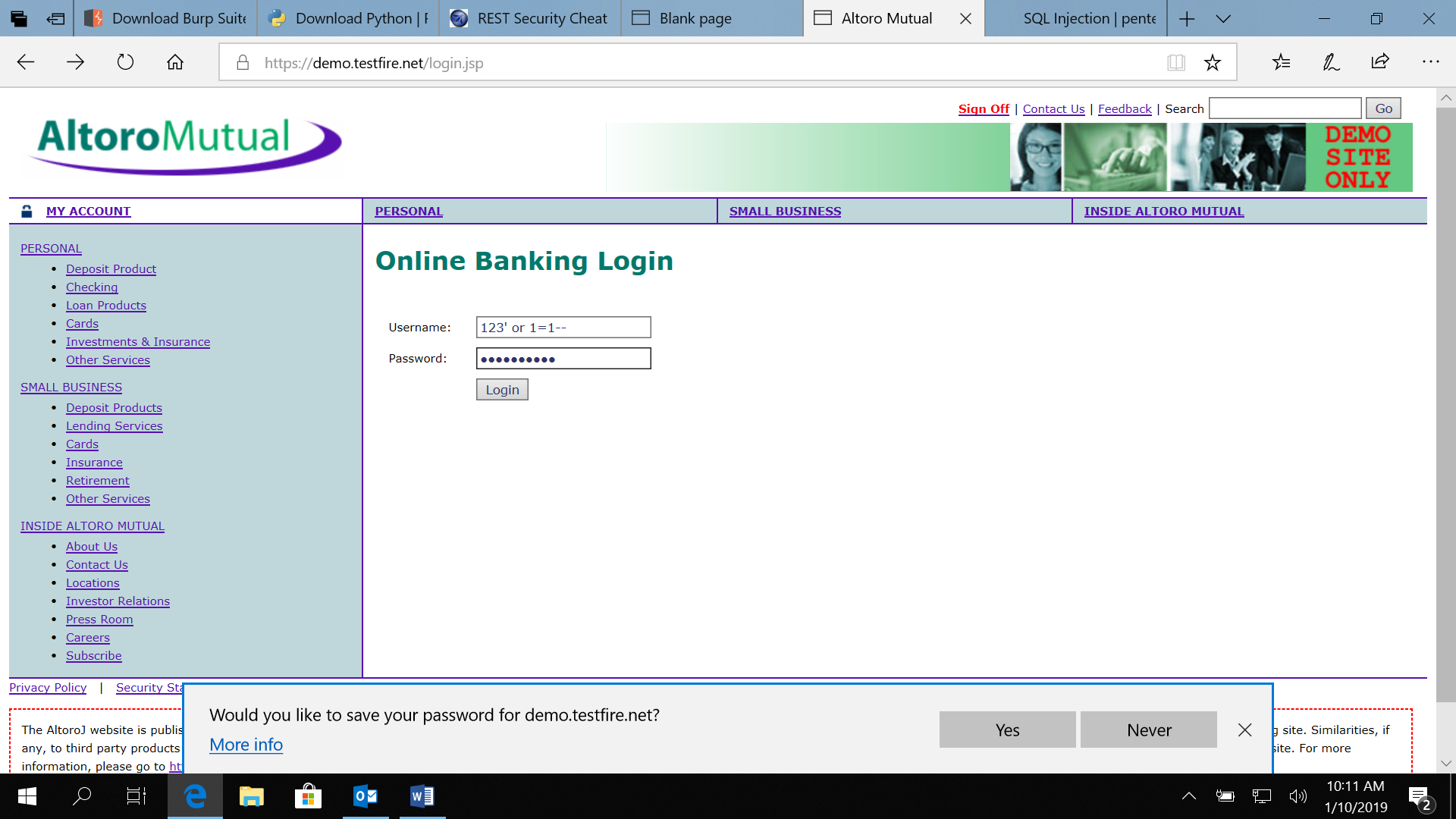
Basic Sql Attack

<https://demo.testfire.net/login.jsp>

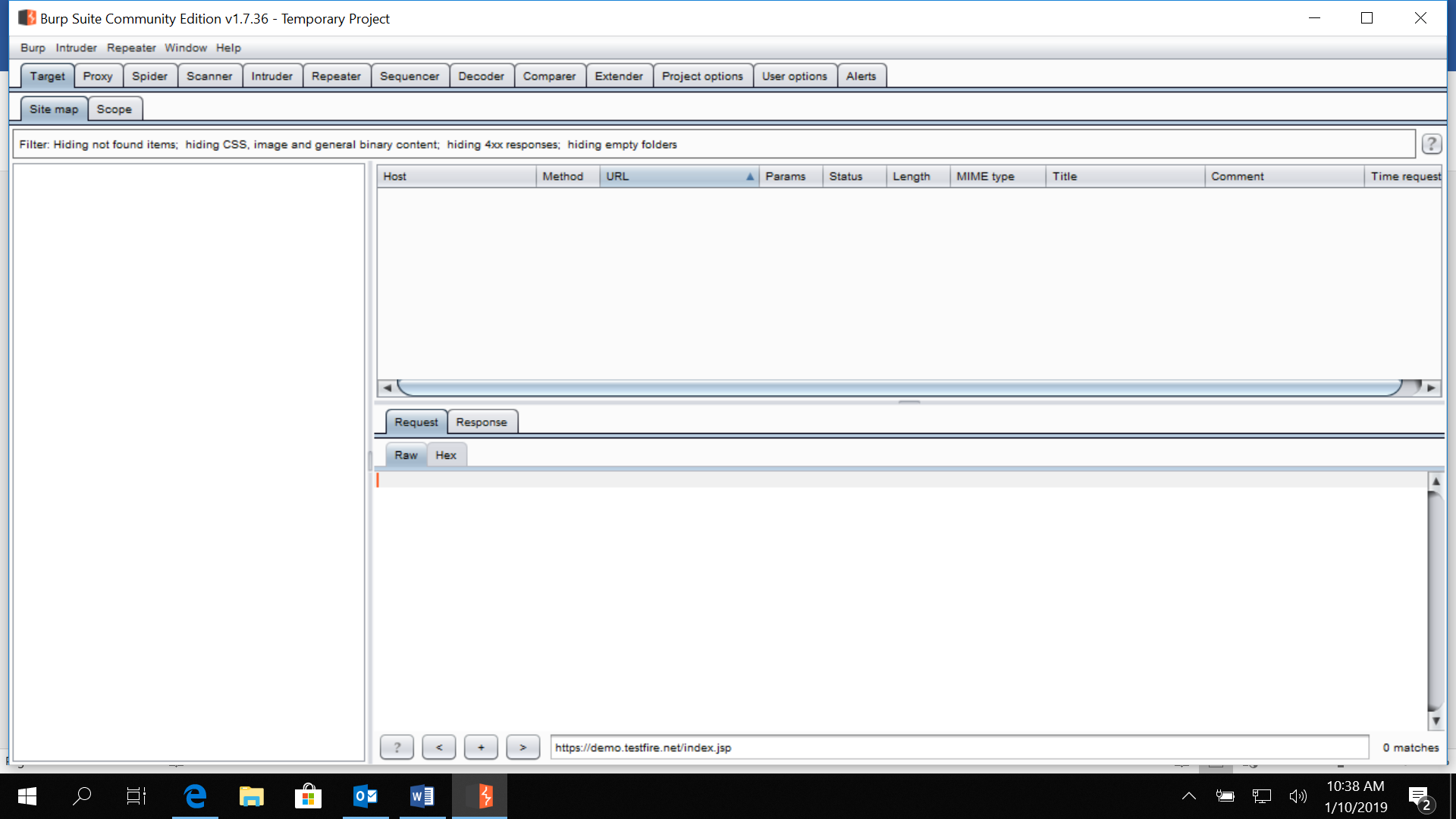


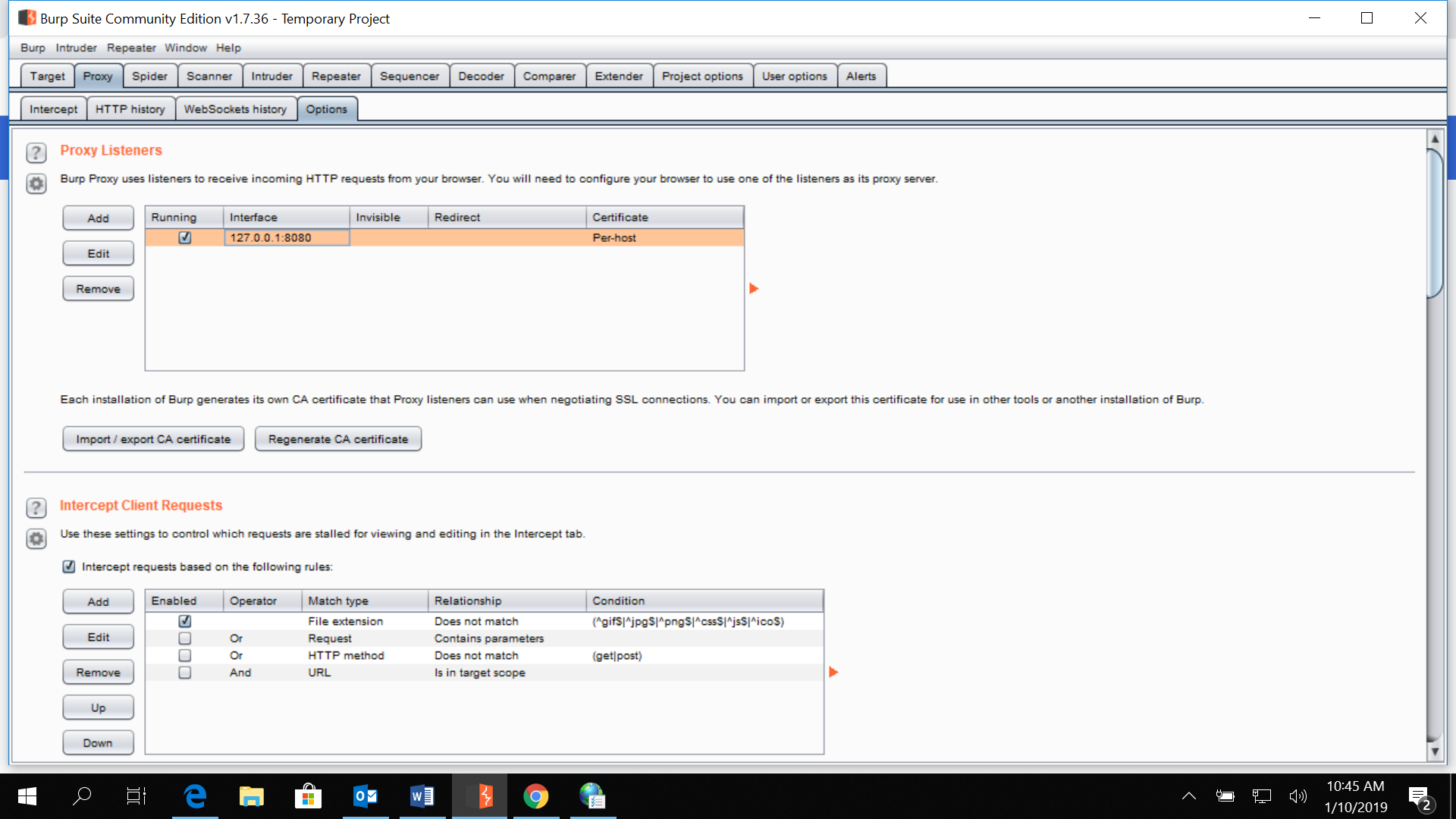
User Name= 123' or 1=1--  
  
Here “ ‘ “ explains that the string is being closed and 1=1 is universal truth “ –” m explains that after everything is commented out.

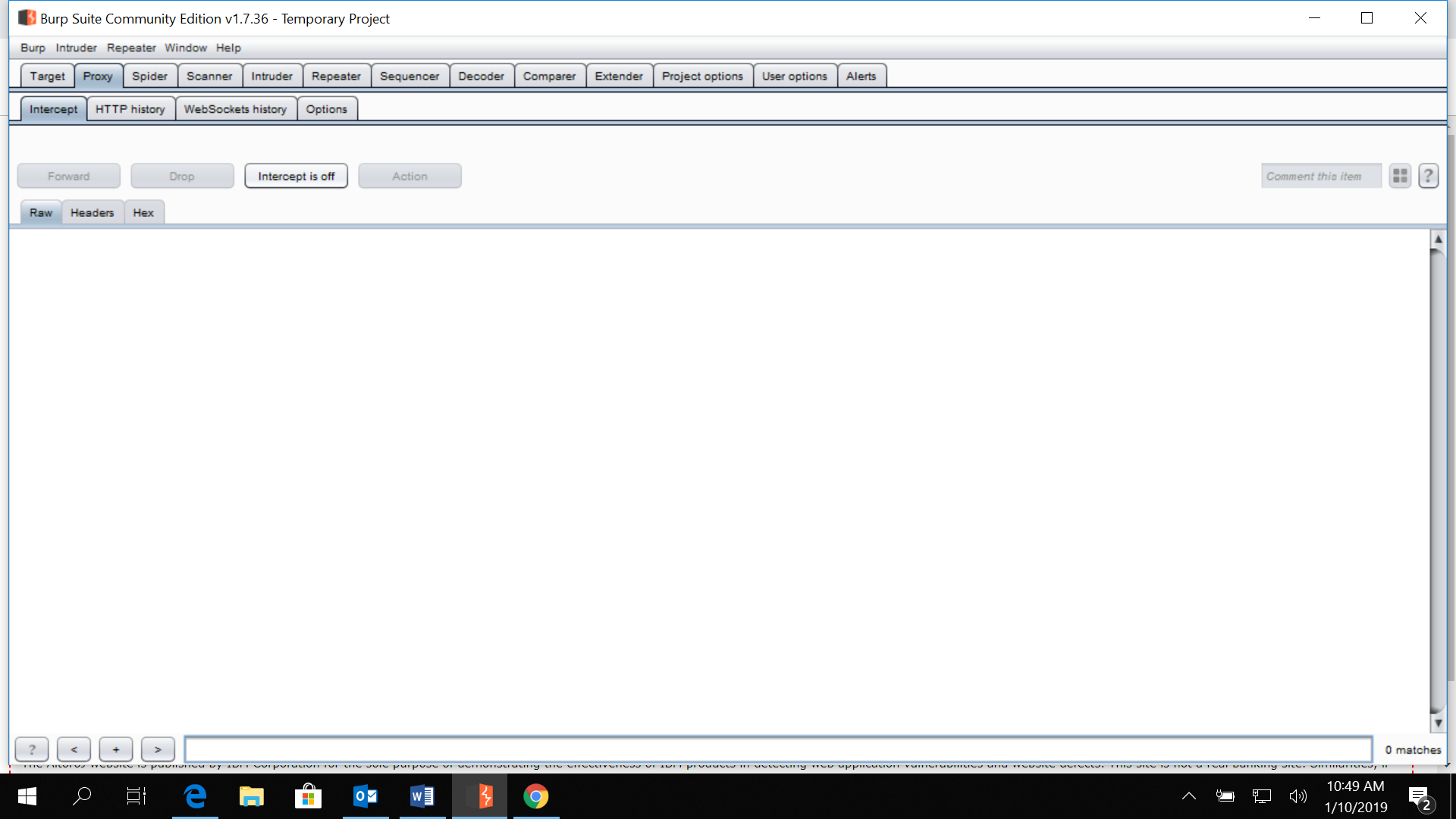
So if we have to login as a particular user User Name= admin'--

