



IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

**Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1**

Aim- Cookie replay

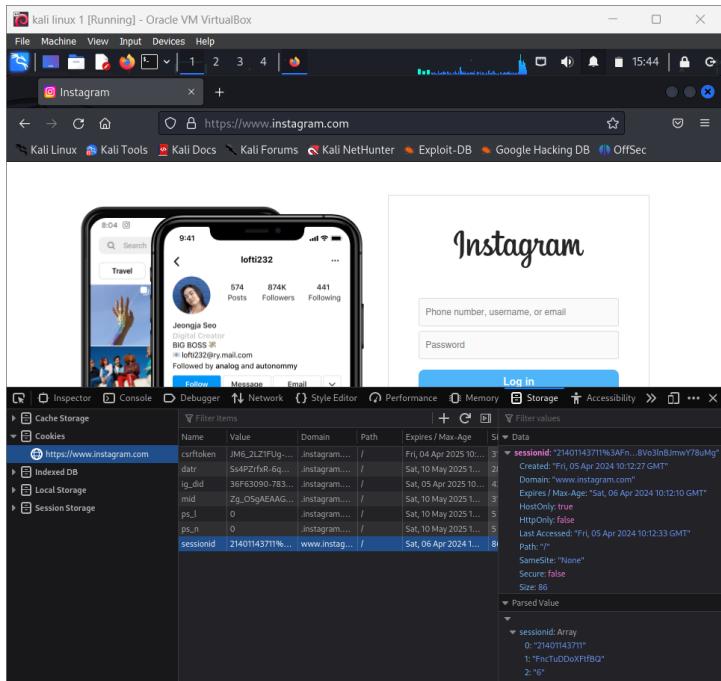
- **Instagram.com**

- Taking cookies from Instagram by inspecting the page then go to storage then cookie in cookie look for session id copy the session id from here

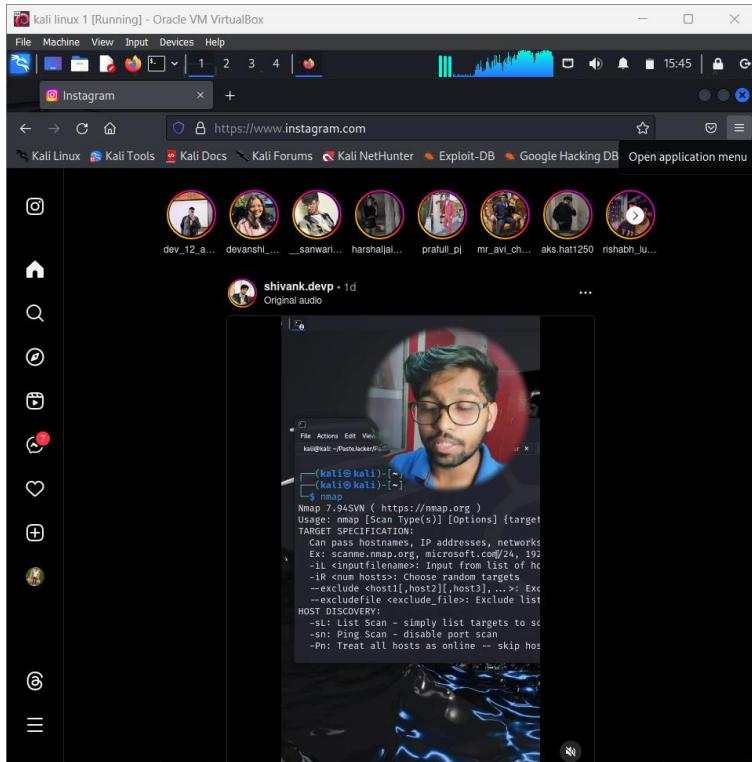
The screenshot shows a Kali Linux VM running in Oracle VM VirtualBox. A Firefox ESR browser window is open to the Instagram homepage. Below the browser, the Kali Linux desktop environment's 'Storage' tab is active, specifically the 'Cookies' section. A cookie for 'https://www.instagram.com' is selected, showing its details:

Name	Value	Domain	Path	Data
sessionid	'21401143711%3AFn...8Vo3lnBjmwY78uMg'	'.instagram....	/	Created: Fri, 05 Apr 2024 10:09:44 GMT Domain: '.instagram.com' Expires / Max-Age: Sat, 05 Apr 2025 10:09:44 GMT HostOnly: false HttpOnly: true Last Accessed: Fri, 05 Apr 2024 10:09:44 GMT Path: '' SameSite: "None" Secure: true Size: 86

