VULNERABILITY ASSESSMENT AND PENETRATION TESTING FOR POORNIMA FOUNDATION

BY

Mukesh Kumar Rao
Saurabh Pandey
Vikram Pareek
Ayush Sharma

UNDER THE GUIDANCE OF
VIPIN KHANDELWAL

MINOR PROJECT REPORT
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF
BACHELOR OF TECHNOLOGY
COMPUTER SCIENCE ENGINEERING (CT&IS)

AT
Poornima University
Jaipur- 303905, INDIA
2017-18

FORWARD

I hereby forward the minor project report entitled **"Vulnerability Assessment and Penetration Testing"** presented by **Mukesh Kumar Rao, Vikram Pareek, Saurabh Pandey and Ayush Sharma,** 6th Semester B.TECH CSE (CT & IS), Session **2017 – 18 ,** under my guidance in partial fulfilment of the requirements for the Degree of Bachelor of Technology.

Vipin Khandelwal

Name of Guide

Dated:

Countersigned, HOD

Acknowledgement

Every project big or small is successful largely due to the effort of a number of wonderful people who have always given their valuable advice or lent a helping hand. We sincerely appreciate the inspiration; support and guidance of all those people who have been instrumental in making this project a success.

The completion of any inter-disciplinary project depends upon cooperation, coordination and combined efforts of several sources of knowledge. We are grateful to **Vipin Khandelwal Sir** for his even willingness to give us valuable advice and Directions; whenever we approached him with a problem .We are thankful to him for providing immense guidance for this project.

Mukesh Kumar Rao	(XXXXXXXXXXXXXXXX)
Vikram Pareek	(XXXXXXXXXXXXXXXX)
Saurabh Pandey	(XXXXXXXXXXXXXXXX)
Ayush Sharma	(XXXXXXXXXXXXXXXX)

INDEX

ABSTRACT 1

CHAPTER – 1 2

1. Introduction 2

1.1 Global Scenario for Cyber Threats 2

1.2 Cyber Security Scenario in India 3

1.3 Cyber Security – Legal Provision 4

CHAPTER – 2 5

2. Vulnerability Assessment and Penetration Testing 5

2.1 What is VAPT? 5

2.2 Need of VAPT 6

2.3 vulnerability Assessment Testing Methods 7

2.4 Benefits 7

2.5 Why does your organization need one? 8

CHAPTER – 3 10

3. Technical Report 10

3.1 Network Security 10

3.2 Web Application Vulnerabilities 11

CHAPTER – 4 15

4. Proof of Vulnerabilities Found 15

4.1 Vulnerability – 1 15

4.2 Vulnerability – 2 16

4.3 Vulnerability – 3 17 4.4

Vulnerability – 4 18 4.5

Vulnerability – 5 19

4.6 Vulnerability – 6 21

CHAPTER – 5 **23**

5. Executive Summary 23

5.1 Summary 23

5.2 Scope 24

5.3 Key Findings 24

5.4 Tabular Summary 31

CHAPTER – 6 **32**

6. Conclusion 32

APPENDIX **33**

Appendix – 1 33

Appendix – 2 35

REFERENCES **37**

TABLE OF CONTENTS

TABLE – 1 14

TABLE – 2 24

TABLE – 3 31

IMAGES

IMAGE – 1 6

IMAGE – 2 15

IMAGE – 3 16

IMAGE – 4 17

IMAGE – 5 17

IMAGE – 6 18

IMAGE – 7 18

IMAGE – 8 19

IMAGE – 9 20

IMAGE – 10 21

IMAGE – 11 22

IMAGE – 12 22

IMAGE – 13 26

IMAGE – 14 36

ABSTRACT

Today’s world is entering a new era, where all things are on Internet, everything is controlled and managed by digital gadgets. All businesses, online payments, education, training, services, etc. are on the online platform. But, as we going in new era there is always a pros and cons of that things. Like that, in Digital Era, Cyber Security becomes a very important issue for every organizations, institutions, and business. To overcome this problem we do VAPT on Web Applications and their Network Infrastructure in their organization to secure them from Malicious Activity and Financial loses.

This way we have done a deep Vulnerability Assessment and Penetration Testing (VAPT) on our Poornima Foundation and Poornima University’s Network Infrastructure to found out the vulnerabilities and loopholes and then give their proper solutions to secure our University from future threats and malicious attacks.

We did a proper analysis of Poornima Foundation websites and in Network Infrastructure to found the loopholes and then get out their solutions and patches. We follow the standard process and all the activities are done in a secret manner with all permission and under the guidance of our instructor and tutor. And we maintain the confidentiality of this project work and testing process.

For future perspective, we chose this project and done in live scenario situations to help our University and secure them. Due to this project, we learn and understand lots of new things. We got a whole new exposure to VATP process and findings their solutions and then propose to our organization.

Then we make a report on this project and given a methodical approach so that a non-technical person can also understand the severity of threats was present in Poornima Foundation Network Infrastructure. And, how we should patch them from the effects of threats and malicious activity on our campus. It would enhance our physical as well as digital security.

1. INTRODUCTION

In today's information-age is as such where everyone shares a common cyberspace with ever increasing penetration of internet technology in the day to day affairs of one's life. The world has become an interconnected village and everyone is connected via common cyberspace. This global interconnection has provided us with many opportunities on one hand & at the same time it has increasingly posed risk of cyber security and governance. Cyber Security is an important vertical of organizations working under various domain such as government, non-government, corporates, financial, educational institutes, defence etc.

An organization's dependence on cyberspace is becoming an ever increasing important aspect pertaining organizational security. As different organizational infrastructure are introduced into cyberspace or a limited intranet/cloud, the level of risk exposure increased to a level where national security concerns start to weigh in. The threat to cyber security is ever growing with varied landscape and attack/threat surface. Globally cyber risk is of great concern for all the enterprises which make use of it.

Almost 42 % of the organizations globally rank Cyber Security as their top concern and priority, even more so than the natural disasters, terrorism and traditional crime. The industries such as banking and economy, defence, information and energy, healthcare are the core targets of the cybercrime. The government sector witnessed 136% increase in cyber threats and the financial organizations witnessed a 126% increase in last 5 years.

1.1 Global Scenario for Cyber Threats

Cyber security can pose a major threat to our social, personal and professional spheres of life. The intruders might tamper with the websites and can view the confidential data in our system without our consent. They can also steal our valuable information like passwords, ID's etc. Cyber risk is not only limited to social networking sites or global enterprises, it is rather a big threat for the government as well as for the society too. The crimes like cyber trafficking, online gambling, forgery, financial crimes, cyber trespass, industrial espionage etc. is going viral in the World Wide Web all around the world.

The expansion of connectivity offers abundant opportunities for businesses, governments, and individuals, but also significant risks, especially those related to cyber security. In 2014, Microsoft produced a report called Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, which examines the complex relationship between policies and the development of ICT. The report forecasts the challenges and risk that cyberspace and cyber security might unfold over the next decade. Thus, it is very important for government & non-government organizations to take Cyber Security as a serious issue.

1.2 Cyber Security Scenario in India

As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still stuck in a catch up mode for both the scope and meaning of security in cyberspace and apportioning the responsibility accordingly.

Cyber Security in India

India has observed a significant increase in cyber-attacks against financials and government organizations with 34% and 43% increase in both of these respectively, up from last year's 15% and 19%, as revealed in the latest CERT-In report.

National security has traditionally been the sole responsibility of governments. But as the world transitioned into the information age, with increased dependence on information infrastructure for the production and delivery of products and services, the new responsibility of securing the critical information infrastructure (CII) against the rising number of cyber-attacks has come within the ambit of national security.

This new responsibility is not, however, solely that of the government; but the private sector now has a major role to play as more and more CII are found to be owned and operated by the Dept. of IT (DIT). Various critical IT-dependent infrastructure have been identified as such, namely

Defense, Finance, Energy, Transportation and Telecommunications. The IT Act, 2000, as amended in 2008, provides for protection of CII under section 70A. The government will designate an organization as the national nodal agency for CII protection, which will be responsible for all measures to protect CII.

Cyber Security in Government Context

At the National level CERT-In (Computer Emergency Response Team of India) is working closely together with their empanelled partner organizations to ensure that a continuous and acceptable security posture of all the identified Critical IT Infrastructures and systems is maintained. CII in India as of now comprises of around 150 Internet and telecom service providers, offering Internet, mobile and wireless connectivity to a user base of nearly 800 million.

CERT-In is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security. In the meantime, real oversight over cyber security may be said to be distributed amongst the Ministries of Communication and Technology, Home Affairs and Defense, and the office of the NSA. However, to safeguard the whole nation and ensure safety of CIIs across the national, the IT Amendment Act, 2008 clearly defines the proactive role of sectorial CERTs, Regional CERTs and State wide CERTs on the lines of CERT-In.

1.3 Cyber Security - Legal Provision

The IT Act of 2008 covers all actions in Cyber Security domain. Sections 69, 69A and 69B contain provisions for intercepting, monitoring or blocking traffic where, amongst other reasons, there is a threat to national security. Section 70A covers protection of critical infrastructure. There is a need to prioritize and protect critical infrastructure. In the USA 18 sectors have been identified. In India's case, the sectors of power, water supply, communications, transportation, defense and finance have been identified as vital constituents primed for national security. These critical sectors need to be defined and suitable protection measures ensured as laid down in the IT Act in a periodic and continuous manner.

