Ethical Hacking

INTERNSHIP PROJECT REPORT
(Start Date: 15th October ,2021
End Date: 15th December ,2021)

Submitted in partial fulfillment of the requirements for the award of the degree

Of

-BACHELOR OF TECHNOLOGY-

In

--CSE (Artificial Intelligence)--

By

-Tanya Chhikara-
-01101172020-

INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN

Certificate

INTERNSHALA TRAININGS

Certificate of Training

Tanya Chhikara

from Indira Gandhi Delhi Technical University has successfully completed an 8-week online training on **Ethical Hacking**. In the training, Tanya learned Basics of Information Security, Computer Networking and Web Development, Information Gathering and VAPT of some important vulnerabilities in the OWASP top 10, Automating VAPT, and Documenting and Reporting Vulnerabilities.
In the final assessment, Tanya scored 80% marks.
We wish Tanya all the best for future endeavours.

Sarvesh Agarwal
FOUNDER & CEO, INTERNSHALA

Date of certification: 2021-11-09 Certificate no. : 02732BE4-3D3C-F7BF-7367-1A9AC2BDBEEC
For certificate authentication, please visit https://trainings.internshala.com/verify_certificate

Undertaking Regarding Anti-Plagiarism

I, ***Tanya Chhikara*** hereby, declare that the material/ content presented in the report are free from plagiarism and is properly cited and written in my own words. In case, plagiarism is detected at any stage, I shall be solely responsible for it.

Tanya Chhikara

(Roll Number: 01101172020)

Acknowledgement

I would like to extend my gratitude towards “Internshala” company for giving me a golden opportunity to be a part of training and internship program in Ethical Hacking.

I would also like to thank my mentor, “Mr. Aman Sachdev”, for motivating me and providing such great knowledge and mentoring throughout the project.

Tanya Chhikara
(Roll Number: 01101172020)

Declaration

I, ***Tanya Chhikara***, solemnly declare that the project report, **Internship in Ethical Hacking and Exploiting Vulnerabilities in an e-commerce website,** is based on my own work carried out during the course of our study under the supervision of **Mr. Aman Sachdev, Subject Matter Expert, Internshala**. I assert the statements made and conclusions drawn are an outcome of my research work. I further certify that:

I. The work contained in the report is original and has been done by me under the supervision of my supervisor.
II. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad.
III. We have followed the guidelines provided by the university in writing the report.
IV. Whenever we have used materials (text, data, theoretical analysis/equations, codes/program, figures, tables, pictures, text etc.) from other sources, we have given due credit to them in the report and have also given their details in the references.

Tanya Chhikara

(Roll Number: 01101172020)

List of Abbreviations

Abbreviations	*Description*
XSS	Cross Site Scripting
VPN	Virtual Private Network
IP	Internet Protocol
TCP	Transmission Control Protocol
SQLi	SQL Injection
VAPT	Vulnerability Assessment and Penetration Testing
CSRF	Cross Site Request Forgery
IDOR	Insecure Direct Object References

INDEX

Abstract/Summary

The internet has considerably enhanced various business critical operations of company's indifferent industry sectors across the globe. However, as more and more organizations become partially or completely dependent on the internet, computer security and the serious threat of computer criminals comes to the foreground. The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few.

As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help.

Unfortunately, most organizations across the globe continue to remain oblivious of the threat posed by computer criminals, corporate espionage and cyber terrorism. Ethical Hacking attempts to pro-actively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties.

The Company

Internshala group are a technology business on a mission to provide students with relevant skills and real-world experience in order to assist them achieve the greatest start in their professions. Imagine a world full with options and freedom. A world where you can find your true calling and make it a career. A future in which you graduate totally confident, assured, and ready to lay a claim on your place in the world. They offer a wide range of courses, workshops, and training sessions for students and professionals at a low cost. They assist students in obtaining internships and employment.

Introduction

The internship was completely online and the people of the organization and the mentor were really helpful and ensured smooth completion of the internship. The mentor guided as well as gave challenges to produce the perfect project during this journey.

Internshala group are a technology business on a mission to provide students with relevant skills and real-world experience in order to assist them achieve the greatest start in their professions. Imagine a world full with options and freedom. A world where you can find your true calling and make it a career. A future in which you graduate totally confident, assured, and ready to lay a claim on your place in the world. They offer a wide range of courses, workshops, and training sessions for students and professionals at a low cost. They assist students in obtaining internships and employment. **Internshala** is known for providing students with cutting-edge talents to master and for assisting them in developing and perfecting such skills.

Internshala Student Partner (ISP) is India's largest campus ambassador programme, in which college students have the opportunity to represent Internshala on a national level. This programme allows students to study, earn, and grow all while honing their marketing and communication abilities.

ISPs compete in a variety of fascinating challenges while gaining professional experience by addressing real-world problems and coming up with novel ways to promote Internshala on their campus.

Work Overview

Module 1 started with a brief introduction to what is Hacking and types of hackers.

Then the course went on to introduce basic concepts of Computer Networking which included concepts of Internal and External IP addresses and NAT.

Various other concepts including Domain Names, the parts of a domain name and Domain Name System (DNS), Ports and commonly used port numbers, Protocols and their types, the TCP-IP and OSI Models. Also, concept of Proxy Server, configuring proxies, VPN's and their installation was introduced.

Module 2 started with introduction of a WhoIS Lookup and Reverse IP Lookup, Google Dorking and went on to teach brief concepts of Web Development.

Module 3 started with an introduction to OWASP – Top 10 vulnerabilities and what is VAPT.

The upcoming lectures taught how to perform Authentication bypass using SQL Injection, GET and POST based SQL Injection, and automating SQL Injections using SQL Map.

Module 4 started with advanced web application attacks. It introduced Burp Suite to bypass client-side filters and also taught IDOR vulnerability, Rate-Limiting Issues and File upload vulnerabilities.

Module 5 began with the fundamentals of Cross Side Scripting (XSS), forced browsing and Cross Site Request Forgery. It went on to explain the two types of Brute Force attacks – Dictionary-based and Logical Brute Forcing.

Module 6 began with an introduction to common security misconfigurations like Descriptive error messages and default debug files, default or weak passwords, and components with known vulnerabilities.

Module 7 was all about Advanced Information Gathering and automating VAPT.

Module 8 taught effective ways to Document and Report Vulnerabilities

Scope

Over the last few decades, information technology has advanced at a breakneck pace. The students aspire to have a successful career in the field of information technology. Students and working professionals now have the option of pursuing a career in cybersecurity.

It is currently the most in-demand field, with numerous opportunities for students, job seekers, and working professionals. Many hopefuls consider it to be a fantastic career choice. Many companies use the best security solution to protect their personnel, data, and information connected to their company processes. For individuals who desire to become a well-known ethical hacker, Ethical Hacking Training in Delhi is really beneficial. The company must hire the best candidate and train them to apply the best data-protection approach.

Ethical hacking is typically used in conjunction with penetration testing to identify vulnerabilities, risks, and flaws in a security system, as well as to take countermeasures against those attacks.

Ethical hacking is an important part of risk assessment, auditing, and fraud detection. Ethical hackers have a lot of potential, and it's one of the fastest-growing jobs right now, since many malevolent attackers pose a threat to businesses and their networks. Ethical hackers are employed by industries such as information technology and banking to protect their data and infrastructure. In addition, due to an enhanced threat of vulnerabilities, demand for this profile will be strong in the coming days compared to other profiles.