- Replying cookie on different vm
- Follow the same step as above at place of copying session id value, Create new instance and set name as sessionid and paste the copied or steeled cookie in value part



- Signed in without id password by replaying the cookie



- <https://demo.testfire.net/>
 - Now we will capture the cookie from base machine(windows) and replay it on kali linux(vm) for <https://demo.testfire.net/>
 - Username-admin
 - Password-admin

Here to apply.' At the bottom, there are links for Privacy Policy, Security Statement, Server Status Check, REST API, and a note: 'This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features.' A footer at the bottom includes a disclaimer about the website being a demonstration and copyright information for HCL Technologies."/>

- After logging in capture cookie using extension cookie editor or you can also capture cookie from settings also

The screenshot shows a web browser window with the Altoro Mutual website loaded. On the right side of the browser, a 'Cookie Editor' extension is open, displaying two captured cookies:

- JSESSIONID**:

Name	JSESSIONID
Value	96781AD46763F81B5513DF6667F0F657
Domain	demo.testfire.net
Path	/
Session	True
Expires	
HttpOnly	true
Secure	true
SameSite	unspecified
- AltoroAccounts**:

Name	AltoroAccounts
Value	ODAwMDAwfknVcnBvcmF0ZX4tMS4wRT...
Domain	demo.testfire.net
Path	/
Session	True
Expires	
HttpOnly	false
Secure	false
SameSite	unspecified

- Now go to kali linux and paste the capture cookie there for replaying

The screenshot shows a Kali Linux desktop environment with a Firefox ESR browser window open to the Altoro Mutual website. The browser interface includes a toolbar with various icons and a status bar indicating the date and time.

The Altoro Mutual website is displayed, showing the same layout as the original site. A red dashed box highlights the bottom of the page, containing the following text:

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/aposcan/>.

- Now inspect this page and go to storage then cookie see for sessions

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSIONID	C893068D4A91E...	demo.testfi...	/	Session	42	true	true	None	Fri, 12 Apr 2024 04:20:28 GMT

- Now edit the session value and paste the captured cookie there

Name	Value	Domain	Path	Expires / Max-Age	Size	Data
JSESSIONID	96781AD46763F81B5513DF6667F0F657	demo.testfi...	/	Session	43	JSESSIONID: "96781AD46763F81B5513DF6667F0F657" Created: "Fri, 12 Apr 2024 04:18:55 GMT" Domain: "demo.testfire.net" Expires / Max-Age: "Session" HostOnly: true HttpOnly: true Last Accessed: "Fri, 12 Apr 2024 04:20:28 GMT" Path: "/" SameSite: "None" Secure: true Size: 43

- Now refresh the page

The screenshot shows a Firefox ESR browser window running on a Kali Linux machine. The title bar indicates it's a snapshot 1 [Running] - Oracle VM VirtualBox. The address bar shows the URL https://demo.testfire.net. The main content area displays the Altoro Mutual website, which is a demo site. It features sections for MY ACCOUNT, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. Under PERSONAL, there are links for Deposit Products, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. Under SMALL BUSINESS, there are links for Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The INSIDE ALTORO MUTUAL section includes links for About Us, Contact Us, and Feedback. The right side of the page has sections for Online Banking with FREE Online Bill Pay, Privacy and Security, Business Credit Cards, and Real Estate Financing. The developer tools sidebar on the left shows the Cookies section with a single entry:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSIONID	96781AD46763F...	demo.testfi...	/	Session	43	true	true	None	Fri, 12 Apr 2024 04...

- After refreshing the page we found that we are signed in without entering id password by just replaying cookie

- Vulnweb.com
- Go to vulnweb.com open securityTweets and login by using id- admin password-123456

- After logging in capture cookie using extension cookie editor or you can also capture cookie from settings also

Name	Value	Domain	Path	Session	Expires	HttpOnly	Secure	SameSite
username	admin	testhtml5.vulnweb.com	/	True	false	false	false	unspecified

- Now go to kali linux and paste the capture cookie there for replaying
- Now inspect this page and go to storage then cookie Now add new instance and paste the captured cookie there then refresh the page

The screenshot shows a dual-monitor setup. The top monitor displays a Kali Linux desktop environment with several icons in the dock and a taskbar at the bottom. A Firefox browser window is open, showing the URL `testhtml5.vulnweb.com/#/popular`. The page content is from "SecurityTweets" and includes a sidebar with navigation links like "Popular", "Latest", "Carousel", "Archive", "WEBSITE", "About", "Contact", and "ACUNETIX". The bottom monitor displays the "Storage" tab of the Firefox developer tools. Under the "Cookies" section, a table lists a single cookie entry:

