Day 9: Identifying and Exploiting Session Fixation Vulnerabilities

Overview:

On the ninth day of our bug hunter practices, the focus was on session fixation vulnerabilities, a critical security issue that can compromise the integrity of user sessions on web applications. This report outlines the steps taken to identify and demonstrate a session fixation vulnerability.

What is session hijacking or fixation:

Session fixation is a security vulnerability that occurs when an attacker sets a user's session ID to a known value, effectively hijacking the user's session. It takes advantage of insecure session management practices within web applications.

Step 1: Identify a Suspected Vulnerability:

1.I selected a web application that allowed session management and logged into the application with my own account.

2.During this login process, I closely observed the URL and cookies for any session-related tokens or parameters that might be susceptible to session fixation.

Step 2: Logout and Acquire the Session ID:

1.I logged out of my account on the web application.

2.I noted the session-related token or parameter value (in this case, the session ID) from the URL or cookies, which would serve as my known session value.

Step 3: Prepare a Malicious URL:

1.I crafted a URL that included the session-related token or parameter with the known session value obtained in Step 2. This URL would be used to set a victim's session to my known value.

Step 4: Lure the Victim:

2.I shared the malicious URL with a potential victim, enticing them to click on it. To simulate the victim's actions, I used a different browser or an incognito window.

Step 5: Observe the Exploit:

1.After the victim clicked on the malicious URL, I asked them to perform an action on the web application.

2.While the victim interacted with the application, I closely monitored their actions to see if their session became tied to the session value I had set in the URL.

3.If the victim's session was successfully set to my known value, it demonstrated the session fixation vulnerability.

Step 6: Reporting the Vulnerability:

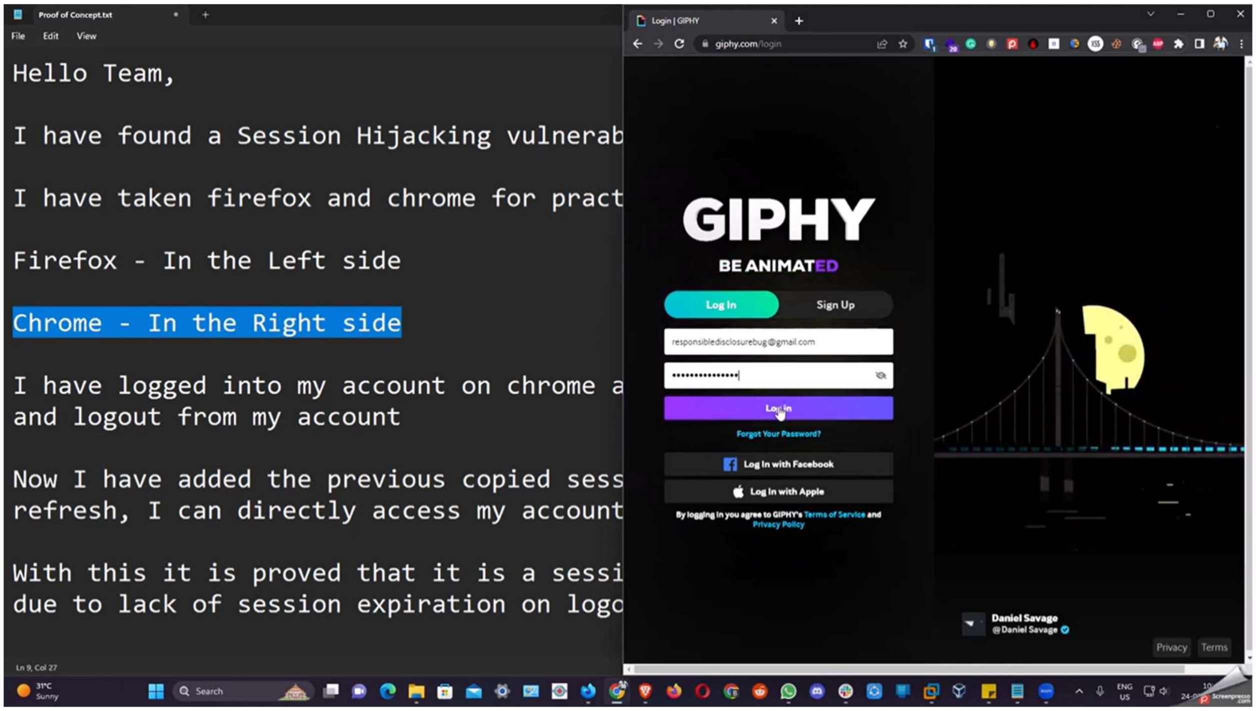
1.Ethically, I reported the vulnerability to the website or application owner, providing them with a detailed account of the steps taken and evidence of the session fixation.