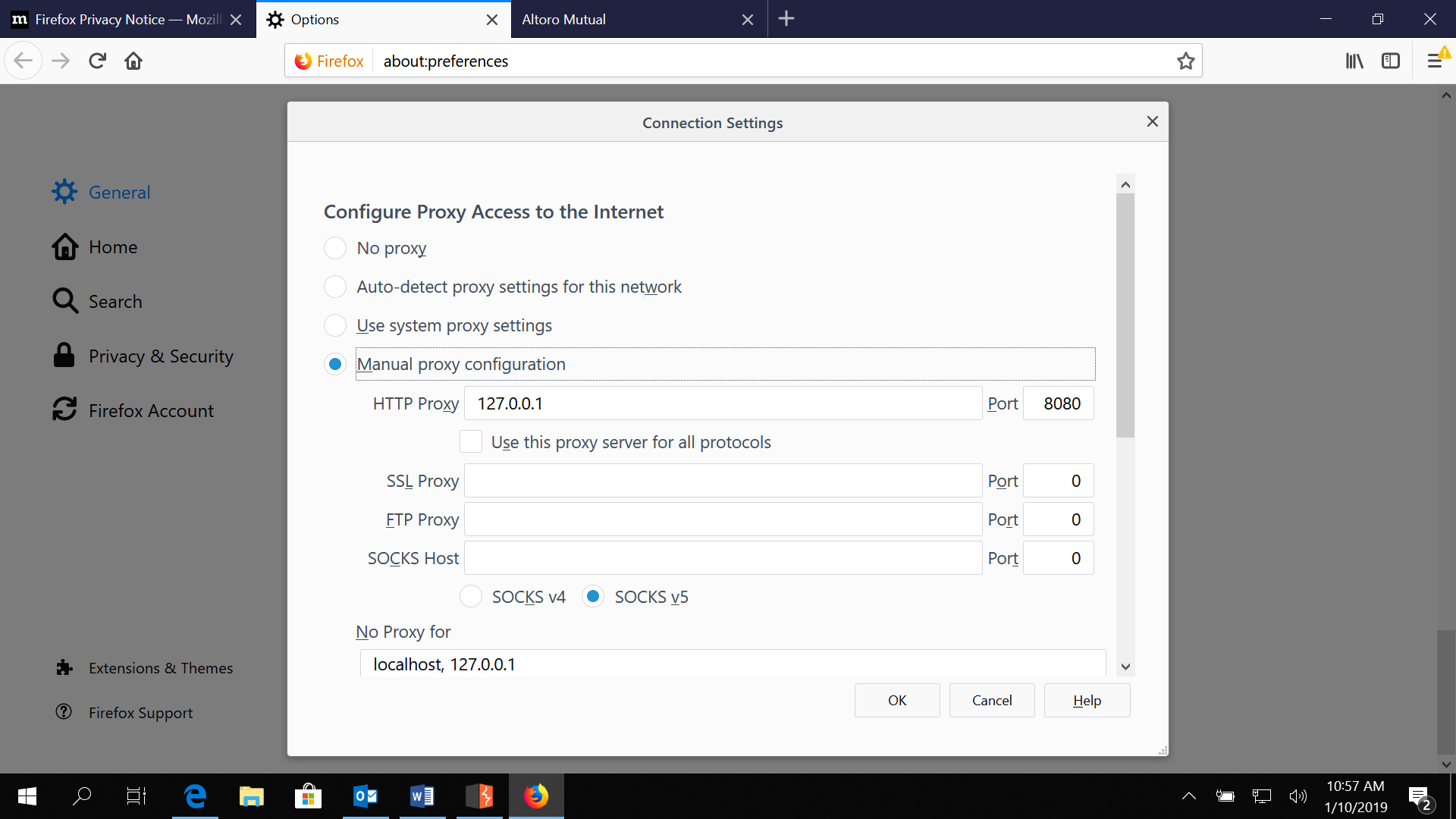
Here we login by the user name of admin

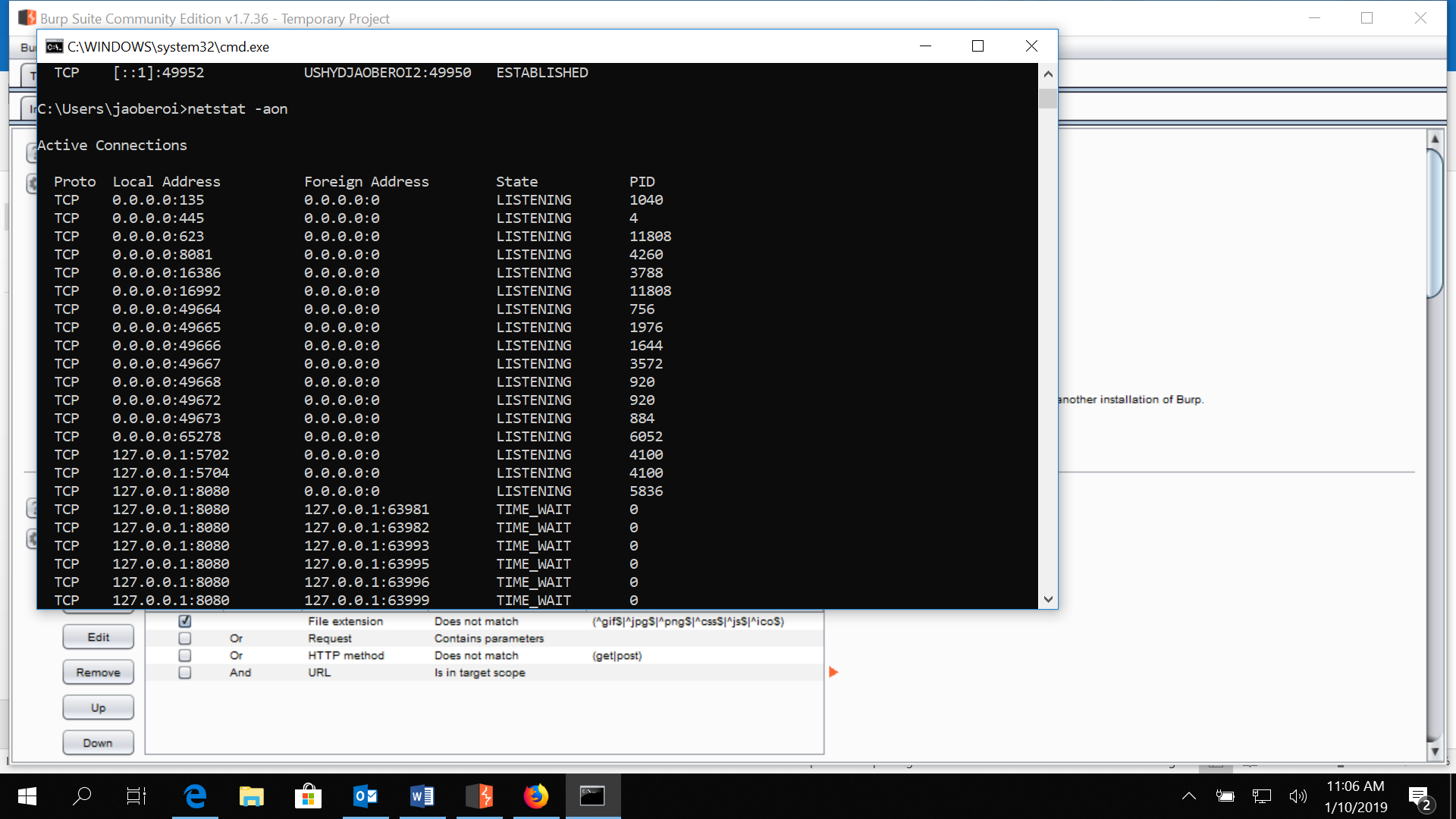
**Burp Suite**

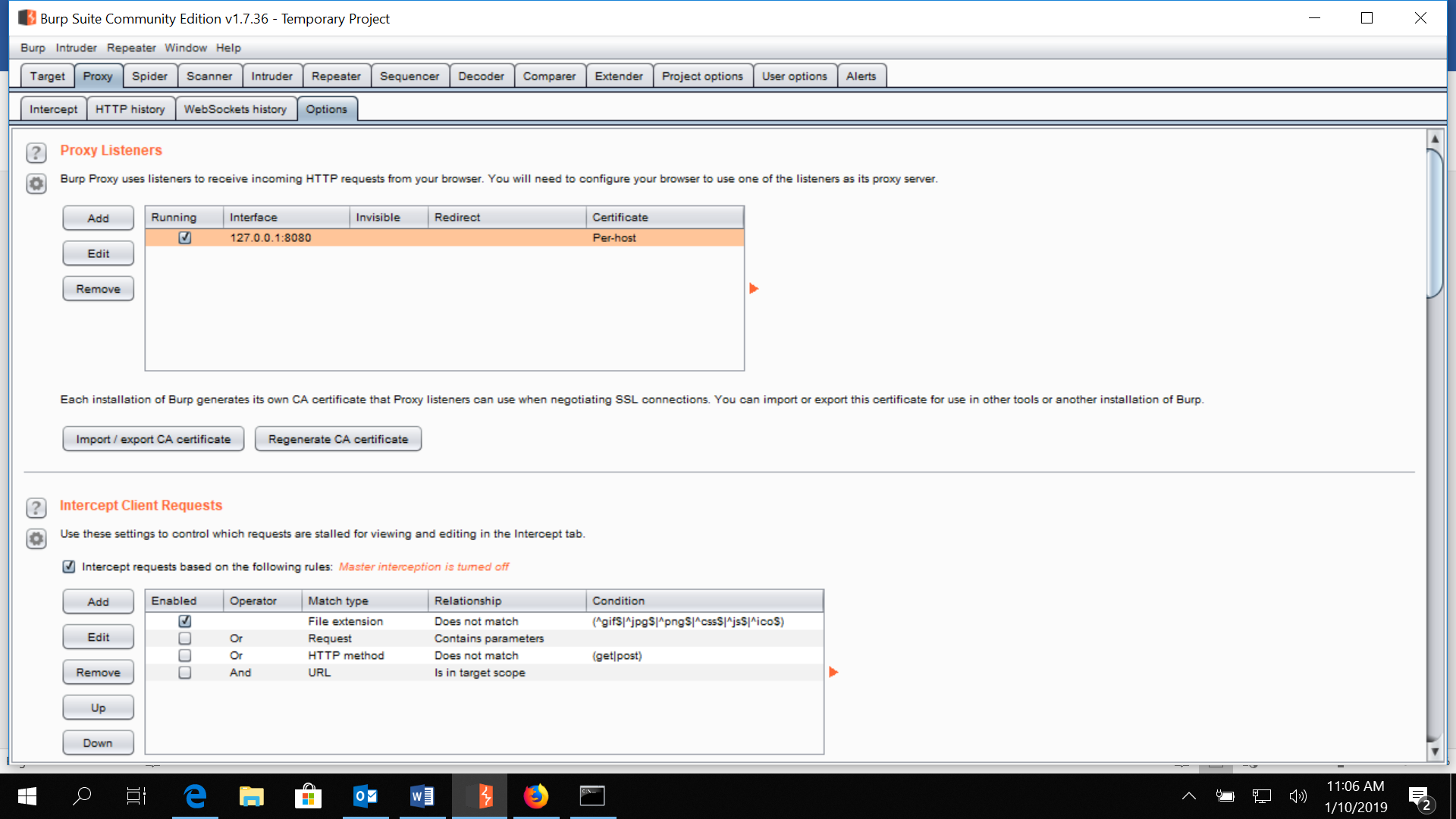


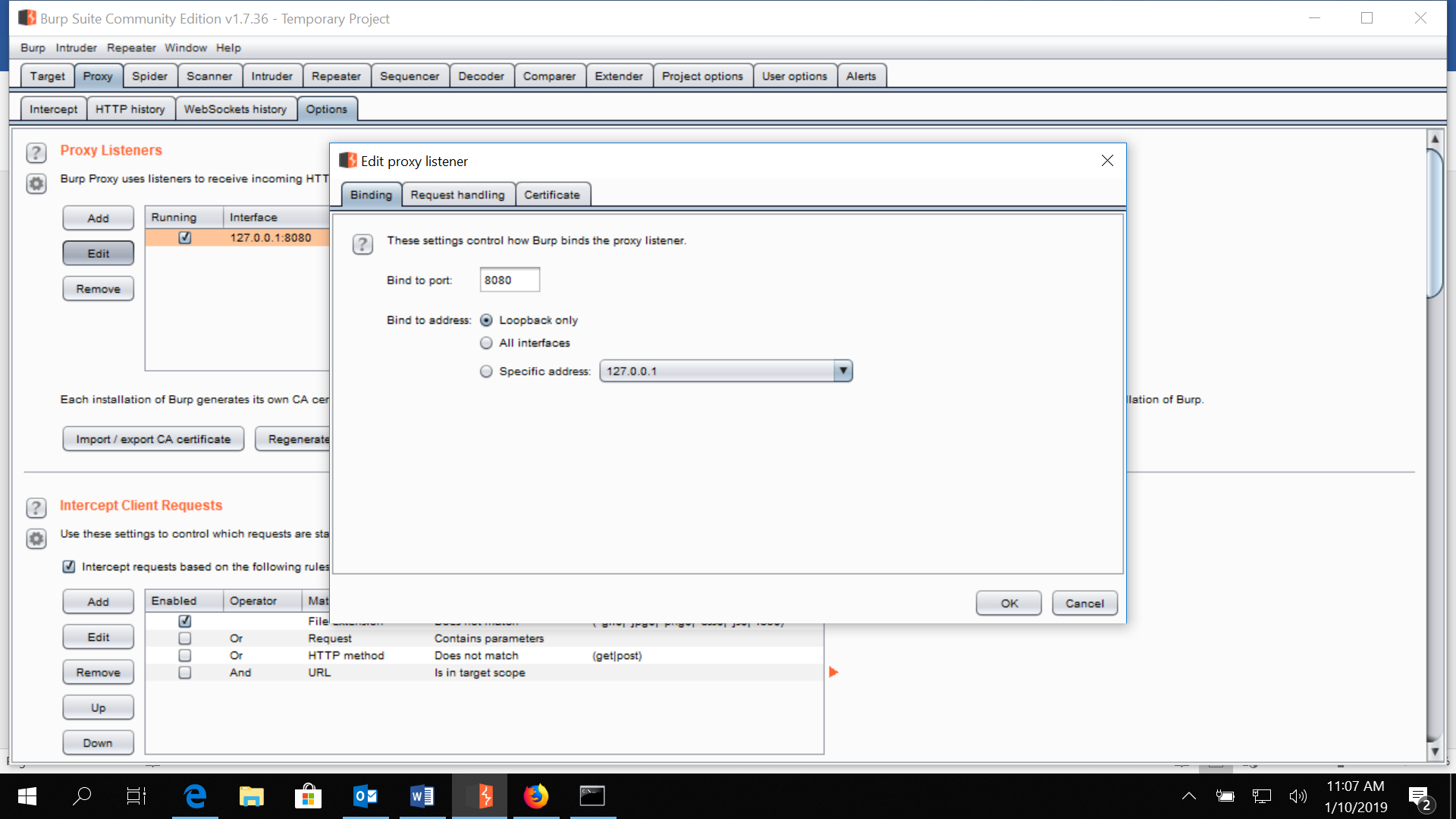




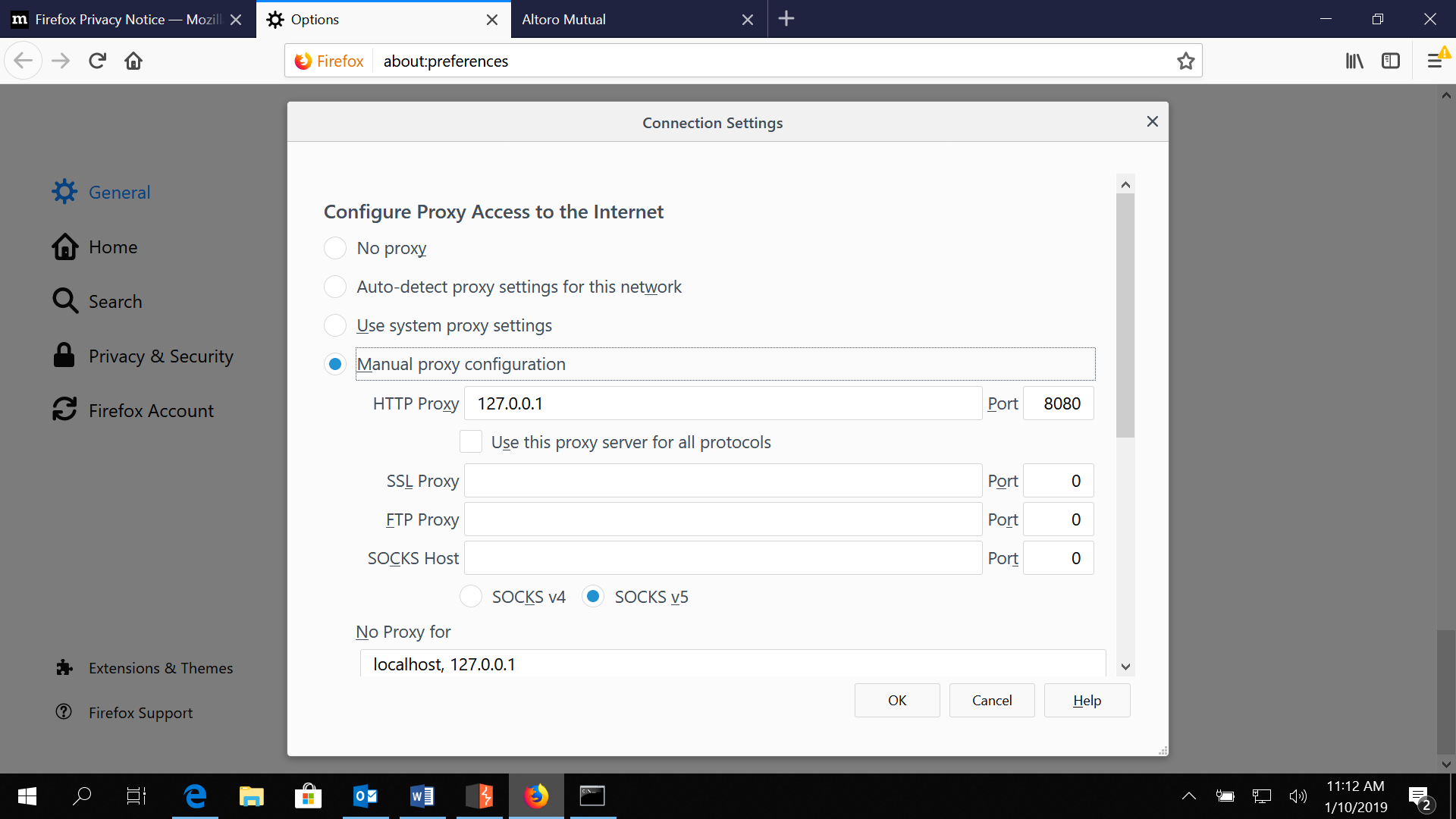






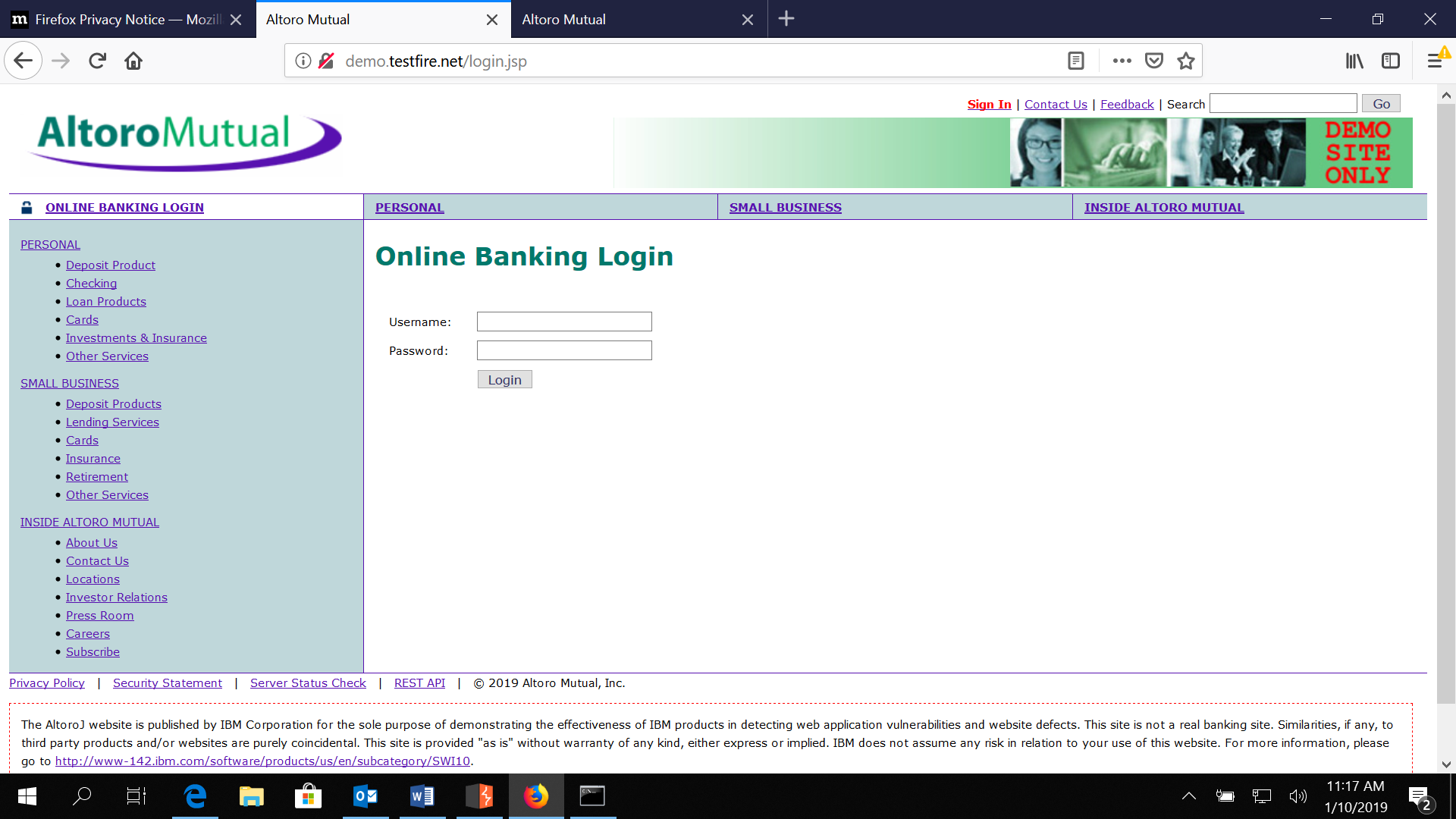


SSl proxy is the HTTPS



SSL proxy must be different for HTTPS

While running proxy put intercept off as the browsers automatically intercept messages



Select \* from users where username=’ ‘ And password=’ ‘

**Blind Sql Injection – Blind as we use universal truth is used in this case**

If comment that is – is black listed use the same in password

User Name= 123' or 1=1—

Password = 123' or 1=1—

Union has a prerequisite that to columns of table must be same and the attribute should also be same

Having should have an aggregate condition

Select \* from users where User Name= 123' or 1=1—and password = ‘admin’ UNION select 1,1,1,1,1,1