Name	Value	Domain	Path	Expires / Max
<code>username</code>	<code>admin</code>	<code>testhtml5.v...</code>	<code>/</code>	<code>Sat, 13 Apr 2024</code>

Details for the `username` cookie are shown on the right side of the developer tools interface:

- Created:** "Fri, 12 Apr 2024 04:44:16 GMT"
- Domain:** "testhtml5.vulnweb.com"
- Expires / Max-Age:** "Sat, 13 Apr 2024 04:44:08 GMT"
- HostOnly:** true
- HttpOnly:** false
- Last Accessed:** "Fri, 12 Apr 2024 04:44:20 GMT"
- Path:** "/"
- SameSite:** "None"
- Secure:** false
- Size:** 13

- After refreshing we get logged in

The screenshot shows a Firefox browser window running on a Kali Linux VM. The title bar reads "kali linux 1 [Running] - Oracle VM VirtualBox". The address bar shows "testhtml5.vulnweb.com/#/popular". The page content is from "SecurityTweets", a vulnerable HTML5 test website. It displays a sidebar with "VIEWS" (Popular, Latest, Carousel, Archive) and "WEBSITE" (About, Contact). The main area shows a "Filter results" input and a "Page 0" button. A "Next" button is visible at the bottom of the list. On the right, there's a "Storage" tab open in the developer tools, showing the "Cookies" section. A single cookie is listed:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Access
username	admin	testhtml5.v...	/	Sat, 13 Apr 2024 04...	13	false	false	None	Fri, 12 Apr 2024 04...

The "Storage" tab also lists "Cache Storage" and "Indexed DB".

● DVWA(for low)

- Login the dvwa in windows with user name- admin and password-password at dvwa security low

The screenshot shows the DVWA Security low level interface. The left sidebar menu includes Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area displays the DVWA logo and the title "DVWA Security". It shows the security level is currently "low". A note states: "You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA." Below this is a dropdown menu with "low" selected and a "Submit" button. The "PHPIDS" section is present, mentioning PHPIDS v.0.6 is disabled. A message box indicates "Security level set to low". At the bottom, it shows the logged-in user is "admin" and the security level is "low".

- And in linux login using id-1337 and password-charley

The screenshot shows the DVWA Security high level interface in a Kali Linux browser. The left sidebar menu is identical to the Windows version. The main content area displays the DVWA logo and the title "Welcome to Damn Vulnerable Web App!". It includes a "WARNING!" section about not uploading to public servers and a "Disclaimer" section. The "General Instructions" section provides help for each vulnerability and security level. A message box at the bottom says "You have logged in as '1337'". At the bottom, it shows the logged-in user is "1337" and the security level is "high".

- Now using extension cookie editor capture and copy the cookie from there

Name	Value	Domain	Path	Session
security	low	192.168.62.129	/dvwa	True
PHPSESSID	85458ced8aec540cd2646a42ce220fc5	192.168.62.129	/	Session

- Now go to linux and inspect the page and go to storage then cookie

Name	Value	Domain	Path	Expires / Max-Age	Size
PHPSESSID	0fb9679e505246828bd925-88aacff*	192.168.62.129	/	Session	41
security	high	192.168.62.129	/dvwa	Session	12

- Now remove the security attribute and edit the phpsid and paste the cookie copied from windows

- Now refresh the page and you will notice you will be logged in as admin account as you have earlier logged in as 1337 that means we had successfully replayed the cookie

• DVWA(for high)

- Login the dvwa in windows with user name- admin and password-password at dvwa security high

The screenshot shows a Microsoft Edge browser window with the URL `192.168.62.129/dvwa/index.php`. The page title is "Welcome to Damn Vulnerable Web App!". On the left, there is a sidebar menu with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

The main content area displays the DVWA logo and the following text:

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable! It is designed to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

- And in linux login using id-1337 and password-charley

The screenshot shows a Firefox browser window on a Kali Linux desktop environment with the URL `192.168.62.129/dvwa/index.php`. The page title is "Welcome to Damn Vulnerable Web App!". The sidebar menu is identical to the Windows version:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

The main content area displays the DVWA logo and the following text:

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as '1337'

Username: 1337
Security Level: high
PHPIDS: disabled

- Now using extension cookie editor capture and copy the cookie from there

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
security	high	192.168.62.129	/dvwa	Session	41	false	false	None	Fri, 12 Apr 2024 05...
PHPSESSID	abf0272887fff4b1bcfb4daa7f07604f	192.168.62.129	/	Session	12	false	false	None	Fri, 12 Apr 2024 05...

