

NIVERSITY Discover. Learn. Empower.

Experiment2.3

Student Name: RAJDEEP JAISWAL.UID: 20BCS2761Branch: CSESection/Group: 902-BSemester: 5thSubject Name: WMS LABSubject Code: 20CSP-338

- 1. Aim: Implementation of Session hijacking attack on http-enabled website
- **2. Objective:** To Identify vulnerable session cookies.

3. Software/Hardware Requirements: Windows 7 & above

4. Tools to be used: Burpsuite

5. Introduction: Session Hijacking:

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

The session token could be compromised in different ways; the most common are:

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
- <u>Man-in-the-middle attack</u>
- <u>Man-in-the-browser attack</u>



HANDIGARH INIVERSITY Discover. Learn. Empower.

6. Steps/Method/Coding:

- First, ensure that Burp is correctly configured with your browser.
- With intercept turned off in the Proxy "Intercept" tab, visit the login page of the application you are testing in your browser.
- Log in to the application you are testing.
- You can log in using the credentials user:user.
- Return to Burp.
- In the Proxy "Intercept" tab, ensure "Intercept is on".
- Refresh the page in your browser.
- The request will be captured by Burp, it can be viewed in the Proxy "Intercept" tab.
- Cookies can be viewed in the cookie header.
- We now need to investigate and edit each individual cookie.
- Right click anywhere on the request and click "Send to Repeater".
- Go to the Repeater tab.
- The cookies in the request can be edited easily in the "Params" tab.
- By removing cookies from the request we can ascertain the function of each cookie.
- The response from the server can be viewed in the "Response" panel in Repeater.

7. Output:



CHANDIGARH UNIVERSITY Discover. Learn. Empower.

Burp Intruder Repeater Window Help									
Target Proxy Spider		Scanner	Intruder	Repeater	Sequencer	Deco			
Interc	Intercept HTTP history			WebSocl	WebSockets history Options				
Fo	rwar	d		Drop	Interc	ept is off	Action	n	
Raw	Para	ams	Headers	Hex					

ack	ee Help Me!
	Please sign-in
	Name [user
	Password
	Dont have an account? Please register here



CHANDIGARH Discover. Learn. Empower.

Target Proxy Spide	er Scanner Int	ruder Repeater	Sequencer	Decod
Intercept HTTP histo	webSockets	history Option	s	
Forward	Drop	Intercept is on	Action	
Davis Davis Used	un Hau			
Raw Params Heade	ers Hex			_

Intercept	HTTP history	WebSocket	ts history	Options	1		
Request to http://172.16.67.136:80							
Forward Drop Intercept is on Action							
Raw Para	ms Headers	Hex					
GET /mutil Host: 172.	<pre>GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1 Host: 172.16.67.136</pre>						
User-Agent Accept: te: Accept_Lap	User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS Accept: text/html,application/xhtml+xml,application/xml;q=0.9,						
Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate							
Cookie: showhints=0; username=user; uid=18; remember_token=PN) acopendivids=swingset,mutillidae,jotto,phpbb2,redmine; acgroup							
Connection: keep-arive Cache-Control: max-age=0							



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

GARH Sitty Discover. Learn. Empower.

Intercept	нтт	P history	WebSo	ckets history	Options		
Reques	Request to http://172.16.67.136:80						
Forward Drop)rop	Intercept	t is on	Action		
Raw Para	ams	Headers	Hex				
GET /mutillidae/index.php?popUpNotif:					ionCode=A	U1 HTTP/1	.1
User-Agent	: Mo	zilla/5.0	O (iP	Send to Spid	ler		os
Accept: te	xt/h	tml,appl: e: en_GB	icati en:g	Do an active	e scan		.9,
Accept-Enc	odin	g: gzip,	defl	Send to Intro	uder	≆ + I	
Referer: h	Referer: http://172.16.67.1				eater	%3+R	gin.
Cookie: showhints=0; userna acopendivids=swingset.mutil				Send to Sequ	uencer		PNK.
Connection	: ke	ep-alive		Send to Con	nparer		
Cache-Cont	rol:	max-age	=0	Send to Dec	oder		
				Request in h	muser	•	

Target Pro:	xy Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Exten
1 ×								
Go	Cancel	< *	> *					
Request								
Raw Param	Headers	Hex						
GET request to	/mutillidae	/index.php	>					
Туре	Name			Value				Add
URL	popUpN	otificatio	nCode	AU1				nara
Cookie	showhi	nts		0		R	emove	
Cookie	usernar	ne		user				
Cookie	uid			18				Up
Cookie	rememb	ber_token		PNkIxJ3D0	8iXL0F4vrAW	VBA.		_
Cookie	PHPSES	PHPSESSID			dk180u6agv	9ldrj6		Down
Cookie	acopen	acopendivids			nutillidae.jot	to,phpbb2,r	red	
Cookie	acgroupswithpersist			nada				



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Go Cancel < T > T Request Raw Params Headers Hex GET request to /mutillidae/index.php					
Туре	Name	Value	Add		
URL	popUpNotificationCode	AU1			
Cookie	username	user	Remove		
Cookie	uid	18			
Cookie	PHPSESSID	8jvpbhpkfidk180u6agv9ldrj6	Up		
			Down		

Request							
Raw Params	Headers Hex						
GET request to /r	GET request to /mutillidae/index.php						
Туре	Name	Value					
URL	popUpNotificationCode	AU1					
Cookie	username	user					
Cookie	uid	1					
Cookie	PHPSESSID	8jvpbhpkfidk180u6agv9ldrj6					
Response Raw Header	rs Hex HTML Render						
Date: Mon, 09 Server: Apach Suhosin-Patch OpenSSL/0.9.8 X-Powered-By:	<pre>0 Mar 2015 14:35:53 GMT ae/2.2.14 (Ubuntu) mod_ a proxy_html/3.0.1 mod_ 8k Phusion_Passenger/3. : PHP/5.3.2-lubuntu4.5</pre>	mono/2.4.3 PHP/5.3.2-lubun python/3.3.1 Python/2.6.5 : 0.17 mod_perl/2.0.4 Perl/v					
Logged-In-Use Content-Lengt Keep-Alive: t Connection: F Content-Type:	er: admin shcoding th: 39191 timeout=15, max=100 Keep-Alive : text/html						
ar parhine e	I thin</td <td>k the database password is</td>	k the database password is					

- Learning Outcomes:Learnt to implement session hijacking.
- Learnt to use burpsuite to perform session hijacking.