Blind SQLi leading to RCE, from Unauthenticated access to a test API Webservice

210

Share:

State	Resolved (Closed)
Disclosed	**July 23, 2019 4:54am +0530**
Reported To	**Starbucks**
Asset	Other assets (Other)
Weakness	SQL Injection
Bounty	$4,000
Severity	Critical (9.3)
Participants	
Visibility	Disclosed (Limited)

Collapse

SUMMARY BY STARBUCKS

@geek_jeremy, at the same time as other hackers who submitted their own reports, discovered a browsable WSDL service on an API endpoint under the starbucks.com.cn domain, running on a non-standard port.
@geek_jeremy demonstrated that the service had several functions that executed without any authentication at all, allowing the listing of users, passwords and other personal information. Fortunately, this was a test service, executing on test data, and as a result, this alone did not constitute a vulnerability worth rewarding.
@geek_jeremy also demonstrated that the service had at least one blind SQLi vulnerability, allowing him to not only access the database behind the service, but also to execute commands through the xp_cmdshell function. The "ping" command was used to demonstrate this safely without causing bad effects to the service. Because this was a Remote Code Execution (RCE) on a production server, even though it was reached through a test instance, this was awarded as a Critical vulnerability.

TIMELINE · EXPORT

geek_jeremy submitted a report to **Starbucks**.	May 29th (about 1 year ago)
still HackerOne triage posted a comment.	May 30th (about 1 year ago)
still HackerOne triage changed the status to **Needs more info**.	May 30th (about 1 year ago)
geek_jeremy changed the status to **New**.	May 30th (about 1 year ago)
still HackerOne triage posted a comment.	May 30th (about 1 year ago)
still HackerOne triage changed the scope from **www.starbucks.com.cn** to **Other assets**.	May 30th (about 1 year ago)
geek_jeremy posted a comment.	May 30th (about 1 year ago)
tealeaf posted a comment.	May 30th (about 1 year ago)
geek_jeremy posted a comment.	May 30th (about 1 year ago)
tealeaf changed the status to **Triaged**.	May 31st (about 1 year ago)
tealeaf changed the report title.	May 31st (about 1 year ago)
geek_jeremy posted a comment.	May 31st (about 1 year ago)

geek_jeremy posted a comment. Jun 1st (about 1 year ago)

geek_jeremy posted a comment. Jun 1st (12 months ago)

geek_jeremy posted a comment. Jun 3rd (12 months ago)

tealeaf posted a comment. Jun 4th (12 months ago)

geek_jeremy posted a comment. Jun 4th (12 months ago)

Starbucks rewarded geek_jeremy with a **$4,000** bounty. Jun 14th (12 months ago)

geek_jeremy posted a comment. Jun 14th (12 months ago)

tealeaf closed the report and changed the status to ○ **Resolved**. Jun 24th (11 months ago)

geek_jeremy requested to disclose this report. Jun 25th (11 months ago)

tealeaf changed the report title. Jun 25th (11 months ago)

tealeaf agreed to disclose this report. Jul 23rd (10 months ago)

This report has been disclosed. Jul 23rd (10 months ago)