- Now go to linux and inspect the page and go to storage then cookie

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	abf0272887fff4b1bcfb4daa7f07604f	192.168.62.129	/	Session	12	false	false	None	Fri, 12 Apr 2024 05...
security	high	192.168.62.129	/dvwa	Session	41	false	false	None	Fri, 12 Apr 2024 05...

- Now remove the security attribute and edit the phpsid and paste the cookie copied from windows

The screenshot shows a browser window with the DVWA homepage. The URL bar shows `192.168.62.129/dvwa/index.php`. The page content includes a warning about the application being vulnerable and instructions for various security tests. On the right side, a developer tools storage panel is open, specifically the 'Cookies' section. It lists a cookie for the domain `http://192.168.62.129`. The cookie details are as follows:

Name	Value	Domain	Path	Expires / Max-Age	Size	Data
PHPSESSID	abf0272887ff4b1bcfd4da7f076044*	192.168.62.129	/	Session	42	PHPSESSID: "abf0272887ff4b1bcfd4da7f076044*" Created: "Fri, 12 Apr 2024 05:32:24 GMT" Domain: "192.168.62.129" Expires / Max-Age: "Session" HostOnly: true HttpOnly: false Last Accessed: "Fri, 12 Apr 2024 05:39:58 GMT" Path: "/" SameSite: "None" Secure: false Size: 42

- Now refresh the page and you will notice you will be logged in as admin account as you have earlier logged in as 1337 that means we had successfully replayed the cookie

The screenshot shows a browser window with the DVWA homepage. The URL bar shows `192.168.62.129/dvwa/index.php`. The page content includes a warning about the application being vulnerable and instructions for various security tests. In the bottom right corner of the page, there is a message: "Username: admin Security Level: high PHPIDS: disabled". This indicates that the user has successfully logged in as the 'admin' account.

Bonous-

➤ Upes lms

- On windows open upes student portal login in with my id dhairyा.105432@stu.upes.ac.in
- open lms of upes student portal site and with the help of cookie editor extension capture and copy cookie

The screenshot shows a web browser window with the URL <https://lms.upes.ac.in/my/>. The main page displays the 'Dashboard' and 'Course Progress' sections. In the 'Course Progress' section, there is a circular progress bar labeled '468'. To the right, a 'Upcoming Activities Due' table lists several assignments with their due dates. A separate 'Calendar' window is open, showing the month of April 2024 with specific dates highlighted. On the right side of the browser, a 'Cookie Editor' extension is active, showing details for a captured cookie named 'MoodleSession'. The cookie information includes Name: MoodleSession, Value: ke7ns7Cibf675js4htvcfaj, Domain: lms.upes.ac.in, Path: /, Session: True, Expires: 2024-04-13, HttpOnly: false, Secure: true, and SameSite: no_restriction.

- on kali linux open upes student portal using your friends id, I am using abhishek id
- now go to lms then inspect page then go to storage and open cookie

The screenshot shows a Kali Linux desktop environment with a browser window displaying the UPES LMS dashboard at <https://lms.upes.ac.in/my/>. The dashboard shows a 'Welcome Back ABHISHEK' message and a circular progress bar. A 'My Courses' section is visible below. To the right, a 'Calendar' window shows the month of April 2024. At the bottom of the screen, the Kali Linux taskbar is visible with various application icons. In the foreground, the developer tools' 'Storage' tab is open, specifically the 'Cookies' section. A cookie for 'https://lms.upes.ac.in' is selected, showing its details: Name: MoodleSession, Value: 0M6dmig95v4gb0g1eh2c9, Domain: lms.upes.ac.in, Path: /, Expires / Max-Age: Session, Size: 39, HttpOnly: false, Secure: true, SameSite: None, and Last Accessed: Fri, 12 Apr 2024 06:56:17 GMT.

- now edit cookie and paste cookie copied from windows in linux

The screenshot shows a Kali Linux VM interface with a browser window open to <https://lms.upes.ac.in/my/>. The browser title bar says "Kali Linux 1 [Running] - Oracle VM VirtualBox". The page content includes a dashboard with course progress, an "Upcoming Activities Due" section, and a "Calendar" view for April 2024. In the bottom-left corner, the developer tools (F12) are open, specifically the Network tab. It lists several cookies, including a "MoodleSession" cookie for the domain <https://lms.upes.ac.in>.