2.I encouraged them to fix the issue by implementing secure session management practices.

Step 7: Mitigation:

1.To mitigate session fixation vulnerabilities, I recommended that the web application should regenerate session IDs upon login or privilege escalation.

2.I also advised the implementation of proper session management practices, such as expiring sessions after a period of inactivity.



Proof of Concept.txt

Hello Team,

I have found a Session Hijacking vulnerab

I have taken firefox and chrome for pract

Firefox - In the Left side

Chrome - In the Right side

I have logged into my account on chrome a
and logout from my account

Now I have added the previous copied sess
refresh, I can directly access my account

With this it is proved that it is a sessi
due to lack of session expiration on logo

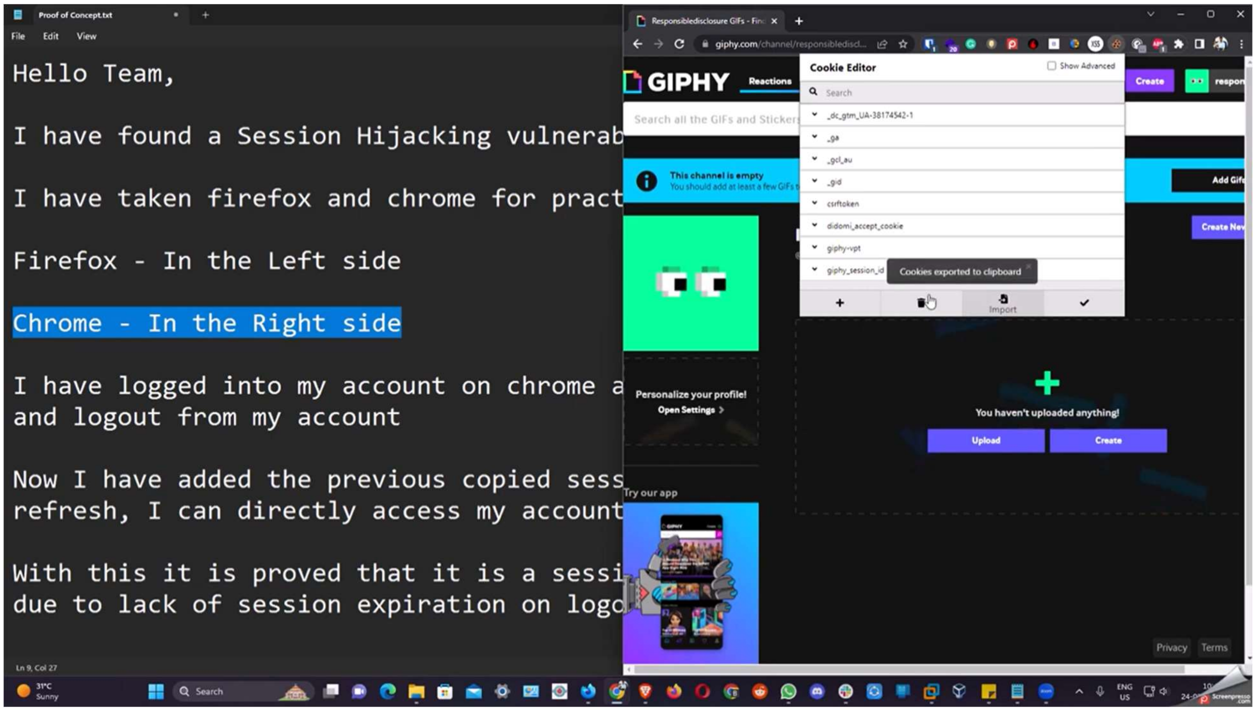
Login | GIPHY

giphy.com/login

responsibledisclosurebug@gmail.com

•••••••••••••••

By logging in you agree to GIPHY's Terms of Service and Privacy Policy



Hello Team,

I have found a Session Hijacking vulnerab

I have taken firefox and chrome for pract

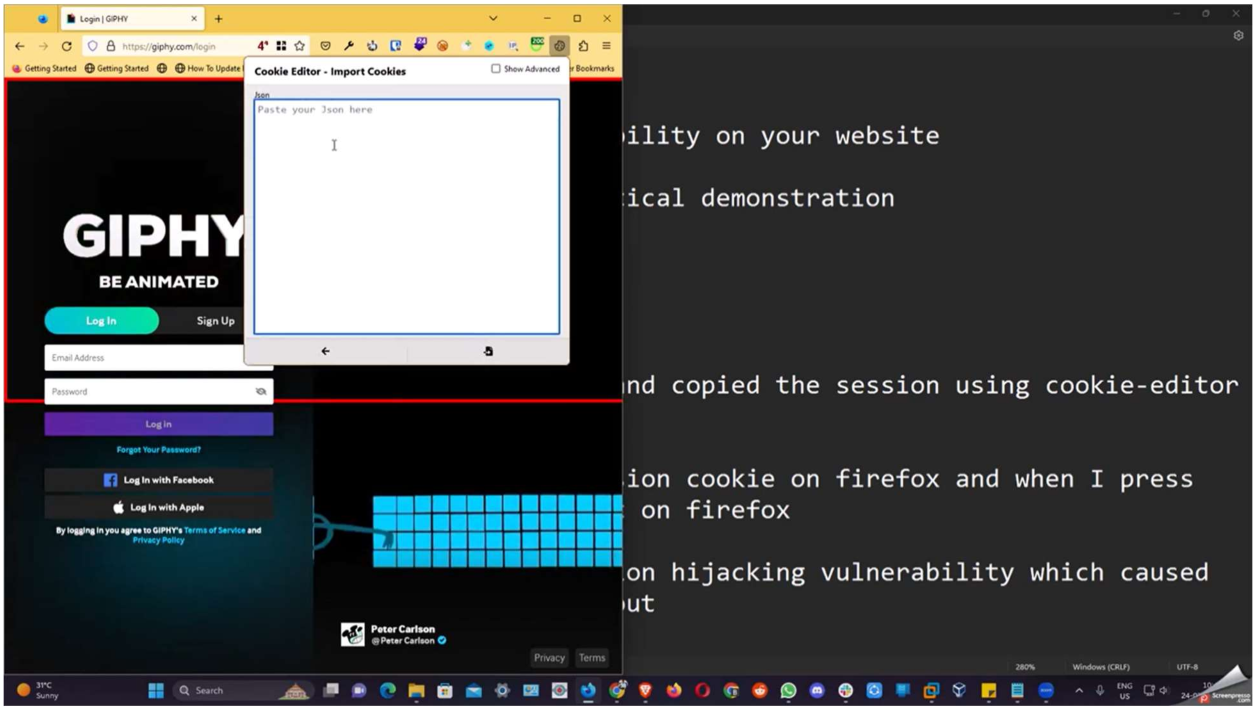
Firefox - In the Left side

Chrome - In the Right side

I have logged into my account on chrome a
and logout from my account

Now I have added the previous copied sess
refresh, I can directly access my account