2. Vulnerability Assessment and Penetration Testing

2.1 What is VAPT?

Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the pre-existing flaws in their code and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.

Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

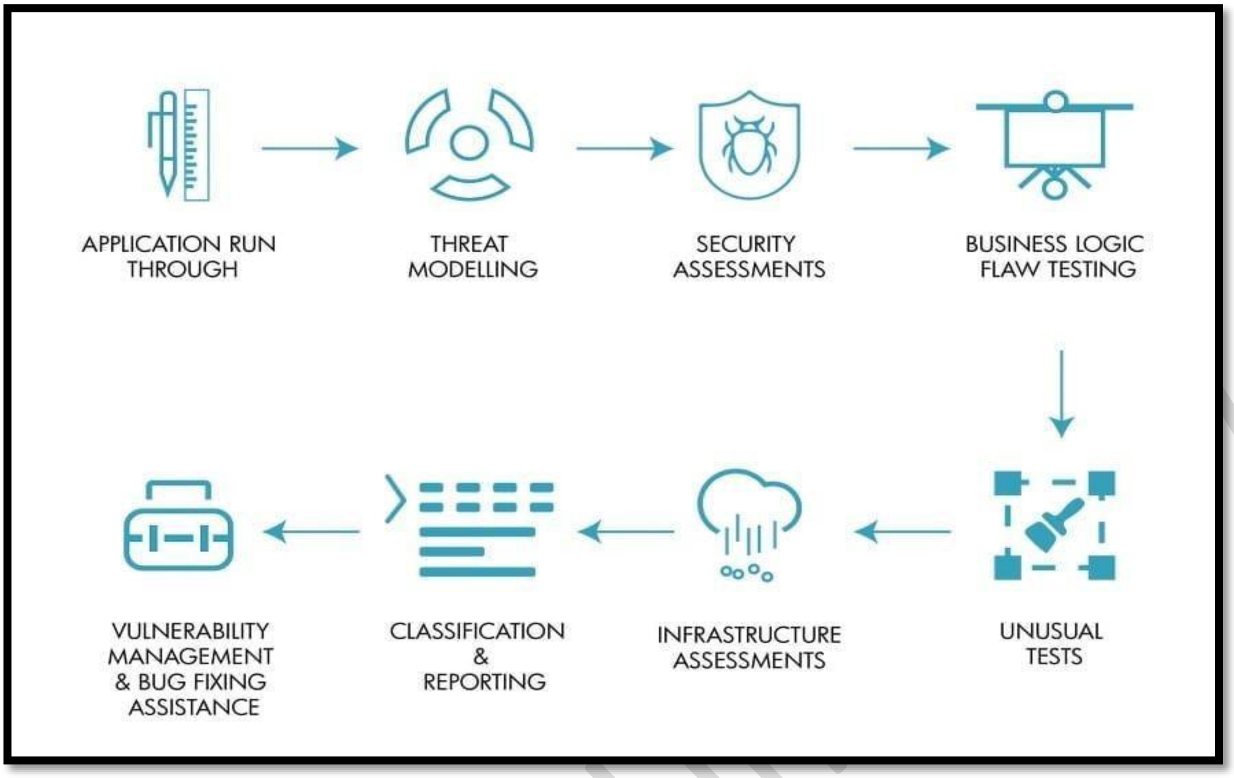

APPLICATION RUN THROUGH
THREAT MODELLING
SECURITY ASSESSMENTS
BUSINESS LOGIC FLAW TESTING
UNUSUAL TESTS
INFRASTRUCTURE ASSESSMENTS
CLASSIFICATION & REPORTING
VULNERABILITY MANAGEMENT & BUG FIXING ASSISTANCE

IMAGE-1 Vulnerability Assessment and Penetration Testing process

2.2 NEED OF VAPT

As the IT Scenario is changing, it is opening up new internet security challenges being faced by many organizations. Conducting business transactions over the internet (online) has always been a risk. It's a world of unforeseen traps, with vulnerabilities and threats manifesting themselves in the least expected place, at the least expected hour.

These challenges are required to be addressed by framing appropriate security policies, application of the controls and regular review & monitoring of the controls to ensure organization's information in protected. The VAPT audits need to be carried out periodically to ensure compliance to the set policy, the controls and adequacy of these controls to address all types of threats.

2.3 Vulnerability Assessment Testing Methods

- **Active Testing –** The tester introduces new test data and actively involves in the process of analysing results.
- **Passive Testing** – Here the tester will be monitoring the results without introducing the new test data or cases.
- **Network Testing** – Here the tester will measure the current state of the network.
- **Distributed Testing** – This type of testing is done for distributed applications. Basically, the applications that work with multiple clients.

2.4 BENEFITS

Web Security testing is a continuous improvement process to get benefited in terms of increasing ROI (Returns on Investment). Benefits of a pen-test are short term as well as long term. Our VAPT services help companies meet their compliance requirements faster. The variety of security flaws we find in your web application are far more than any standard tools or primitive ways of pentesting. We are one of the best web security testing companies in India, with customer all over the world. Our report gives you a detailed picture of what need to be improved in your web application inside out, from cyber security standpoint.

- Secure website from hackers
- Prevent information stealing
- Prevent monetary loss
- Prevent reputational loss
- Induce confidence in customer
- Higher long term profits
- Increased ROI

2.5 Why does your organization need one?

Penetration testing helps businesses understand if their investment in security actually affords them the protection they want. To help in your understanding, let's start with defining some terms to make sure we are using the same vocabulary.

- **Threat** – agent or actor that can cause harm
- **Vulnerability** – a flaw someone can exploit to cause harm
- **Risk** – Where threat and vulnerability overlap
- **Exploit** – code or technique that a threat uses to take advantage of a vulnerability
- **Penetration testing** – involves modelling the techniques used by real-world computer attackers to find vulnerabilities and under controlled circumstances to exploit these flaws in a professional, safe manner according to a carefully designed scope and rules of engagement to determine business risk and potential impact. All with the goal of helping the organization improve security.
- **Security/Vulnerability assessment** – focus is on finding security vulnerabilities, which may or may not be used to get in or steal data. These assessments are broader, and often include explicit policy and procedure review.

A penetration test can help answer the following questions:

- Can vulnerabilities that are found be exploited to gain access or steal data?
- Can lower-risk vulnerabilities be exploited in a way together that opens up a higher-risk vulnerability?
- What does this mean to the business or operations if successful?
- At what level can your business successfully detect and respond to attacks?

Other reasons a penetration test can provide value to your business:

- Meeting compliance with regulatory standards
- Automated network or application vulnerability scanning software can have difficulty detecting some types of vulnerabilities.
- Provide evidence to support increased investments in security personnel and technology
- Post security incident- to validate new security controls put in place will stop a similar attack in the future.

Penetration tests can be scoped to your business needs from general to narrow. On the general side of scope is a black box test. The tester is given little to no information and tries to see if they can get access or business information. On the narrow side of scope is a white box test. This could be something like testing a new application with full knowledge of what it should do. The tester in this case is given valid user accounts with different roles like a regular user and an admin user to test what each can do in the application.

3. Technical Report

3.1 Network Security

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

3.1.1 IP Addressing

We found that IP Addressing of Poornima Internal Network is not managing properly. Doing wastage of IP's for the machine

We get information after scanning the internal network that sub-netting of IP's is done but, Super netting is not done.

Severity Level: **High**

3.1.2 VLAN configuration

We found that for different departments of Poornima University, there is no implementation of VLAN for the Machine.

Which can be destructible for the internal network and there is changes of malicious activities by the students or any intruder.

Severity Level: **Medium**

3.1.3 Unmanaged Switches

We found that switches which are used in Poornima Network are Unmanaged. Due this if any IP is assign to a particular machine then in the next time the same IP will be assign to another Machine.

Which is more dangerous if any malicious activity we can find out the intruder who perform this activities.

Severity Level: **High**

3.2 Web Application Vulnerabilities

Risk **cription**	**Threat Level**	**Affected URL**	**Recommendation**
Improper Session Handling Through improper session handling user can login with their own application ID and make changes to work of admin like	**L** **CRITIC**	http://10.X.X.79/UI	□ Cookie Based Authenticatio n (old approach), which uses the server side cookies to Authenticate the user on each request.

Approved, reject application.			□ Token Based Authentication (new Approach) depends on a signed token, which is sent to the Server on each request.

