Content negotiation With CSRF

Arbaz Hussain Follow
Apr 13, 2018 · 3 min read

. . .

In this blog post i would like to share some Content Negotiation behavior while Performing CSRF Request .

. . .

While Performing Penetration Testing on Application API , I Came across ***Content Negotiation behavior .*** *Let's discuss this with live example which i encountered .*

Following is the Request which Server made with ClientID in order to generate AUTH Token.Since it has no protection against CSRF Attack .

Request

Raw | Params | Headers | Hex

```
POST /api/authentication HTTP/1.1
User-Agent: Mozilla
Accept: application/vnd.[redacted]-api+json;version=2
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate

data_type=authentication&provider=installations&credentials=bffd87b6-b5c4-4718-80ec-d146c92e0319
```

Response

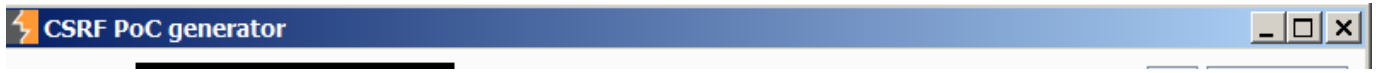
Raw | Headers | Hex

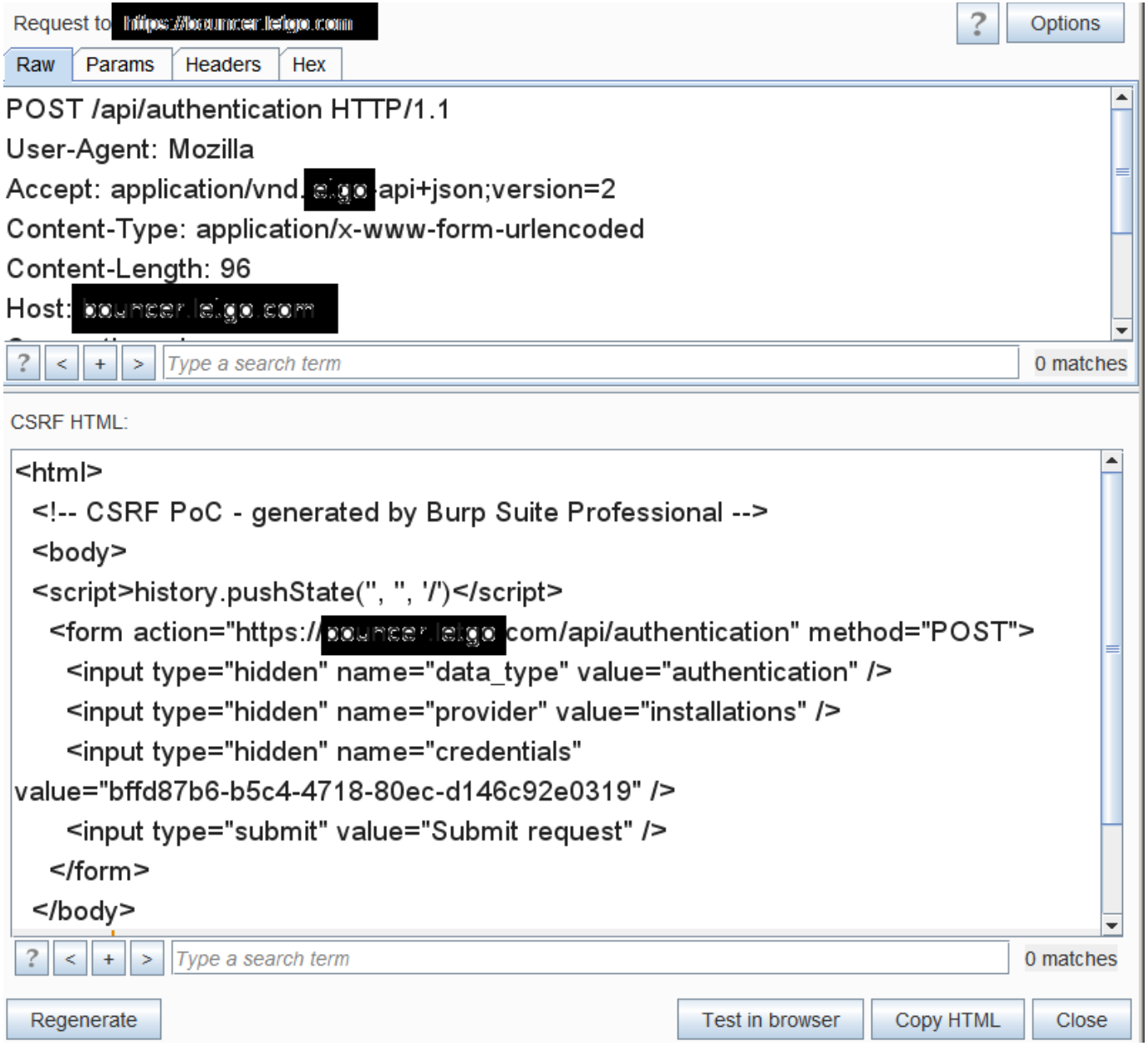
```
HTTP/1.1 201 Created
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept, client-security-token
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 1000
Content-Type: application/vnd.[redacted]-api+json;version=2
Server: Apache
Status: 201 Created
Content-Length: 645
Expires: Sat, 18 Nov 2017 07:18:49 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Sat, 18 Nov 2017 07:18:49 GMT
Connection: close

{
   "id": "bffd87b6-b5c4-4718-80ec-d146c92e0319",
```