- now refresh the page you will find that your id is logged in instead of your friends id

This screenshot is identical to the one above, showing the same Kali Linux VM setup and browser session. The developer tools Network tab again shows the "MoodleSession" cookie for the <https://lms.upes.ac.in> domain, indicating that the user's session has been successfully hijacked.

➤ upes library

- open upes library site on chrome and login using your sapid and password and then inspect page and go to application and then go to cookie and copy cookie

The screenshot shows a browser window for 'Your library home - UPES LIBRARY' at ils.ddn.upes.ac.in:8001/cgi-bin/koha/opac-user.pl. The page displays a 'Messages for you' box with 'WELCOME TO UPES LIBRARY'. Below it, a message says 'Hello, Dhairy Jain' and provides a link to log out. A sidebar on the left includes links for 'UPES Library Portal', 'Access e-Library', and 'OpenAthens Guide'. A green arrow points upwards from the sidebar towards the DevTools.

The DevTools Application tab is open, specifically the Cookies section. It lists cookies for the domain <https://ils.ddn.upes.ac.in>. One cookie is highlighted: 'CGISESSIONID' with the value '6e31a012585cf6ecfb7261...'. The DevTools interface includes tabs for Elements, Console, Sources, Network, Performance, Memory, Application, and a bottom bar with various icons.

- now open edge and open upes library and do not login in this and also inspect and check cookie

The screenshot shows a Microsoft Edge browser window for 'upes library login - Search' at <https://ils.ddn.upes.ac.in:8001/cgi-bin/koha/opac-user.pl>. The page displays a 'Log in to your account' form with fields for 'Login:' and 'Password:', and a 'Log in' button. Below the form is a note: 'Please use SAP ID as your Login-ID'. The bottom of the page includes a footer with copyright information and a 'Report a problem' link.

The DevTools Application tab is open, showing the same cookie list as the previous screenshot. The cookie 'CGISESSIONID' is again highlighted with the value '59e451a0687d597fd4d480a5b575e289a'. The DevTools interface is consistent with the Chrome version, with tabs for Manifest, Service workers, Storage, Cookies, Background services, and a bottom bar with various icons.

- now paste the copied cookie from chrome in edge

The screenshot shows a Microsoft Edge browser window. The main content area displays a login form for 'Log in to your account'. Below the form, a blue banner provides copyright information and credits to 'AVIOR TECHNOLOGIES PVT LTD.' The right side of the screen shows the Edge developer tools open, specifically the 'Application' tab under the 'Cookies' section. A table lists various cookies, including one highlighted in yellow with the value '6e31a012585cf6ecfb72610ac05eb80'.

Name	Value	D.	P.	E.	S.	H.	S.	P.	P.
CGISESSID	6e31a012585cf6ecfb72610ac05eb80	...	/	S.	4...	✓	✓	L...	M...
_biz_fl...	%7B%22Versi...	...	/	Z...	9...				M...
_biz_nA...	5	...	/	Z...	8				M...
_biz_p...	%5B%5D	...	/	Z...	1...				M...
_click	fn2zowW7C2...	...	/	Z...	3...				M...
_fbp	fb.217053989...	...	/	Z...	3...				M...
_ga	GA1.1218801...	...	/	Z...	2...				M...
_ga_7...	GS1.170539...	...	/	Z...	5...				M...
_ga_F...	GS1.1.170862...	...	/	Z...	5...				M...
_gd_au	1.1.109404536...	...	/	Z...	3...				M...
_jetvfd	b0cef14020a8...	...	/	Z...	3...				M...

- now refresh you will be logged in without id password

The screenshot shows the Microsoft Edge browser after a refresh. The main content area displays a 'Your summary' page for 'Dhairya Jain'. It includes sections for 'Messages for you' (with a welcome message) and 'Checked out (0)' (showing 'You have nothing checked out'). At the bottom, there's a sidebar with links like 'UPES Library Portal', 'Access e-Library', 'OpenAthens Guide', and 'Download'. The right side of the screen shows the Edge developer tools 'Application' tab under the 'Cookies' section, which is identical to the previous screenshot, displaying the same list of cookies including the highlighted one.

- **Countermeasure**

- Session timeout after short interval of time
- Encrypted communication channel ssl
- Anti replay mechanishim