This is My Topic

Phitchayaphong Tantikul
Ph.D. student, Faculty of ICT,
Mahidol University

Advisor: .....

November 29, 2017

Overview

1 Introduction

2 Security Countermeasures

Introduction

Statistics for Web Attacks

Something...[1]

[1] Paul Wood et al. *Symantec Internet Security Threat Report 2016*. Symantec, 2016. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Web Application Attacks

OWASP Top-10 (v. 2013)

Most Critical Web Application Security Risks[2]

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Cross-Site Scripting (XSS)
- A4-Insecure Direct Object References
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A7-Missing Function Level Access Control
- A8-Cross-Site Request Forgery (CSRF)
- A9-Using Components with Known Vulnerabilities
- A10-Unvalidated Redirects and Forwards

[2] OWASP. *OWASP Top-10 Most Critical Web Application Security Risks*. online. Apr. 2017. URL: `https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`.

Web Application Attacks: SQL Injection

```
$sql = "SELECT * FROM users
        WHERE username='admin' AND password='".$_POST['password']."'";
mysql_query($sql);
```

What if `$_POST['password']` contains string “’ or ’1’=’1”

Then, `$sql` will be

“SELECT * FROM users WHERE username=’admin’ AND password=” or ’1’=’1’ ”

It is equivalent to

”SELECT * FROM users WHERE true”

which returns back everything in the table.

This let attacker eventually gains access

to view or manipulate other data on the server

Security Countermeasures

Security Countermeasures

Something...

OWASP. *SQL Injection Prevention Cheat Sheet*. online. July 2016. URL: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

Summary

Summary:

- abc
- def

Q & A

Q&A and Suggestions

References

[1] OWASP. *OWASP Top-10 Most Critical Web Application Security Risks.* online. Apr. 2017. URL: `https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`.

[2] OWASP. *SQL Injection Prevention Cheat Sheet.* online. July 2016. URL: `https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet`.

[3] Paul Wood et al. *Symantec Internet Security Threat Report 2016.* Symantec, 2016. URL: `https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf`.