2 [redacted] SQL

Share:

State	Resolved (Closed)
Disclosed	October 9, 2019 12:17am +0530
Reported To	U.S. Dept Of Defense
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

manshum12 submitted a report to U.S. Dept Of Defense. Jul 15th (about 1 year ago)

hi , i think i find a SQL in https://[redacted]/

POST /requestaccount.php? HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/requestaccount.php?
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
Cookie: _ga=GA1.2.797825707.1531527624; PHPSESSID=h46aobnksi6rqe0dki7b34thn10qqf7j;
TS0136a92d=0141bba1871c30b60b2555c9145e093817841b5f20a39085c1ff77e556280571aa32dcc2ebf57d0d397334f8207e32f1153478dbc7;
Hm_lvt_dde6ba2851f3db0ddc415ce0f895822e=1531606739; Hm_lpvt_dde6ba2851f3db0ddc415ce0f895822e=1531623251
Connection: close
Upgrade-Insecure-Requests: 1

fname=&lname=&uname=&email=&phone=&dsn=&cmdName=&title=&rank=&rate=Not+specified&message=&curID=-1

SQL vulnerable in curID=-1'
if you puy ' u will see screenshot 49 and 48

Impact

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution

BOT: U.S. Dept Of Defense posted a comment. Jul 15th (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

manshum12 posted a comment. Updated Jul 15th (about 1 year ago)

.

ag3nt-z3 changed the status to ○ **Needs more info**. Jul 17th (about 1 year ago)

Greetings,

To validate [your report] [the reported vulnerability], We require additional information.

Can you please answer the following questions?

Your PoC results in a non-descriptive error regarding accounts requiring a CaC and how to request an account.

Does your PoC require an account be created first?

...

I will continue processing your report on receipt of your response. You will receive another status update upon completion of this review. If I have any other questions in the interim, I will be back in touch.

If we do not receive a response within two weeks, we will send you a second request for this information. If we do not receive a response from you within two weeks of the second notice, we will have to close this report without action.

If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

manshum12 changed the status to ○ **New**. Updated Sep 25th (16 days ago)

you don't need to create a account , when you go to https://[redacted]/requestaccount.php?
you will see screenshot 52 , and then click > click here , you will go to the User Account Request page form, you just need to fill something in the form , like Screenshot(55) , you can see i put everything aaaa , and click submit request , but before make sure u open intercept is on in burp suite
in the parameter curID=-1 put ' ' < screenshot 57 , and click forward in burp
then u can see Warning: ociexecute(): ORA-00933: SQL command not properly ended in /docroot/dcsst-httpds/html/ClassODbo.php on line 1907
< screenshot 58

ag3nt-z3 updated the severity to High. Jul 18th (about 1 year ago)

ag3nt-z3 changed the status to ○ **Triaged**. Jul 18th (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

manshum12 posted a comment. Jul 18th (about 1 year ago)
ur welcome :)

manshum12 posted a comment. Jul 20th (about 1 year ago)
im sorry , i got a question , after you fix the bug , i will got pay for that or not ?

deez_nops posted a comment. Jul 20th (about 1 year ago)
@csgolife The DoD Vulnerability Disclosure Program (VDP) is not a cash reward program but reporting can positively impact your HackerOne reputation. Check out the VDP policy information and let me know if you have questions.

manshum12 posted a comment. Updated Jul 26th (about 1 year ago)
.

ag3nt-j7 posted a comment. Jul 26th (about 1 year ago)
@csgolife We will provide updates as we receive them from the system owner. Thanks for supporting the DoD Vulnerability Disclosure Program.

manshum12 posted a comment. Aug 7th (about 1 year ago)
any update?

manshum12 posted a comment. Aug 13th (about 1 year ago)
any updates?

manshum12 posted a comment. Sep 16th (about 1 year ago)
any updates , that 3 months already

manshum12 posted a comment. Oct 1st (about 1 year ago)
hello?

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Oct 11th (about 1 year 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

manshum12 posted a comment. Jan 16th (9 months ago)
Hi U.S. Dept Of Defense

can you Disclosed (Limited) this report pls ? @@

manshum12 requested to disclose this report. Jan 16th (9 months ago)

agent-1 agreed to disclose this report. Oct 9th (3 days ago)
disclosure approved

This report has been disclosed. Oct 9th (3 days ago)