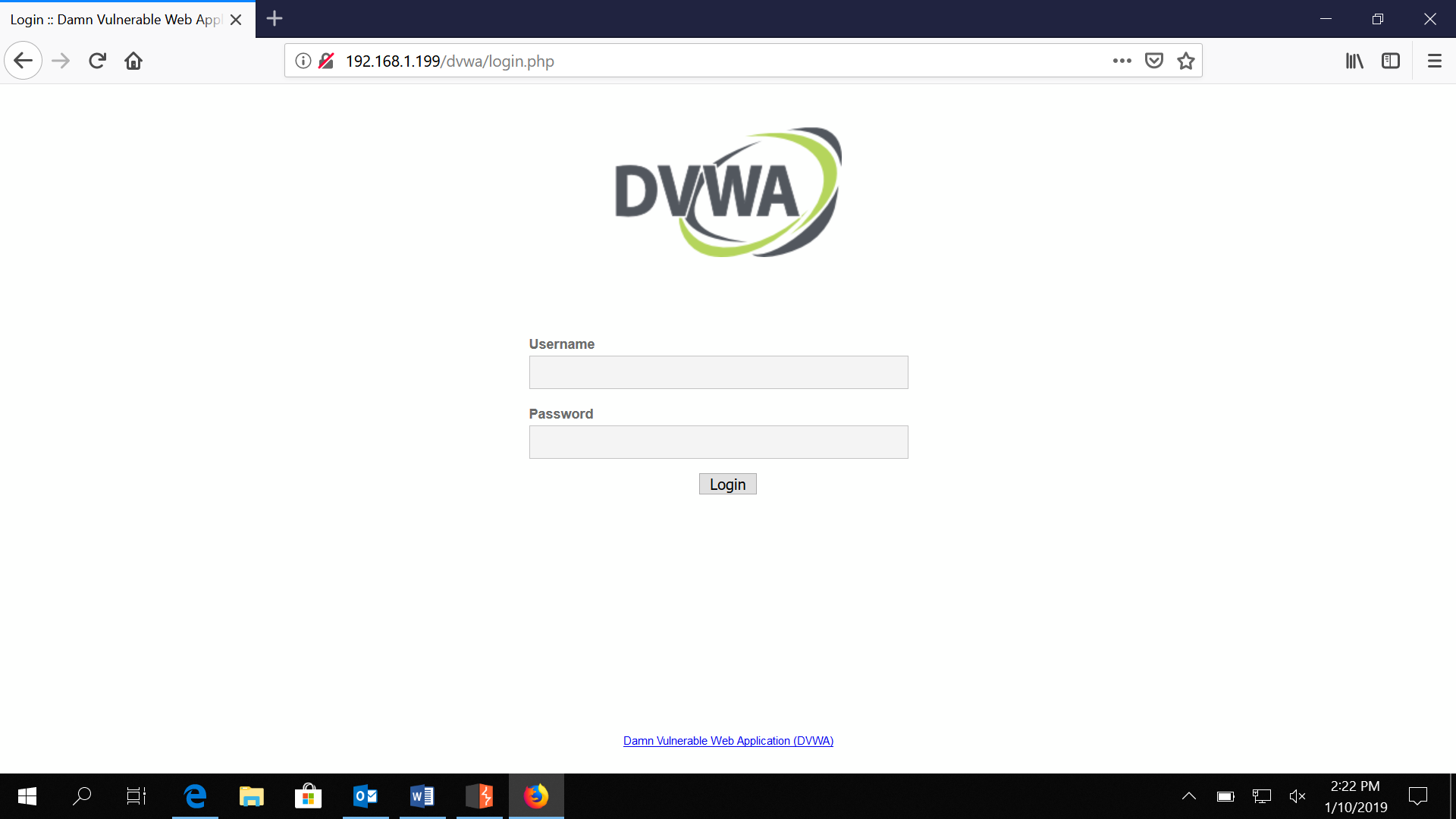
**Sql Injection**

Delay is basically an indication understand how it is used

**Broken Authentication and Session Management**

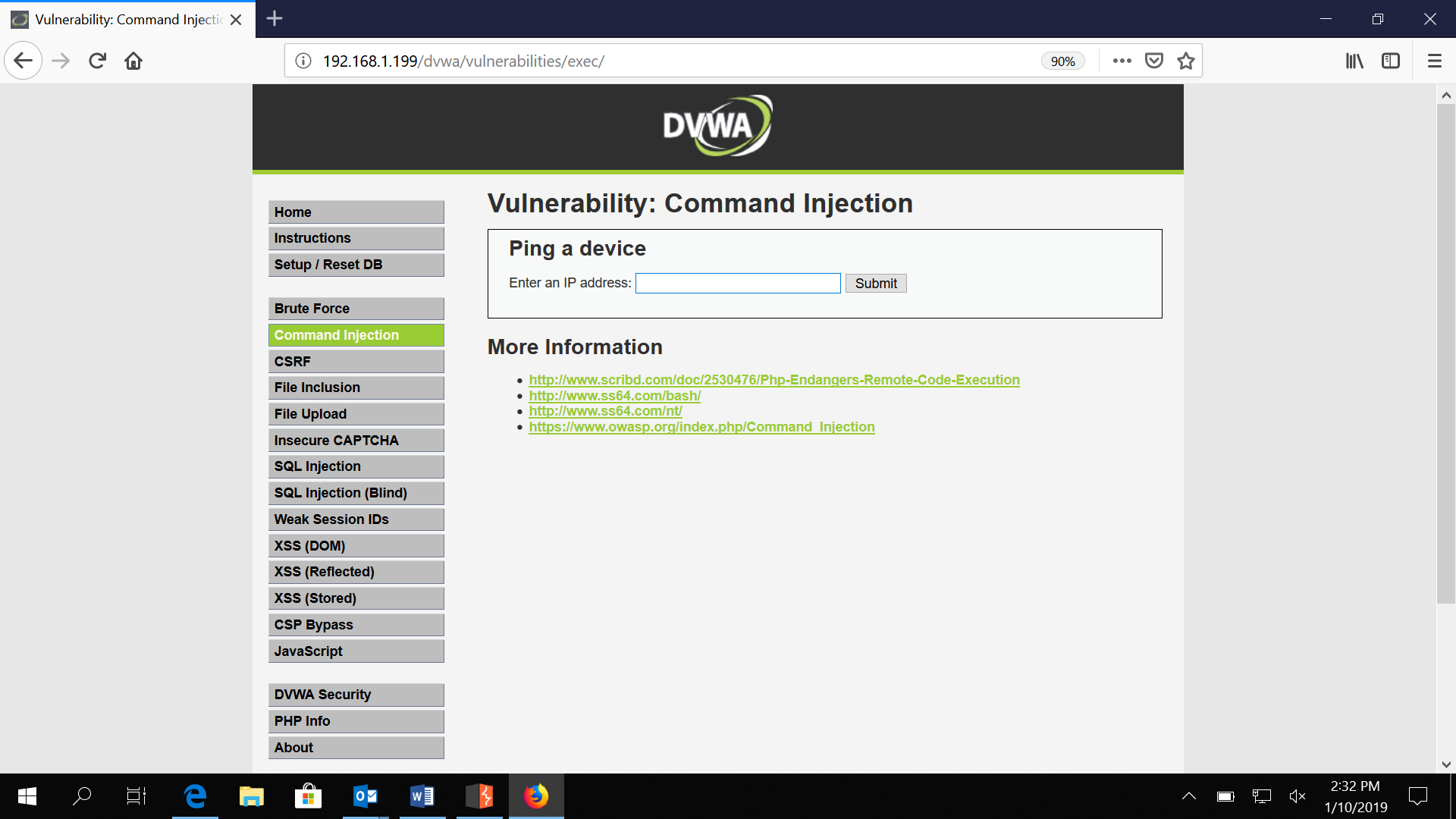
**Authentication Vulnerabilities are checked via the burp suite tool.**

