Major SQL Injection Attack

HOW ARMOR HELPED STOP A MAJOR SQL INJECTION ATTACK INVOLVING MULTIPLE BANKING SITES

1

Alert: Armor's security team is ready for action 24/7/365. So when a customer alerted them to a large number of malformed files being submitted into their website document processor, they jumped into action.

2

Response: Now on alert, Armor's incident response and forensics (IRF) team got to work analyzing the malformed files and the document submission form being exploited by threat actors.

3

Discovery: After neutralizing the threat and investigating the cause, it was concluded that the SQL injection was successful due to a misconfiguration regarding validation of user input.

4

Remediation: Working with Armor, the client was able to rework their website with added protection against future SQL injection attacks. This ensures threat actors don't have easy access to their network.

ATTACK & RESPONSE SUMMARY

FORTIFIED DEFENSES.

ARMOR HELPED THE CLIENT STRENGTHEN THEIR CYBER SECURITY.

IMMEDIATE RESPONSE. ARMOR'S SECURITY EXPERTS SPRUNG INTO ACTION. STAVING OFF EXTERNAL THREATS.

8HRS

ARMOR'S ELITE OPERATIVES PROVED EFFECTIVE.

RESOLUTION TIME:

8 HOURS

Your data doesn't belong to them.

WE WON'T LET THEM TAKE IT.

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™