62

# SQL Injection in [redacted]

Share:

| | |
|---|---|
| State | Resolved (Closed) |
| Disclosed | **August 19, 2019 5:52pm +0530** |
| Reported To | **U.S. Dept Of Defense** |
| Weakness | SQL Injection |
| Severity | High (7 ~ 8.9) |
| Participants | |
| Visibility | Disclosed (Full) |

Collapse

TIMELINE · EXPORT

arinerron2 submitted a report to **U.S. Dept Of Defense**. Oct 4th (about 1 year ago)

## Summary:

There is an SQL injection vulnerability in the SSN field at https://[redacted]/[redacted]/candidate_app/status_scholarship.aspx

### Impact

An attacker could use this vulnerability to control the content in the database, exfiltrate information, and potentially obtain remote code execution.

### Step-by-step Reproduction Instructions

Follow these steps:

1. Visit https://[redacted]/[redacted]/candidate_app/status_scholarship.aspx
2. Right click on the SSN field, click Inspect Element, and edit `maxlength="9"` by changing it to `maxlength="9999"` (or something similar, so that a longer payload can be put in)
3. Choose a random birth date, for example, January 1, 1990.
4. Enter in your SQL injection payload into the SSN field. For example, try `' OR '1'='1`.
5. Click "Check Status". Your SQLi payload will execute. If you did the example payload in step 4, assuming someone has the birth date you entered, it will log in as them and check their scholarship status.

Also, I didn't do much testing, but I think the birth date is also vulnerable to SQL injection. After sending the request, in the network tab, Edit and Resend Request after changing the birth day, month, or year to a payload that will cause invalid syntax like `'`. It will give you an HTTP 500 response. If you do a payload that won't cause invalid syntax like `''`, it will give you an HTTP 200.

### Suggested Mitigation/Remediation Actions

Sanitize everything (use prepared statements) and validate the data.

### Impact

An attacker could use this vulnerability to control the content in the database, exfiltrate information, and potentially obtain remote code execution.

**BOT:** U.S. Dept Of Defense posted a comment. Oct 4th (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. Oct 4th (about 1 year ago)

ag3nt-j1 changed the status to ○ **Triaged**. Oct 4th (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

arinerron2 posted a comment. Oct 23rd (12 months ago)

It looks like a fix was implemented; I can no longer reproduce this issue.

arinerron2 posted a comment. Dec 7th (10 months ago)

Hi, just following up- I think this issue is ready to be closed (and has been for 2 months). I've extensively tested this particular page, and there do not appear to be any more SQL injection vulnerabilities in it.

deez_nops closed the report and changed the status to ○ **Resolved**. Apr 2nd (6 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

arinerron2 requested to disclose this report. Apr 7th (6 months ago)

ag3nt-j1 agreed to disclose this report. Aug 19th (2 months ago)

This report has been disclosed. Aug 19th (2 months ago)