"Ethical hacking describes the process of attacking and penetrating computer systems and networks to Discover and point out potential security weaknesses for a client which is responsible for the attacked Information technology environment."

Literature Review

1.1 Ethical Hacking Terminology

Being able to understand and define terminology is an important part of a CEH's responsibility. This terminology is how security professionals acting as ethical hackers communicate. In this section, we'll discuss a number of terms used in ethical hacking as:

Threat : An environment or situation that could lead to a potential breach of security. Ethical Hackers look for and prioritize threats when performing a security analysis. Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's Information security.

Exploit : A piece of software or technology that takes advantage of a bug, glitch, or vulnerability ,Leading to unauthorized access, privilege escalation, or denial of service on a computer system. Hackers are looking for exploits in computer systems to open the door to an initial Attack. Most exploits are small strings of computer code that, when executed on a system, expose Vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any Programming skills to be an ethical hacker as many hacking software programs have ready-made Exploits that can be launched against a computer system or network. An exploit is a defined way to breach the security of an IT system through vulnerability.

Vulnerability : The existence of a software flaw, logic design, or implementation error that can Lead to an unexpected and undesirable event executing bad or damaging instructions to the System. Exploit code is written to target vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation : A system, program, or network that is the subject of a security Analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that Contain sensitive information such as account numbers, passwords, Social Security numbers or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high value TOEs to determine the vulnerabilities and patch them to protect against exploits and Exposure of sensitive data.

Attack : An attack occurs when a system is compromised based on vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an Exploit because of the operating system, network configuration, or applications installed on the Systems, and to prevent an attack. There are two primary methods of delivering exploits to computer systems:

Remote : The exploit is sent over a network and exploits security vulnerabilities without any prior Access to the vulnerable system. Hacking attacks against corporate computer systems or networks Initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term hacker, but in reality most attacks are in the next category.
Local : The exploit is delivered directly to the computer system or network, which requires prior Access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function. These concepts are commonly referred as "need to know" and "least privilege" and, when used properly, would prevent local exploits. Most hacking attempts occur from within an organization and are perpetuated by employees, contractors, or others in a trusted position. In order for an insider to launch an attack; they must have higher privileges than necessary based on the concept of "need To know." This can be accomplished by privilege escalation or weak security safeguards.

1.2 Hacker

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a Computer or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.

1.2.1 Types Of Hackers

Hackers can be divided into three groups :

White Hats :

White hats are the good guys, the ethical hackers who use their hacking skills for defensive Purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker tool set and who use this knowledge to locate weaknesses and implement Countermeasures. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any Hacking activity. This is what makes a security professional a white hat versus a malicious Hacker who cannot be trusted.

Black Hat Hacker :

Black Hats Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, Deny legitimate users service, and just cause problems for their targets. Black-hat hackers and Crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people

consider a hacker to be.

Grey Hat Hacker :
Grey hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Grey-hat hackers may just be interested in Hacking tools and technologies and are not malicious black hats. Grey hats are self-proclaimed Ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly.

1.2.2 Ethical Hackers Versus Cracker

Ethical hackers are usually security professionals or network penetration testers who use their Hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are Security professionals test their network and systems security for vulnerabilities using the same Tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.
The term cracker describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-of-service (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

1.3 The Job Role Of An Ethical Hacker

Ethical hackers are employed to protect networks and computers from attacks from unethical hackers who illegally penetrate computers to access private and sensitive information. Though they possess technical skills to those of an unethical hacker, an ethical hacker utilizes these skills for protection.

1.4. What Do Ethical Hackers Do?

The purpose of ethical hacker is usually the same as that of crackers: they're trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information. This process of testing the security of a system or network is known as a *penetration test*, or *pen test*.
Many ethical hackers detect malicious hacker activity as part of the security team of an organization tasked with defending against malicious hacking activity. When hired, an ethical hacker asks the organization what is to be protected, from whom, and what resources the company is willing to expend in order to gain protection. A penetration test plan can then be built around the data that needs to be protected and potential risks.

1.4.1 An Ethical Hacker's Skill Set

Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking, and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement. Patience, persistence, and immense perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off. Networking, web programming, and database skills are all useful in performing Ethical hacking and vulnerability testing. Most ethical hackers are well rounded with wide Knowledge on computers and networking. In some cases, an ethical hacker will act as part of a "Tiger team" who has been hired to test network and computer systems and find vulnerabilities. In This case, each member of the team will have distinct specialties, and the ethical hacker may need More specialized skills in one area of computer systems and networking. Most ethical hackers are Knowledgeable about security areas and related issues but don't necessarily have a strong Command of the countermeasures that can prevent attacks.

Weekly Overview Of Internship Activities

	Date	Day	Name of Topic/Module Completed
1st Week	**15/10/21**	**Friday**	Introduction to Information Security
	16/10/21	**Saturday**	Hacking Methodologies and Security Auditing
	17/10/21	**Sunday**	Computer Networking
	18/10/21	**Monday**	IP addressing and NAT
	19/10/21	**Tuesday**	The Google Maps of the Internet
	20/10/21	**Wednesday**	Ports and Services
	21/10/21	**Thursday**	Protocols, TCP/IP and OSI Model
	22/10/21	**Friday**	Proxy and VPN

	Date	Day	Name of Topic/Module Completed
2nd Week	**24/10/21**	**Sunday**	Digital Footprints and Information Gathering
	25/10/21	**Monday**	Advanced Information Gathering about People and Websites
	27/10/21	**Wednesday**	Google Dorking- Hacking using Google
	28/10/21	**Thursday**	Introduction to Web Architecture and Understanding Common Security Misconceptions
	29/10/21	**Friday**	HTML Basics
	30/10/21	**Saturday**	HTML and Introduction to Javascript
	31/10/21	**Sunday**	Introduction to PHP and Setting up XAMPP
	01/11/21	**Monday**	Working with PHP
	02/11/21	**Tuesday**	Handling User Input and Building basic Application using PHP

	Date	Day	Name of Topic/Module Completed
3rd Week	03/11/21	Wednesday	Introduction to VAPT and OWASP
	04/11/21	Thursday	Basics of databases and SQL
	05/11/21	Friday	Authentication Bypass using SQL Injection
	06/11/21	Saturday	GET- Based SQL Injection Part 1
	07/11/21	Sunday	GET- Based SQL Injection Part 2
	08/11/21	Monday	POST- Based SQL Injection Part 1
	09/11/21	Tuesday	POST- Based SQL Injection Part 2
	10/11/21	Wednesday	Advanced SQL Injections
	11/11/21	Thursday	Automating SQL Injections – SQL Map

	Date	Day	Name of Topic/Module Completed
4th Week	**14/11/21**	**Sunday**	Bypassing Client - Side Filters using Burp Suite
	15/11/21	**Monday**	IDOR and Rate Limiting Issues
	16/11/21	**Tuesday**	Arbitrary File Upload Vulnerabilities

	Date	Day	Name of Topic/Module Completed
5th Week	**17/11/21**	**Wednesday**	Understanding important Response Headers, DOM, and Event Listeners
	18/11/21	**Thursday**	Fundamentals of Cross Site Scripting (XSS)
	19/11/21	**Friday**	Understanding Forced Browsing and Session – Cookie Flaws
	20/11/21	**Saturday**	Cross – Site Request forgery (CSRF) and Open Redirections
	21/11/21	**Sunday**	Dictionary Based brute force Attacks
	22/11/21	**Monday**	Logical brute force Attacks
	23/11/21	**Tuesday**	Personally Identifiable Information (PII) Leakage and Sensitive Information Disclosure

