Security Advisory: Banks Security (Web)

Militan.c7

DEMO1

- function focusWin()
  {window.focus();
  …
  window.location.href =
  "http://www.banksa.com.au/business/business-banking-online/user-guide/?source=applet&origin=CBS"";

//document.write("http://www.banksa.com.au/business/business-banking-online/user-guide/?source=applet&origin=CBS"");
  }
  window.onload = focusWin;

DEMO2

Hack bank

- result = expression1 & expression2
- FillForm & Response.write("ccccc") ‘
- FillForm & Response.write("ccccc") %0d%0a Response.write("kerker") '

Introduction

- **Bank Web sites full of security holes, University of Michigan survey finds**

- Comments: this data is outdated.

Banks in Taiwan

- Exploit
- Error message
  - No
  - Strip
  - Full of Error
- Information Disclosure

Response(Not ALL)

- We`re SECUUURRRRREEEEEEE!!!

…You dxmn hacker!

Ask for accusation, huh? Fxck!

Q:SxCK HACKER!

A:Im not cracker.

Q:我們已經掌握你的姓名,mail跟單位!

A:是我寄給你的..

Q:保安~!保安~!

A:

Forget it.

I`m so kind.

```
<? …
   $sql="select * from vvvvv where a='".$a."' and
   b=".$b." and passwd=password('$passwd') ";
   …
        $_SESSION[‘b']=$b;
        $_SESSION[‘adminlogin']=“True";
        mysql_close($link);
        header("location: ccccc.php");
   }else{
        mysql_close($link);
        header("location: ddddd.php");   }
?>
```

Press Release

- xx銀行採用xx解決方案，提供Web內容與應用的安全防護與控管功能，並大幅加快員工網路應用存取時間。 相關人員表示：「爲提昇客戶服務品質，網路存取效能及安全性對銀行而言非常重要。xx的產品不僅符合我們在規格、產品、售後服務等方面的要求，更完善規劃了未來的應用建議。自去年導入xx產品後，不僅提升內部網路內容傳送速度，也協助我們成功地阻擋病毒、惡意和間諜軟體等攻擊。」
- xx的產品具備了高效能、高擴充性及可升級的代理伺服器平台體系，可保障網路通訊安全並加速Web應用傳輸。

Press Release

- xx提供一個最佳的Web安全解決方案，可以讓企業防護內部與外部Web安全威脅，xx具備間諜軟體（spyware）、惡意程式碼（MMC）、網路釣魚（phishing）以及網址嫁接（pharming）等攻擊與威脅，不同於其他解決方案，xx可以阻擋間諜軟體與keylogger透過後門通道而與其外部的任何伺服器聯繫。此外，目前只有xx提供a、b與c等服務，以協助防護企業的網站與品牌。
- xx銀行定期漏洞檢查、入侵偵測防護與防毒掃描：以安全軟體，監控網路活動，杜絕可能的攻擊

Truth.

- Banks Like:
  - Product
  - Solution
  - License
  - Ad

Funny

- Arch Info
- SPLIT
- Trust
- Stealth

Discussion

- Exploit
  - Input handle
  - Authentication, Access control, Logic flow, Session, Web Server Security
  - Dir Traversal & File Download?
  - Login Field

- Fallacy
  - Secure the Entrance
  - Programming Integrity

  - Multiple Service
  - Parameters
  - Architecture

- Fallacy 2
  - Entered, Trust
  - Both Convenience
  - Nothing = Secure

- Common Mechanism
  - ASP
  - PHP, JSP
  - SQL
  - CGI

- Unusual
  - Index Server
  - Xpath
  - LDAP
  - Gridview
  - NET AJAX Control Toolkit
  - Flash + XDP
  - ashx, Jsf, shtml(SSI), SOAP,etc

- Secure: Banks in Japan, 40hrs.
  - Parameters
  - Static
  - Single Entrance, Diff Hosts
  - Forget Password
  - Disclosure?

- HSBC.

- Tool
  - Tamper Data, Live HTTP Headers
  - Perl, wget
- No Burp / Webscrab
- Sample : Nation > 5. (subjective)
- Feb & May, leisure time

Conclusion

- Severe Problem
- Hackers wither, Crackers burgeon
- Security Advisory