Click jacking: XFrame-Options header missing Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially	**MEDIUM**	https://www.poornima.org/xxxxxxxxxxx	□ Sending the proper Content Security Policy (CSP) frame ancestor's directive response headers that instruct the browser to not allow framing from other domains. (This replaces the older X-Frame Options HTTP headers.)

revealing confidential information or taking control of their computer while clicking on seemingly Innocuous web pages.			Employing defensive code in the UI to ensure that the current frame is the most top level window

Cookie without secure flag set
This cookie does not have the secure flag set. When a cookie is set with the secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security Protection for session cookies.
	LOW	•
		•
		PHPSESSID=to846jj9voujabgm908j1403n6; path=/
		X-Mappingmhjbcgol=A1202DB1EFE43320DF571B947904F1F4; path=/
			The secure flag should be set on all cookies that are used for transmitting sensitive data when Accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are

			accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be Transmitted over unencrypted communications.
SQL Injection SQL injection exits in the username and password fields. This may also allow an attackers to run arbitrary SQL Query on the server.	**CRITICAL**	http://techvault.poornima.org/pryogaminfo.pxxxxxxxxxxx	It is advisable to filter all the input data before running the SQL Query and allow only valid characters. User least privilege principle and allow only the necessary privileges.

Cross Site Scripting It allows an			All data on all the pages should have input as well as output
Attacker to run arbitrary script in the victim’s browser	**HIGH**	http://www.poornima.edu.in http://www.poornima.org	Filtering. If possible meta-characters like <>,?^&/\`~\”-()

Table – 1 Web Vulnerability Report

4. Proof of Vulnerabilities Found

4.1 Vulnerability – 1

Improper Session Handling

 Vulnerable Locations: http://10.X.X.79/UI

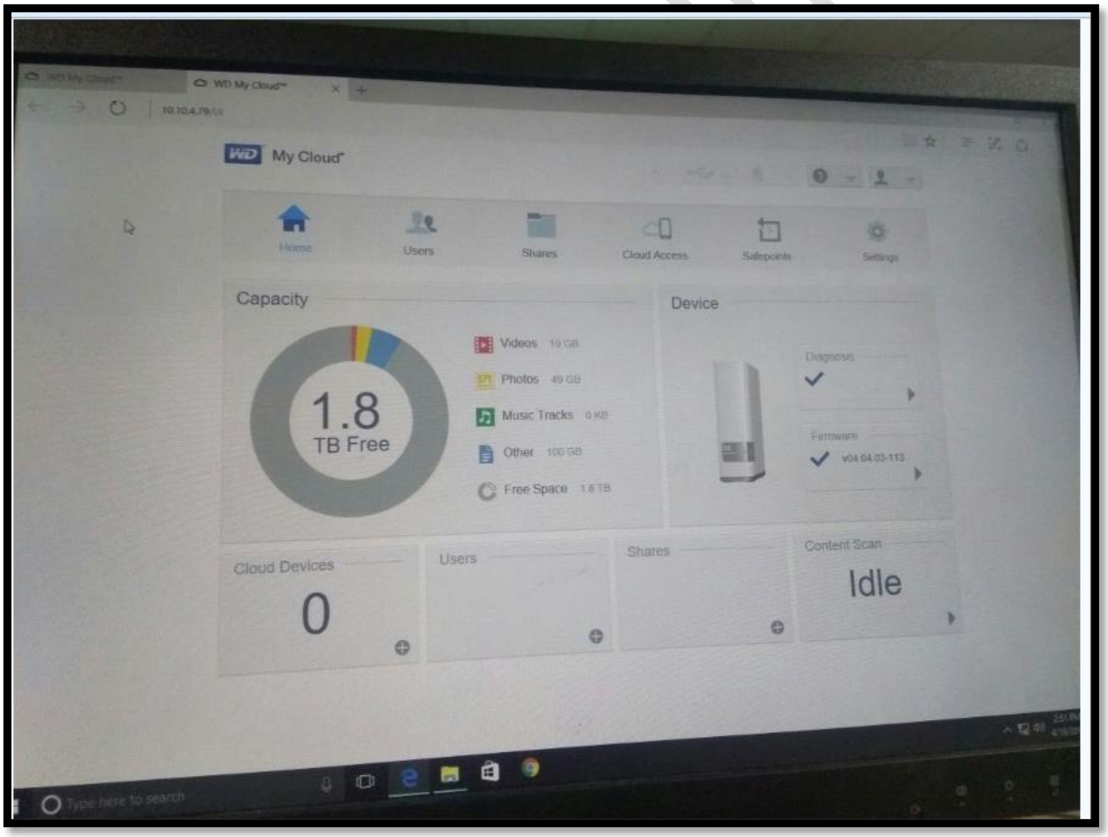


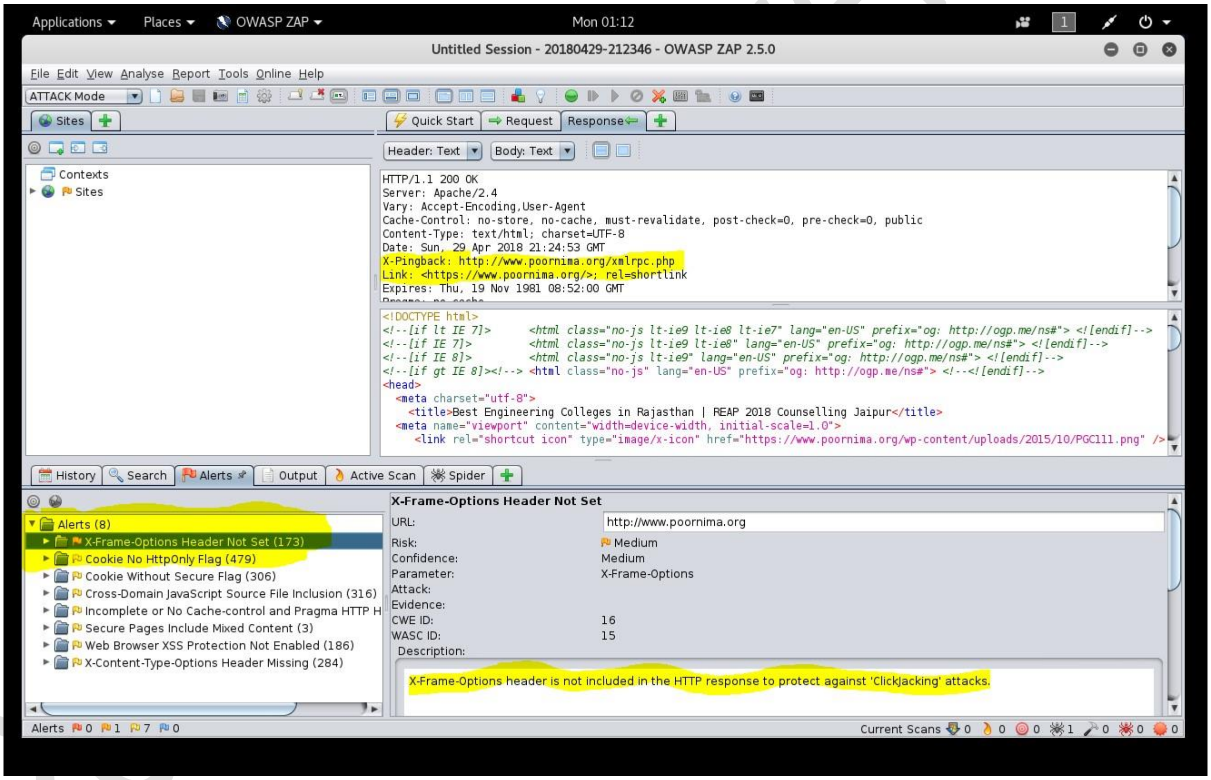
Image-2 Improper session handling

4.2 Vulnerability – 2

X-Frame-Options header missing

- **Vulnerable Locations:**

https://www.poornima.org/xXXXXXXXX



```
HTTP/1.1 200 OK
Server: Apache/2.4
Vary: Accept-Encoding,User-Agent
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, public
Content-Type: text/html; charset=UTF-8
Date: Sun, 29 Apr 2018 21:24:53 GMT
X-Pingback: http://www.poornima.org/xmlrpc.php
Link: <https://www.poornima.org/>; rel=shortlink
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
<!DOCTYPE html>
<!--[if lt IE 7]>      <html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="en-US" prefix="og: http://ogp.me/ns#"> <![endif]-->
<!--[if IE 7]>         <html class="no-js lt-ie9 lt-ie8" lang="en-US" prefix="og: http://ogp.me/ns#"> <![endif]-->
<!--[if IE 8]>         <html class="no-js lt-ie9" lang="en-US" prefix="og: http://ogp.me/ns#"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US" prefix="og: http://ogp.me/ns#"> <!--<![endif]-->
<head>
  <meta charset="utf-8">
    <title>Best Engineering Colleges in Rajasthan | REAP 2018 Counselling Jaipur</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="shortcut icon" type="image/x-icon" href="https://www.poornima.org/wp-content/uploads/2015/10/PGC111.png" />
```

```
Alerts (8)
  X-Frame-Options Header Not Set (173)
  Cookie No HttpOnly Flag (479)
  Cookie Without Secure Flag (306)
  Cross-Domain JavaScript Source File Inclusion (316)
  Incomplete or No Cache-control and Pragma HTTP H
  Secure Pages Include Mixed Content (3)
  Web Browser XSS Protection Not Enabled (186)
  X-Content-Type-Options Header Missing (284)
```

X-Frame-Options Header Not Set

URL:	http://www.poornima.org
Risk:	Medium
Confidence:	Medium
Parameter:	X-Frame-Options
Attack:	
Evidence:	
CWE ID:	16
WASC ID:	15