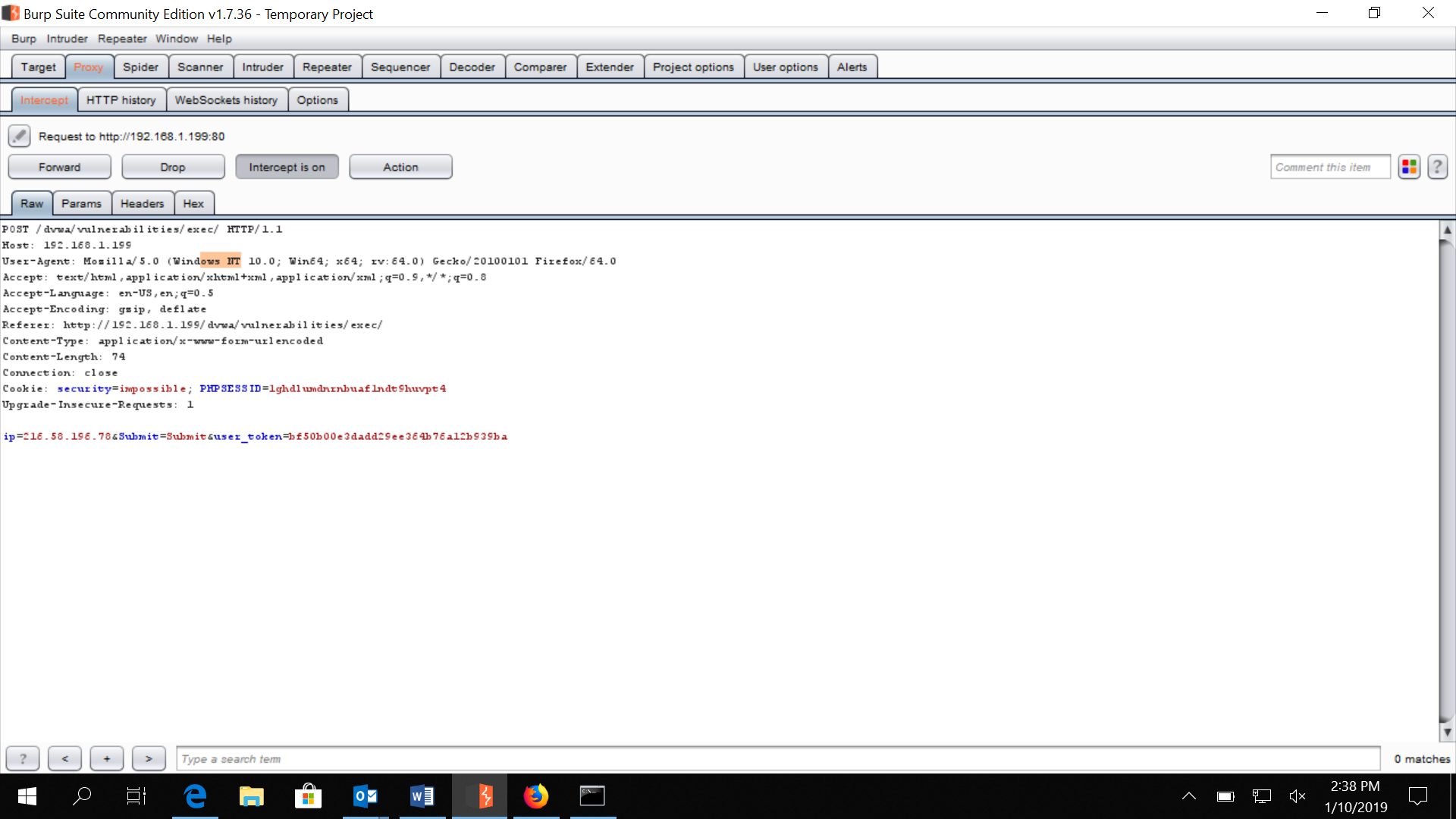
**Cross Site Scripting (XSS)**

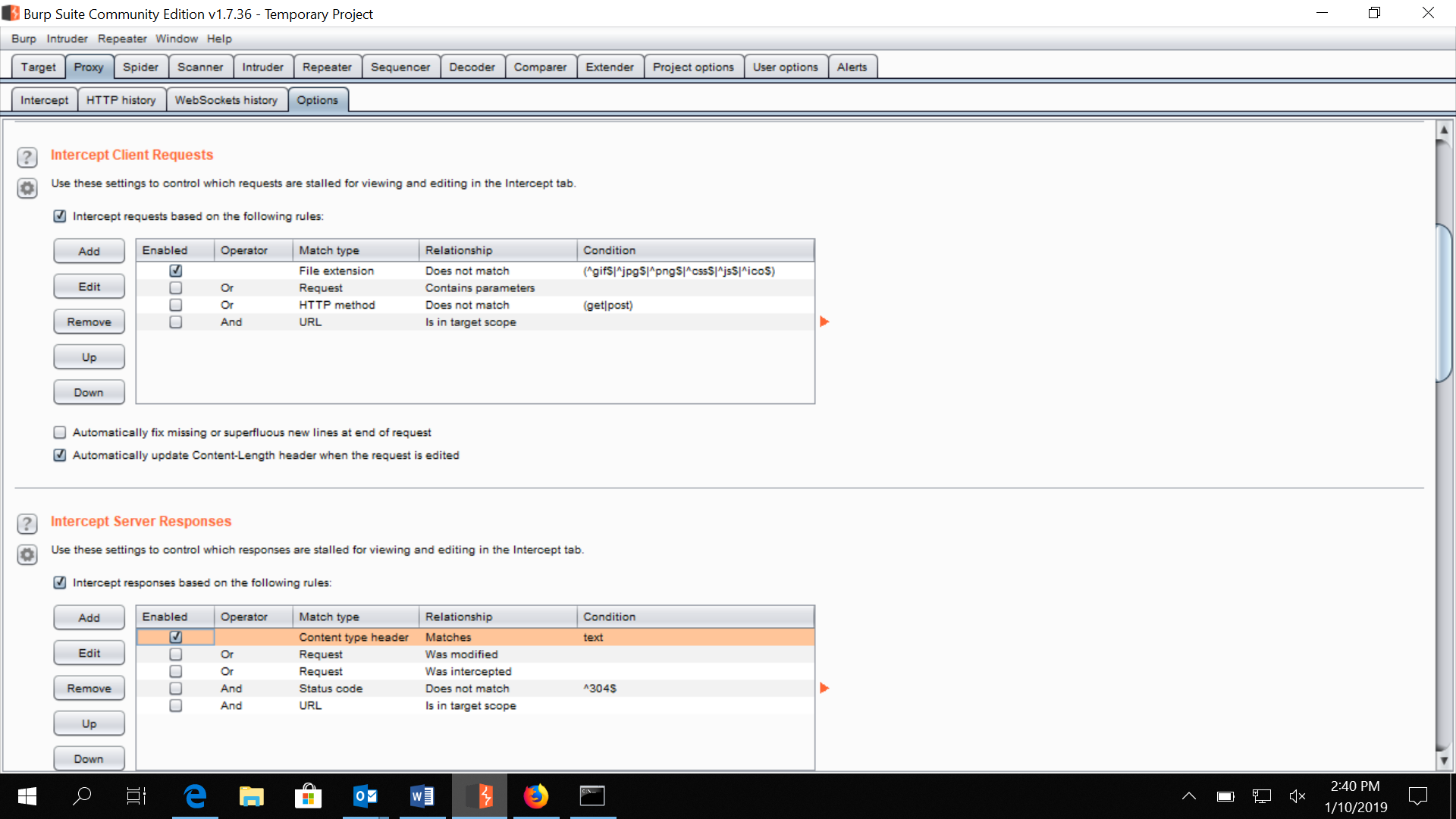




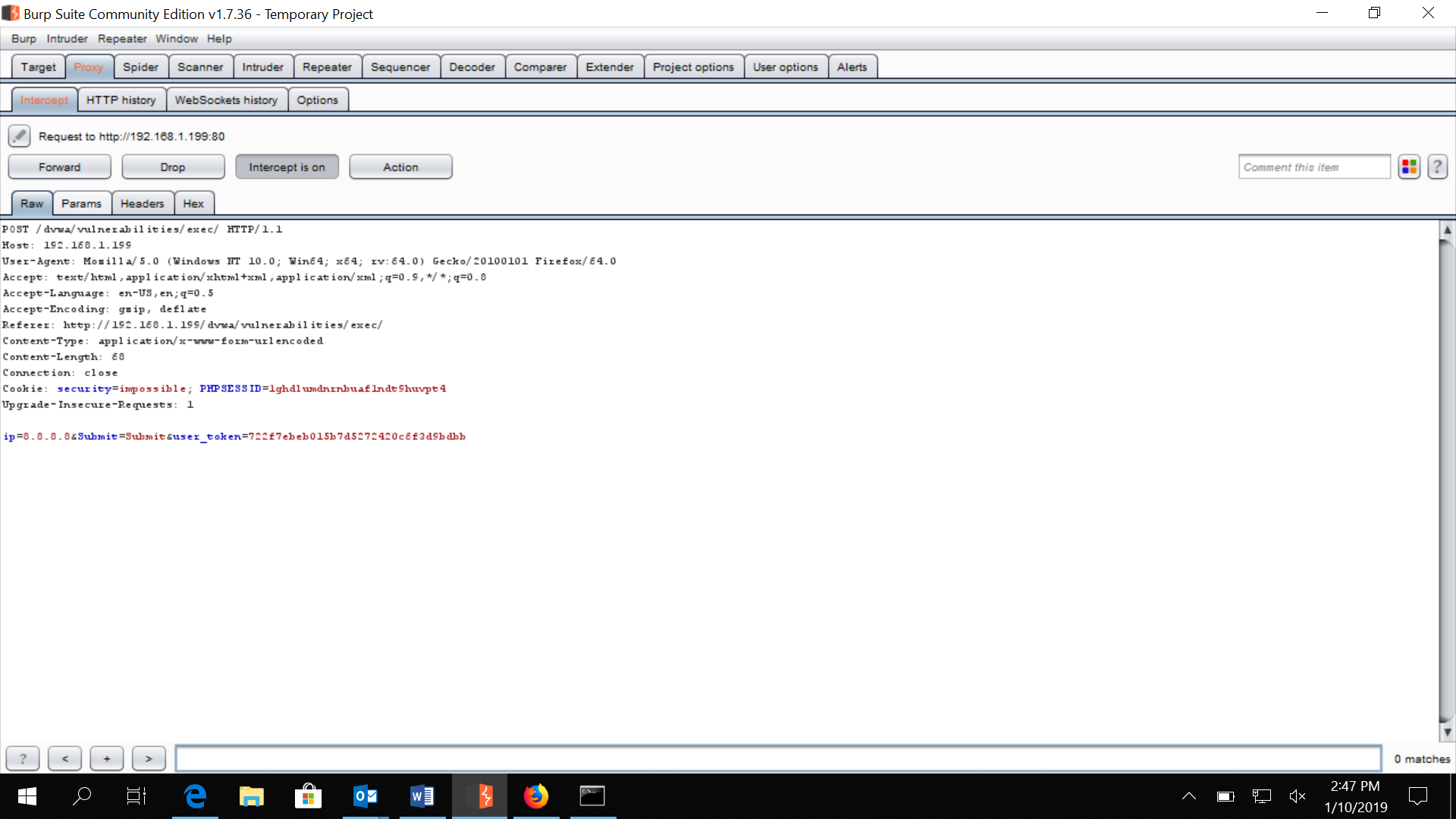
**Target finding files**

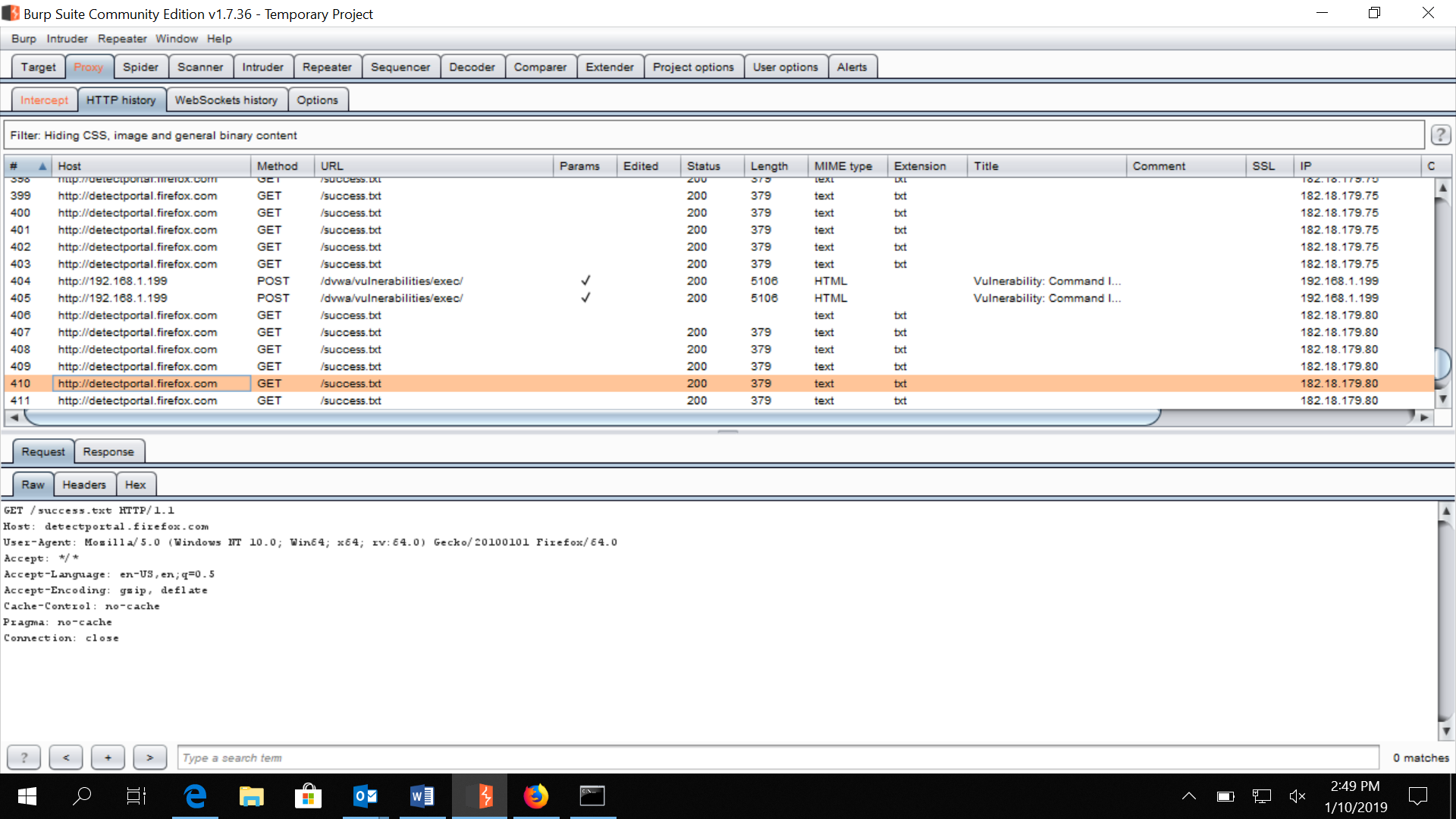


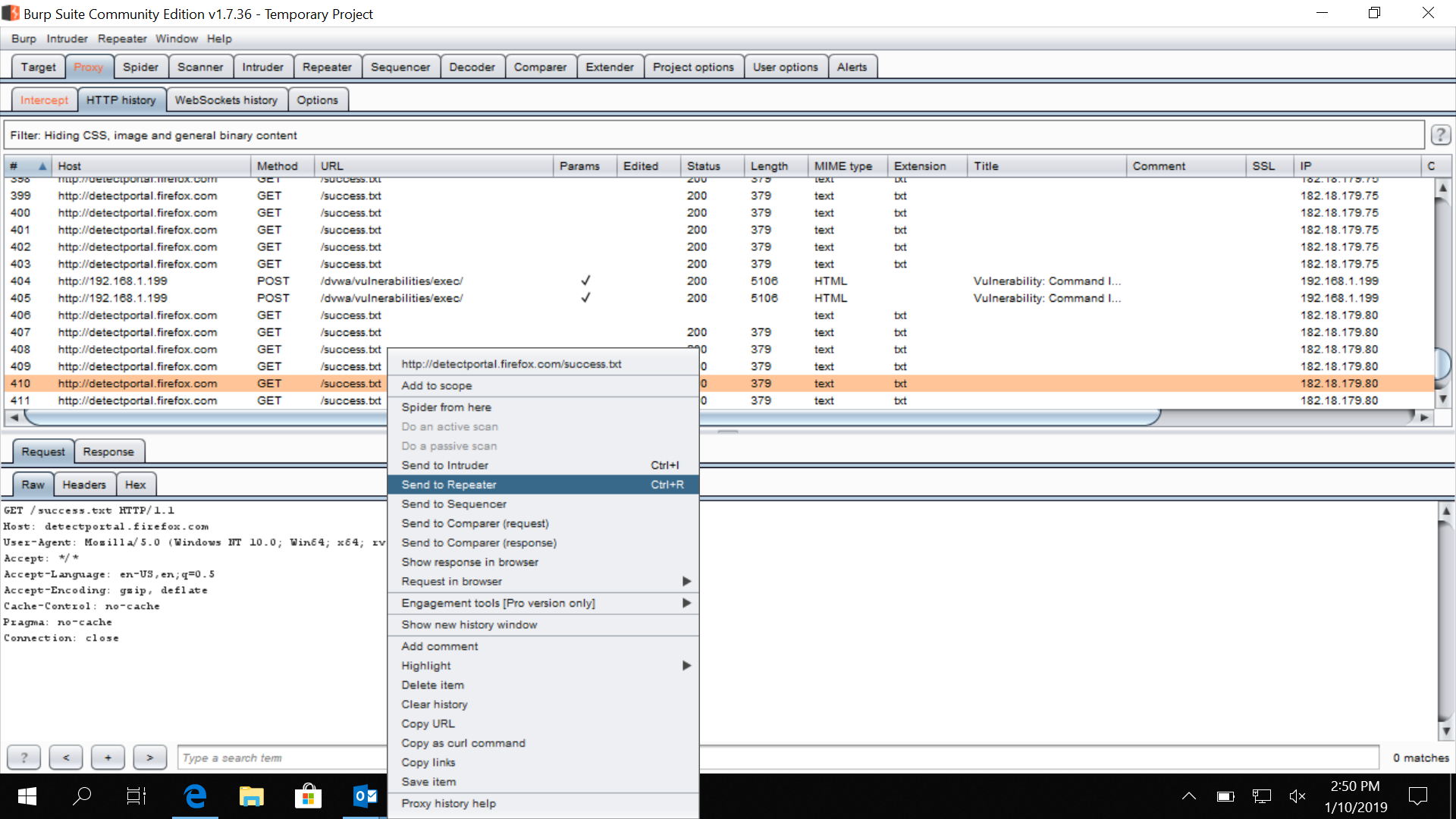


 **to capture response**

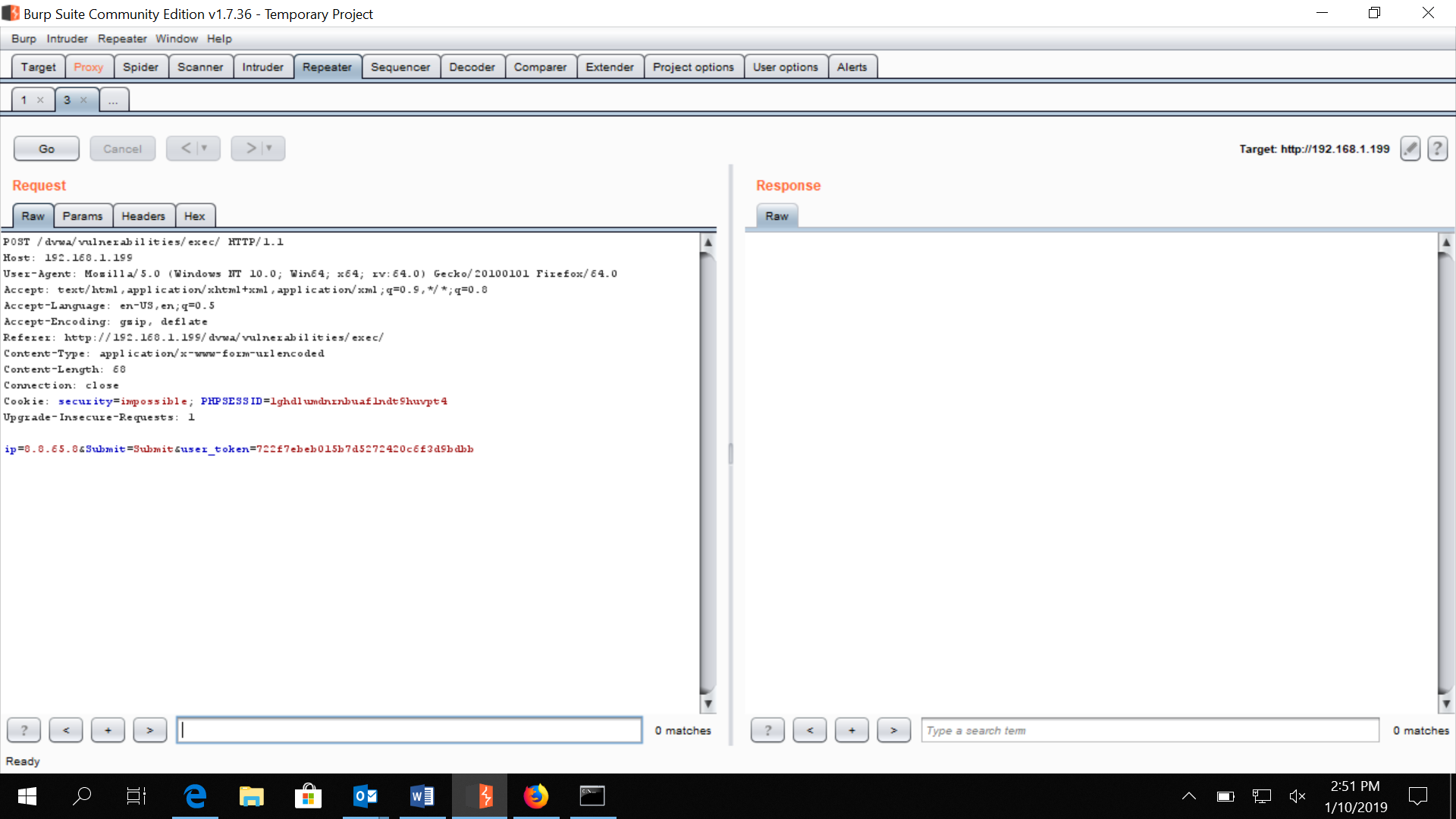
**Headers has info of the server where app is hosted**

