Nguy cơ từ việc Upload File không an toàn - C99 Shell và giải pháp

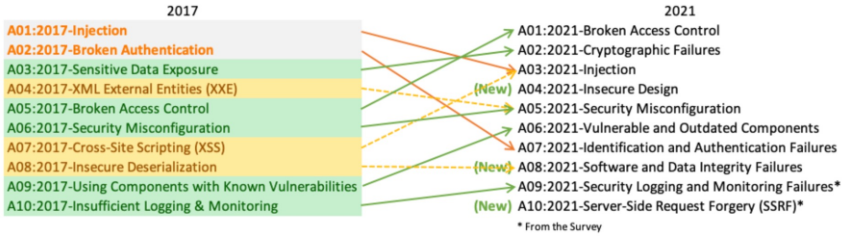
HV: LÊ THANH DŨNG

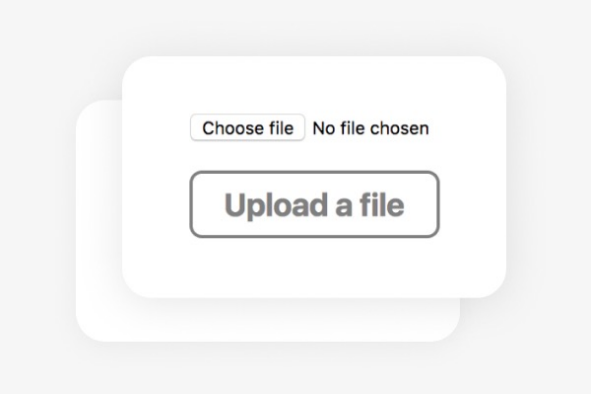
230101074

OWASP Top 10

- **OWASP Top 10**: https://owasp.org/www-project-top-ten

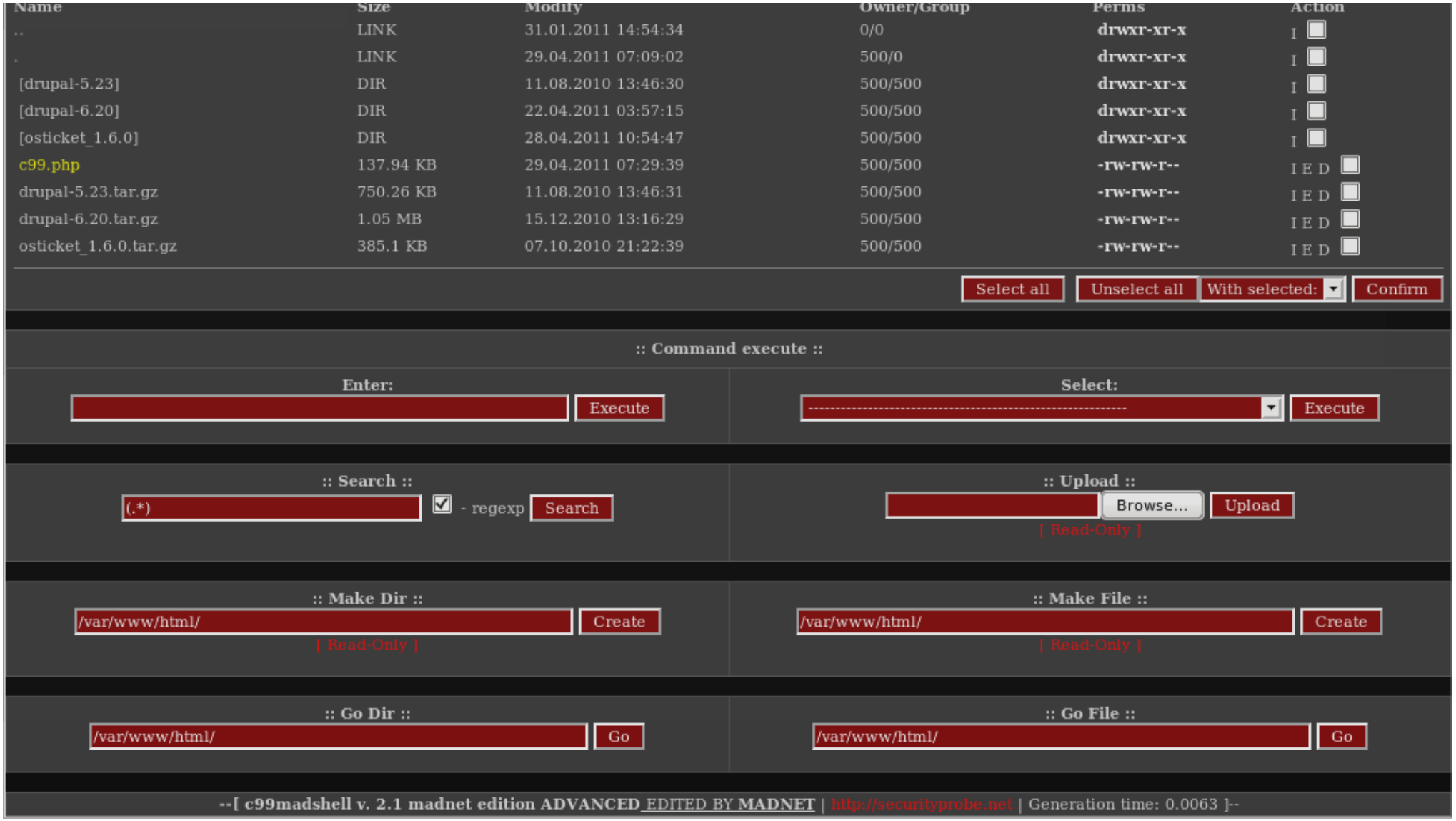
- Upload file không an toàn thuộc nhóm **A5: Security Misconfiguration** hoặc **A1: Broken Access Control**.





