# SQL Injection Attack & PCI Data Breach

## Case Study

Heartland Payment Systems / Heartland Payment Customers, Clients, and Insurers

October 2020

By Kyler Kent

Design credit to International Business Machines Corporation (IBM) Cybersecurity Analyst Professional Certificate program for template

# Attack- SQL Injection

SQL Injection:

Infiltration, usually through a web-based host accepting database queries, by malevolent SQL queries designed to obtain unauthorized information, unauthorized access, or to have unauthorized actions performed by the host's web-facing system.[1]

An unusual feature of SQL injection attacks includes its more recent rising use against the manufacturing industry, according to the IBM X-Force Threat Intelligence Index 2020.[2]

It is a prevalent and primitive web application attack method that is well-known in the cybersecurity industry and is usually well-defended through standard cybersecurity architectures and practices such as web-application firewalls and vulnerability scanning.[3]

Was shadowed by the 53% XSS (cross-site scripting) attack vulnerability category of web application vulnerabilities calculated in 2012, however, SQL injection rates for web apps were still at 25% of total web app vulnerabilities as of 2012.4 In 2019, Akamai found SQL injection attack vulnerabilities at a spike at 65.1% of total web app vulnerabilities.[5]

Heartland Payment Systems was a US-incorporated payment processor that accepted common PCI (payment card industry) methods such as debit, prepaid, and credit cards. It was one of the largest processors in the industry and was acquired in 2015 by Global Payments for $4.3 billion.[6] Its platform sat between the banks and POS terminals (point-of-sale) in its deployment nationwide.[7]

The initial exploitation by the organized hacker group was a SQL injection attack on the web login page in 2007 that allowed entry into the SQL databases where the attackers started persistence into Heartland. They established a foothold, and developed persistence, using masking and decoy techniques for almost 8 months where enough lateral movement occurred to where they were able to gain access to PCI in POS systems through locally installed spyware that captured PCI data at the terminal. This occurred in 2008. Subsequently, they were able to breach credit card information for millions of cards ready for illegal reuse.[7]

Next, HPS lost its PCI-DSS (data security standard) compliance, losing access to major credit card providers until 2009, resulting in over $200 million in total losses.[7] This started the end-to-end encryption techniques described as industry standards in later PCI-DSS in the Coursera IBM Cybersecurity Analyst Certificate program to prevent the collection of PCI data-at-rest.

The perpetrators were organized cyber criminals, including a US Citizen-- Albert Gonzalez, and were all indicted, captured by the FBI, and sentenced to the US federal prison system for lengthy terms.[7]

# Timeline

Heartland Payment Systems Inc.
SQL Injection

1. **Dec. 2007 : SQL Injection attack conducted by Albert Gonzalez was successful in Heartland Payment Systems and its affiliates and persistence was started in Heartland to disseminate PCI POS spyware.**
2. Oct. 2008: Visa warns Heartland of possible breach. Heartland ensues internal investigation.
3. Nov. 2008: Heartland loses its PCI-DSS compliance status.
4. Jan. 2009: HPS discovers the most likely responsible spyware responsible for the PCI data collection on their systems, and this is made public.
5. Mar. 2009: Heartland loses Visa due to PCI-DSS compliance failure.
6. April 2009: Heartland regains PCI-DSS compliance status.

Source: McGlasson, Linda, and Ron Ross. "Heartland Breach: Inside Look at the Plaintiffs' Case." Bank Information Security, 2009, www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844.

# Vulnerabilities

## Overall Summary

Basic web application firewall (WAF) misconfiguration failed to prevent SQL injection attacks. Not using vulnerability scanners and documenting scores during regular audits caused a failure to detect SQL injection vulnerabilities. Not using SIEM collectors to monitor real-time SQL injection attempts did not allow an early response. Faulty DLP practices without P2PE at POS. Failure to use defense-in-depth for zero-day assaults.

## Vulnerability #1

Insufficient input validation and, more importantly, stored procedures on WAF for the web server led to the successful initial exploitation of Heartland's and affiliates' resources through an allowed, web-facing SQL injection attack on a login page.