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Alerts 0 1 7 0 Current Scans 0 0 0 1 0 0 0

Image-3 X-frame-options Header Missing

4.3 Vulnerability – 3

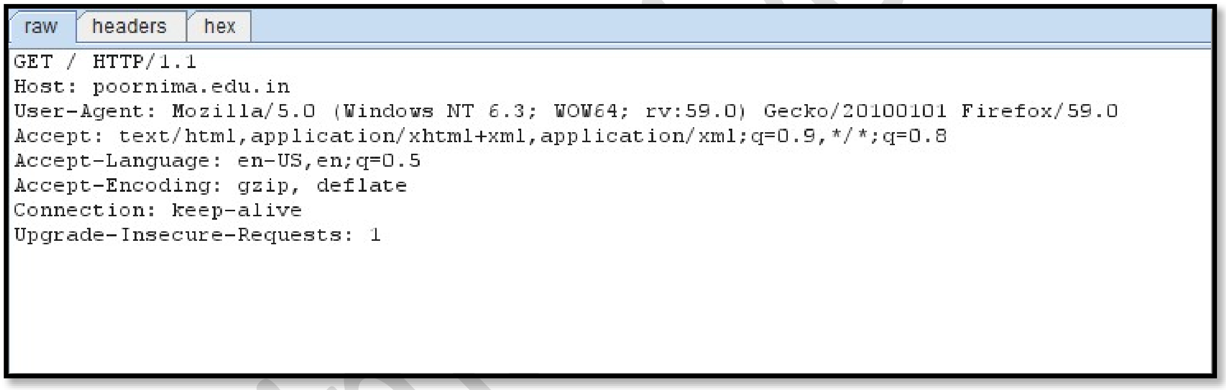
Cookie without secure flag set ➢

Issue detail:

 The following cookies were issued by the application and do not have the HttpOnly flag set:

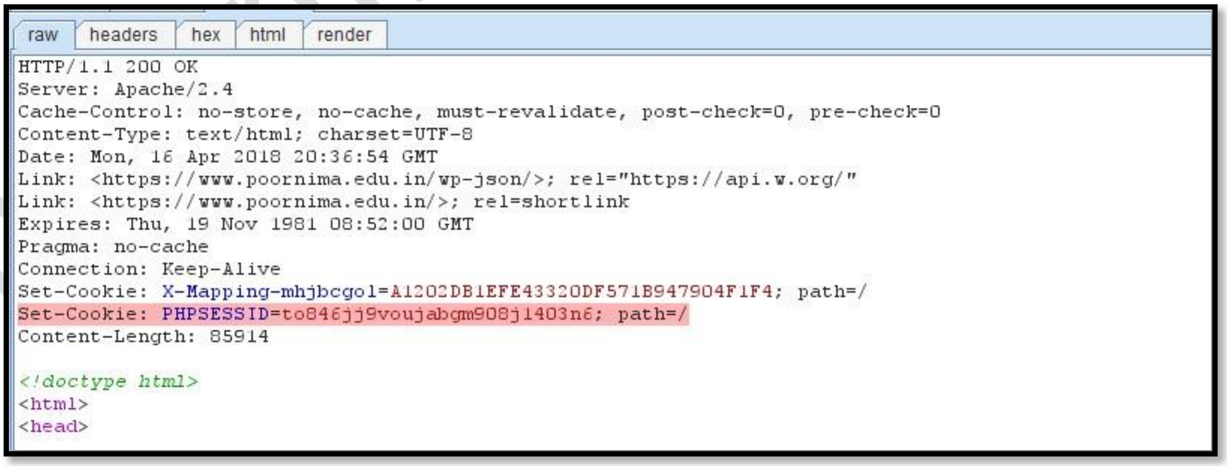
 PHPSESSID=to846jj9voujabgm908j1403n6; path=/

 X-Mapping-mhjbcgol=A1202DB1EFE43320DF571B947904F1F4; path=/



```
GET / HTTP/1.1
Host: poornima.edu.in
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Image-4 Cookie-1



```
HTTP/1.1 200 OK
Server: Apache/2.4
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Type: text/html; charset=UTF-8
Date: Mon, 16 Apr 2018 20:36:54 GMT
Link: <https://www.poornima.edu.in/wp-json/>; rel="https://api.w.org/"
Link: <https://www.poornima.edu.in/>; rel=shortlink
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Connection: Keep-Alive
Set-Cookie: X-Mapping-mhjbcgol=A1202DB1EFE43320DF571B947904F1F4; path=/
Set-Cookie: PHPSESSID=to846jj9voujabgm908j1403n6; path=/
Content-Length: 85914

<!doctype html>
<html>
<head>
```

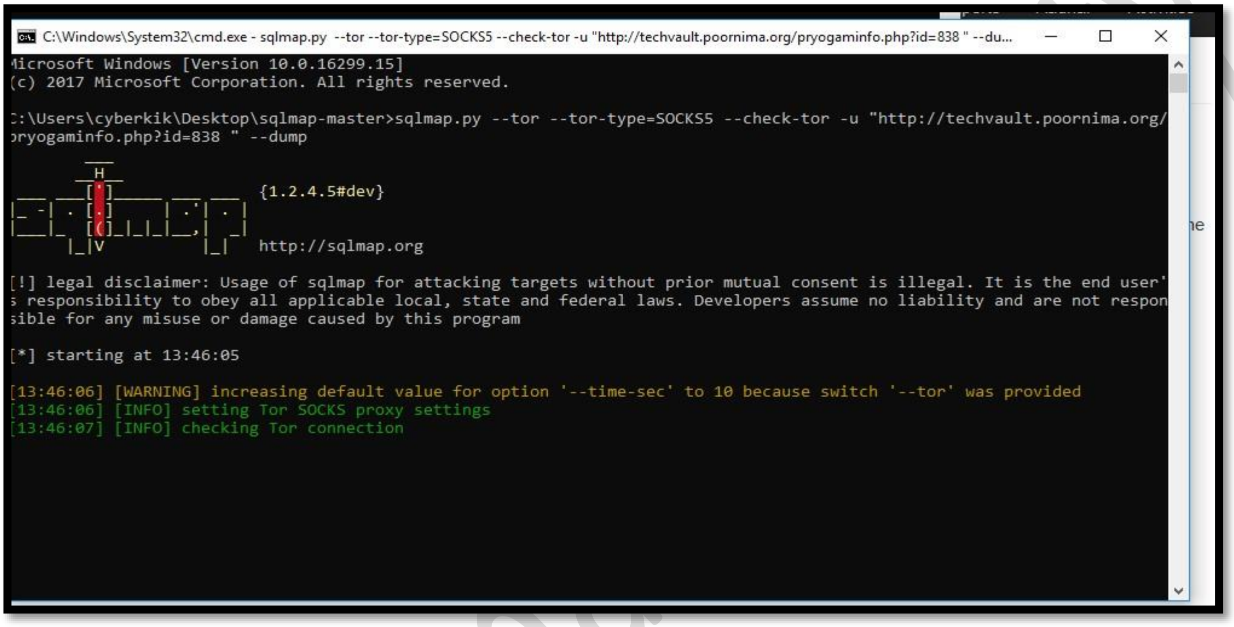
Image-5 Cookie-2

4.4 Vulnerability – 4

SQL Injection

□ Vulnerable Location

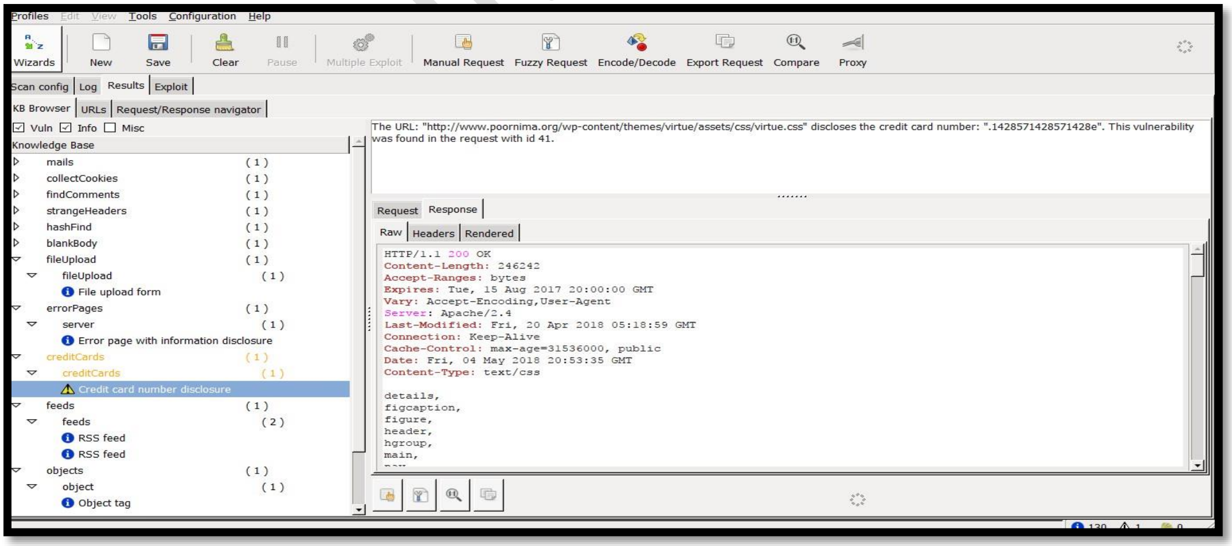
http://techvault.poornima.org/pryogaminfo.phXXXXX



C:\Windows\System32\cmd.exe - sqlmap.py --tor --tor-type=SOCKS5 --check-tor -u "http://techvault.poornima.org/pryogaminfo.php?id=838 " --du...

