How to hack a website

Mr. Amit S Hariyani
Department of Computer Science, Bhavnagar
Maharaja Krishnakumarsinhji Bhavnagar University,
Sardar Patel Campus, Gardi Gate, Bhavnagar

Abstract— Hackers are actually coming out states of black and white, there are some black hate hackers who violates computer security for little reason. There are some ways hackers works out on some forums like security holes. These hacker enjoys the challenge of trying to find security vulnerability but they never often report the security hole to the company after they found the particular hole they looking for. Basically they are skilled programmer proficient in machine code and computer operating systems.

Keywords—Black Hat Hackers, Security Holes, Vulnerability

I. INTRODUCTION

Generally websites are used to carry sensitive data from a people to an entity with online based presence. They contains materials that are shown after authentication only. Most of time some users stores their credit card details for purchasing some item online and that may harmful and hackers are always trying to get those details to hack their account. I have provided here some few techniques to hack a website with practical implementation.

Why the internet is a hacker's playground?

1) **Ubiquity:** So many web applications out there have serious security vulnerability. Almost 80% of web applications have their serious security vulnerability that is proved by White Hat security 2009 report.
2) **Profitability:** If you can find an attack that have just a very low weight of return because it is automated and skilled you can make a huge profit on a think. Automation makes attacks with a minimal rate of return profitable.
3) **Simplicity:** Attack tools are published on the internet so only the first attacker has to be skilled and creative and intelligent. Hackers loves to boast about their exploits.
4) **Anonymity:** Just under hack a particular application you can have 100 of results and also it is very safely to break and if you know the application is hacked it is very difficult to track down. Attacks often go undetected. Attackers are difficult to trace.

II. MAPPING THE APPLICATION

A. *Infrastructure*

a. **Server Identification:** Attack usually target the exploits in the software to gain authorized entry to server. Some default settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also alows perform certain tasks such as running commands on server which can be exploited. Certain configurations such as allowing users to execute commands on the server can be dangerous if the user does not have good password. Discovered bugs in the operation system or web server software can also be exploited to gain unauthorized acess to the system. Lake of security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loop holes for attackers.

b. **Port Scanning:** Some time port scanning is used by hackers to identify open ports and services available on a network host to target victims. It is similar like doors or windows of home if hacker found its open then hacker check possible connections could made in most areas and it is not considered as a crime also.

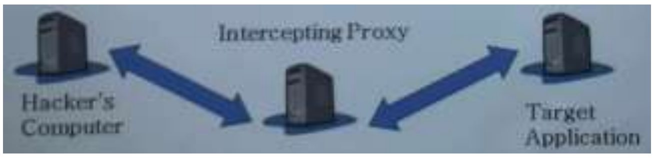
B. *Application Profiling*

Some of the Application Profiling used in the hacking a website are as follows:

a. URL Query Strings and Profiling
b. Authentication Mechanisms
c. Use of TLS / SSL
d. Application software in use (PHP, Java)
e. Directory Structure
f. Session Management

III. PLAYGROUND EQUIPMENT : PROXY SERVER

It speeds up access to a web page (caching). To hack a website you must have one intercepting proxy server. You can examine all the messages, it's very helpful because there is lot hidden traffic those between client and server that you normally can see that using proxy server can allows you to examine all their content, furthermore it allows you to alter that content. That means on the client side it really doesn't matter the kind of controls you put in the code in the client side because a good hacker can always transfer that control by taking directly it to the server with whatever your browser has been sent. So we need to get a proxy server with the application that you can just download and use. You may keep machines behind it anonymous and also you may use content filtering. It enables viewing and modifying all HTTP messages passing between the browser and the target application.



