likely a hidden input in the form that you're missing. Make another request from the browser and double check to make sure you are POSTing everything that fiddler catches in the request.

EDIT: I would also do view-source and inspect element to see if anything that was POSTed changes with each request.

freesix - December 5, 2018, 7:57 am

(Dec 1, 2018 03:53 AM)Zettabit Wrote: [\[CITE\]](#) There is most likely a hidden input in the form that you're missing. Make another request from the browser and double check to make sure you are POSTing everything that fiddler catches in the request.

EDIT: I would also do view-source and inspect element to see if anything that was POSTed changes with each request.

There's no really hidden field I just inspected that again.

But if I use the below cookies from Fiddler, it does post.

Code [b]request.Headers.Set(HttpRequestHeader.Cookie, "machguid=ee80e2cf-5fc1-4...")[/b]
and I found another _csrf=oJSCg51C4NtpWFm4fuzg5hWL in the cookies when i login from the browser. not sure how to collect it,
but when i login from the bot i'm not able to see the _csrf from the cookies.

can you please help?

Alien - December 6, 2018, 12:43 pm

(Dec 5, 2018 08:57 AM)freesix Wrote: [\[CITE\]](#) There's no really hidden field I just inspected that again.

But if I use the below cookies from Fiddler, it does post.

Code [b]request.Headers.Set(HttpRequestHeader.Cookie, "machguid=ee80e2cf-5fc1-4...")[/b]
and I found another `_csrf=oJSCg51C4NtpWFm4fuzg5hWL` in the cookies when i login from the browser. not sure how to collect it,
but when i login from the bot i'm not able to see the `_csrf` from the cookies.

can you please help?

I ran into this issue the other night.

This is the resolution I found:

Send a request to the login page and use the following code as if you were grabbing the html source

Code `TokenResponse.Headers.ToString`

freesix - December 11, 2018, 6:59 am

Hi Ed Sheeran, sorry for late reply as my internet went down.

I did it as described and below is the reponse I got.

The website I'm working on is : `w3.gumtree.co.za`

Code X-DNS-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000000; includeSubDomains; preload
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: connect-src * 'self'
X-Track-Guid: `cjppjvazj52yzpl3axp3mo3ufe`
Content-Encoding: gzip
X-Cluster: fe
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 17235
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Tue, 11 Dec 2018 14:55:14 GMT
Set-Cookie: machguid=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00
GMT,machguid=314a9bd4-a07c-4f52-8bb8-7430ac589d7e-1679dc3cd60; Max-Age=31536000;
Path=/; Expires=Wed, 11 Dec 2019 14:55:14 GMT; HttpOnly;
Secure,anonUsrId=cjppjvazj62yzql3axyksqm2hr; Path=/; HttpOnly; Secure
X-Powered-By: Bolt 2.0

X-DNS-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=31536000000; includeSubDomains; preload
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: connect-src * 'self'
X-Track-Guid: cjpjvazj52yzpl3axp3mo3ufe
Content-Encoding: gzip
X-Cluster: fe
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 17235
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Tue, 11 Dec 2018 14:55:14 GMT
Set-Cookie: machguid=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00
GMT,machguid=314a9bd4-a07c-4f52-8bb8-7430ac589d7e-1679dc3cd60; Max-Age=31536000;
Path=/; Expires=Wed, 11 Dec 2019 14:55:14 GMT; HttpOnly;
Secure,anonUsrId=cjpjvazj62yzql3axyksqm2hr; Path=/; HttpOnly; Secure
X-Powered-By: Bolt 2.0

freesix - December 13, 2018, 4:02 am

(Dec 6, 2018 01:43 PM)ED SHEERAN Wrote: [\[CITE\]](#) I ran into this issue the other night.

This is the resolution I found:

Send a request to the login page and use the following code as if you were grabbing the html source

Code TokenResponse.Headers.ToString
Hi Ed, the issue is still on.

Can you please help me out?

Alien - December 28, 2018, 11:27 pm

(Dec 13, 2018 05:02 AM)freesix Wrote: [\[CITE\]](#) Hi Ed, the issue is still on.

Can you please help me out?

Sorry for late response, I didn't realize you had replied to my early posts.

So, When you go to the login page (example.com/loginform.php).. have you tried searching 'csrf' with fiddler just to see what comes up in the source?

Also, can you show a screenshot of fiddler or more of your code? These type of situations can be tricky without more information. You can blur out/erase the website's URL if needed.

freesix - January 1, 2019, 11:22 pm

Sorry for not posting the code, I always post code but when I tried to post code here the first time, the forum showed me the below message.

[Sorry, you cannot post links, videos, or images until you've made more than 50 total posts or have upgraded.]

I also posted the same issue with code on blackhatworld(DOT)com, you can find it here below.

blackhatworld(DOT)com/seo/getting-error-invalid-csrf-when-trying-httpwebrequest-post-data.1073313/

I have the fiddle session archive as a file, i'm able to email it to you as I can't attach on this post because I have not a total of 50 posts yet.

If you want it, you can PM me with your email address.

The fiddler has the whole process from login, filling the form, submitting the form and posting.

I managed to upload the fiddler session archive into Google Drive, this is the link (drive(DOT)google(DOT)com/file/d/1URCMkid6OjOJO_bS6REkXgGyttlLHnt2/view?usp=sharing)

please change (DOT) to .

Alien - January 2, 2019, 4:38 pm

(Jan 2, 2019 12:22 AM)freesix Wrote: [\[CITE\]](#) Sorry for not posting the code, I always post code but when I tried to post code here the first time, the forum showed me the below message.