Origin Request

- *As soon as i saw the above Request , I Quickly tried CSRF .*





CSRF ON ORIGINAL REQUEST

- *~ And Here is the Response ~.OOPS*

CSRF ON ORIGINAL REQUEST DIDN'T WORKED

- ***Let's Check What's Wrong in Burp Proxy History!!!!***

- *Request looks good and it should get executed at server side , After trying changing parameters and few thing's i came to know that they are accepting* ***only Limited Type of Content .***
- *Let's look at first* ***Original Request Again*** *.By Looking at* ***Accept:application/vnd.domain-api+json;version=2 it is clear that*** *server expect the JSON data from the client in order to validate.*

. . .

~ Let's make CASE'S in order to check for Bypasses :

1. ***Trying By Removing Request Header :***

Accept: application/vnd.domain-api+json;version=2

- *On Forcing Server with **application/x-www-form-urlencoded** content ,we can see that Application is Strictly Validating the content to be JSON.*

Hence it is clear that we can't try any other content beside given by Request Header(Accept: JSON)

- *Also we can use **SWF-based JSON CSRF exploitation(aka. 307 Trick)** here to Spoof **Content Type : application/vnd.domain-api+json;version=2,** but would not work in this case . since our request data is not in JSON .*

2. *Convert REQUEST Data into JSON Data :*

- *Now we have optional to convert the request data into JSON in order to use it along with* ***SWF-based JSON CSRF exploitation.***

So i need to convert the following request data into JSON :

data_type=authentication&provider=installations&credentials=bffd87b6-b5c4–4718–80ec-d146c92e0319

TO

{“data”:{“type”:”authentication”,”attributes”:{“provider”:”installations”,”credentials”:”bffd87b6-b5c4–4718–80ec-d146c92e0319"}}}

Success!