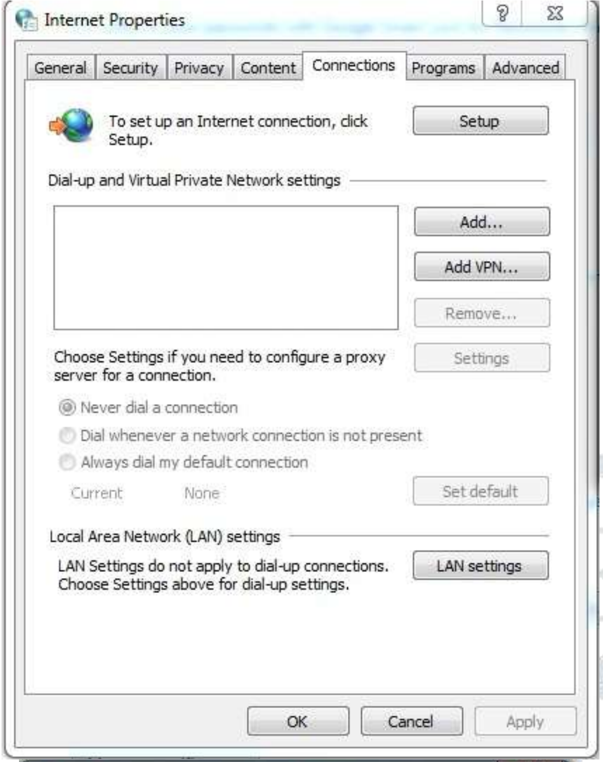
A. *Installing an Intercepeting Proxy*

To install an intercepting proxy you may download a free suit such as

a. Web Scarab: http://www.owasp.org/index.php/Category:owasp webscrabe project
b. Burp Suite: http://www.portswigger.net/suit/

c. Paros:
http://www.parosproxy.org/functions.shtml/
These are the leading three proxy servers you can download even better they are free so doesn't coasting anything. You can install them like any other application.

B. *Configure your web browser to use the proxy*



Internet Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

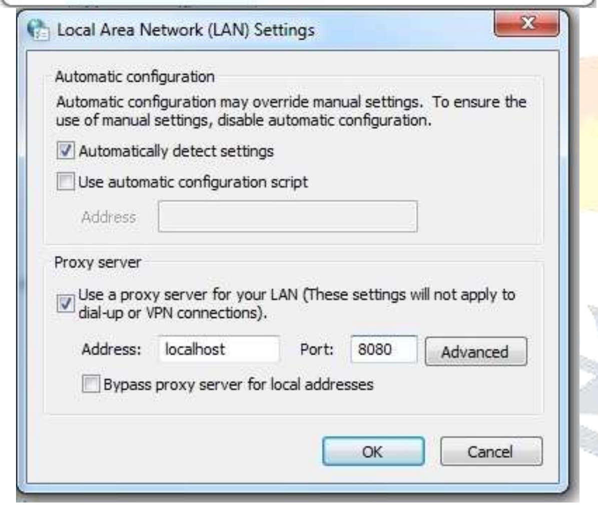
Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

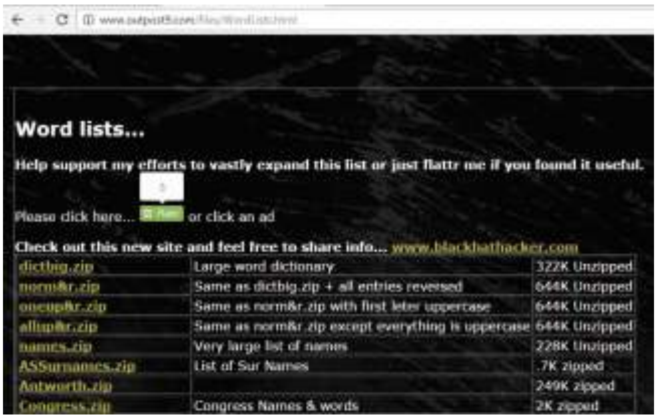
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: localhost Port: 8080

□ Bypass proxy server for local addresses

IV. DICTIONARY ATTACK

Use a list of common and default passwords or a comprehensive dictionary. All the dictionary attack is trying to get someone's password by going through a big list of passwords and trying each one until you get the success. So that's the dictionary attack just like anything else if you need a dictionary you may download it from:
http://www.outpost9.com/files/WordLists.html



www.outpost9.com/files/WordLists.html

Word lists...