```
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

:\Users\cyberkik\Desktop\sqlmap-master>sqlmap.py --tor --tor-type=SOCKS5 --check-tor -u "http://techvault.poornima.org/
pryogaminfo.php?id=838 " --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.4.5#dev}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 13:46:05

[13:46:06] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[13:46:06] [INFO] setting Tor SOCKS proxy settings
[13:46:07] [INFO] checking Tor connection
```

Image-6 SQL-1



```
mails                     ( 1 )
collectCookies            ( 1 )
findComments              ( 1 )
strangeHeaders            ( 1 )
hashFind                  ( 1 )
blankBody                 ( 1 )
fileUpload                ( 1 )
    fileUpload                ( 1 )
        File upload form
errorPages                ( 1 )
    server                    ( 1 )
        Error page with information disclosure
creditCards               ( 1 )
    creditCards               ( 1 )
        Credit card number disclosure
feeds                     ( 1 )
    feeds                     ( 2 )
        RSS feed
        RSS feed
objects                   ( 1 )
    object                    ( 1 )
        Object tag
```

The URL: "http://www.poornima.org/wp-content/themes/virtue/assets/css/virtue.css" discloses the credit card number: ".1428571428571428e". This vulnerability was found in the request with id 41.

```
HTTP/1.1 200 OK
Content-Length: 246242
Accept-Ranges: bytes
Expires: Tue, 15 Aug 2017 20:00:00 GMT
Vary: Accept-Encoding,User-Agent
Server: Apache/2.4
Last-Modified: Fri, 20 Apr 2018 05:18:59 GMT
Connection: Keep-Alive
Cache-Control: max-age=31536000, public
Date: Fri, 04 May 2018 20:53:35 GMT
Content-Type: text/css

