

Project: Major  
Member: konark patel (8849492455)  
Aravind Dattathreya Nandala ( 9000499796)  
Santhosh Rajan(7448645467)  
Shakir Ahmad Barbhuiya( 9101494287)  
project name: openbugbounty

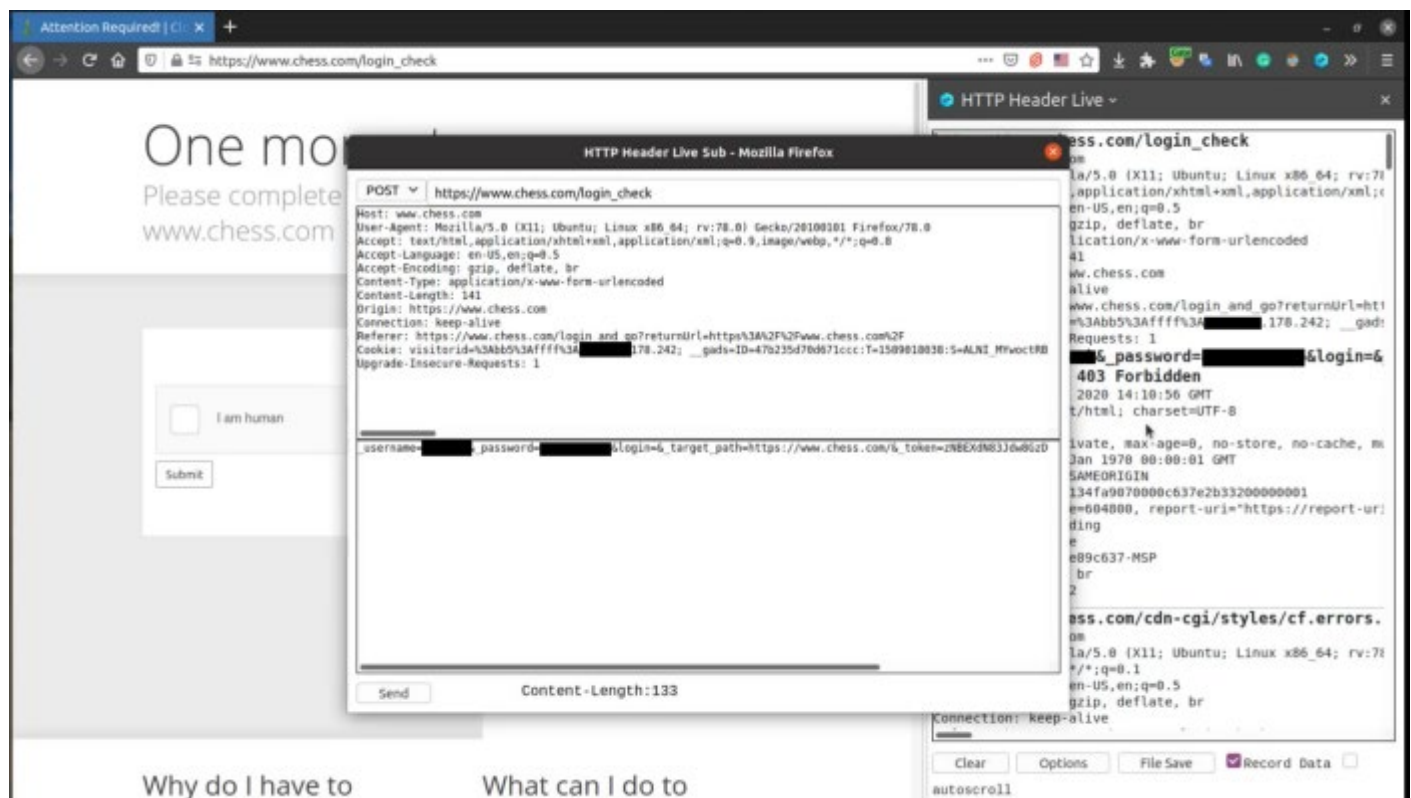
Chess.com is the #1 online chess website and has an [internal bug bounty program](#)

## Don't rely on one tool

The hunting story started one day on login page, Chess.com redirected me to another page for solving Cloudflare hCaptcha. I think, It was for using my VPS IP on login page by proxy and Cloudflare had placed my IP in graylist.