	Date	Day	Name of Topic/Module Completed
6th Week	**01/12/21**	**Wednesday**	Common Security Misconfigurations
	02/12/21	**Thursday**	Default Weak Password Vulnerability
	03/12/21	**Friday**	Fingerprinting components with known Vulnerabilities
	04/12/21	**Saturday**	Scanning for Bugs in Wordpress and Drupal
	05/12/21	**Sunday**	Using Public Exploits
	06/12/21	**Monday**	Handling User Input and Building basic Application using PHP

	Date	Day	Name of Topic/Module Completed
7th Week	**07/12/21**	**Tuesday**	Information Gathering for Endpoints
	08/12/21	**Wednesday**	Application Assessment using N-Maps
	09/12/21	**Thursday**	Automating VAPT with Nikto and Burp Suite Pro

	Date	Day	Name of Topic/Module Completed
8th Week	**10/12/21**	**Friday**	Documenting stages of vulnerabilities using Tools
	11/12/21	**Saturday**	VAPT Reports Developer Report Vs. Higher Management Report
	12/12/21	**Sunday**	Concepts of Code Security and Patching
	13/12/21	**Monday**	Parts of a VAPT Report
	14/12/21	**Tuesday**	Common Good Practices and Bad Practices

Internship Discussion

Course Description

Introduces the ethical hacking methodologies. Covers applying cyber security concepts to discover and report vulnerabilities in a network. Explores legal and ethical issues associated with ethical hacking.

Intended Outcomes for the Course

Upon completion of the course students should be able to:

- Plan a vulnerability assessment and penetration test for a network.
- Execute a penetration test using standard hacking tools in an ethical manner.
- Report on the strengths and vulnerabilities of the tested network.
- Identify legal and ethical issues related to vulnerability and penetration testing.

A. **Knowledge:** Students will learn the underlying principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. They will become familiar with the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation and result reporting.

B. **Skills:** For every offensive penetration technique the students will learn the corresponding remedial technique. By this, the students will develop a practical understanding of the current cybersecurity issues and the ways how the errors made by users, administrators, or programmers can lead to exploitable insecurities.

Technical Skills :

Knowledge of ethical hacking and penetration testing techniques including the following:

• Penetration Testing / Ethical Hacking tools and forms of attack and associated tools (Internet Security Scanner, System Security Scanner, SATAN) using war dialing and internet scanning.

• Hacker exploit scripts/programs to test whether vendor/developer patches operate as intended and fix the identified vulnerability or identify the malicious code.

- Intrusion Detection Environments and forms of attack with the ability to perform analysis of the systems and application logs for Intrusion signs.
- Firewalls (Gauntlet, Cisco PIX, CheckPoint, Raptor).
- Network Traffic Monitoring Tools (Network General Sniffer, LANalyzer, NetXray).
- Network Protocols (TCP/IP, NetBIOS / Netbeui, IPX, OSI) and associated technologies (DNS, FTP, HTTP).
- Network Topologies (Token Passing, Ethernet).
- Operating Systems: UNIX, Argus, Solaris and Microsoft Operating Environments.
- Advanced knowledge of security and encryption mechanisms and strong experience with systems implementation.
- Application Servers (Websphere, Weblogic).
- Web Servers (Netscape, Apache, Microsoft).
- Mail Servers (POP3).
- Security Authorization/Transaction, Network Security (VPN, SSL, Smart Cards, Biometrics).
- Cryptographic tools, methods, systems and protocols: HTTPS, IPsec, PGP, DES etc.
- Exceptional interpersonal communication and presentation skills are must.

Project Results and Observations :

(The following are the screenshots of the Detailed Developer Report that I prepared after VAPT on the website)

E-Commerce Website

Detailed Developer Report

Security Status – Extremely Vulnerable

- Hacker can steal all records in Internshala databases (SQLi)
- Hacker can take control of complete server including View, Add, Edit, Delete files and folders (Shell Upload)
- Hacker can change source code of application to host malware, phishing pages or even explicit content (Shell Upload)
- Hacker can inject client side code into applications and trick users by changing how page looks to steal information or spoil the name of Internshala (XSS)
- Hacker can extract mobile number of all customers using Userid (IDOR)

Vulnerability Statistics

Critical	Severe	Moderate
17	15	2

Low
2

Vulnerabilities:

No	Severity	Vulnerability	Count
1	Critical	SQL Injection	8
2	Critical	Access to sales dashboard	1
3	Critical	Access to admin panel	1
4	Critical	Account takeover via OTP Bypass	2
5	Critical	Unauthorized Access To Customer Details	5
6	Severe	Reflected cross site scripting	15
7	Moderate	Directory Listing of Configuration FIles	2
8	Low	Information disclosure due to Apache Default Pages	2

1. SQL Injection

SQL Injection (Critical)	Here are other similar SQLi in the application **Affected URL :** • http://url.com/sql3.php (ID GET parameter) • http://url.com/sql4.php (jkl POST parameter) • http://url.com/sql5.php (pqr 5 GET parameter) • http://url.com/sql6.php (abcd cookie paramter) • http://url.com/sql7.php (User-agent Header) • http://url.com/sql8.php (xyz POST parameter)

6

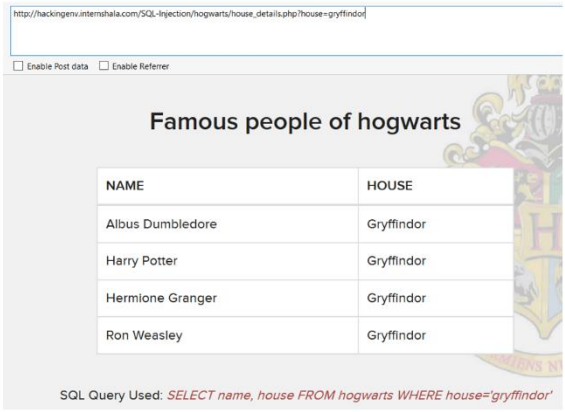
1. SQL Injection

SQL Injection (Critical)	Below mentioned URL in the **Hogwarts House Details module** is vulnerable to SQL injection attack **Affected URL :** • http://url.com/hogwarts/house_details.php?house=HERE **Affected Parameters :** • house (GET parameter) **Payload:** • house=gryffindor'

5

Observation

- Navigate to Houses page where you will see list of houses. Click anyone like Gryffindor. You will see famous people of that house in a table. Notice the GET parameter **house** in the URL:



Observation

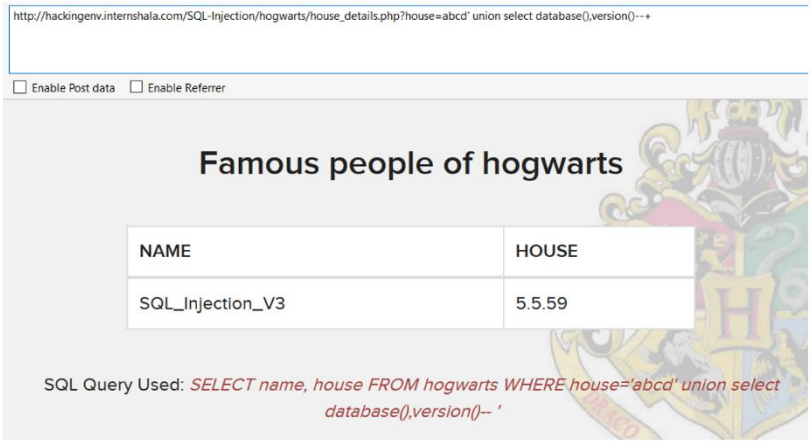
- We apply single quote in house parameter: **house_details.php?house=Gryffindor' and we get complete MySQL error:**