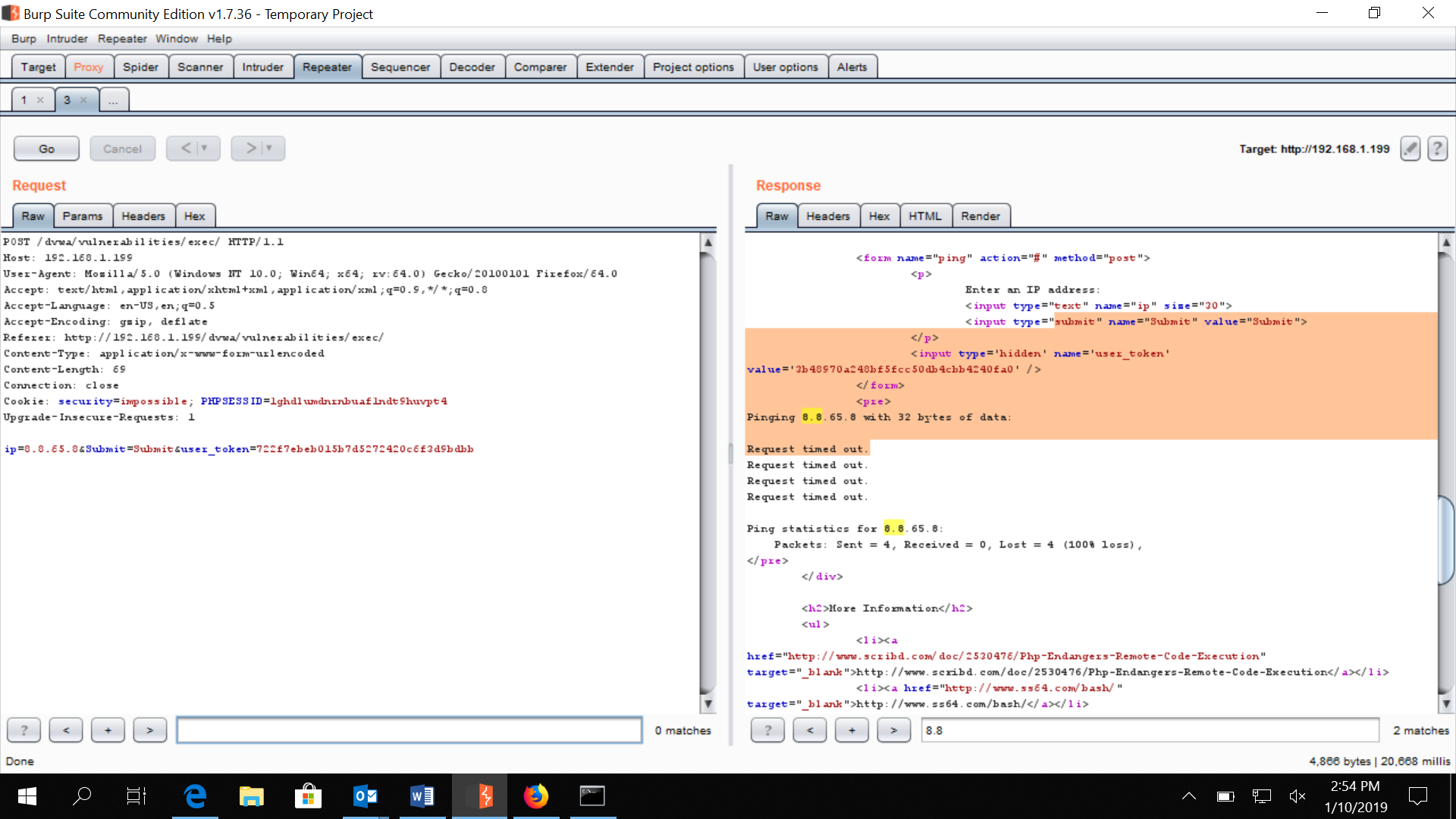
**When we type in** **the ip as 8.8.8.8   
we see the ip in body captured at body** **Changing the ip from repeater**

