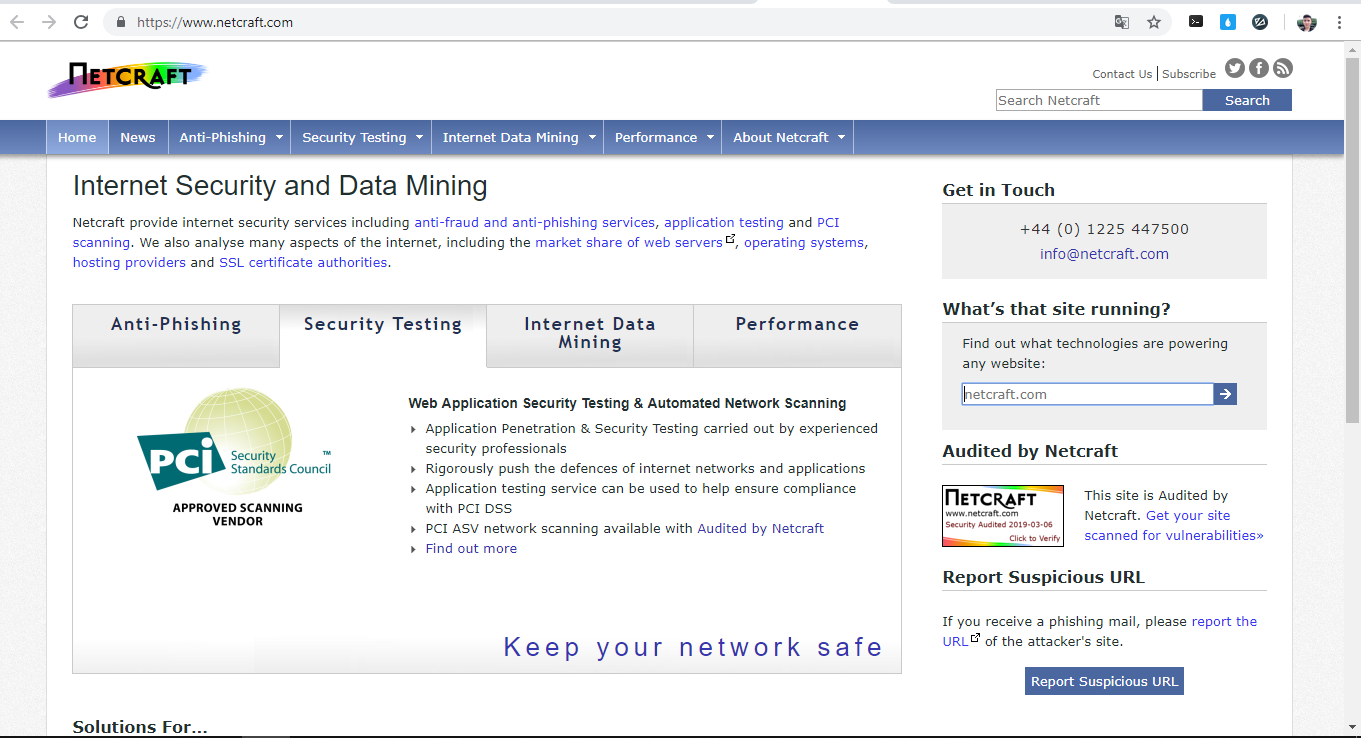
BÀI THỰC HÀNH

***Tiến hành thăm dò, liệt kê những thông tin bổ ích của 1 website bằng những công cụ đã được học (ở đây em chọn dùng công cụ Netcraft).***

Bây giờ mình sẽ sử dụng Netcraft để thu thập thông tin về website: piay.iflix.com

