**TEAM : ANONYMOUS**

* ***Session Fixation***

1. **TARGET -I**

**DESCRIPTION:** Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

**VULNERABLE TARGET: netflix**

**STEPS TO TEST THE session fixation**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Add the cookies extensions to the respective browsers

**Step3:** now login into some accounts with login credentials and logout of the session

**Step4:** now open the cookie icon to the top-right of the browser

**Step5:** export the cookies from there and paste it in a notepad and save it with .txt extension

**Step6:** now delete the cookies from the browser

**Step7:**  now import the cookies from notepad and then here cookies are created

**Step8:** Thus the respective sessions are hijacked and the websites allow the cookies to expire after some time

**IMPACT:**

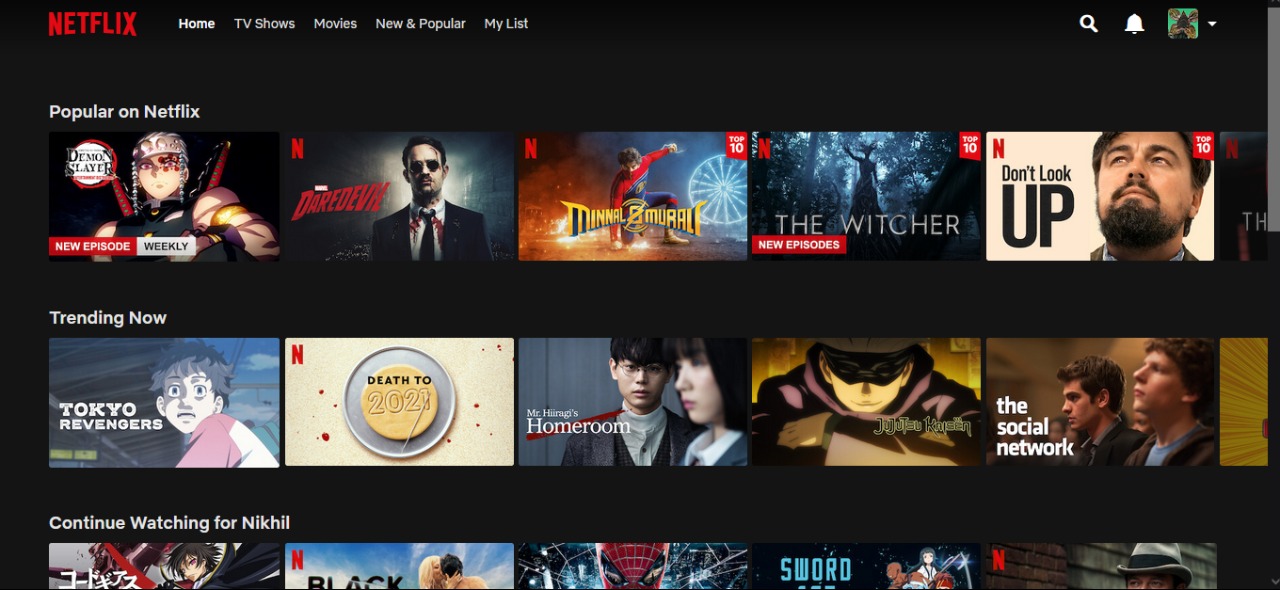
the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance

**MITIGATION:**

The developers must take care of cookies as the sensitive data might reside in the cookies session

So developer must develop the code in such a way that session cookies expires as soon as the session ends.

**PROOF OF CONCEPT:**



**TEAM : ANONYMOUS**

* ***Session Fixation***

1. **TARGET -I**

**DESCRIPTION:** Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

**VULNERABLE TARGET: flipkart**

**STEPS TO TEST THE session fixation**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Add the cookies extensions to the respective browsers

**Step3:** now login into some accounts with login credentials and logout of the session

**Step4:** now open the cookie icon to the top-right of the browser

**Step5:** export the cookies from there and paste it in a notepad and save it with .txt extension

**Step6:** now delete the cookies from the browser

**Step7:**  now import the cookies from notepad and then here cookies are created

**Step8:** Thus the respective sessions are hijacked and the websites allow the cookies to expire after some time

**IMPACT:**

the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance

**MITIGATION:** The developers must take care of cookies as the sensitive data might reside in the cookies session

So developer must develop the code in such a way that session cookies expires as soon as the session ends.

**PROOF OF CONCEPT:**

**TEAM : ANONYMOUS**

* ***Session Fixation***

1. **TARGET -I**

**DESCRIPTION:** Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

**VULNERABLE TARGET: Quikr**

**STEPS TO TEST THE session fixation**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Add the cookies extensions to the respective browsers