details,
figcaption,
figure,
header,
hgroup,
main,
```

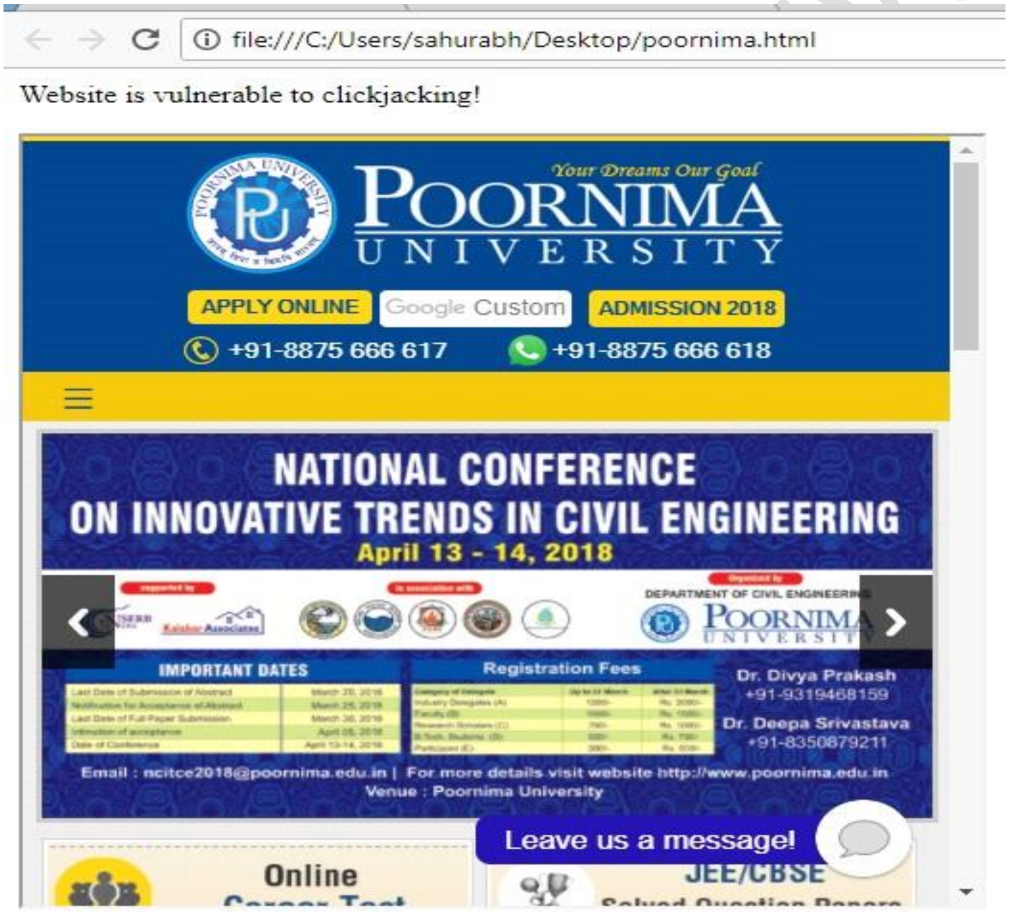
Image-7 SQL-2

4.5 Vulnerability – 5

ClickJacking

- **Vulnerable Locations**

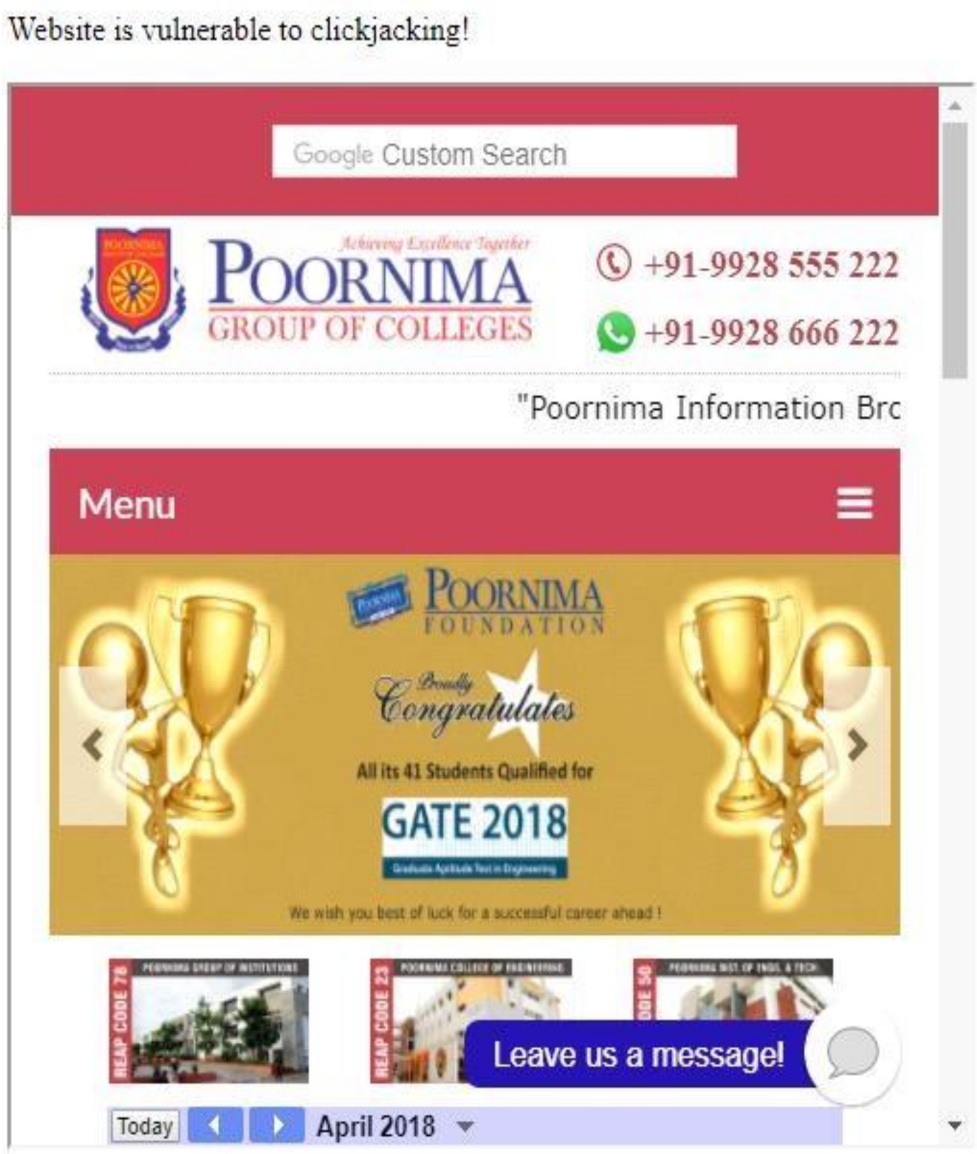
https://www.poornima.org https://www.poornima.edu.in



file:///C:/Users/sahurabh/Desktop/poornima.html

Website is vulnerable to clickjacking!

Image-8 Clickjacking- 1



Website is vulnerable to clickjacking!

Google Custom Search
Achieving Excellence Together
POORNIMA
GROUP OF COLLEGES
+91-9928 555 222
+91-9928 666 222
"Poornima Information Brc
Menu
POORNIMA
FOUNDATION
Proudly Congratulates
All its 41 Students Qualified for
GATE 2018
Graduate Aptitude Test in Engineering
We wish you best of luck for a successful career ahead !
REAP CODE 76
REAP CODE 23
POORNIMA COLLEGE OF ENGINEERING
Leave us a message!
Today
April 2018

<u>Image-9</u> Clickjacking- 2

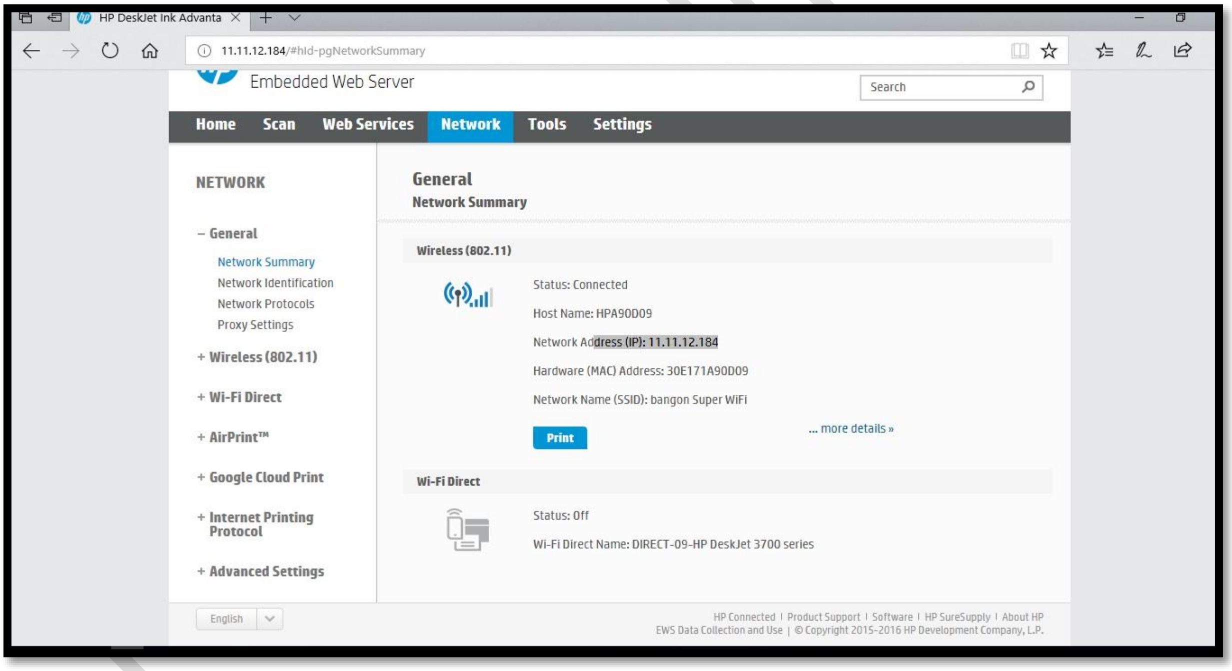
4.6 Vulnerability – 6

Network Security Loopholes

- **Issues**

- Printer is access

  Router is access
- Mac-Spoofing
  can be done



HP DeskJet Ink Advanta

11.11.12.184/#hId-pgNetworkSummary

Embedded Web Server

NETWORK

- General
  - Network Summary
  - Network Identification
  - Network Protocols
  - Proxy Settings
- + Wireless (802.11)
- + Wi-Fi Direct
- + AirPrint™
- + Google Cloud Print
- + Internet Printing Protocol
- + Advanced Settings

General

Network Summary

Wireless (802.11)

Status: Connected

Host Name: HPA90D09

Network Address (IP): 11.11.12.184

Hardware (MAC) Address: 30E171A90D09

Network Name (SSID): bangon Super WiFi

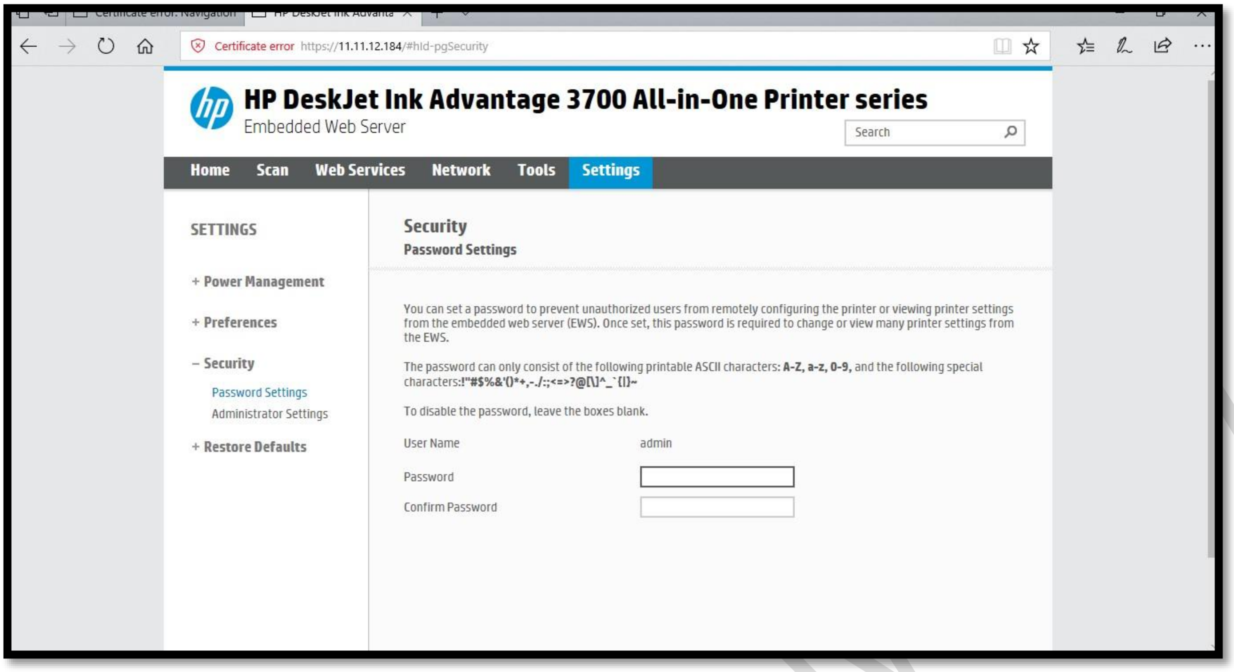
Wi-Fi Direct

Status: Off

Wi-Fi Direct Name: DIRECT-09-HP DeskJet 3700 series

HP Connected | Product Support | Software | HP SureSupply | About HP
EWS Data Collection and Use | © Copyright 2015-2016 HP Development Company, L.P.

Image-10 Network security-1



Security

Password Settings

You can set a password to prevent unauthorized users from remotely configuring the printer or viewing printer settings from the embedded web server (EWS). Once set, this password is required to change or view many printer settings from the EWS.

The password can only consist of the following printable ASCII characters: **A-Z, a-z, 0-9,** and the following special characters:**!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~**

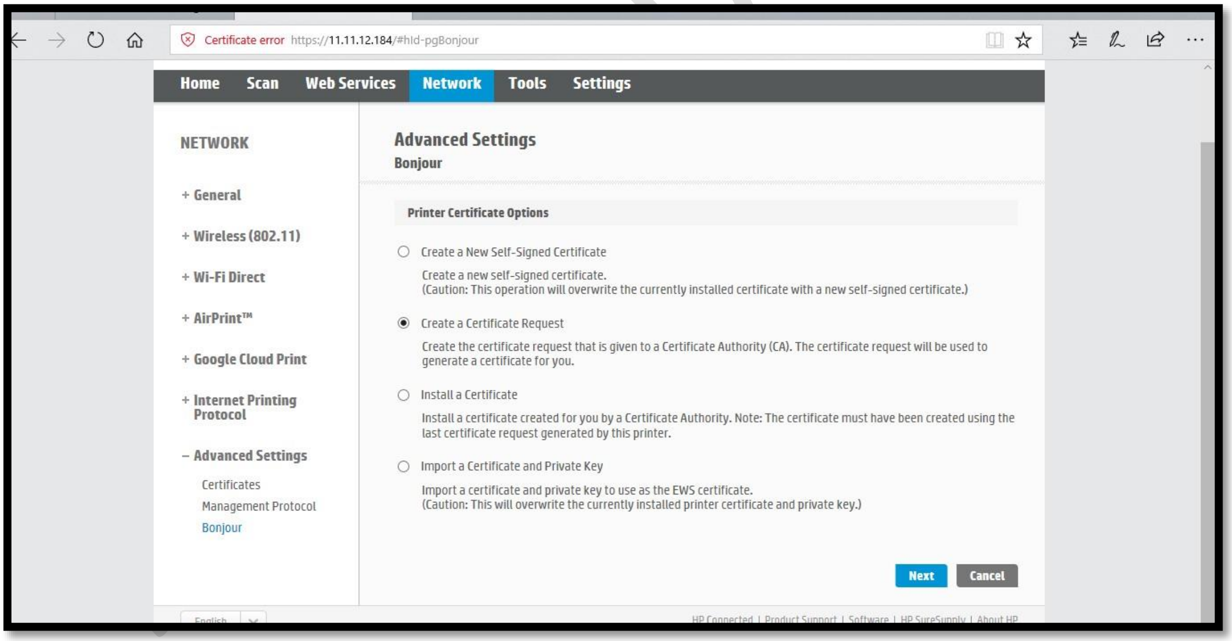
To disable the password, leave the boxes blank.

User Name admin

Password

Confirm Password

Image-11 Network Security-2



Advanced Settings

Bonjour

Printer Certificate Options

○ Create a New Self-Signed Certificate

Create a new self-signed certificate.
(Caution: This operation will overwrite the currently installed certificate with a new self-signed certificate.)

● Create a Certificate Request

Create the certificate request that is given to a Certificate Authority (CA). The certificate request will be used to generate a certificate for you.

○ Install a Certificate

Install a certificate created for you by a Certificate Authority. Note: The certificate must have been created using the last certificate request generated by this printer.

○ Import a Certificate and Private Key

Import a certificate and private key to use as the EWS certificate.
(Caution: This will overwrite the currently installed printer certificate and private key.)

Next Cancel

Image-12 Network security-3

5. Executive Summary

5.1 Summary

This report is generated by student of B.Tech Computer Science (Cloud & IS) to gauge the security posture of **POORNIMA FOUNDATION**. The result of assessment is then analysed for vulnerabilities. The vulnerabilities which could make service unavailable has not been performed practically such as Denial of Service, Ping of Death etc.

The purpose of the test is to determine security vulnerabilities in the Poornima Infrastructure and Web applications running on the servers specified as a part of the scope. The tests are carried out assuming the identity of an attacker or a user with malicious intent. At the same time due care is taken not to harm the server and Poornima infrastructure and it Business Profits.

Approach

- Perform broad scars to identify potential areas of exposure and services that may act as entry points
- Perform targeted scans and manual investigation to validate vulnerabilities Test identified components to gain access to:

  < IP addressed devices >
- Identify and validate vulnerabilities
- Rank vulnerabilities based on that level, loss potential, and likelihood of exploitation
- Perform supplement research and development activities to support analysis
- Identify issues of immediate consequences and recommend solutions
- Develop long-term recommendations to enhance security
- Transfer Knowledge

- During the network level security checks we tried to probe the ports present on the various servers and detect the services running on then with the existing security holes, if any.

- At the web application level we checked the web servers, configuration issues, and more importantly the logical errors in the web application itself.

5.2 Scope

The scope of this VAPT was limited to the below range, for what we got permissions

Target	1. www.poornima.edu.in 2. www.poornima.org 3. Poornima Internal Infrastructure. Network

Table-2 Scope of target

5.3 Key Findings

In this section we would like to highlight summary of the critical issues that we discovered during our Penetration Testing process.

5.3.1 Improper Session Handling

Through improper session handling user can login with their own application ID and make changes to work of admin like approved, reject application.

Risks

- Undermined authorization and accountability controls.
- Cause privacy violation.
- Identity theft.

Recommendations:

We can implement authentication in two ways as below

- Cookie Based Authentication (old approach), which uses the server side cookies to authenticate the user on each request.
- Token Based Authentication (new approach) depends on a signed token, which is sent to the Server on each request.

Token based approach and Cookie based approach

As we know, when we use the cookie based approach, the generated ASP_SessionId will be stored in the Browser cookies. When we use a token-based approach, the generated token will be stored in the Browser Cookies and with every request, the generated token will be passed as an attribute of the request header.

The following diagram explains how both the methods work:

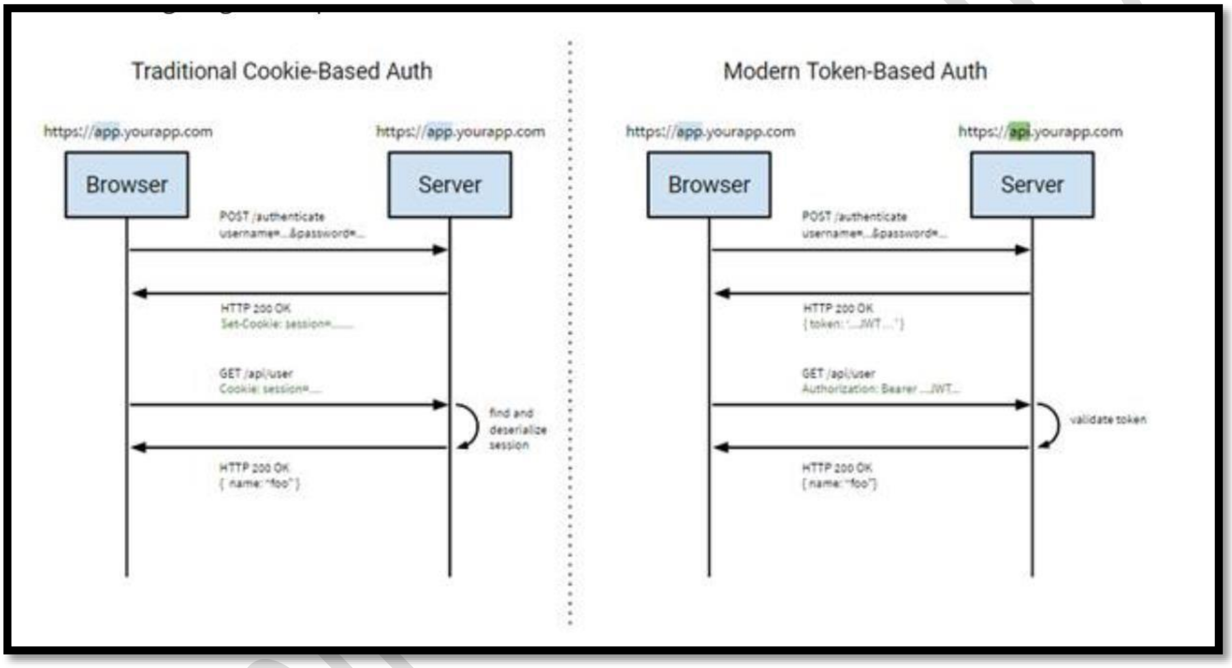


Image-13 Traditional vs. Modern Token Based authentications

Advantages of using a token-based approach

- *CORS*

  Cookies are a Token-based approach, which allows you to make the AJAX calls to any domain, any Server because you use HTTP header to transfer the user data.

- *Stateless (Server side scalability)*

There is no need to keep a session store. The token is a self-contained entity, which passes all the user information and the rest of the state lives in the cookies or local storage on the client side.

- *CDN*

  You can refer to the required client side scripts from a CDN (e.g. JavaScript, HTML, images, etc.) and your Server side is just API.

- *Mobile ready* when you start working on a native platform like Windows 8, android, iOS etc., cookies are not perfect, when consuming a secure API. Using a Token-based approach simplifies this a lot.

- *CSRF*

  As you are not depending on the cookies, you have no need to protect against cross site requests.

- *Standard-based*

  Your API methods can accept a JSON Web Token (JWT). This is standard and there are multiple frameworks like .NET, Ruby, Java, Python and PHP etc. For instance, Firebase allows its customers to use any authentication approach, as long as you produce a JSON Web Token with the certain pre-defined attributes and signed with a shared secret to call their API.

5.3.2 Click jacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Recommendations:

There are two main ways to prevent clickjacking:

1. Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. (This replaces the older X-Frame-Options HTTP headers.)
2. Employing defensive code in the UI to ensure that the current frame is the most top level window

5.3.3 Cookie without secure flag set

This cookie does not have the secure flag set. When a cookie is set with the secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

