

第63回スクエアfreeセミナー

SQLインジェクションと戦う○×△

株式会社OPENスクエア

田中 昭造

2016年1月28日

SQLインジェクションとは何だろう？

私も良く知りませんので、この機会に勉強してみました。

こんな環境でテストしてみました。



アプリケーションサーバ
DVWM

SQLインジェクション体験



動画を御覧ください

■ デモアプリで実際にSQLインジェクション攻撃を行なって見ました



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: SQL Injection

User ID:

Submit

User IDに会員番号を入力すると姓名が表示される。

ID: 1
First name: admin
Surname: admin

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

SQLを注入して全ユーザを表示



動画を御覧ください



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

SQLを注入してユーザのパスワードを取得



動画を御覧ください



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

パスワードの復号



動画を御覧ください



Decrypt Md5 Hash

Decrypt Md5

Create Md5 Hash

Create MD5

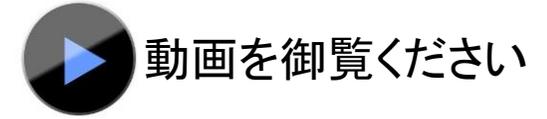
It's gone. [Undo](#)

What was wrong with this ad?

- Irrelevant Repetitive Inappropriate

Google

SQLインジェクションと戦う○×△



1 LoadMasterのAFP機能でSQLインジェクション攻撃をブロックできました。

2 LoadMasterのAFP機能ではクロスサイトスクリプティング攻撃などもブロックできます。

3 Free LoadMaster(VLM)でもAFP機能を利用できます。

サイバー攻撃対策は“知る”ことから

攻撃見えるくんはサイバー攻撃をリアルタイムに可視化する無料で利用できるサービスです。



現在の攻撃状況



※デモデータにて公開中です。実際の攻撃状況ではございません。

ご清聴ありがとうございました。

株式会社OPENスクエア

田中 昭造