**ITP 125 - Homework 11**

**Tanuja Mohan**

Footholds

Exploit: [inurl:"lists/?p=subscribe" | inurl:"lists/index.php?p=subscribe"](http://www.google.com/search?q=inurl:%22lists/%3Fp%3Dsubscribe%22+%7C+inurl:%22lists/index.php%3Fp%3Dsubscribe%22)

Operators: The inurl operator is used to restrict results to those containing the query terms you specify in the URL. This search looks for lists that are subscription lists. These returned lists could contain credit card information that was used for the payment of the subscription.

File Containing Usernames

Exploit: [inurl:/profile.php?lookup=1](https://www.google.com/search?q=inurl:/profile.php?lookup=1)

Operators: The inurl operator is used to restrict results to those containing the query terms you specify in the URL. The lookup operator is used to find the specific term after the lookup within the URL file returned.

Sensitive Directories

Exploit: [inurl:admin inurl:uploads](https://www.google.com/search?q=inurl:admin%20inurl:uploads)

Operators: The inurl operator is the same as the one above in the “File Containing Usernames” section. This operator allows us to get results that have the following terms in it. In this case, we are getting results that have the term admin and uploads in it so we can access images that an administrative account has uploaded.

Web Server Detection

Exploit: [intitle:"Shoutcast Administrator"](http://www.google.com/search?q=intitle%3A%22Shoutcast+Administrator%22)

Operators: The intitle operator returns results that have the term in the title of the page.This exploit is returning searches that allows us to find the administrator page. We can use this page to detect unlisted Shoutcast servers since the administrator has a list of all these servers.

Vulnerable Files

Exploit: [filetype:lit lit (books|ebooks)](http://www.google.com/search?num=100&q=filetype%3Alit+lit+%28books%7Cebooks%29)

Operators: The filetype operator restricts results to pages whose names end in that given suffix. In this case the suffix is “lit” which is the suffix given to Microsoft Reader books. This exploit returns a list of thousands Microsoft Reader ebooks.

Vulnerable Servers

Exploit: [inurl:rpSys.html](http://www.google.com.my/search?hl=en&q=inurl%3ArpSys.html&btnG=Google+Search&meta=)

Operators: The inurl returns results that have the term in the url. In this case, we get results that have rpSys in them which is commonly found in urls that are configuration pages for various types of systems. We can look through these configuration pages and find systems that are not password protected.

Error Messages

Exploit: ["mySQL error with query"](http://www.google.com/search?q=%22mySQL+error+with+query%22)

Operators: This search does not explicitly use operators and just uses keyword search to return results that have the same words. The results that appear show this error message along with other information that attackers can use to exploit the website. Error messages give a lot of information about went wrong and can expose vulnerabilities.

Files Containing Juicy Info

Exploit: [site:github.com inurl:"id\_rsa" -inurl:"pub"](http://www.google.com/search?q=site:github.com%20inurl:%22id_rsa%22%20-inurl:%22pub%22)

Operators: The site operator specifically looks through github’s website. The operator inurl then looks for a specific terms in the url. The second inurl operator looks for the second term as well. By splitting the two terms separately we are letting the search know that terms do not have to be in a specific order but just both have to be in URL.

Files Containing Passwords

Exploit: [filetype:xls "username | password"](http://www.google.com/search?q=filetype:xls%20%22username%20%7C%20password%22)

Operators:The filetype operator restricts results that are in that file type. For this search, we return results that are in the .xls format (excel spreadsheets). The following “username | password” look for spreadsheets that have columns titled “username” and “password”. This search gives results of spreadsheets that administrators might have not put directly on their website but are still accessible.

Sensitive Online Shopping Info

Exploit: [site:ups.com intitle:"Ups Package tracking" intext:"1Z ### ### ## #### ### #"](http://www.google.com/search?hl=en&lr=&safe=off&q=site%3Aups.com+intitle%3A%22Ups+Package+tracking%22+intext%3A%221Z+%23%23%23+%23%23%23+%23%23+%23%23%23%23+%23%23%23+%23%22&btnG=Search)

Operators: The site operator restricts the searches to return results that are from ups.com. The intitle operator returns results that have “Ups Package tracking” in the title of the webpage. In the intext operator returns results that have the following text in the body of the web page. This search allows us to find the location of packages based on having the tracking number.

Network or Vulnerability Data

Exploit: [inurl:/cgi-bin/finger? "In real life"](http://www.google.com/search?q=inurl:/cgi-bin/finger%3F+%22In+real+life%22&num=100&hl=en&lr=&ie=UTF-8&filter=0)

Operators: The inurl operator returns searches that have the term in the result url. The finger command on unix displays information about the system users. This search returns pre-fingered users, so an attacker would not have to guess their victims’ accounts.

Pages Containing Login Portals

Exploit: [inurl:"login.php?action=recover"](http://www.google.com/search?q=inurl:%22login.php?action=recover%22)

Operators: The inurl operator returns searches that have the term in the result url. The action operator tells the php form what state it should be in. In this case, the sites should be in the “recover” state, which occurs when a user is requesting to reset or get access to their password because they have forgotten it.

Various Online Devices

Exploit: [inurl:/net/net/protocol.html](http://www.google.com/search?q=inurl:/net/net/protocol.html)

Operators: The inurl operator returns searches that have the term in the result url. This search returns printers that do not have a login allowing attackers to print to the printers.

Advisories and Vulnerabilities

Exploit: ["error\_log" inurl:/wp-content](http://www.google.com/search?q=%22error_log%22%20inurl:/wp-content)

Operators: The inurl operator returns searches that have the term in the result url. This search returns error logs with server side debugging info, such as home path directory names, which are often the same user names for logging into the server over FT and SSH.

I am surprised by the amount of information available to me just by doing certain searches. I always knew that Google was a powerful tool in extracting private information but did not know how to use it. These search operators are very useful when trying to narrow down to specific information but people need to be aware of how easy it is for attackers to use Google for malicious reasons. We just put content on the internet without understanding how what we are putting on the internet can actually harm us if the information falls into the wrong hands.