- **Issue detail:**

- The following cookies were issued by the application and do not have the HttpOnly flag set:
- **PHPSESSID=to846jj9voujabgm908j1403n6; path=/**
- X-Mapping-mhjbcgol=A1202DB1EFE43320DF571B947904F1F4; path=/

<u>Recommendations:</u>

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

5.3.4 SQL Injections

SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious *payload*) that control a web application's database server (also commonly referred to as a *Relational Database Management System – RDBMS*). Since an SQL Injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities.

By leveraging an SQL Injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL Injection can also be used to add, modify and delete records in a database, affecting data integrity.

To such an extent, SQL Injection can provide an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information.

Recommendations:

What’s the worst an attacker can do with SQL?

SQL is a programming language designed for managing data stored in an RDBMS, therefore SQL can be used to access, modify and delete data. Furthermore, in specific cases, an RDBMS could also run commands on the operating system from an SQL statement.

Keeping the above in mind, when considering the following, it’s easier to understand how lucrative a successful SQL Injection attack can be for an attacker.

- An attacker can use SQL Injection to bypass authentication or even impersonate specific users.
- One of SQL’s primary functions is to select data based on a query and output the result of that query. An SQL Injection vulnerability could allow the complete disclosure of data residing on a database server.
- Since web applications use SQL to alter data within a database, an attacker could use SQL Injection to alter data stored in a database. Altering data affects data integrity and could cause repudiation issues, for instance, issues such as voiding transactions, altering balances and other records.
- SQL is used to delete records from a database. An attacker could use an SQL Injection vulnerability to delete data from a database. Even if an appropriate backup strategy is employed, deletion of data could affect an application’s availability until the database is restored.
- Some database servers are configured (intentional or otherwise) to allow arbitrary execution of operating system commands on the database server. Given the right conditions, an attacker could use SQL Injection as the initial vector in an attack of an internal network that sits behind a firewall.

5.3.5 Network Access Attacks

Technology is forever evolving, so is hacking! It might come as a surprise to many that, as one wakes up in the morning and prepares for work, gets to the office and spends nine to twelve hour working; the same way a professional hacker spends all day modifying hacking techniques and looking for networks to exploit!

Firstly, for an attacker to gain access to a system network, the intruder has to find out the vulnerabilities or weaknesses in the network authentication, FTP and web services. Finding and exploiting these vulnerabilities will enable the attacker to gain access to web account and other confidential or sensitive information.

Types of access attacks

1. Password attack
2. Trust Exploitation
3. Port Redirection
4. Man-in-the middle attack
5. Mac Spoofing

<u>Recommendations:</u>

We assign and manage the following activities to protect from insider attacks

1. Assigning Owners and Custodians
2. Network File Shares
3. Legacy Permissions
4. Data Portability
5. Change Control
6. Logging and Monitoring
7. Making Network Security Policies

8. Assign Group Security Policies

5.4 Tabular Summary

The following table summarizes the Vulnerability Assessment:

Value	Number of Risks
Critical	1
High	2
Medium	1
Low	1

Table – 3 Vulnerability Assessment Risk Level

6. Conclusion

Experience has shown that a focused effort to address the problems outlined in this report can result in dramatic security improvements. Most of the identified problems do not require high-tech solutions, just knowledge of and commitment to good practices.

For system to remain secure, however, security posture must be evaluated and improve continuously. Establishing the organization structure that will support these ongoing improvements is essential in order to maintain control of corporate information systems.

APPENDIX

1. ClickJacking

The most popular way to defend against Clickjacking is to include some sort of "frame breaking" functionality which prevents other web pages from framing the site you wish to defend. This cheat sheet will discuss two methods of implementing frame-breaking: first is XFrame-Options headers (used if the browser supports the functionality); and second is JavaScript frame-breaking code.

Defending with Content Security Policy (CSP) frame-ancestors directive

The frame-ancestors directive can be used in a Content-Security-Policy HTTP response header to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid Clickjacking attacks by ensuring that their content is not embedded into other sites.

Frame-ancestors allows a site to authorize multiple domains using the normal Content Security Policy semantics.

Content-Security-Policy: frame-ancestors Examples Common

uses of CSP frame-ancestors:

- **Content-Security-Policy: frame-ancestors 'none';** - This prevents any domain from framing the content. This setting is recommended unless a specific need has been identified for framing.
- **Content-Security-Policy: frame-ancestors 'self';** - This only allows the current site to frame the content.
- **Content-Security-Policy: frame-ancestors 'self' '*.somesite.com' 'https: //myfriend.site.com';** - This allows the current site, as well as any page on somesite.com (using any protocol), and only the page myfriend.site.com, using HTTPS only on the default port (443).

Note that the “single quotes” are required.

Limitations

- **Browser support:** CSP frame-ancestors is not supported by all the major browsers yet.
- **X-Frame-Options takes priority:** X -Frame-Options should be ignored if CSP frame-ancestors is specified, but Chrome 40 & Firefox 35 ignore the frame-ancestors directive and follow the X-Frame-Options header instead.

2. SQL Injection

SQL Injection attacks are unfortunately very common, and this is due to two factors:

1. The significant prevalence of SQL Injection vulnerabilities, and
2. The attractiveness of the target (i.e., the database typically contains all the interesting/critical data for your application).

It’s somewhat shameful that there are so many successful SQL Injection attacks occurring, because it is EXTREMELY simple to avoid SQL Injection vulnerabilities in your code.

SQL Injection flaws are introduced when software developers create dynamic database queries that include user supplied input. To avoid SQL injection flaws is simple. Developers need to either: a) stop writing dynamic queries; and/or b) prevent user supplied input which contains malicious SQL from affecting the logic of the executed query.

This article provides a set of simple techniques for preventing SQL Injection vulnerabilities by avoiding these two problems. These techniques can be used with practically any kind of programming language with any type of database. There are other types of databases, like XML databases, which can have similar problems (e.g., XPath and XQuery injection) and these techniques can be used to protect them as well.

Primary Defences:

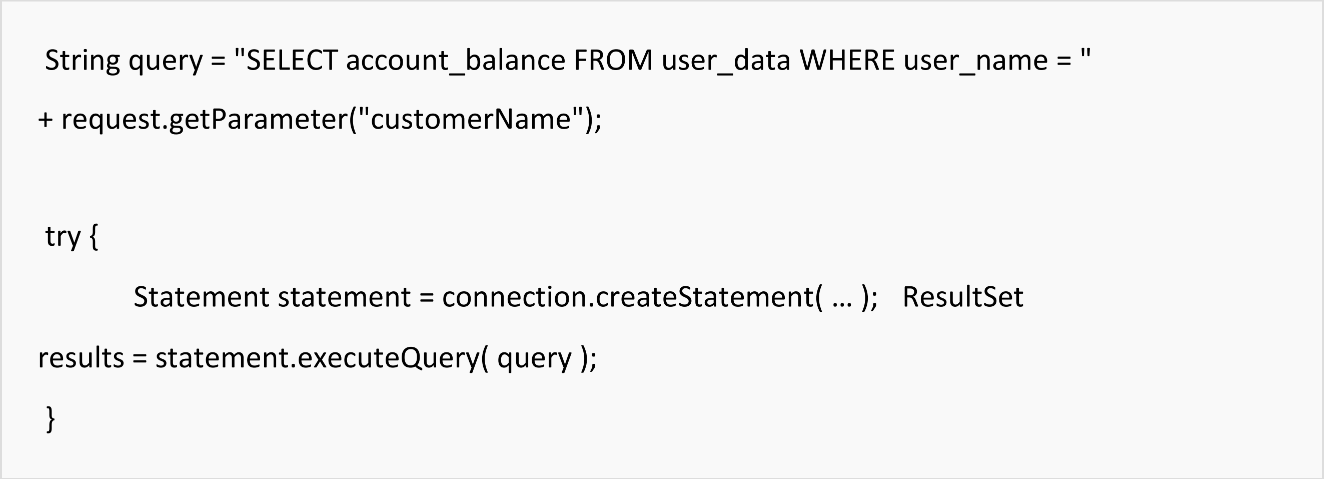
- **Option 1: Use of Prepared Statements (with Parameterized Queries)**
- **Option 2: Use of Stored Procedures**
- **Option 3: White List Input Validation** **Option 4: Escaping All User Supplied Input** Additional Defences:

- **Also: Enforcing Least Privilege**
- **Also: Performing White List Input Validation as a Secondary Defence**

Unsafe Example

SQL injection flaws typically look like this:

The following (Java) example is UNSAFE, and would allow an attacker to inject code into the query that would be executed by the database. The invalidated "customerName" parameter that is simply appended to the query allows an attacker to inject any SQL code they want. Unfortunately, this method for accessing databases is all too common.