Observation

- We then put --+ : **house_details.php?house=Gryffindor'--+ and we error is removed confirming SQL injection:**

Proof of Concept (PoC)

- Attacker can execute SQL commands as shown below. Here we have used the payload below to extract the database name and MySQL version information:
  house=abcd' union select database(),version()--+



PoC – Attacker can dump arbitrary data

- No of databases: 3
  - Information_schema
  - SQL_Injection_V3
  - Test

- No of tables in SQL_Injection_V3: 2
  - Hogwarts
  - Users

Business Impact – Extremely High

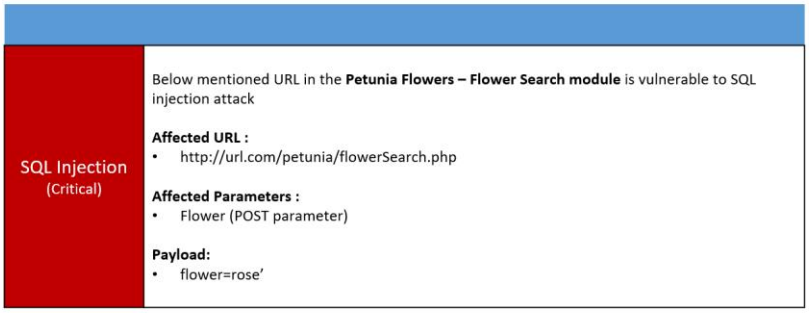
Using this vulnerability, attacker can execute arbitrary SQL commands on Lifestyle store server and gain complete access to internal databases along with all customer data inside it.

Below is the screenshot of users table which shows user credentials being leaked that too in plain text without any hashing/encryption.

Attacker can use this information to login to admin panels and gain complete admin level access to the website which could lead to complete compromise of the server and all other servers connected to it.

ID	USERNAME	PASSWORD
1	princess	123456
2	coolguy	p@$$word
3	bond_007	jamesbond
4	demo	test@123
5	admin	default

1. SQL Injection



13

PoC – Attacker can dump arbitrary data

- No of databases: 3
  - Information_schema
  - SQL_Injection_V3
  - Test
- No of tables in SQL_Injection_V3: 2
  - Hogwarts
  - Users
- Critical Table: Users

ID	USERNAME	PASSWORD
1	princess	123456
2	coolguy	p@$$word
3	bond_007	jamesbond
4	demo	test@123
5	admin	default

Recommendation

Take the following precautions to avoid exploitation of SQL injections:

- Whitelist User Input: Whitelist all user input for expected data only. For example if you are expecting a flower name, limit it to alphabets only upto 20 characters in length. If you are expecting some ID, restrict it to numbers only
- Prepared Statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query
- Character encoding: If you are taking input that requires you to accept special characters, encode it. Example. Convert all **‘ to \’** , **“ to \”**, **\ to \\.** It is also suggested to follow a standard encoding for all special characters such has HTML encoding, URL encoding etc
- Do not store passwords in plain text. Convert them to hashes using SHA1 SHA256 Blowfish etc
- Do not run Database Service as admin/root user
- Disable/remove default accounts, passwords and databases
- Assign each Database user only the required permissions and not all permissions

References

- *https://www.owasp.org/index.php/SQL_Injection*
- *https://en.wikipedia.org/wiki/SQL_injection*

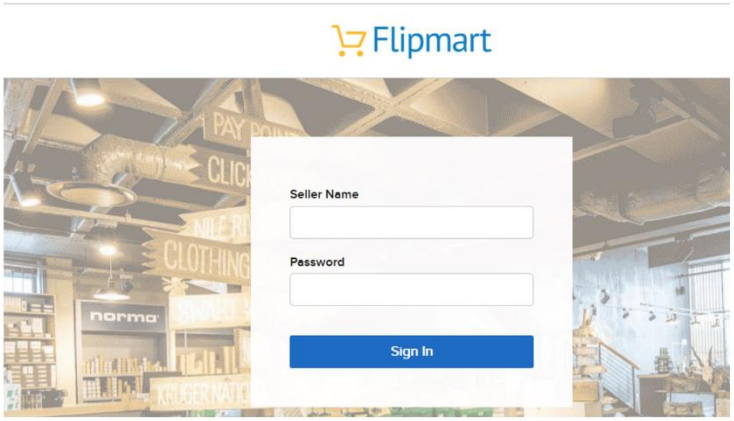
2. Access to Sales Dashboard

Access to Sales Dashboard (Critical)	The Sales dashboard at the below mentioned URL has default/weak password allowing complete admin access **Affected URL :** • http://url.com/salesdashboard.php **Affected Parameters :** • Username, password (POST parameters) **Payload:** • Username=admin password=sales@123

17

Observation

- Navigate to http://url.com/salesdashboard.php You will see sales admin login page



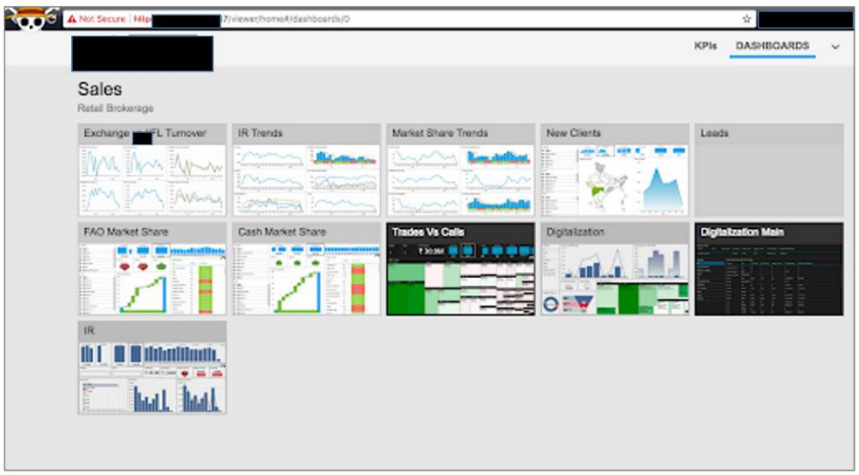
Business Impact – Extremely High

A malicious user can access the Sales Dashboard which discloses many critical information of organization including:

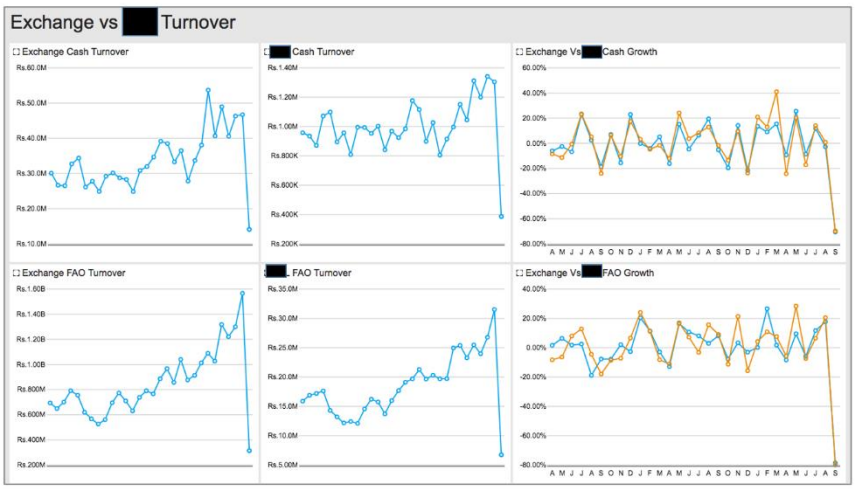
- Sales Trends
- Client information
- Leads information
- Sales Calendar information
- Income and revenue information
- And much more…