I've used [HTTP Header Live](#) sometimes and in this case use it too. After login the server will redirect user to the following link for solving Captcha:

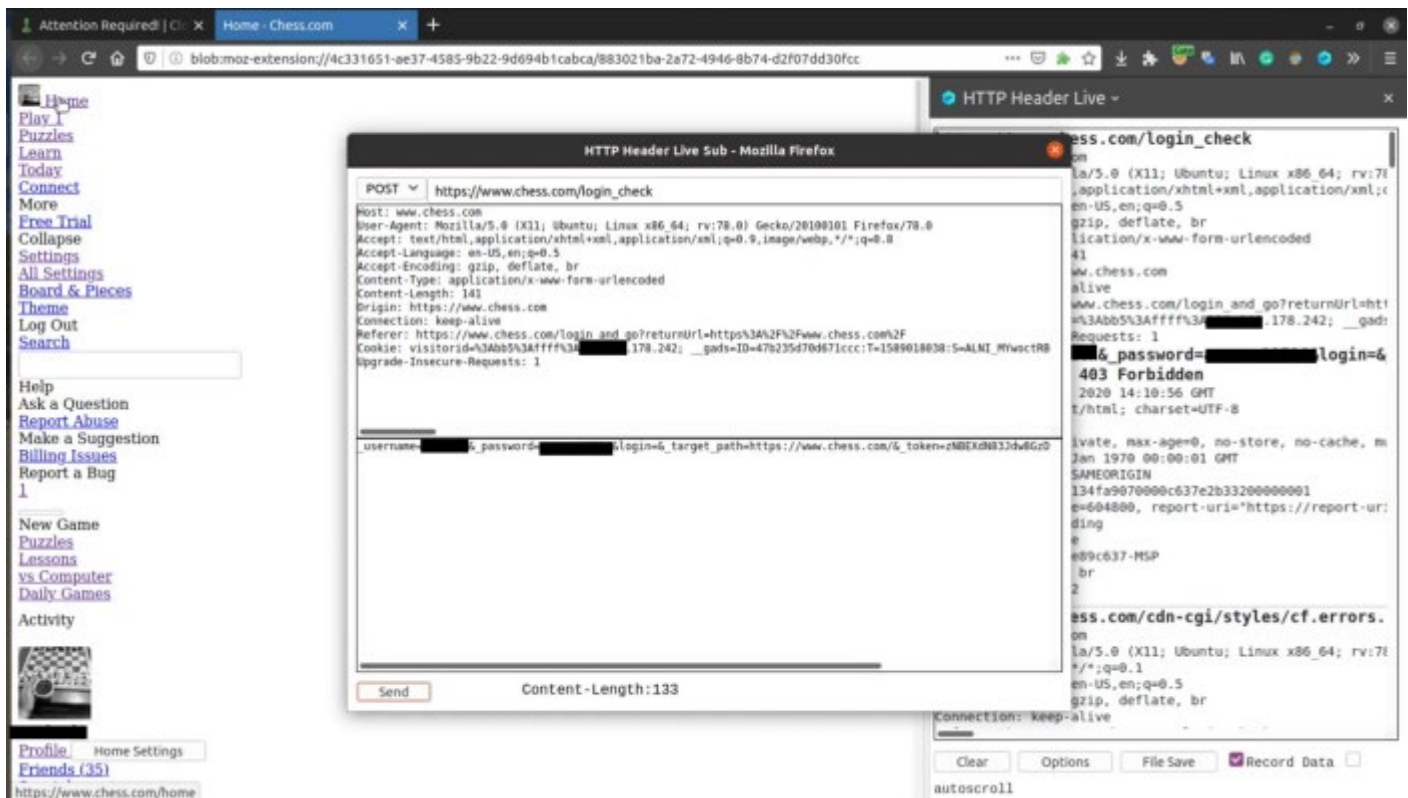
[https://www.chess.com/login\\_check](https://www.chess.com/login_check)



[https://www.chess.com/login\\_check](https://www.chess.com/login_check)

The **HTTP Header Live** intercepts requests like Burp. If you click on a request a window will appear on screen and you can change or resend request.

In this case request was POST and my username and password was in body. I've just resend it and the following page loaded!



