Print This Page

08: Assisted Lab: Exploiting Weaknesses in a Website

PenTest+ (PT0-002) 2022 Update

Congratulations, you passed!

Duration: 1 hour, 27 minutes

☑ What is the result of the *whoami* command injected in this step? *Score: 1*

- ☐ jaime
- ☐ localhost
- ☐ 172.16.0.201
- ☑ www-data

Congratulations, you have answered the question correctly.

Print This Page

09: Assisted Lab: Exploiting Weaknesses in a Database

PenTest+ (PT0-002) 2022 Update

Congratulations, you passed!

Duration: 25 minutes, 18 seconds

☑ What is the name of the first database discovered with SQLMap? *Score: 1*

dvwa

Congratulations, you have answered the question correctly.

Print This Page

10: Assisted Lab: Using SQL Injection
PenTest+ (PT0-002) 2022 Update

Congratulations, you passed!

Duration: 19 minutes, 21 seconds

☑ What user account name is not present in this SQLi result? *Score: 1*

- admin
- Hack
- Morgan
- Bob
- Pablo

Congratulations, you have answered the question correctly.

Thesis Statement :

The purpose of this paper is to describe a data breach of Sony Pictures Entertainment faced from a SQL injection attack, therefore the following will discuss the 2011 Sony data breach.

1. **What company was impacted by the cyber attack?**

   Sony Pictures Entertainment

2. **When did this happen and what was exploited?**

   Back in 2011, Sony Pictures Entertainment, a subsidiary of the prestigious Sony Corporation, was subjected to a malevolent data breach that was orchestrated by a nefarious

SQL injection attack. This malevolent attack resulted in the brazen theft of highly sensitive data, such as a multitude of employees' personal information, including email addresses, passwords, social security numbers, and other intricate details that cannot be disclosed.

3. **What did the Threat Actor take during the breach?**

The perpetrators were also able to infiltrate the company's email system, which harbored a plethora of sensitive and highly confidential information that was pertinent to the company's day-to-day operations. The heist included a bevy of email correspondence between senior executives, reports detailing the financial transactions of the company, and other highly confidential information that was intended to be kept under wraps.

4. **How did this impact the brand of the organization and were there any regulatory fines such as HIPAA or PCI violations?**

The nefarious data breach wrought a significant impact on Sony Pictures Entertainment's brand. The unauthorized acquisition of highly sensitive employee information set off a wave of concern among employees, while the exfiltration of confidential information also caused irreparable reputational harm to the company. To make matters worse, the incident became the center of a media frenzy and the intense public scrutiny that followed created immense pressure on the organization to take steps to restore its reputation and win back the trust of its stakeholders.

In addition to the reputational damage, the data breach led to punitive regulatory fines and legal action. Although HIPAA and PCI violations were inapplicable in this instance, the company became the target of regulatory investigations and fines from several regulatory bodies, including

the Federal Trade Commission (FTC) and the Office of the Information Commissioner in the UK. In 2013, Sony Pictures Entertainment came to a settlement with the FTC for a paltry sum of $250,000, and in 2014, the company reached an agreement to pay out a whopping $8 million to settle a lawsuit filed by employees who claimed that the company failed to safeguard their personal information. The settlement terms included provisions for identity theft protection and credit monitoring for impacted employees.

All in all, the Sony Pictures Entertainment data breach had a profound and far-reaching impact on the organization, both in terms of reputation and financial penalties. The incident serves as a stark reminder that companies must make cybersecurity a top priority and take all necessary measures to safeguard sensitive information and fend off cyber attacks.

References :

Caltagirone, S., Pendergast, M., & Clark, J. (2011). "A targeted attack on Sony PlayStation Network".

Carey, M. (2011). "Sony Data Breach: Timeline".

Greenberg, A. (2011). "Sony Pictures' Hacking Nightmare Gets Worse With Studio's Data Dump".

Kerner, S. (2011). "Sony Hack Explained: How a Security Flaw Led to a Devastating Breach".

Manion, M. (2011). "Sony's 2011 PlayStation Network hack ruled not "unfair"".

Singh, S. (2014). "SQL Injection Attacks and Defense Mechanisms". International Journal of Engineering Science and Innovative Technology, 3(2), 231-238.

Swartz, J. (2011). "Sony data breach leads to lawsuits".