## Vulnerability #2

The failure of HPS's cybersecurity team to detect the initial exploitation/attack. Possibilities included ignoring repeated SQL database errors and anomalous queries in SIEM or the SIEM not even being configured to collect traffic, events, and alerts from the web application appliance and the web server. False negatives were also possible.[8]

## Vulnerability #3

Betting on generic network perimeter defense products. Failure of the IT security team to detect zero-day attackers' persistence, lateral movement, and data exfiltration throughout the business. Attackers spent almost a year doing this, installing malware on POS systems to exfiltrate PCI data before an outside warning flagged the attack. Current PCI-DSS compliance is NOT enough to ensure security.[9]

## Vulnerability #4

Failure to use P2PE (point-to-point encryption) at POS systems to process PCI confidentially. Established as a new PCI-DSS as a remedial effort by Heartland and others.[10]

# Costs

- Total: $200 million estimated losses for all parties.
- Heartland received a $12.6 million loss in Q1 2009 due to breach expenses and fines.
- MasterCard reported $6 million fine in Q1 2009.
- Heartland self-reported $32 million total losses in June 2009.
- Heartland reports a $19.4 million loss in Q2 2009, which were mainly settlement attempts for the breach.
- Total compensation spent by Heartland for the breach was estimated to be $145 million [7]

McGlasson, Linda, and Ron Ross. "Heartland Breach: Inside Look at the Plaintiffs' Case." *Bank Information Security*, www.bankinfosecurity.com/heartland-breach-inside-look-at-plaintiffs-case-a-1844.

# Prevention

- PCI-DSS should be considered a minimum standard or business license, not an end-all, stand-alone security practice.
- The WAF must be properly configured, regularly scanned, and constantly forwarding logs to a monitored SIEM.
- P2PE is required for all POS PCI data movement.
- SIEMs and the IT security team personnel are critical assets in detecting zero-day attacks.
- Defense-in-depth strategies detect or stop complicated attacks, including APTs, even at the late stages when damage has peaked.
- A basic audit with a free network analysis tool (e.g., Wireshark) may have caught the massive PCI exfiltration, as suspicious network artifacts are left by most PCI DLP events.[11]

# Bibliography


- 1https://en.wikipedia.org/wiki/SQL_injection
- 2IBM Incident Response and Intelligence Services (IRIS), 2020, *X-Force Threat Intelligence Index 2020*, www.ibm.com/downloads/cas/DEDOLR3W. Page 37
- 3Nakar, Ori, and Johnathan Azaria. "SQL Injection Attacks: So Old, but Still So Relevant. Here's Why (Charts): Imperva." Blog, Imperva, 5 Sept. 2019, www.imperva.com/blog/sql-injection-attacks-so-old-but-still-so-relevant-heres-why-charts/.
- 4Franklin, et al. . IBM Security Systems, 2013, pp. 52–52, *IBM X-Force 2012 Trend and Risk Report*.
- 5 Vijayan, Jai. "SQL Injection Attacks Represent Two-Third of All Web App Attacks." *Dark Reading*, Dark Reading, 13 June 2019, www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-two-third-of-all-web-app-attacks/d/d-id/1334960.
- 6Dexheimer, Elizabeth. "Global Payments to Buy Heartland Payment for $4.3 Billion." Bloomberg.com, Bloomberg, 15 Dec. 2015, www.bloomberg.com/news/articles/2015-12-15/global-payments-to-buy-heartland-payment-for-about-4-3-billion.
- 7 Judge, Kevin. "The Heartland Breach: A Cautionary Tale for E-Commerce." Comodo News and Internet Security Information, Comodo, 5 Oct. 2020, blog.comodo.com/e-commerce/the-heartland-breach-a-cautionary-tale-for-e-commerce/.
- 8 Vijayan, Jaikumar. "Heartland Data Breach Sparks Security Concerns in Payment Industry." *Computerworld*, Computerworld, 22 Jan. 2009, www.computerworld.com/article/2530279/heartland-data-breach-sparks-security-concerns-in-payment-industry.html.
- 9Gordover, Michael, and Team ObserveIT. "Throwback Thursday: Lessons Learned from the 2008 Heartland Breach." ObserveIT, 24 Apr. 2018, www.observeit.com/blog/throwback-thursday-lessons-learned-from-the-2008-heartland-breach/.
- 10Chadran, Achmad. "The 3 Worst Data Breaches of All Time (and the Lessons Learned)." *Smarter MSP*, 13 July 2020, smartermsp.com/3-worst-data-breaches-time-learned/.
- 11 Smith, David C. Naval Postgraduate School, 2014, *PREVENTING POINT-OF-SALE SYSTEM INTRUSIONS Thesis*, apps.dtic.mil/dtic/tr/fulltext/u2/a607543.pdf . Pages 10-11.