## HTTP Header Live

After clicking on **Home** button the hCAPTCHA bypasses and you can login without solving the captcha because hCAPTCHA has a misconfiguration on the server. You can't reproduce these steps by Burp because **HTTP Header Live** uses blob URL (Look at address bar in the image above). So don't rely on one tool!!!

## Test all functions in applications

There are two methods for logging in to Chess.com. The first one is via username and the second one is via email. If you enter wrong password more than 10 times you have to solve a captcha. But what's the bug?

In fact there was a misconfiguration on login page via email which after entering 10 wrong attempts login the captcha doesn't appear and an attacker can run brute-force attack for each user leads to lock victim's account.



Invalid security CAPTCHA code. Please try again.

██████████@gmail.com

Password

[Forgot Password?](#)

☐ Remember

Log In

or connect with

 Facebook

 Google

New? [Sign up - it's FREE!](#)

[Help](#) | [Terms & Privacy](#) | Chess.com © 2020

If the user uses mobile app will see the following error:




10 min

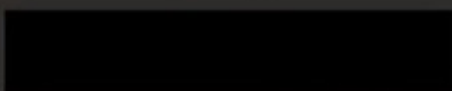


vs Random



Options 

**Play!**



...



vs Computer



Tournaments

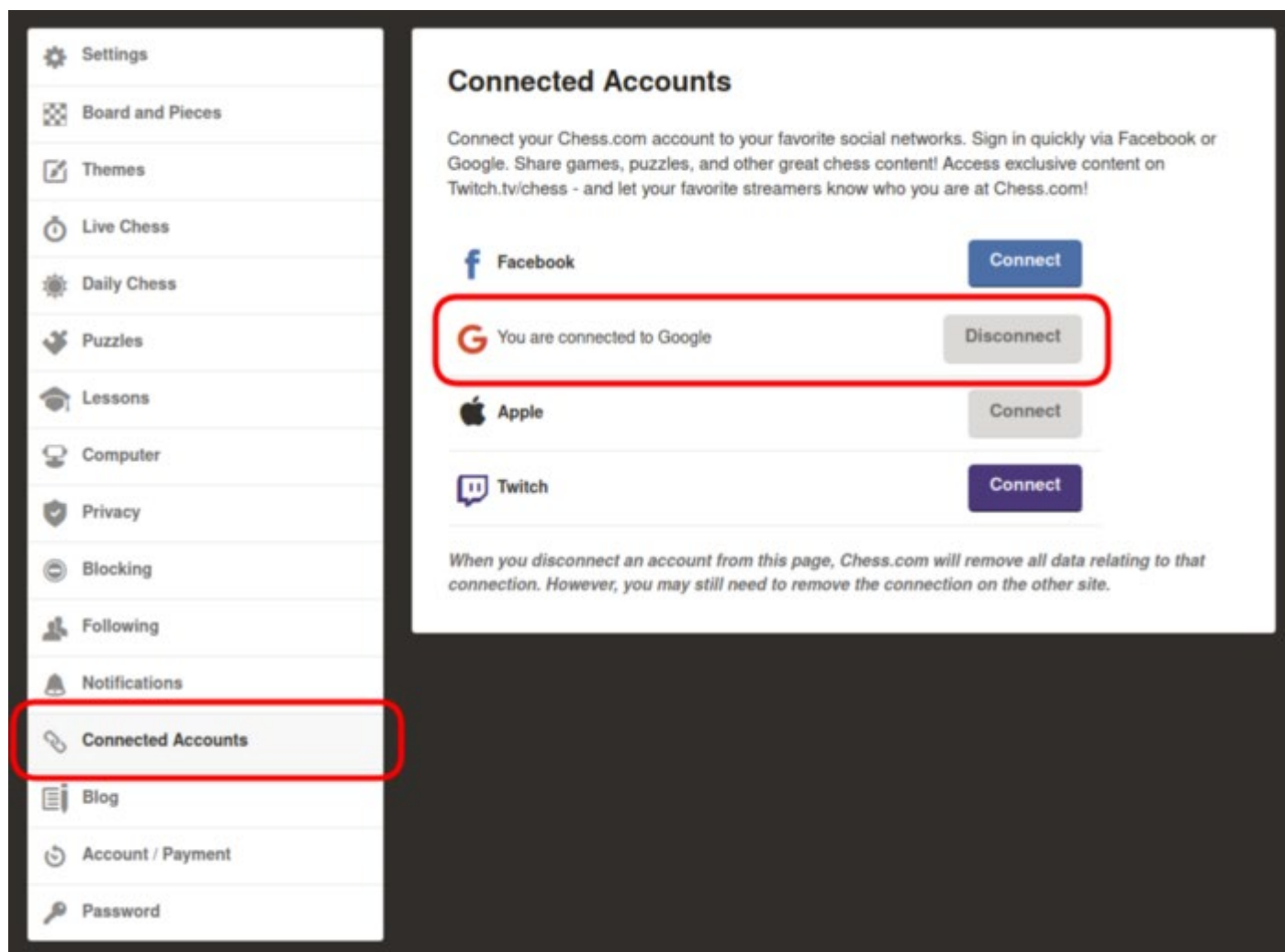
The user should login on the Chess.com website and solve the Captcha for unlocking the account.