Help support my efforts to vastly expand this list or just flattr me if you found it useful.

Please click here... or click an ad

Check out this new site and feel free to share info... www.blackhathacker.com

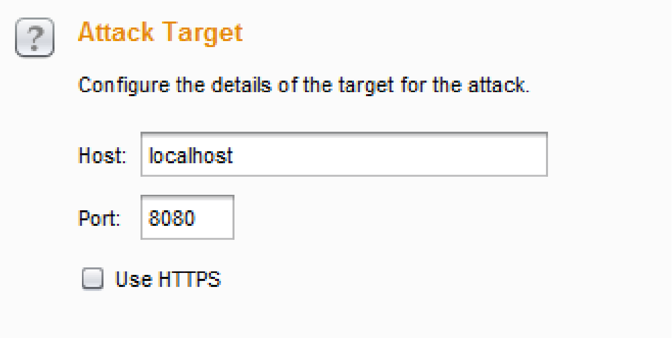
dictbig.zip	Large word dictionary	322K Unzipped
norm&r.zip	Same as dictbig.zip + all entries reversed	644K Unzipped
oneup&r.zip	Same as norm&r.zip with first leter uppercase	644K Unzipped
allup&r.zip	Same as norm&r.zip except everything is uppercase	644K Unzipped
names.zip	Very large list of names	228K Unzipped
ASSurnames.zip	List of Sur Names	.7K zipped
Antworth.zip		249K zipped
Congress.zip	Congress Names & words	2K zipped

You may use your intercepting proxy to automate the attack. Now before you launch the dictionary attack the one of the thing you should examine really carefully what is the password supposed could application you trying to attack, for login facility we need to examine that the best way to get examine passwords is you go to the password reset screen, because they often give you some clue, suppose I have entered some wrong password and tried to logged in, it will post some message such as "Login Error". We know that our dictionaries don't tell any words they listen a characters one, and also trace letters both in upper and lower case, numbers and symbols with attack.

Here, I have presented one sample example by using burp suit. Follow the given steps using burp suit and you may hack password using burp suit.

Step 1: If your browser is not configured to listen proxy first set it for local host as above.

Step 2: Download and start burp suit and set up given options



Attack Target

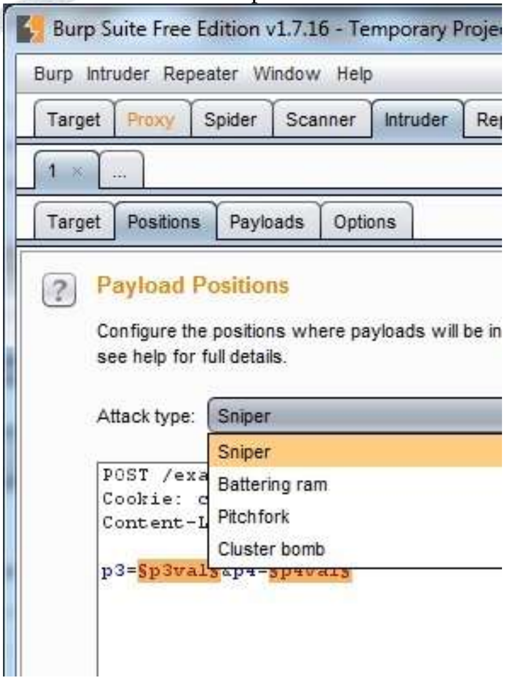
Configure the details of the target for the attack.

Host: localhost

Port: 8080

□ Use HTTPS

Provide host name and port address for attack target.