**Step3:** now login into some accounts with login credentials and logout of the session

**Step4:** now open the cookie icon to the top-right of the browser

**Step5:** export the cookies from there and paste it in a notepad and save it with .txt extension

**Step6:** now delete the cookies from the browser

**Step7:**  now import the cookies from notepad and then here cookies are created

**Step8:** Thus the respective sessions are hijacked and the websites allow the cookies to expire after some time

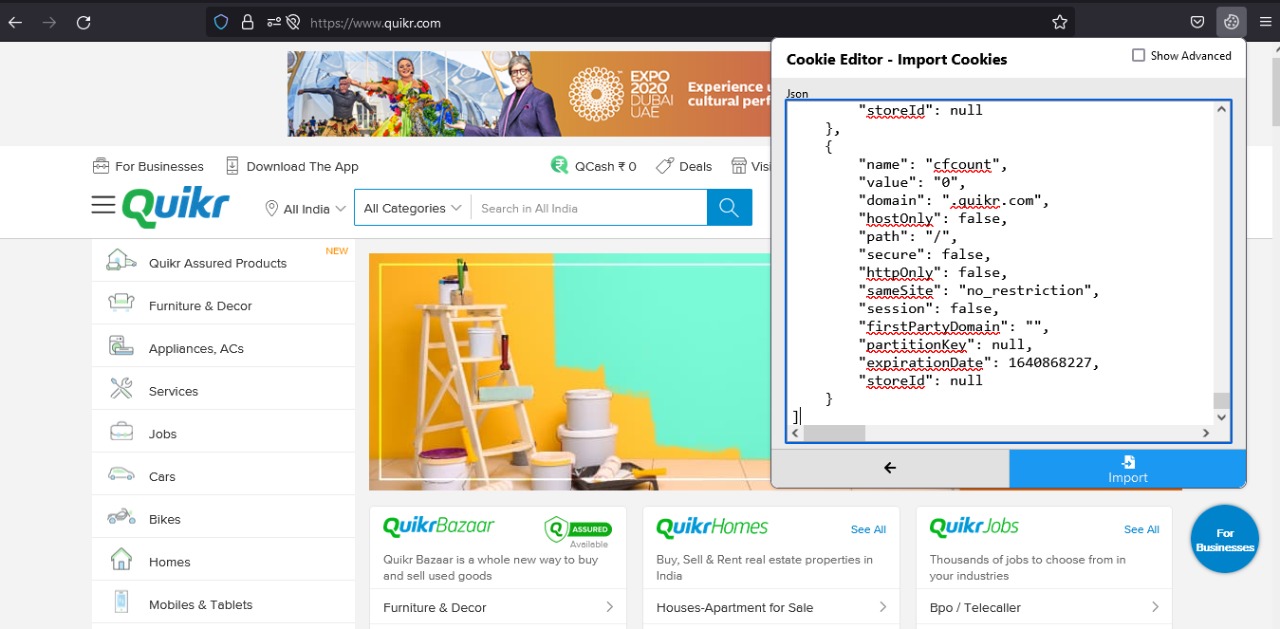
**IMPACT:**

the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance

**MITIGATION:** The developers must take care of cookies as the sensitive data might reside in the cookies session

So developer must develop the code in such a way that session cookies expires as soon as the session ends.

**PROOF OF CONCEPT:**



**TEAM : ANONYMOUS**

* ***Session Fixation***

1. **TARGET -I**

**DESCRIPTION:** Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

**VULNERABLE TARGET: amazon**

**STEPS TO TEST THE session fixation**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Add the cookies extensions to the respective browsers

**Step3:** now login into some accounts with login credentials and logout of the session

**Step4:** now open the cookie icon to the top-right of the browser

**Step5:** export the cookies from there and paste it in a notepad and save it with .txt extension

**Step6:** now delete the cookies from the browser

**Step7:**  now import the cookies from notepad and then here cookies are created

**Step8:** Thus the respective sessions are hijacked and the websites allow the cookies to expire after some time

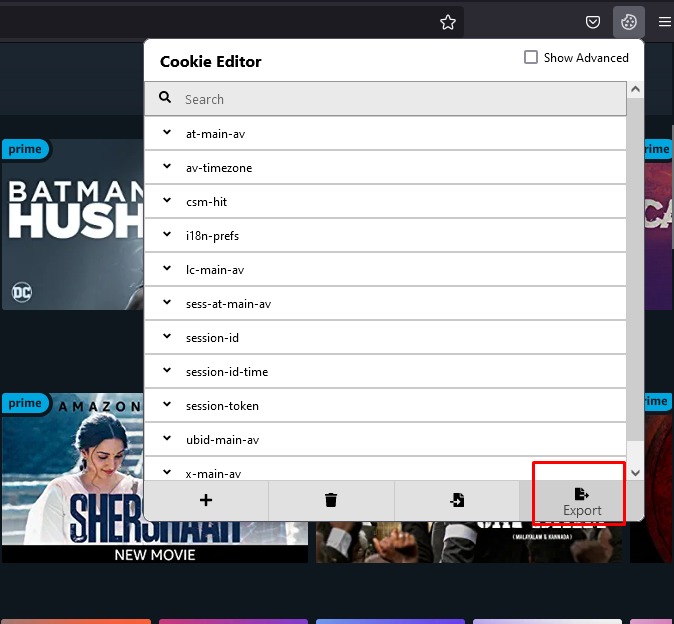
**IMPACT:**

the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance

**MITIGATION:** The developers must take care of cookies as the sensitive data might reside in the cookies session

So developer must develop the code in such a way that session cookies expires as soon as the session ends.

**PROOF OF CONCEPT:**



**TEAM : ANONYMOUS**

* ***Session Fixation***

1. **TARGET -I**

**DESCRIPTION:** Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

**VULNERABLE TARGET: amazon**

**STEPS TO TEST THE session fixation**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Add the cookies extensions to the respective browsers

**Step3:** now login into some accounts with login credentials and logout of the session

**Step4:** now open the cookie icon to the top-right of the browser

**Step5:** export the cookies from there and paste it in a notepad and save it with .txt extension

**Step6:** now delete the cookies from the browser

**Step7:**  now import the cookies from notepad and then here cookies are created

**Step8:** Thus the respective sessions are hijacked and the websites allow the cookies to expire after some time

**IMPACT:**

the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance

**MITIGATION:** The developers must take care of cookies as the sensitive data might reside in the cookies session

So developer must develop the code in such a way that session cookies expires as soon as the session ends.

**PROOF OF CONCEPT:**



**THANK YOU**

**BY :**

**M.VUJWALA (CSE BTECH-II)**

**B.SAI TEJA (CSE-CS BTECH-I)**

**A.VAMSHI (CSE-CS BTECH-I)**

**SRI NIKHIL.C (CSE-CS BTECH-I)**