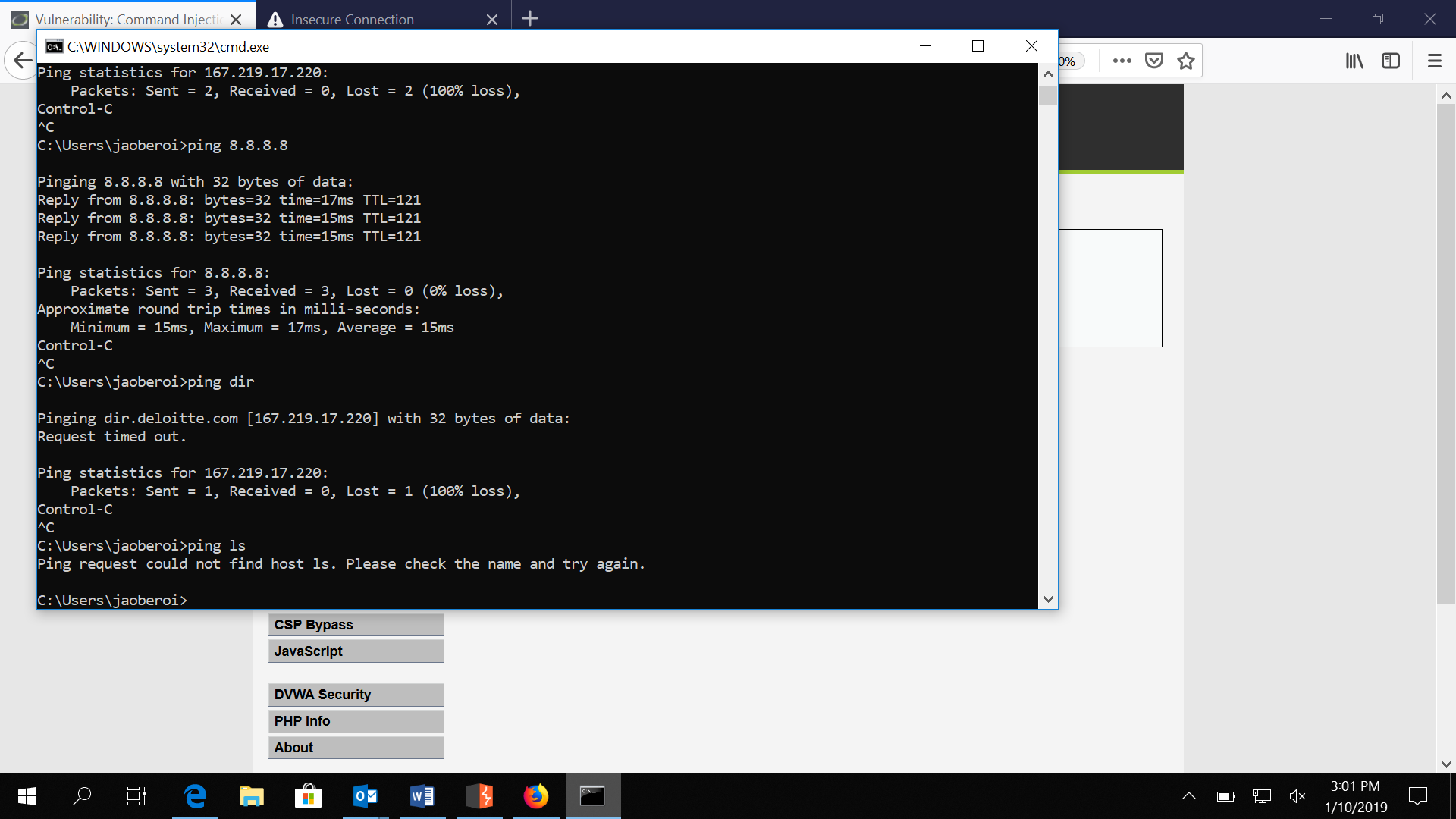


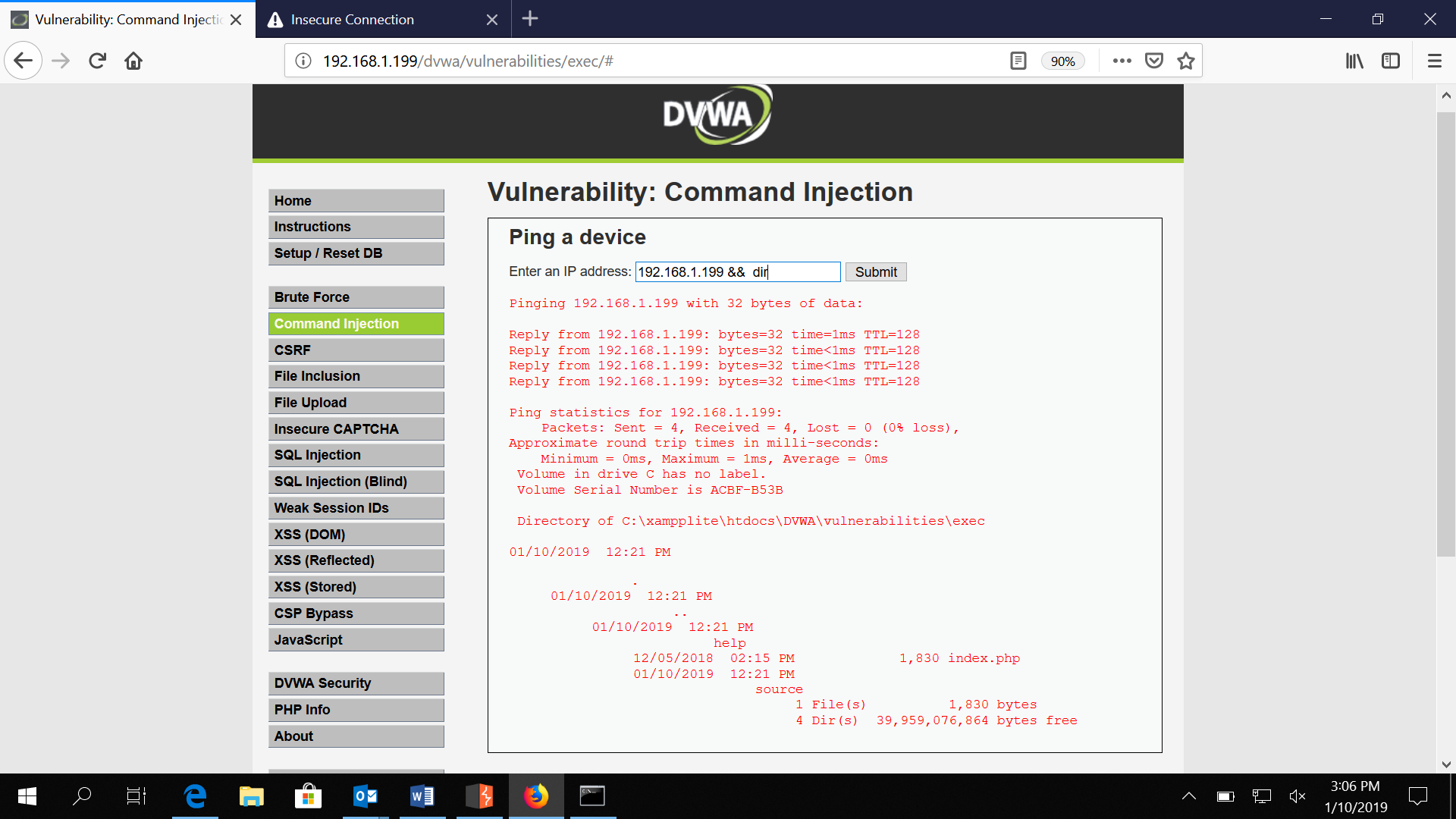


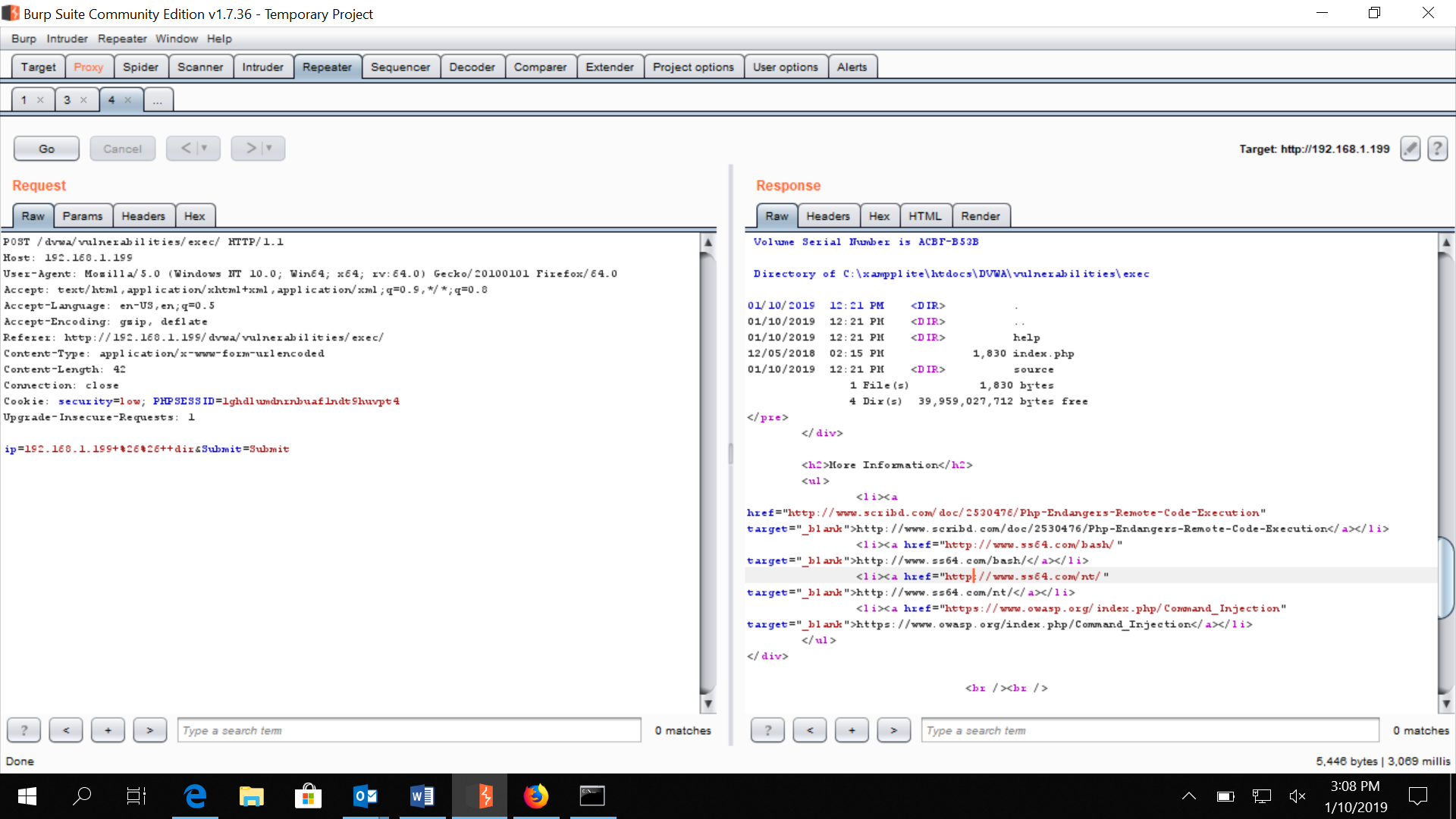
**Change ip and click go**

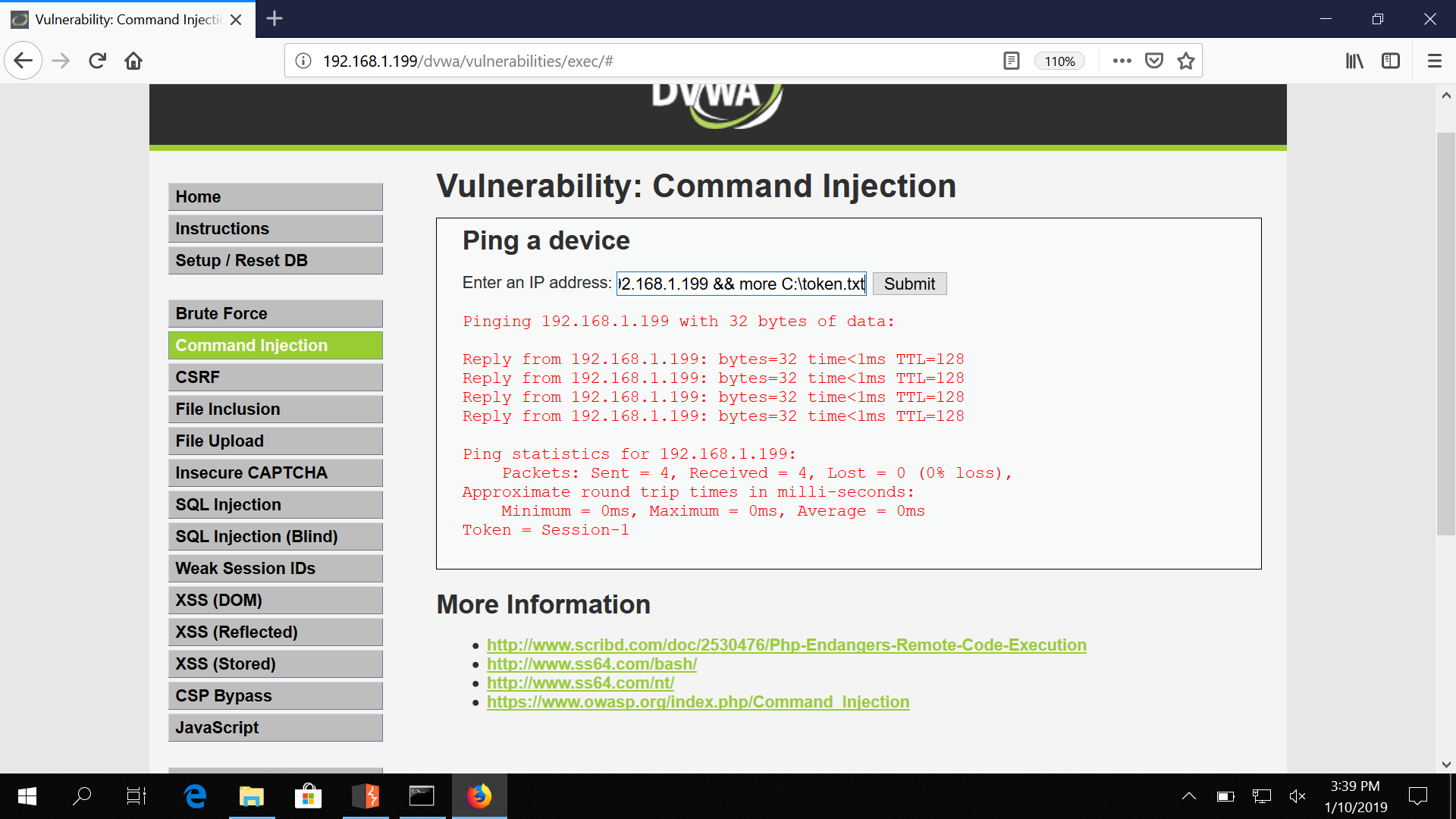


After forwarding 







And here we got the session 

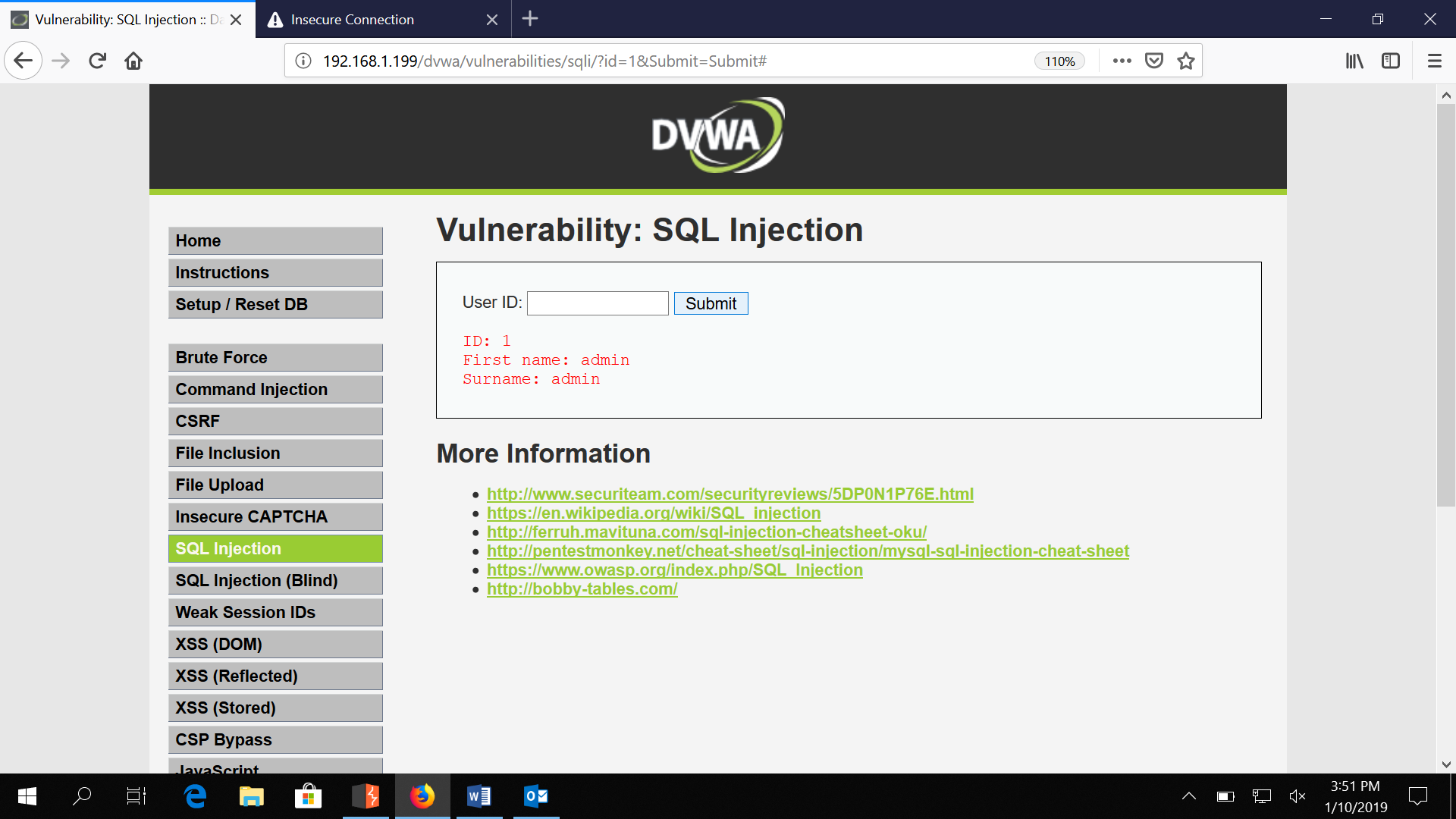
Learning

1. Understand the os of target