C99 Sheel là gì?

- **Định nghĩa**:C99 shell là web shell giúp hacker điều khiển server từ xa.
- **Cách thức hoạt động**:Hacker upload file PHP chứa mã độc (C99).
- Truy cập URL của file đó để:
  - Thực thi lệnh trên server.
  - Quản lý file và dữ liệu.
  - Tạo cửa hậu (backdoor) để truy cập liên tục.


Name Size Modify Owner/Group Perms Action
.. LINK 31.01.2011 14:54:34 0/0 drwxr-xr-x I
. LINK 29.04.2011 07:09:02 500/0 drwxr-xr-x I
[drupal-5.23] DIR 11.08.2010 13:46:30 500/500 drwxr-xr-x I
[drupal-6.20] DIR 22.04.2011 03:57:15 500/500 drwxr-xr-x I
[osticket_1.6.0] DIR 28.04.2011 10:54:47 500/500 drwxr-xr-x I
c99.php 137.94 KB 29.04.2011 07:29:39 500/500 -rw-rw-r-- I E D
drupal-5.23.tar.gz 750.26 KB 11.08.2010 13:46:31 500/500 -rw-rw-r-- I E D
drupal-6.20.tar.gz 1.05 MB 15.12.2010 13:16:29 500/500 -rw-rw-r-- I E D
osticket_1.6.0.tar.gz 385.1 KB 07.10.2010 21:22:39 500/500 -rw-rw-r-- I E D
Select all
Unselect all
With selected:
Confirm
:: Command execute ::
Enter:
Execute
Select:
Execute
:: Search ::
(.*)
- regexp
Search
:: Upload ::
Browse...
Upload
[Read-Only]
:: Make Dir ::
/var/www/html/
Create
[Read-Only]
:: Make File ::
/var/www/html/
Create
[Read-Only]
:: Go Dir ::
/var/www/html/
Go
:: Go File ::
/var/www/html/
Go
--[c99madshell v. 2.1 madnet edition ADVANCED EDITED BY MADNET | http://securityprobe.net | Generation time: 0.0063]--

Kỹ thuật hacker sử dụng

- **Thủ thuật upload file độc hại**:
  - Đổi tên file thành shell.php.jpg để bypass kiểm tra extension.
  - Nhúng shell vào file hợp lệ như .pdf hoặc .png.
- **Lợi dụng lỗ hổng server-side**:
  - Không kiểm tra MIME type chính xác.
  - Lưu file trong thư mục có quyền thực thi.

Hậu quả

- **Nguy cơ chính**:
  - Hacker chiếm quyền kiểm soát server.
  - Đánh cắp dữ liệu (e.g., cơ sở dữ liệu khách hàng).
  - Server bị sử dụng để phát tán mã độc hoặc tấn công DDoS.

Các biện pháp phòng tránh

1. **Kiểm tra MIME Type và Extension**:
   - ✓ Chỉ cho phép upload file hợp lệ, như .jpg, .png, .pdf.
   - ✓ Dùng thư viện hoặc API để kiểm tra header file.
2. **Thay đổi tên và lưu file vào thư mục an toàn**:
   - ✓ Đổi tên file thành chuỗi ngẫu nhiên.
   - ✓ Lưu file ở thư mục không có quyền thực thi.
3. **Quét virus/mã độc**:
   - ✓ Sử dụng công cụ quét file trước khi xử lý (e.g., ClamAV).
4. **Thiết lập quyền thư mục**:
   - ✓ Tắt quyền thực thi (exec) trên thư mục upload.
5. **Sử dụng sandbox**:
   - ✓ Kiểm tra file trong môi trường cách ly trước khi cho phép sử dụng.

Demo

Tổng kết

- **Tóm tắt**:
  - Upload file không an toàn là lỗ hổng phổ biến.
  - Hacker có thể khai thác qua file như C99 shell.
  - Các biện pháp phòng tránh giúp bảo vệ hệ thống.

"Kiểm soát việc upload file để bảo vệ hệ thống khỏi những cuộc tấn công đơn giản nhưng nguy hiểm!"