Observation

- Enter username: admin & password: sales@123. You will get logged in to the admin panel



POC


Exchange vs [redacted] Turnover
Exchange Cash Turnover
[redacted] Cash Turnover
Exchange Vs [redacted] Cash Growth
Exchange FAO Turnover
[redacted] FAO Turnover
Exchange Vs [redacted] FAO Growth

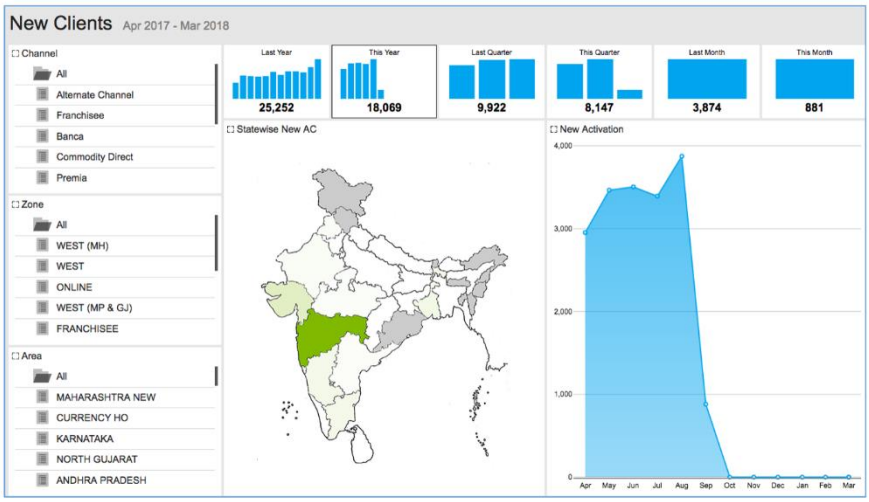
21

POC


Cash Market Share Sep 2017
Channel
All
Premia
Franchisee
HOST
Banca
Commodity Direct
CAL
Alternate Channel
CAT
Zone
All
WEST (MP & GJ)
PREMIA
RM/EA
FRANCHISEE
ONLINE
WEST (MH)
NORTH
EAST
Last 30 Days
271.62
Last Month
279.28
This Month
274.32
MTD %
1.8%
QTD %
4.1%
YTD %
1.5%
Zonal Contribution
Trend by Area
Area
Cash MS
Cash Growth
MADHYA PRADESH 0.26 +0.02 (9%)
DELHI 1 2.62 +0.72 (22%)
SAURABH RM 0.58 +0.05 (9%)
GUJARAT 0.01 +0.01 (262%)
ORISSA 0.97 +0.12 (15%)
RAJASTHAN 0.21 +0.10 (32%)
EAST MUMBAI 6.73 +0.57 (8%)
NCR 0.13 +0.08 (38%)
MAHARASHTRA 0.00 +0.00 (2238%)
CDR 0.89 +0.12 (16%)
DELHI 0.00 +0.00 (30%)
WEST BENGAL 17.17 +13.0 (43%)
SOUTH MUMBAI 5.94 +1.40 (31%)
KOLKATA-1 0.02 +0.00 (12%)
NORTH GUJARAT 0.42 +0.03 (7%)
MAHARASHTRA 0.57 +0.31 (122%)
CDR 0.31 +0.07 (18%)
JHARKHAND 0.18 +0.04 (25%)
BIHAR 0.00 +0.00 (2286%)
MANISH SAHIJWANI 0.48

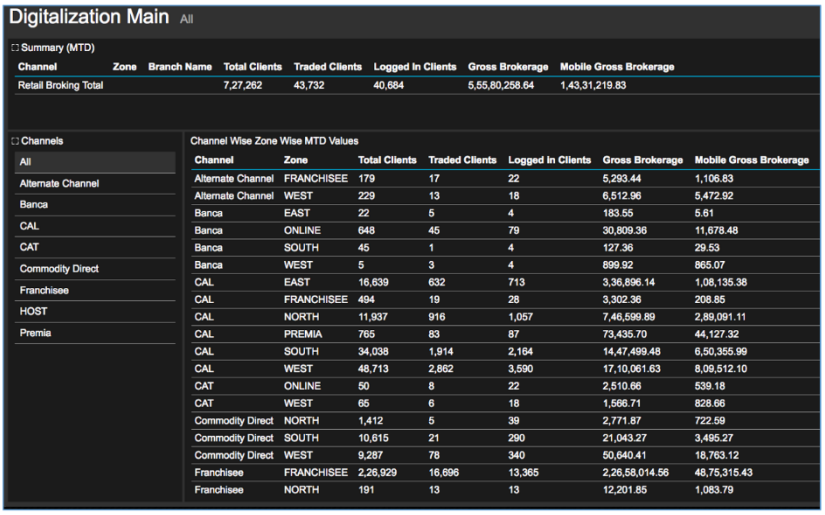
22

POC


New Clients Apr 2017 - Mar 2018
Channel
All
Alternate Channel
Franchisee
Banca
Commodity Direct
Premia
Zone
All
WEST (MH)
WEST
ONLINE
WEST (MP & GJ)
FRANCHISEE
Area
All
MAHARASHTRA NEW
CURRENCY HO
KARNATAKA
NORTH GUJARAT
ANDHRA PRADESH
Last Year
25,252
This Year
18,069
Last Quarter
9,922
This Quarter
8,147
Last Month
3,874
This Month
881
Statewise New AC
New Activation
4,000
3,000
2,000
1,000
0
Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar

23

POC


Digitalization Main All
Summary (MTD)
Channel Zone Branch Name Total Clients Traded Clients Logged In Clients Gross Brokerage Mobile Gross Brokerage
Retail Broking Total 7,27,262 43,732 40,684 5,55,80,258.64 1,43,31,219.83
Channels
All
Alternate Channel
Banca
CAL
CAT
Commodity Direct
Franchisee
HOST
Premia
Channel Wise Zone Wise MTD Values
Channel Zone Total Clients Traded Clients Logged in Clients Gross Brokerage Mobile Gross Brokerage
Alternate Channel FRANCHISEE 179 17 22 5,293.44 1,106.83
Alternate Channel WEST 229 13 18 6,512.96 5,472.92
Banca EAST 22 5 4 183.55 5.61
Banca ONLINE 648 45 79 30,809.36 11,678.48
Banca SOUTH 45 1 4 127.36 29.53
Banca WEST 5 3 4 899.92 865.07
CAL EAST 16,639 632 713 3,36,896.14 1,08,135.38
CAL FRANCHISEE 494 19 28 3,302.36 208.85
CAL NORTH 11,937 916 1,057 7,46,599.89 2,89,091.11
CAL PREMIA 765 83 87 73,435.70 44,127.32
CAL SOUTH 34,038 1,914 2,164 14,47,499.48 6,50,355.99
CAL WEST 48,713 2,862 3,590 17,10,061.63 8,09,512.10
CAT ONLINE 50 8 22 2,510.66 539.18
CAT WEST 65 6 18 1,566.71 828.66
Commodity Direct NORTH 1,412 5 39 2,771.87 722.59
Commodity Direct SOUTH 10,615 21 290 21,043.27 3,495.27
Commodity Direct WEST 9,287 78 340 50,640.41 18,763.12
Franchisee FRANCHISEE 2,26,929 16,696 13,365 2,26,58,014.56 48,75,315.43
Franchisee NORTH 191 13 13 12,201.85 1,083.79