2. Understand cmd of Windows
3. We understand string concatenation

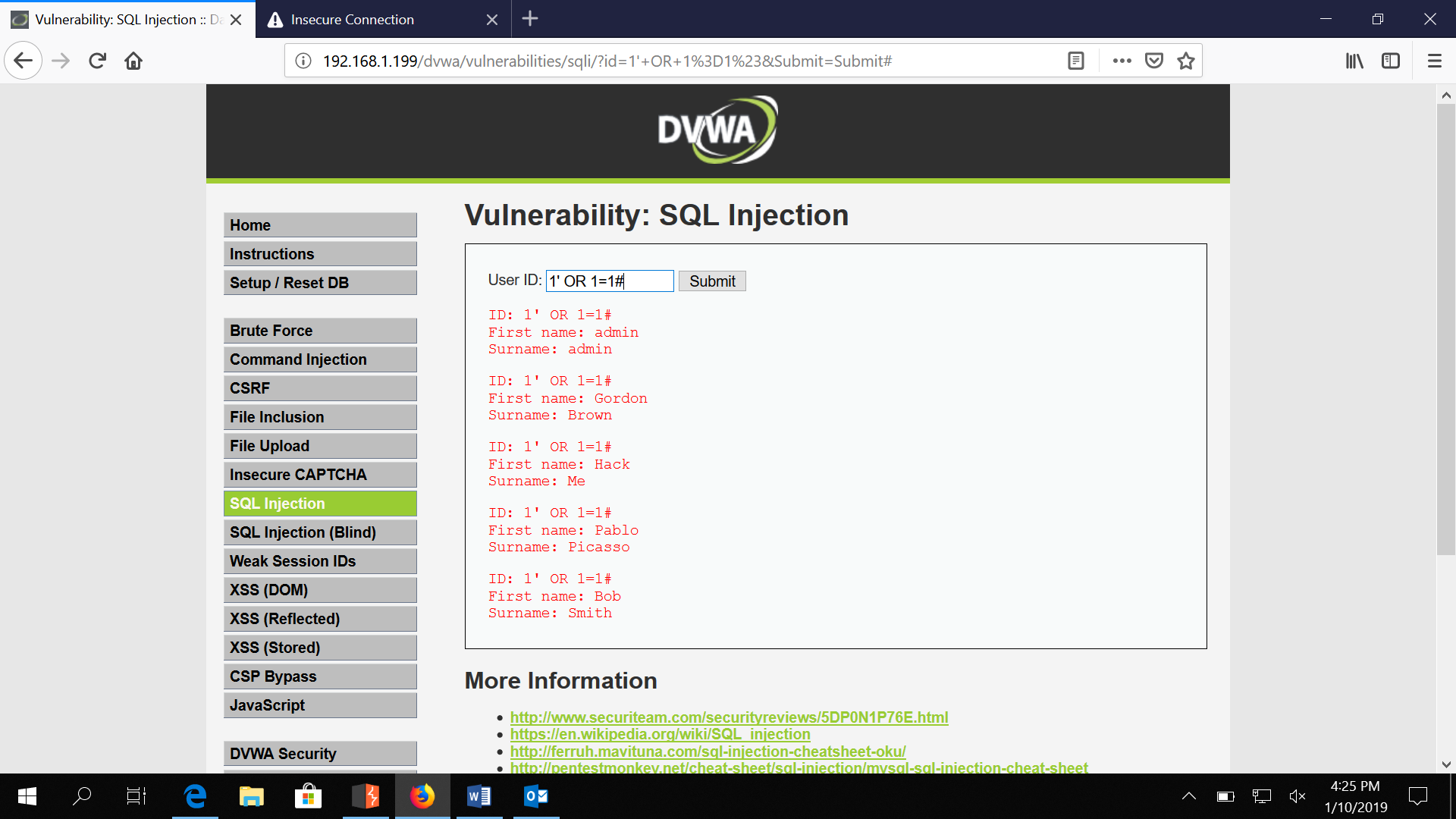
Response is **INPUT ENCODING**

**Also try learning output encoding and input encoding.**

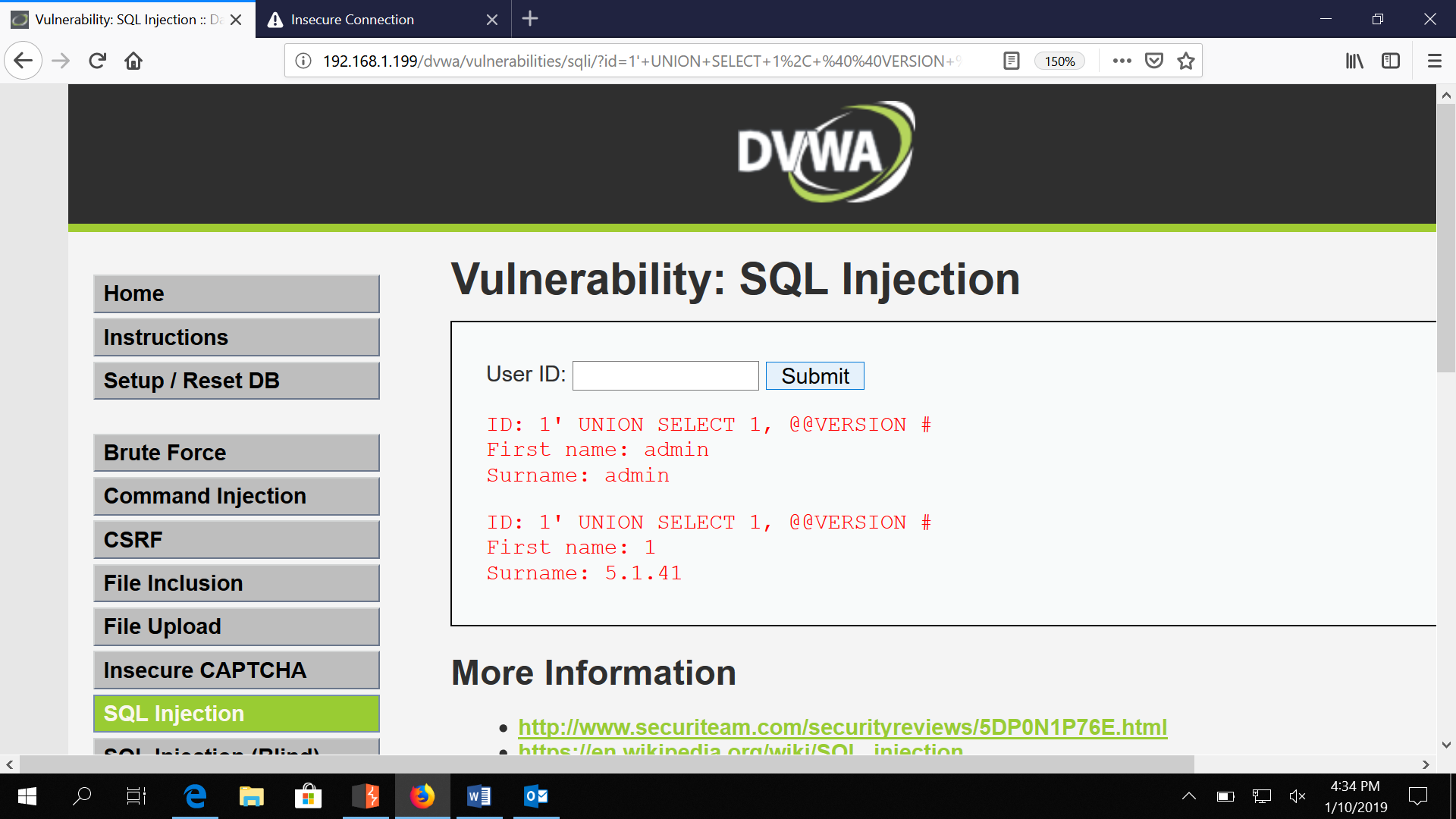
**MY SQL ----- SQL INJECTION**



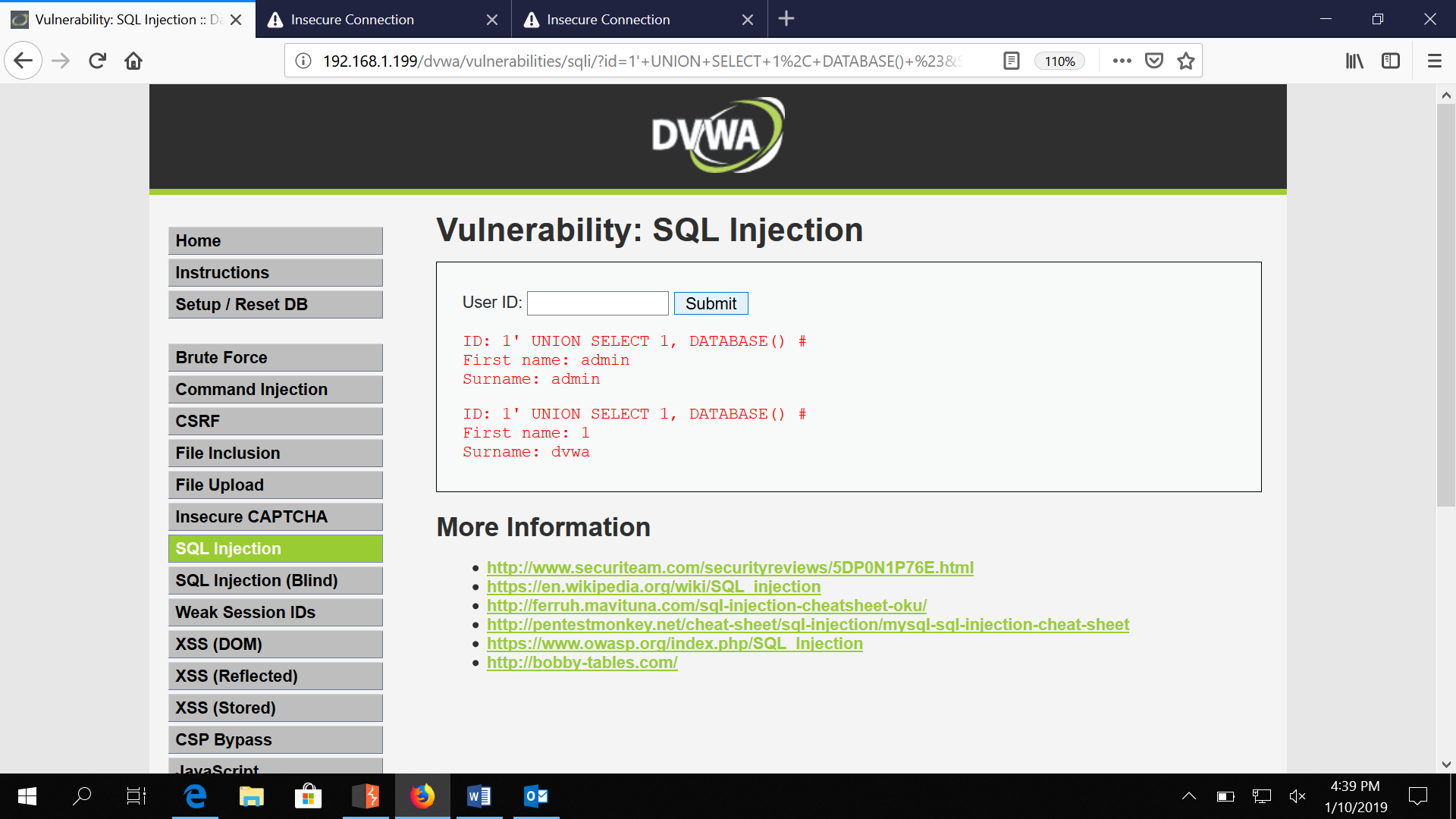
Till 5