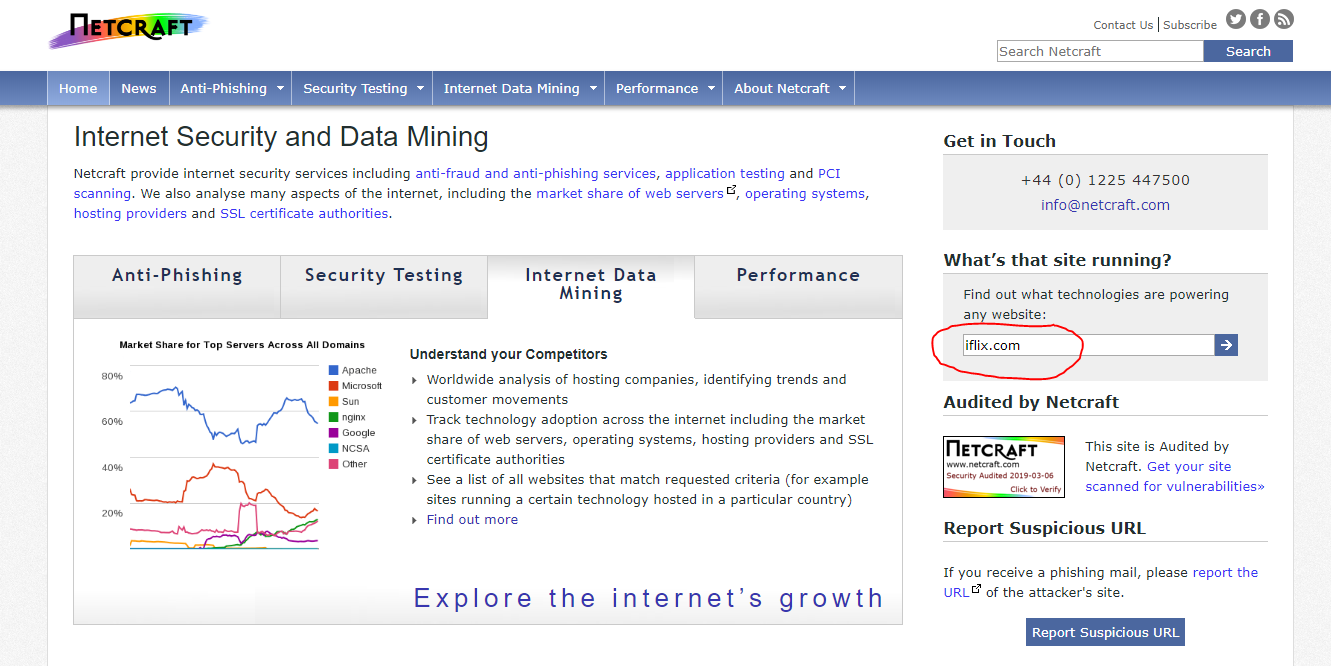


Đây là trang chủ của Netcraft



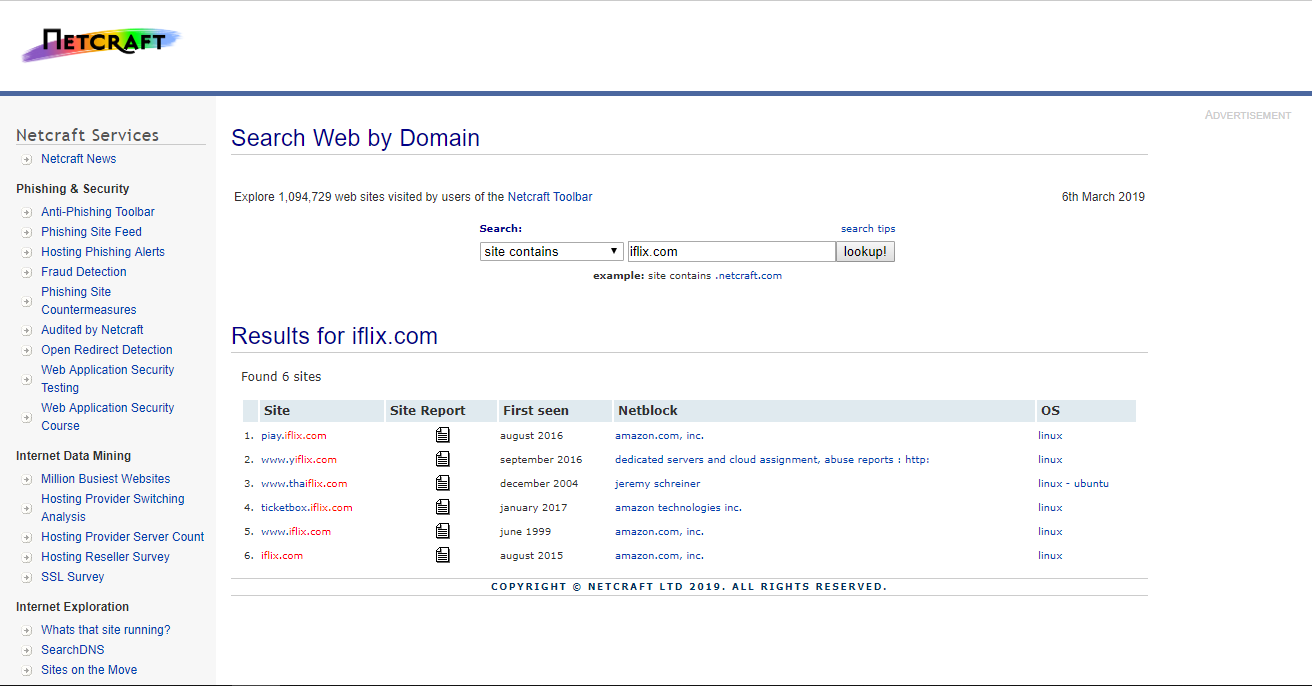
Nhìn vào góc bên phải “What’s that site Running?”. Tại đây mình bắt đầu điền website cần thu thập.