24

Recommendation

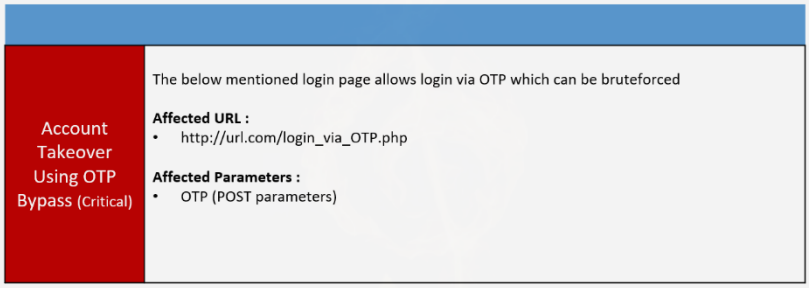
Take the following precautions:

- Use a strong password 8 character or more in length with alphanumerics and symbols
- It should not contain personal/guessable information
- Do not reuse passwords
- Disable default accounts and users
- Change all passwords to strong unique passwords

References:

https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)
https://www.owasp.org/index.php/Default_Passwords
https://www.us-cert.gov/ncas/alerts/TA13-175A

3. Account Takeover Using OTP Bypass



3. Account Takeover Using OTP Bypass

Account Takeover Using OTP Bypass (Critical)	Similar issue is observed on the below mentioned login pages too **Affected URL :** • http://url.com/admin/login_via_OTP.php **Affected Parameters :** • code (POST parameters)

27

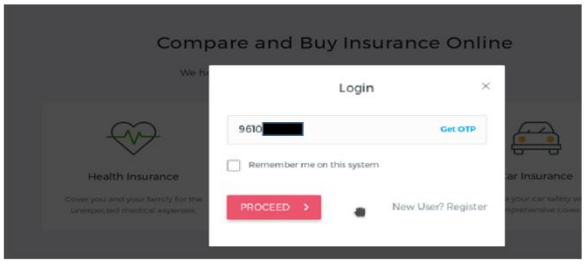
3. Account Takeover Using OTP Bypass

Account Takeover Using OTP Bypass (Critical)	The below mentioned login page allows login via OTP which can be bruteforced **Affected URL :** • http://url.com/login_via_OTP.php **Affected Parameters :** • OTP (POST parameters)

26

Observation

- Navigate to http://url.com/login_via_OTP.php You will see user login page via OTP. Enter victim's mobile number while capturing requests in a local proxy and click Get OTP



Observation

- Following request will be generated containing OTP parameter.

```
POST /[redacted] HTTP/1.1
Host: www.5paisainsurance.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.(
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Referer: http[redacted]
Content-Length: 43

Connection: close

{UserID:'96[redacted]3','OTP:'1234','Persist:''}
```

Observation

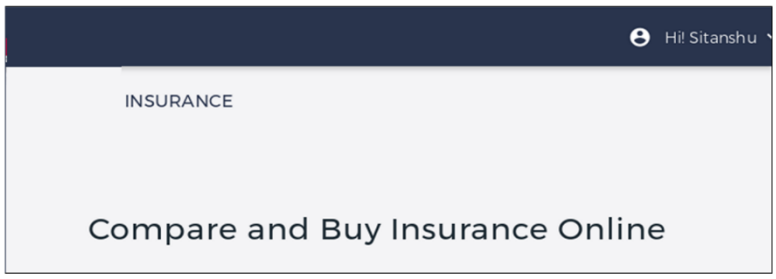
- We shoot the request with all possible combinations of 4 Digit OTPs and upon a successful hit, we get a response containing user details. We can use the same OTP then to login.

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: application/json; charset=utf-8
ETag:
Date: Thu, 02 Nov 2017 08:38:32 GMT
Connection: close
Content-Length: 59