[Sorry, you cannot post links, videos, or images until you've made more than 50 total posts or have upgraded.]

I also posted the same issue with code on blackhatworld(DOT)com, you can find it here below.

blackhatworld(DOT)com/seo/getting-error-invalid-csrf-when-trying-httpwebrequest-post-data.1073313/

I have the fiddle session archive as a file, i'm able to email it to you as I can't attach on this post because I have not a total of 50 posts yet.

If you want it, you can PM me with your email address.

The fiddler has the whole process from login, filling the form, submitting the form and posting.

I managed to upload the fiddler session archive into Google Drive, this is the link (drive(DOT)google(DOT)com/file/d/1URCMkid6OjOJO_bS6REkXgGyttlLHnt2/view?usp=sharing)

please change (DOT) to .

Look up how to use regex and how use it to extract from the source code. Regex is the common function used for this type of situation

Also, I looked at your source for submitting a post request.. and its kinda hectic. Here is a better template for the future.. its a lot more organized

```
Code Dim postData As String = "email=&password=&username=" & userName
    'when POSTing data, it needs to be in byte format.
    Dim bytes() As Byte = ASCIIEncoding.UTF8.GetBytes(postData)
    'this is the page we are loggin into
```

```

Dim postReq As HttpWebRequest = WebRequest.Create("www.example.com/login")
'decrypts encrypted responses
postReq.AutomaticDecompression = DecompressionMethods.GZip Or
DecompressionMethods.Deflate
'sets the request method as POST
postReq.Method = "POST"
postReq.KeepAlive = True
'holds our cookies
postReq.CookieContainer = cookiejar
postReq.ContentType = "application/x-www-form-urlencoded"
postReq.Host = "www.example.com"
postReq.Accept = "*/*"
postReq.Headers.Add("Accept-Language", "en-US,en;q=0.9") '
postReq.Headers.Add("Accept-Encoding", "gzip, deflate, br")
postReq.Headers.Add("Origin", "example.com")
postReq.Headers.Add("X-CSRFToken", Key)
postReq.Referer = "https://www.example.com/"
postReq.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36"
'length of our post data
postReq.ContentLength = bytes.Length
'gets the stream to send data on
Dim postStream As Stream = postReq.GetRequestStream()
'send the data
postStream.Write(bytes, 0, bytes.Length)
'close the stream
postStream.Close()
'get the response from the website
Dim postResponse As HttpWebResponse
postResponse = postReq.GetResponse()
'add the login cookies
cookiejar.Add(postResponse.Cookies)
'reads the response
Dim reader As New StreamReader(postResponse.GetResponseStream())
'puts the response into a string
Dim strSource As String = reader.ReadToEnd

```

freesix - January 3, 2019, 9:01 am

Hi thanks a lot,

I have two concerns :

The first is the code you provided me, the "CSRFToken" is generated/collected from the login, whereas on w3(DOT)gumtree(DOT)co.za the "CSRFToken" is not present when login, so it's not generated when trying to login, only when clicking on "Post FREE Ad" button located on right top corner. (you can check it yourself, on Chrome using "View page source" when clicking on "Post FREE Ad", then search for "csrf")

Second of all, the line "postReq.Headers.Add("X-CSRFToken", Key)" : How will I get the Key ? Should I use Regex ?

Alien - January 3, 2019, 3:06 pm

(Jan 3, 2019 10:01 AM)freesix Wrote: [\[CITE\]](#) Hi thanks a lot,

I have two concerns :

The first is the code you provided me, the "CSRFToken" is generated/collected from the login, whereas on w3(DOT)gumtree(DOT)co.za the "CSRFToken" is not present when login, so it's not generated when trying to login, only when clicking on "Post FREE Ad" button located on right top corner. (you can check it yourself, on Chrome using "View page source" when clicking on "Post FREE Ad", then search for "csrf")

Second of all, the line "postReq.Headers.Add("X-CSRFToken", Key)" : How will I get the Key ? Should I use Regex ?

Send a GET request (which is just retrieving the source code of a webpage) to this link:
"https://www.gumtree.co.za/post.html"

make sure the same cookiecontainer used for logging into your account is set as the cookie container used in the GET request(retrieving source code).

After you have successfully retrieved the source code of "/post.html" use regex function to identify and extract the csrf code. Store the csrf key as a string variable and use it in the "/api/create/" post request.

the x-csrf-token was an example. Check the headers in fiddler to find out what gumtree uses to pass the csrf token

HardStoN - January 18, 2019, 6:58 am

hey guys ive never understood what is regex exactly and i would like to know how you can extract csrf_token bHKXN8PPTyBvd729fLCsqWgN7oBIQMhF

in csrf_token":"bHKXN8PPTyBvd729fLCsqWgN7oBIQMhF",

Thanks for all the helpers

StarZ - January 19, 2019, 1:14 am

(Jan 18, 2019 07:58 AM)HardStoN Wrote: [\[CITE\]](#) hey guys ive never understood what is regex exactly and i would like to know how you can extract csrf_token bHKXN8PPTyBvd729fLCsqWgN7oBIQMhF

in csrf_token":"bHKXN8PPTyBvd729fLCsqWgN7oBIQMhF",

Thanks for all the helpers

Your Regex:

Code csrf_token\"\\\":\"(\\w{32})\\\"

Although I'm assuming based off the structure you're parsing JSON, You can use RegEx to parse the token. I would use some sort of JSON parser personally.

Code Dim Token as String = System.Text.RegularExpressions.Match(JSONSource, "csrf_token\"\\\":\"(\\w{32})\\").Groups(1).Value