# IS COMMENTING FOR MYSQL

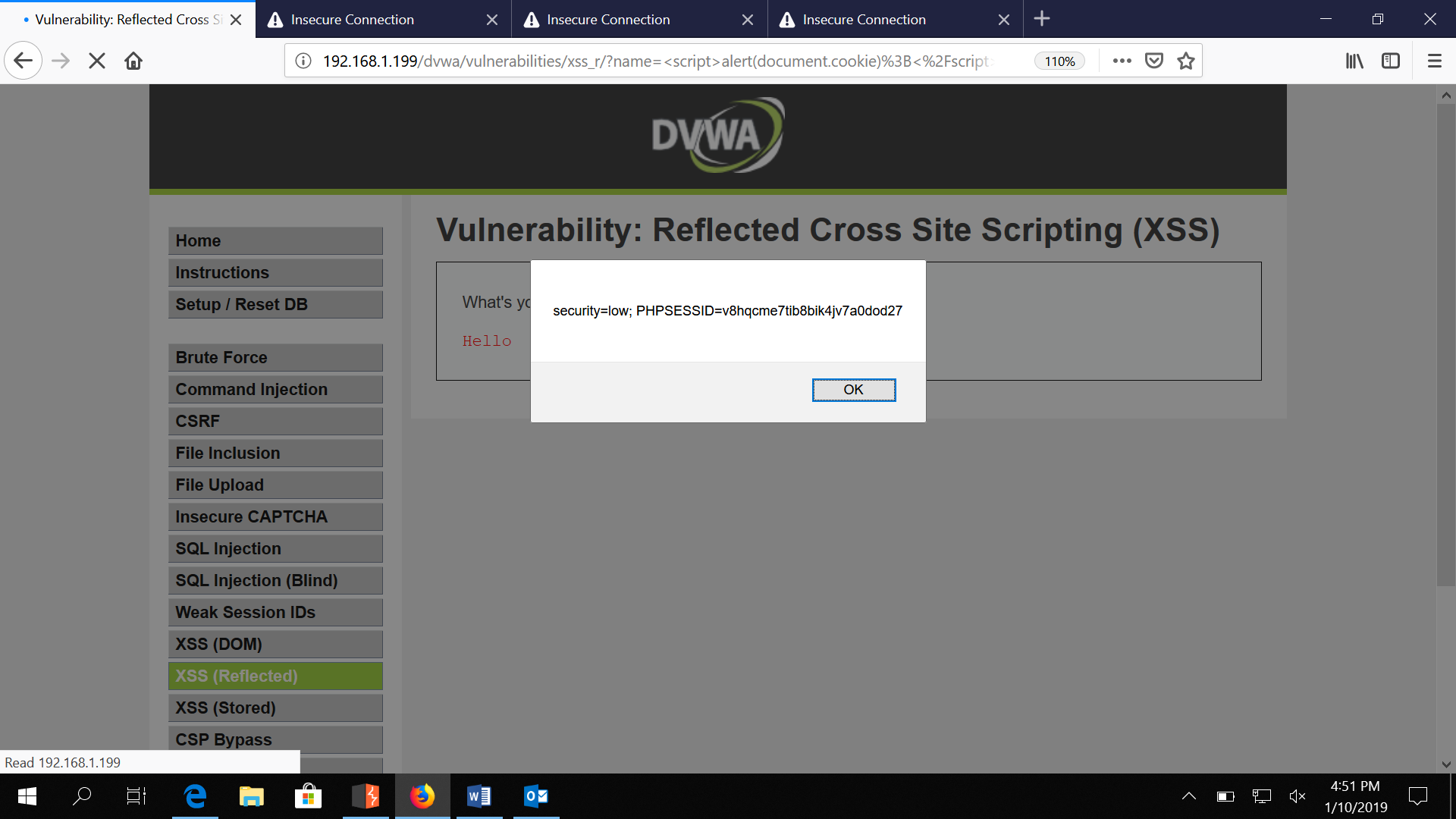
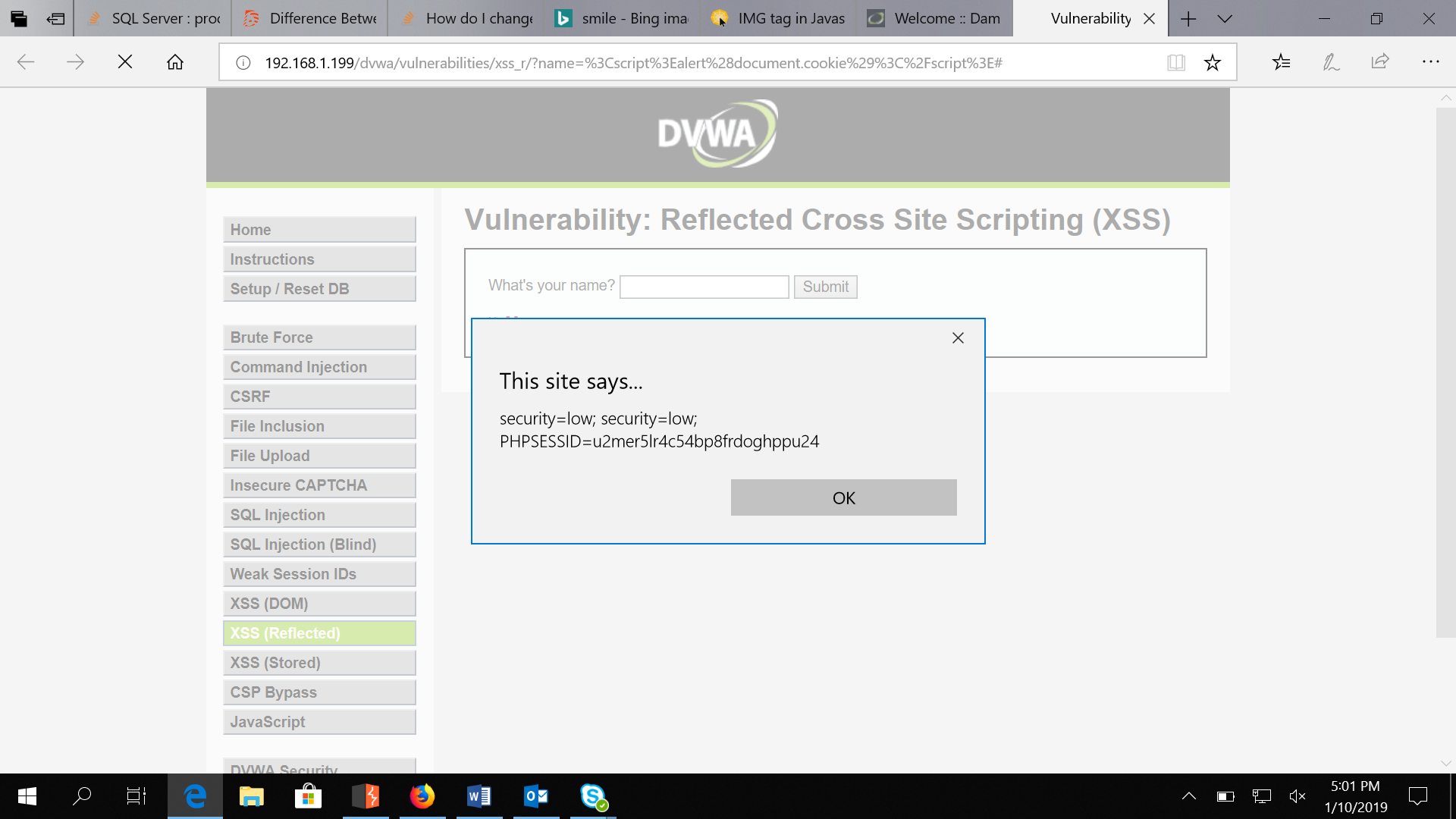


Fing Database Name



<script>alert(document.cookie);</script>

We capture our own cookie js payloa script for our won browser



Send url for this

http://192.168.1.199/dvwa/vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28document.cookie%29%3B%3C%2Fscript%3E#