{"d":["Sitanshu","31694","Gender","0","0","","[redacted]"]}
```

Business Impact – Extremely High

A malicious hacker can gain complete access to any account just by knowing the registered phone number. This leads to complete compromise of personal user data of every customer.
Attacker once logs in can then carry out actions on behalf of the victim which could lead to serious financial loss to him/her.



31

Recommendation

Take the following precautions:

- Use proper rate-limiting checks on the no of OTP checking and Generation requests
- Implement anti-bot measures such as ReCAPTCHA after multiple incorrect attempts
- OTP should expire after certain amount of time like 2 minutes
- OTP should be at least 6 digit and alphanumeric for more security

References:

https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009)
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

4. Unauthorised Access to Customer Details

Unauthorised Access to Customer Details (Critical)	The Show My Bill module suffers from an Insecure Direct Object Reference (IDOR) that allows attacker get access to anyones Bill details **Affected URL :** • http://hackingenv.internshala.com/Insecure-Direct-Object-Reference/GET-Based-IDOR-in-URL-Variant-1/bill.php **Affected Parameters :** • user_id (GET parameters)

33

4. Unauthorised Access to Customer Details

Unauthorised Access to Customer Details (Critical)	Similar issue is found on below modules too **Affected URL :** • http://url/invoice.php **Affected Parameters :** • invoice_id (GET parameter) **Affected URL :** • http://url/call_history.php **Affected Parameters :** • mobile_no (POST parameter) **Affected URL :** • http://url/recharge.php **Affected Parameters :** • from_accountno (POST parameter) **Affected URL :** • http://url/sms_history.php **Affected Parameters :** • mobile_no(GET parameter)

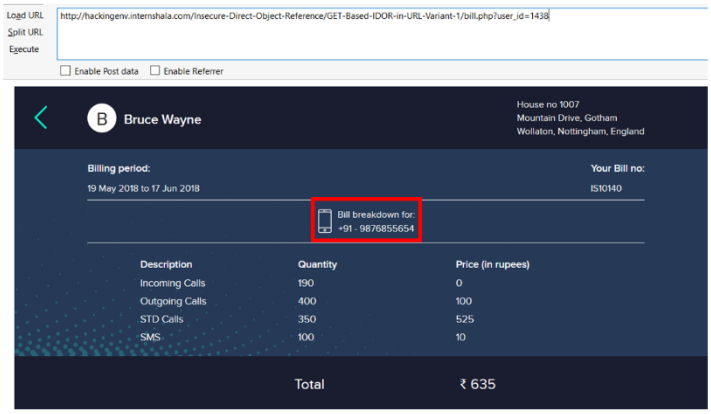
34

Observation

- Login to your account and navigate to Bill page on http://hackingenv.internshala.com/Insecure-Direct-Object-Reference/GET-Based-IDOR-in-URL-Variant-1/ and click on Show My Bill button

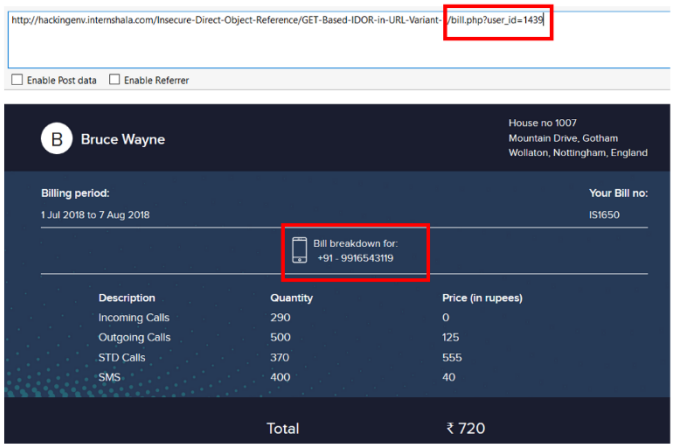
Observation

- Your bill will be shown to you like below. Notice the URL: http://hackingenv.internshala.com/Insecure-Direct-Object-Reference/GET-Based-IDOR-in-URL-Variant-1/bill.php?user_id=1438
- It contains user_id of our user and we get bill details of our user's **mobile number: 9876855654**



Observation

- We change this user_id from 1438 to 1439 and we get bill information of a different user with **mobile number: 9976543119**



Business Impact – Extremely High

A malicious hacker can read bill information of any user just by knowing the User ID. This discloses critical billing information of users including:

- Mobile Number
- Bill Number
- Billing Period
- Bill Amount and Breakdown

This can be used by malicious hackers to carry out targeted phishing attacks on the users and the information can also be sold to competitors/blackmarket.

More over, as there is no ratelimiting checks, attacker can bruteforce the user_id for all possible values and get bill information of each and every user of the organization resulting is a massive information leakage.

Other IDORs on the application are leaking much more information including Payment details, call history and even allow attacker to recharge his mobile number deducting money from any one else's account which can be used to steal money from users.

As a PoC, Bill details of 100 users are dumped in the attached excel file below:

Microsoft Excel
7-2003 Workshe

38

Recommendation

Take the following precautions:

- Implement proper authentication and authorisation checks to make sure that the user has permission to the data he/she is requesting
- Use proper rate limiting checks on the number of request comes from a single user in a small amount of time
- Make sure each user can only see his/her data only.

References:

https://www.owasp.org/index.php/Insecure_Configuration_Management
https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

5. Reflected Cross Site Scripting (XSS)

Reflected Cross Site Scripting (Severe)	Below mentioned parameters are vulnerable to reflected XSS **Affected URL :** • hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-1/hello.php **Affected Parameters :** • user_name(GET parameters) **Payload:** • <script>alert(1)</script>

40

5. Reflected Cross Site Scripting (XSS)

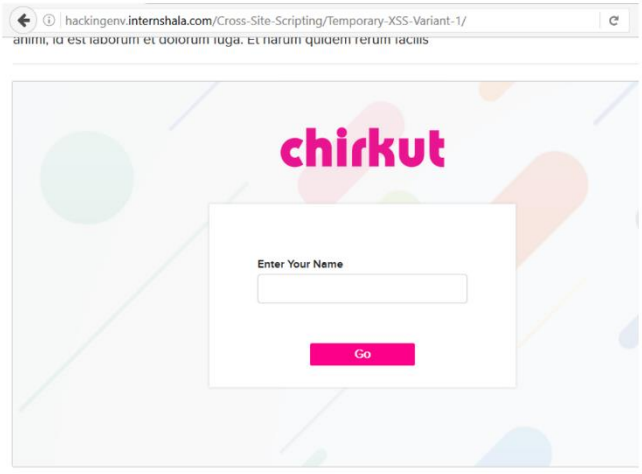
Reflected Cross Site Scripting (Severe)	Similar issue is found on below modules too **Affected URL :** • http://hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-2/xss/testing* **Affected Parameters :** • URL – anything after testing **Payload:** • <body onload=alert(1)>
	Affected URL : • http://hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-4/ **Affected Parameters :** • url (POST parameters) **Payload:** • " onload="alert(1)

41

Observation

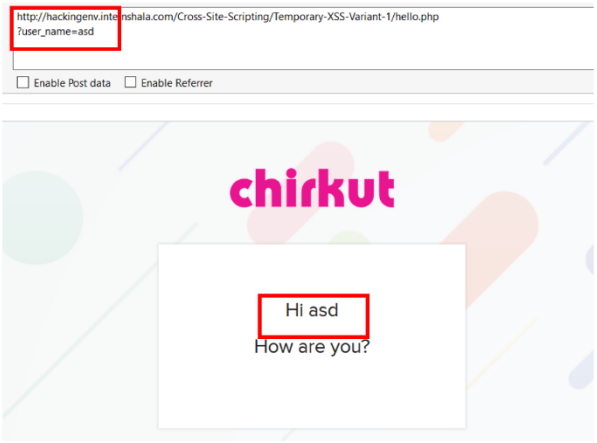
Navigate to hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-1/hello.php

You will see a field to enter some text



Observation

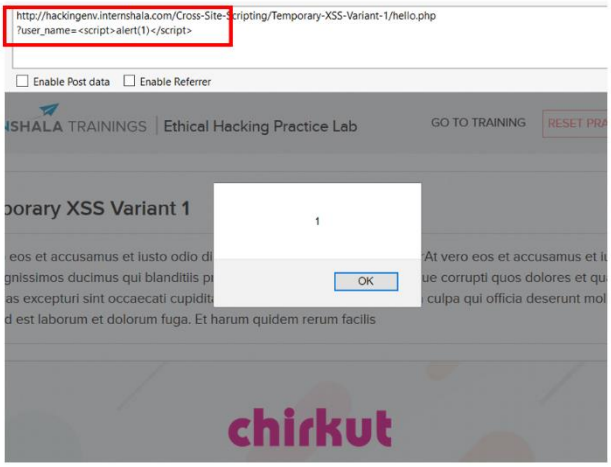
Enter any text and click the button, you will see it reflected in the next page and value will be in GET parameter **user_name**



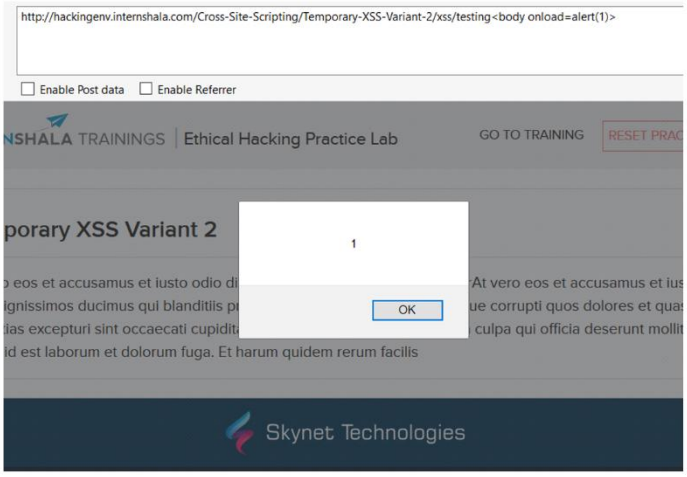
Observation

Put the payload instead of asd: **<script>alert(1)</script>**

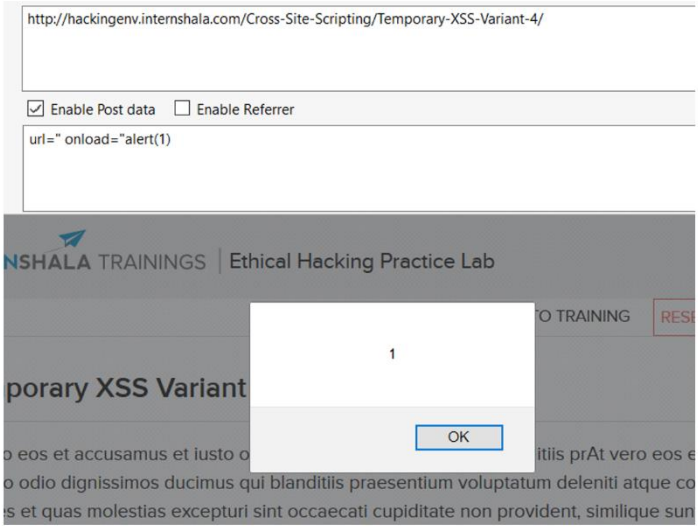
As you can see we executed custom JS causing popup



PoC


http://hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-2/xss/testing<body onload=alert(1)>
Enable Post data
Enable Referrer
NSHALA TRAININGS | Ethical Hacking Practice Lab
GO TO TRAINING
porary XSS Variant 2
1
OK
Skynet Technologies

PoC


http://hackingenv.internshala.com/Cross-Site-Scripting/Temporary-XSS-Variant-4/
Enable Post data
Enable Referrer
url=" onload="alert(1)
NSHALA TRAININGS | Ethical Hacking Practice Lab
1
OK

Business Impact – High

As attacker can inject arbitrary HTML CSS and JS via the URL, attacker can put any content on the page like phishing pages, install malware on victim's device and even host explicit content that could compromise the reputation of the organization

All attacker needs to do is send the link with the payload to the victim and victim would see hacker controlled content on the website. As the user trusts the website, he/she will trust the content.

47

Recommendation

Take the following precautions:

- Sanitise all user input and block characters you do not want
- Convert special HTML characters like ' " < > into HTML entities " %22 < > before printing them on the website

References:

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://en.wikipedia.org/wiki/Cross-site_scripting
https://www.w3schools.com/html/html_entities.asp

6. Directory Listing

Directory Listing (Moderate)	Below mentioned parameters are vulnerable to reflected XSS **Affected URL :** • http://URL1/backup/ • http://url2/profile_pictures/

Observation

- Navigate to http://URL1/backup/