```
 String query = "SELECT account_balance FROM user_data WHERE user_name = "
+ request.getParameter("customerName");

 try {
          Statement statement = connection.createStatement( … );   ResultSet
results = statement.executeQuery( query );
 }
```

Image-14 SQL Injection example script

References

a. https://www.sans.org/network-security/

b. https://www.ermt.net/docs/papers/Volume_3/4_April2014/V3N4-184.pdf

c. https://mapit.gov.in/securityaudit/downloads/MAPITSecurityAuditInitiationDocument.docx

d. http://www.kellerschroeder.com/news/2016/07/penetration-testingwhy-does-your-organization-need-one/

e. https://www.wilsoncgrp.com/the-real-benefits-of-conductingvulnerability-assessment-and-penetration-testing-vapt/

f. https://www.veracode.com/security/vulnerability-assessment-andpenetration-testing

g. http://www.indiumsoft.com/Blog/what-is-vapt-and-why-would-yourorganization-need-it/

h. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

i. https://www.owasp.org/index.php/Top_10-2017_Top_10

j. https://www.acunetix.com/websitesecurity/cross-site-scripting/

k. https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

l. https://security.stackexchange.com/questions/84377/is-clickjackinga-real-security-vulnerability

m. https://www.rapid7.com/db/vulnerabilities/http-generic-click-jacking

n. https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frameoptions-header-missing

o. https://www.owasp.org/index.php/Testing_for_Clickjacking_(OTGCLIENT-009)

p. https://thehackernews.com/2018/04/auth0-authenticationbypass.html

q. https://www.owasp.org/index.php/Testing_for_Bypassing_Authentication_Schema_(OTG-AUTHN-004)