Ở đây mình sẽ tìm kiếm thử thông tin của website [iflix.com](http://searchdns.netcraft.com/?host=*.iflix.com) để thu thập thông tin của website [iflix.com](http://searchdns.netcraft.com/?host=*.iflix.com) có trên Netcraft



Sau khi Netcraft search domain “[iflix.com](http://searchdns.netcraft.com/?host=*.iflix.com)” và thu thập các dữ liệu về website mục tiêu thành công. Chúng ta có thể thấy:

* Site là những sub domain của website
* Netcraft sẽ thống kê thành một report trong phần Site Report
* Netblock cho mình biết tên công ty mà webserver đặt.
* OS: Cho biết hệ điều hành của server đặt website.



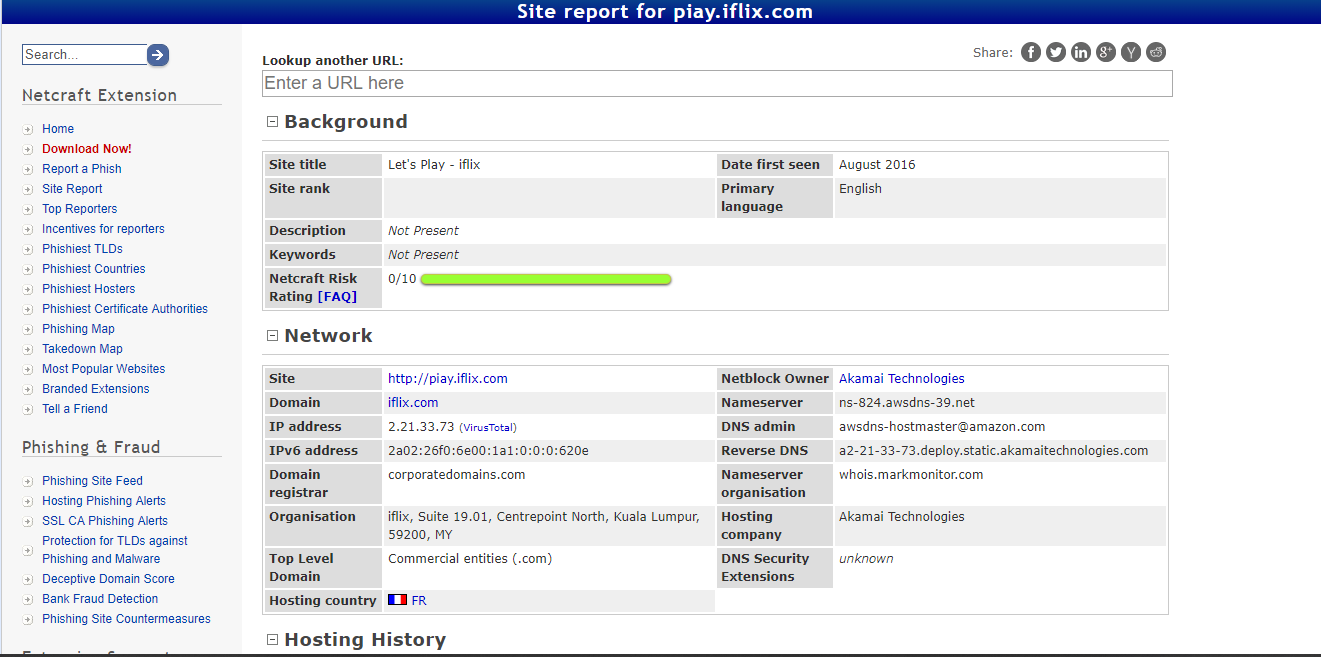
Click vào report ở cột Site Report ở trên để xem chi tiết thông tin dữ liệu mà Netcraft thu thập được

Ở đây em sẽ xem report của [piay.iflix.com](http://piay.iflix.com/).