**So as a bug hunter, you should test all functions on the application.**

## Checking CSRF's deeply

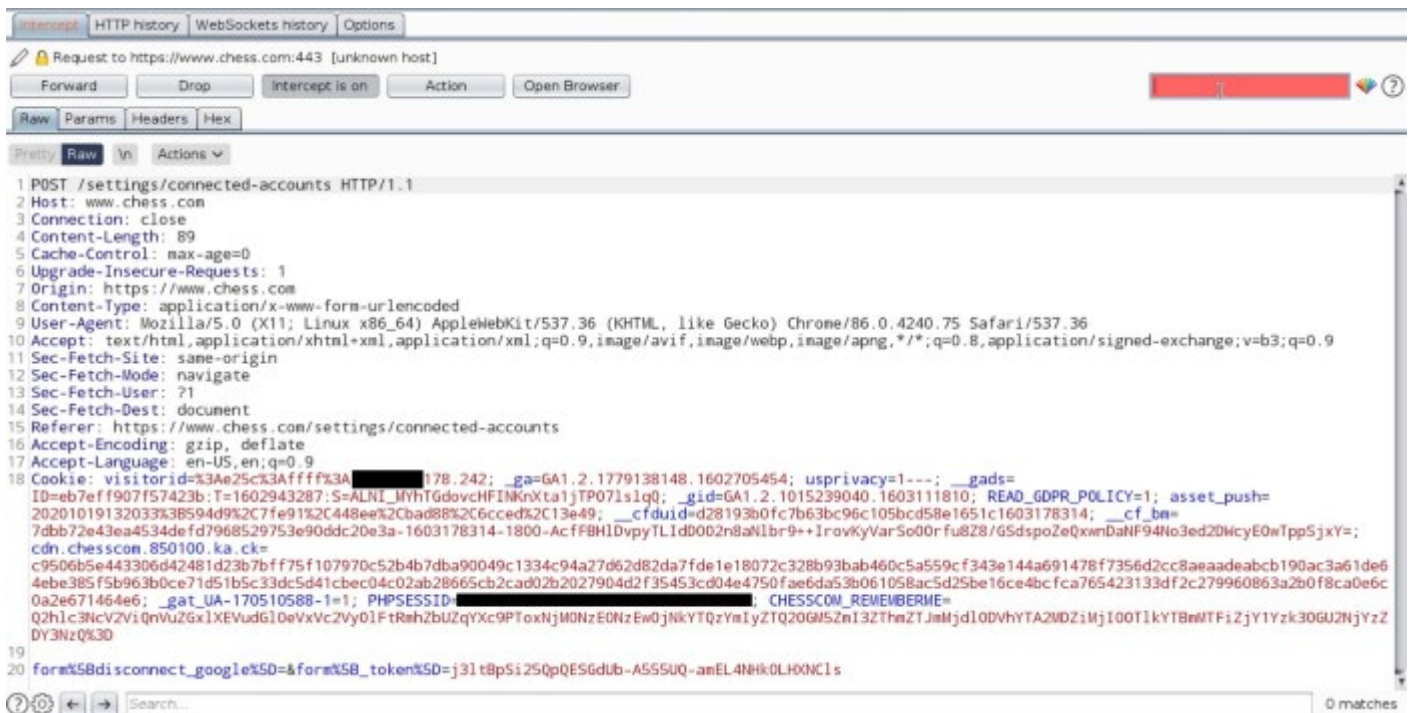
There is a function in Chess.com that you can login via Google, Facebook, ... accounts but there is a problem there.