With this it is proved that it is a sessi
due to lack of session expiration on logo



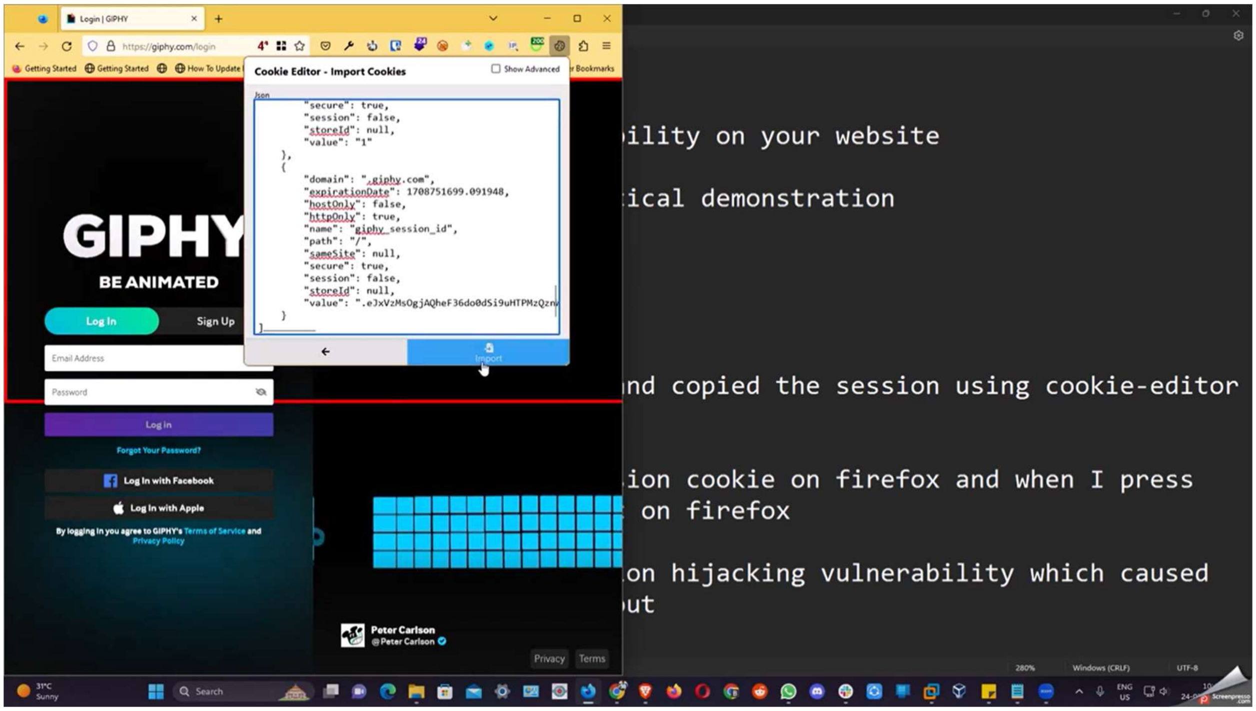
ility on your website

ical demonstration

nd copied the session using cookie-editor

ion cookie on firefox and when I press
 on firefox

on hijacking vulnerability which caused
ut



Cookie Editor - Import Cookies

□ Show Advanced

Json

```
        "secure": true,
        "session": false,
        "storeId": null,
        "value": "1"
    },
    {
        "domain": ".giphy.com",
        "expirationDate": 1708751699.091948,
        "hostOnly": false,
        "httpOnly": true,
        "name": "giphy_session_id",
        "path": "/",
        "sameSite": null,
        "secure": true,
        "session": false,
        "storeId": null,
        "value": ".eJxVzMsOgjAQheF36do0dSi9uHTPMzQzn
    }
]
```