Phần report này chứa những thông tin nhạy cảm về website [piay.iflix.com](http://piay.iflix.com/) mà một hacker cần.

Chúng ta có thể thấy các thông tin quan trọng của website [piay.iflix.com](http://piay.iflix.com/) được Netcraft được thu thập như:

* Site Rank. Cho biết thứ hạng của website. (Ở trường hợp này website không có hạng)
* Primary langguage: English. Cho biết ngôn ngữ sử dụng chính trong website [piay.iflix.com](http://piay.iflix.com/)
* IP address: 2.21.33.73. Là IP address của website [piay.iflix.com](http://piay.iflix.com/)
* Nameserver organisation: whois.markmonitor.com. Là nơi cung cấp tên miền cho website [piay.iflix.com](http://piay.iflix.com/)



Kéo xuống một chút, chúng ta sẽ thấy thêm các thông tin thú vị hữu ích cho tìm năng tấn công.  
Chúng ta có thể thấy lịch sử của hosting website svuit.vn như:

* Netblock owner: Chủ sở hữu hosting của [piay.iflix.com](http://piay.iflix.com/)
* IP address
* OS: Linux. Hệ điều hành sử dụng Hosting website [piay.iflix.com](http://piay.iflix.com/) là Linux
* Web server: AmazonS3. Ở đây Hosting [piay.iflix.com](http://piay.iflix.com/) sử dụng Web Server là AmazonS3.
* Last Seen

Tất cả những thông tin này rất hữu dụng đối với hacker bao gồm Last Seen.

Ví dụ: Last Seen này có thể là ngày mà hệ thống reboot hoặc được update.

Vào ngày 25-7-2017 website [piay.iflix.com](http://piay.iflix.com/) được chuyển qua một hệ thống mới hoặc reboot lại. Ở đây, chúng ta có thể thấy hosting [piay.iflix.com](http://piay.iflix.com/) ban đầu có địa chỉ IP là 54.192.11.228 và sau đó được chuyển qua IP 54.192.197.148. Điều này có thể cho biết hosting [piay.iflix.com](http://piay.iflix.com/) đã được chuyển sang một hệ thống khác.  
  
Bên cạnh đó thông tin thay đổi cuối cùng của website [piay.iflix.com](http://piay.iflix.com/) cũng cho hacker biết được rằng. Kể từ ngày 25-7-2017 Hosting [piay.iflix.com](http://piay.iflix.com/) không có thay đổi gì. Điều này có nghĩa là không có một tác động nào hay một bản vá security OS cho Hosting [piay.iflix.com](http://piay.iflix.com/) kể từ thời điểm này.  
  
Hacker có thể lợi dụng điểm này để tìm kiếm những lỗ hỗng của hệ thống không được update những bản vá lỗi kể từ thời điểm 25-7-2017.



Kéo xuống dưới một chút chúng ta sẽ có thêm một số thông tin về các công nghệ đang được chạy trên website này.

Dựa vào các thông tin về các công nghệ của website này đang chạy mà các hacker có thể tìm kiếm những lỗ hổng dựa trên tên những công nghệ đó. Điều này khá hữu ích cho hacker vì bọn họ không cần phải đoán những công nghệ phía sau web server đang chạy là gì. Như vậy hacker có thể nhận dạng được những công nghê, biết các công nghệ đang chạy điều này giúp các hacker dễ dàng tìm kiếm cách hack thích hợp nhất.  
  
Điều này cho thấy dữ liệu mà Netcraft thu thập được là không hề đơn giản. Mình có thể có được 80-85 % thông tin là chính xác và nó quá đủ để trinh sát thu thập các thông tin có giá trị của một website trước khi tấn công vào website đó.