Burp Suite Free Edition v1.7.16 - Temporary Proje

Payload Positions

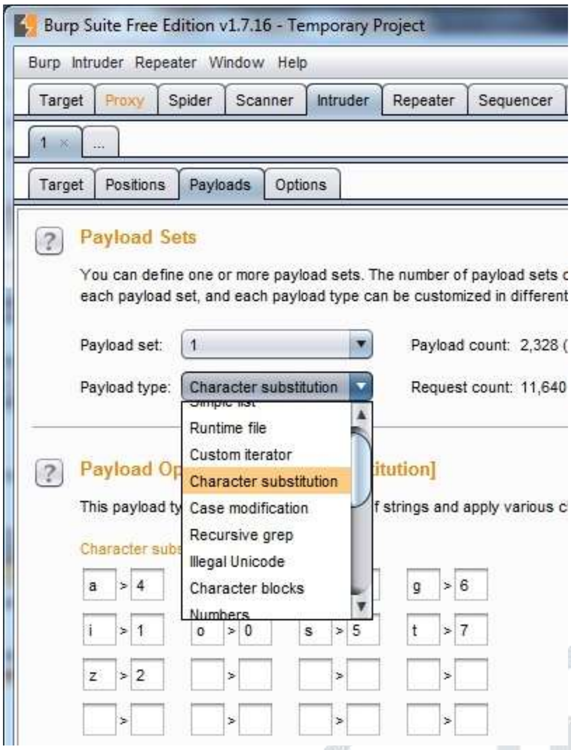
Configure the positions where payloads will be in see help for full details.

Attack type: Sniper

```
POST /exa
Cookie: c
Content-L

p3=§p3val§&p4=§p4val§
```

Set payload positions to sniper


Burp Suite Free Edition v1.7.16 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer
1 × ...
Target Positions Payloads Options
?
Simple list
Runtime file
Custom iterator
Character substitution
Case modification
Recursive grep
Illegal Unicode
Character blocks
Numbers

Payload Sets

You can define one or more payload sets. The number of payload sets c
each payload set, and each payload type can be customized in different

Payload set: 1

Payload count: 2,328 (

Payload type: Character substitution

Request count: 11,640

Payload Op itution]

This payload ty f strings and apply various c

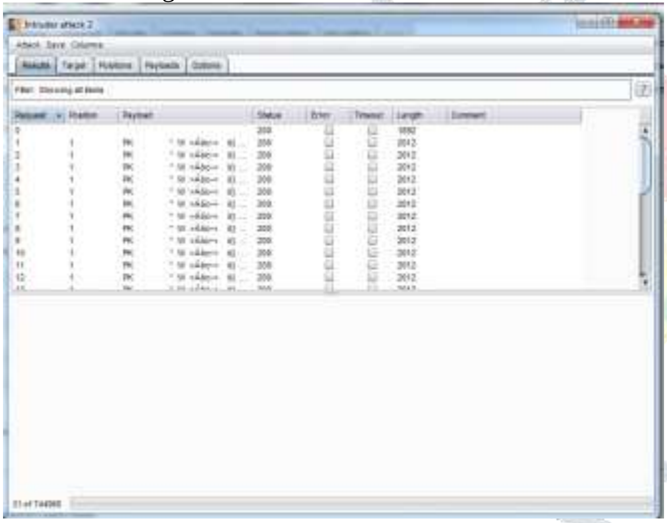
Character subs

a > 4 g > 6

i > 1 o > 0 s > 5 t > 7

z > 2

Then set payloads for example here we have selected character substitution in this example. Also we can provide some payload processing rules. At last clicking on Attack button we will get results.



Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			200	□	□	1882	
1	1	[illegible]	200	□	□	2012	
2	1	[illegible]	200	□	□	2012	
3	1	[illegible]	200	□	□	2012	
4	1	[illegible]	200	□	□	2012	
5	1	[illegible]	200	□	□	2012	
6	1	[illegible]	200	□	□	2012	
7	1	[illegible]	200	□	□	2012	
8	1	[illegible]	200	□	□	2012	
9	1	[illegible]	200	□	□	2012	
10	1	[illegible]	200	□	□	2012	
11	1	[illegible]	200	□	□	2012	
12	1	[illegible]	200	□	□	2012	

V. SESSION IDENTIFICATION : COOKIES

Web services are also helpful in hacking process, basically the protocol between web client like a browser and a server is HTTP and it is stateless protocol by that the web server doesn't remember who you are but when you use a web application it knows who you are because you put some items in your shopping cart and you may go back and look another items so it does remember you in some sense. Commonly to remember that it is using some session id and cookies. What the web server does is after you logged in it generates one of the cookies, these cookies tense to be mixtures of letters and details and they can have any particular name that the webserver give them and then once the cookies issued the web server sends them over to the browser and the browser stores that cookie locally on your computer then any time the browser request back from the server it sends the cookie back. The server can then look up who you are based on that cookie that can sent back. So that is a common way for web application to do identification.

- **Server sends a sessionId cookie to the browser**
  Set cookie: tracking=tI8rk7joMx44S2Uu85nsWc
- **Browser returns the cookie in all requests**
  Cookie: tracking=tI8rk7joMx44S2Uu85nsWc

VI. CROSS – SITE SCRIPTING (XSS) ATTACKS

The ID with an XSS attack if you want to enforce the web browser to execute some delicious code, now the code can be anything often its java script used for XSS attack. The goal can be anything but often the goal is to capture the victim's session id and use the victim's account to perform defacement, carry out an automatic action or injection of Trojan code. XSS attack finds a vulnerability and look for a place where a client supplied data can be sent to the web server and then echoed back to the screen for example search boxes are often vulnerable. The way java script code is delaminated is it always starts with opening script tag and a closing script tag. So, in this case the dangerous characters will be the <script> tags. An application developers are not totally stupid so they can try and put some filtering mechanisms inside their codes to check with these dangerous characters and remove them. But hackers are little bit smarter they have a website out here: http://ha.ckers.org/xss.html and this website have all kind of sophisticated ways of circumventing the controls, so this is one of the way to get through the application. The main goal of this attack is to Test the potential vulnerability for sanitization. Some of the dangerous characters such that they have special meaning in code are: (<,>OR'). Now Sanitization means filtering out or replacing dangerous characters.

A. How XSS attacks are executed?

This type of attack occurs when an attacker uses some web app to send malicious code, most of times in form of client side script to user. This attack can be categorized in three ways.

a. Where string generated from website
b. Or else as per client request
c. Either with the help of scripting languages.

VII. HOW SUCCESSFUL ARE AUTHENTICATION ATTACKS?

- Approximately 70% of web sites have authentication vulnerabilities.
- In 5th January 2009 Twitter accounts hacked in Brute force dictionary attack against an administrator account.
- 33 accounts of famous people broken into (including Obama's) and used to post the hacker's "Jokes"

VIII. CONCLUSIONS

I have simulated some of the dictionary attacks, cookie attacks and cross – site scripting attacks (XSS attacks) here and to carry out this simulation I have used burp suit, proxy server and java script code to demonstrate things. I have analyzed most of times attacks done by hackers are on basis of the mistakes done by computer user.

Secondly, with my simulation study I found that attacks done using cross site scripting are more powerful and easy to implement. Most of the hackers are using cross site scripting to target someone's PC. Here, I have also demonstrated some of the tools used in hacking.

IX. REFERENCES

[1] https://www.blackhat.com/presentations/bh-usa-06-Grossman by B Hat - 2006
[2] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).
[3] https://portswigger.net/burp/
[4] web.cs.du.edu/~mitchell/forensics/information/pass_crack.html
[5] http://www.parosproxy.org/functions.shtml/
[6] http://www.outpost9.com/files/WordLists.html
[7] http://ha.ckers.org/xss.html