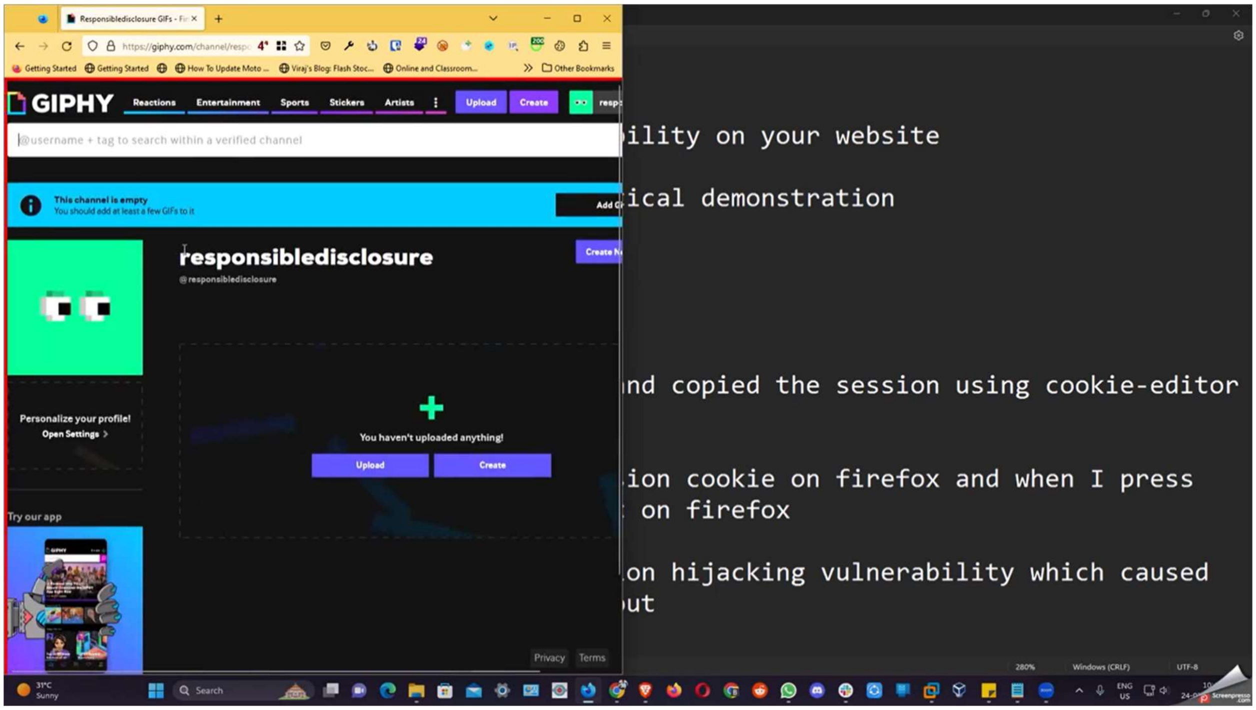
```
ility on your website

ical demonstration

nd copied the session using cookie-editor

ion cookie on firefox and when I press
 on firefox

on hijacking vulnerability which caused
ut
```



This channel is empty
You should add at least a few GIFs to it

responsibledisclosure
@responsibledisclosure

You haven't uploaded anything!

```
ility on your website

ical demonstration

nd copied the session using cookie-editor

ion cookie on firefox and when I press
 on firefox

on hijacking vulnerability which caused
ut
```

Responsibledisclosure GIFs
https://giphy.com/channel/resp
GIPHY
Reactions
Entertainment
Sports
Stickers
Artists
Upload
Create
@username + tag to search within a verified channel
Personalize your profile!
Open Settings
Try our app
Upload
Create
Privacy
Terms

Conclusion:

Day 9 of bug hunter practices focused on understanding and demonstrating session fixation vulnerabilities. By identifying and exploiting this vulnerability, I gained practical experience in recognizing the risks associated with insecure session management in web applications. Ethical reporting and responsible disclosure are essential aspects of this process, and addressing session fixation is crucial for ensuring the security of web applications and protecting user sessions from compromise.