- Complete listing of directory is shown containing month wise HTML backups of the website

Business Impact – Moderate

Although this vulnerability does not have a direct impact to users or the server, though it can aid the attacker with information about the server and the users

Also, attacker can simply download the backups and images and view them

Recommendation

Take the following precautions:

- Disable Directory Listing
- Put an index.html in all folders with default message

References:

https://cwe.mitre.org/data/definitions/548.html
https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/

7. Information Disclosure

Information Disclosure due to Apache Info Pages (Low)	Below mentioned urls disclose server information **Affected URL :** • http://URL/server-status • http://URL/server-info

54

Observation

- server-info page

Observation

- Navigate to mentioned URL
- Default server-status page opens which discloses server information

Business Impact – Moderate

Although this vulnerability does not have a direct impact to users or the server, though it can help the attacker in mapping the server architecture and plan further attacks on the server

Recommendation

Take the following precautions:

- Disable all default pages and folders including server-status and server-info

References:

https://vuldb.com/?id.88482
https://httpd.apache.org/docs/current/mod/mod_status.html
https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_apache_http_server_httponly_cookie_information_disclosure

57

Challenges faced and Effective Solutions

The first day of doing new things in new environment is not an easy task because of new responsibility that is not routinely done but I tried all my best for that the following are some of the problems encountered during my internship period:
Any job will have challenges, but after two months of my own internship experience, I've found that there are some common intern challenges in my internship.

- **Issues with Time Management/Self - Management**

  This issue was something which I faced almost before every test submission and even before the last project submission. I feel that due to many subjects at hand it was difficult to complete every week's work in the given time.

  Solution:

  I made sure that I did at least half a module (if it was only theory) and ¼ of the module if it required practical aspects. I also made notes so that I can revise the previous modules regularly.

- **Hesitant to ask questions**

  One of the major reasons for not completing the work in allotted time was that I did not clear my doubts before moving on to the next module. This led to inconsistency and low self-confidence. Thus, this was one of the major reasons why I finished the modules late.

  Solution:

  As I wasn't sure whether I would get answers in the online chat section so I was reluctant to ask questions there. Luckily, I found all my answers and cleared my doubts on the internet via video tutorials and editorials.

- **Lack of adequate direction**

  Watching the videos and deriving your own conclusions is a very common thing to do when you do not have proper guidance. At the same time,

keeping in mind that all clear explanations on what to do and how to proceed were really helpful.

Solution:

Whenever I came across any difficulties, I searched for it on google and various other reference links given at the end of every video. Also, every activity had a video solution following it which was helpful in checking my solution to the problem.

Conclusion

HOW TO BE ETHICAL?

Ethical hacking is usually conducted in a structured and organized manner, usually as part of a penetration test or security audit. The ethical hacker must follow certain rules to ensure that all ethical and moral obligations are met. An ethical hacker must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.

- Maintain and follow a nondisclosure agreement (NDA) with the client in the case of confidential information disclosed during the test.

- Maintain confidentiality when performing the test. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, DoS attacks should only be run as part of the test if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers as a result of the testing.

PERFORMING A PENETRATION TEST

Many ethical hackers acting in the role of security professionals use their skills to perform security evaluations or penetration tests. These tests and evaluations have three phases.

1. **Preparation**

   This phase involves a formal agreement between the ethical hacker and the organization. This agreement should include the full scope of the test, the types of attacks (inside or outside) to be used, and the testing types: white, black, or grey box.

2. **Conduct**

   Security Evaluation During this phase, the tests are conducted, after which the tester prepares a formal report of vulnerabilities and other findings.

3. **Conclusion**

   The findings are presented to the organization in this phase, along with any recommendations to improve security.

End Result

The result of a network penetration test or security audit is an ethical hacking, or pen test report. Either name is acceptable, or they can be used interchangeably. This report details the results of the hacking activity, the types of tests performed, and the hacking methods used. The results are compared against the expectations initially agreed upon with the customer. Any vulnerability identified are detailed countermeasures are suggested. This document is usually delivered to the organization in hard-copy format, for security reasons. The details of the ethical hacking report must be kept confidential, because they highlight the organization's security risk and vulnerabilities. If this document falls into the wrong hands, the results could be disastrous for the organization. It would essentially give someone the roadmap to all the security weaknesses of an organization.

Bibliography

- *https://www.owasp.org/index.php/SQL_Injection*
- *https://en.wikipedia.org/wiki/SQL_injection*
- *https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)*
- *https://www.owasp.org/index.php/Default_Passwords*
- *https://www.us-cert.gov/ncas/alerts/TA13-175A*
- *https://www.owasp.org/index.php/Testing_Multiple_Factors_Authentication_(OWASP-AT-009)*
- *https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks*
- *https://www.owasp.org/index.php/Insecure_Configuration_Management*
- *https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References*
- *https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)*
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.w3schools.com/html/html_entities.asp
- *https://cwe.mitre.org/data/definitions/548.html*
- https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/
- *https://vuldb.com/?id.88482*
- *https://httpd.apache.org/docs/current/mod/mod_status.html*
- *https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_apache_http_server_httponly_cookie_information_disclosure*