You can disconnect from those accounts from the setting menu and the bug still stays there.



When the user clicks on disconnect button, a POST request sends to server like the following image:

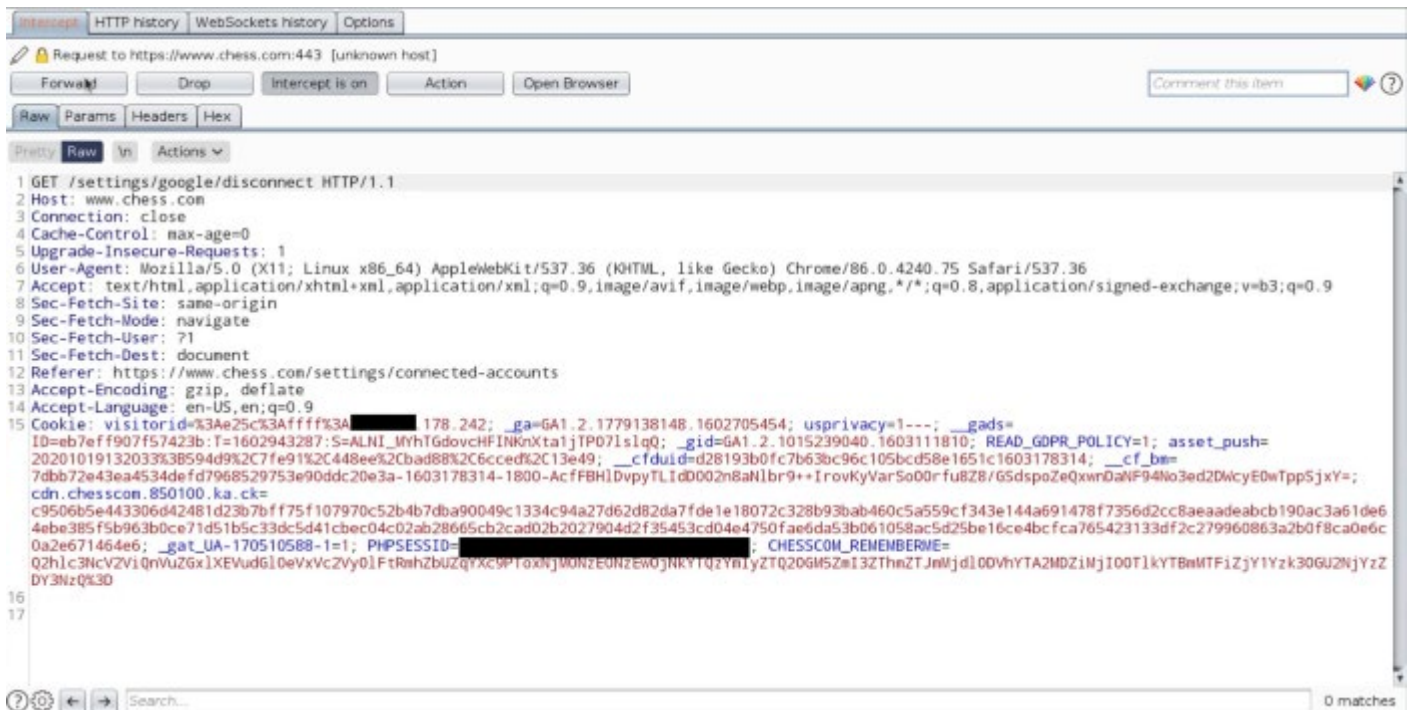




But after sending this POST request nothing happens!

It seems everything is correct! These kind of requests should send a POST request with a token. Logic is true but answer is in the next request.

In fact, POST request does nothing and next GET request disconnect the user from Google account.



So, any attacker can send just a link for victims then the victims will disconnect from their account or use the following code for hosting CSRF file:

```
<html>
<body><form action="https://www.chess.com/settings/google/disconnect"><input
type="submit" value="Submit request" />
</form><script>
```

```
document.forms[0].submit();  
</script></body>  
</html>
```