~ Keep Trying

Bug Bounty | Pentesting | Bug Hunting | Hacking | Infosec

358 claps

WRITTEN BY

Arbaz Hussain

~Kiraak-Boy~

Follow

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Powered by Hackrew

Follow

See responses (4)

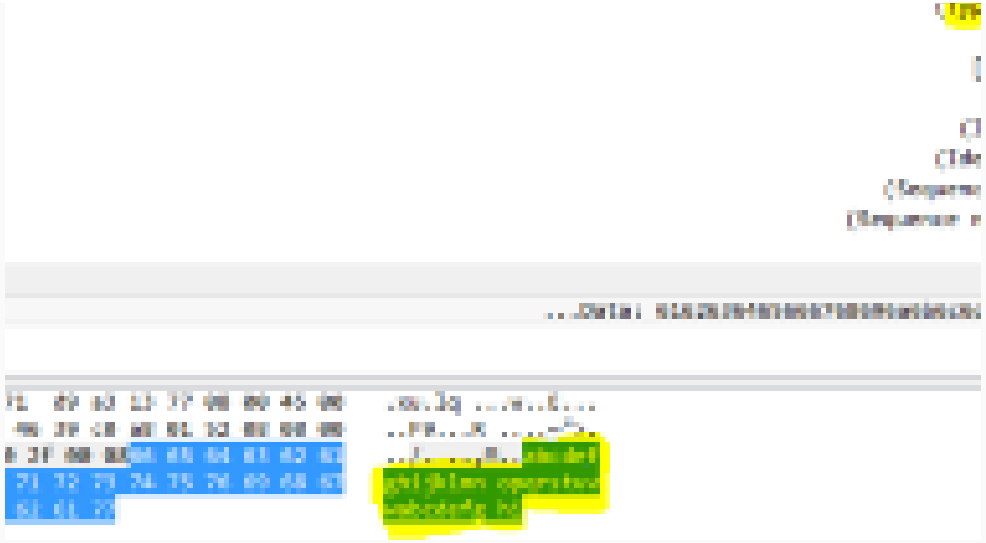
More From Medium

More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups
Dec 17, 2018 · 8 min read

1.1K



More from InfoSec Write-ups

Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups
Aug 16 · 16 min read ★

483

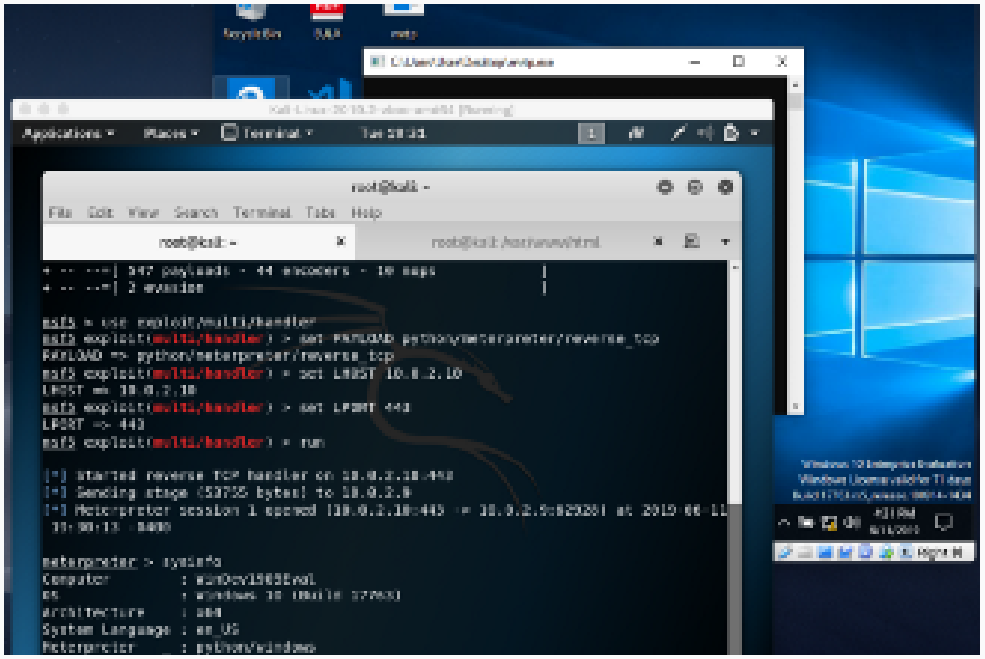
More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read ★

610



Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal