ASSIGNMENT – 4

Q-1) Scan any five websites with nikto tool.

```
200420116059@kali:~$ nikto -host facebook.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          31.13.66.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2022-10-04 06:12:52 (GMT0)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcK3coyOff22bLTCR8Lf-JuNcUIMBmQT5nIu6YDXBr73LwJm
JThg3ooPRce0oI37XVfz6UcndtPofw"; e_fb_vipaddr="AcK9Efg88boyHKCau_Q17us85FWDo8ncw9WPpaNFjY1krT-Geg2DrEUaelbvqhSlBl5qakY"; e_fb_builduser="
AcJcFkpkztCvvuxrZG7Sjj46TzQnAYbLrvd5f28nx1NcRnLbRW1lmdnrHxJN-w"; e_fb_binaryversion="AcKVczh0BGxGH4Q0cjDPKYdTT8O3Kj3A_oCewnfh02JSUqfppMSa
pQHDADWO8G6d4olTHjKb3RJ5S8Hy4p24S7f8NgMaerXner8"; e_proxy="AcKOKclYVj496x2MWFc7PsjuBdadMkj1bGfGscWo6fQopwJcyN2Xg_R2qndgx_DH_tqxCPFMhn-Be-
l3"
+ 7785 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-10-04 06:13:11 (GMT0) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
200420116059@kali:~$ nikto -host google.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          142.250.81.206
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2022-10-04 06:17:55 (GMT0)
---------------------------------------------------------------------------
+ Server: gws
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie 1P_JAR created without the httponly flag
+ Uncommon header 'x-hallmonitor-challenge' found, with contents: CgwIvqDvmQYQu6OvswISBANXRlg
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer or proxy is in place
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Allowed HTTP Methods: GET, HEAD
+ 7786 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-10-04 06:18:46 (GMT0) (51 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
200420116059@kali:~$ nikto -host gmail.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.253.62.18
+ Target Hostname:    gmail.com
+ Target Port:        80
+ Message:            Multiple IP addresses found: 172.253.62.18, 172.253.62.19, 172.253.62.83, 172.253.62.17
+ Start Time:         2022-10-04 06:20:13 (GMT0)
---------------------------------------------------------------------------
+ Server: sffe
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Root page / redirects to: https://www.google.com/gmail/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'cross-origin-opener-policy-report-only' found, with contents: same-origin; report-to="static-on-bigtable"
+ Uncommon header 'report-to' found, with contents: {"group":"static-on-bigtable","max_age":2592000,"endpoints":[{"url":"https://csp.with
google.com/csp/report-to/static-on-bigtable"}]}
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Server banner has changed from 'sffe' to 'gws' which may suggest a WAF, load balancer or proxy is in place
+ Cookie 1P_JAR created without the httponly flag
+ Uncommon header 'x-hallmonitor-challenge' found, with contents: CgwIzaHvmQYQocPIkgISBANXRlg
+ 7789 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-10-04 06:20:59 (GMT0) (46 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
200420116059@kali:~$ nikto -host amazon.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          205.251.242.103
+ Target Hostname:    amazon.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 205.251.242.103, 52.94.236.248, 54.239.28.85
+ Start Time:         2022-10-04 06:26:02 (GMT0)
---------------------------------------------------------------------------
+ Server: Server
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://amazon.com/
+ Retrieved cneonction header: close
+ Uncommon header 'cneonction' found, with contents: close
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  13 error(s) and 5 item(s) reported on remote host
+ End Time:           2022-10-04 06:26:20 (GMT0) (18 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
200420116059@kali:~$ nikto -host facebook.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          31.13.66.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2022-10-04 06:12:52 (GMT0)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcK3coyOff22bLTCR8Lf-JuNcUIMBmQT5nIu6YDXBr73LwJm
JThg3ooPRce0oI37XVfz6UcndtPofw"; e_fb_vipaddr="AcK9Efg88boyHKCau_Q17us85FWDo8ncw9WPpaNFjY1krT-Geg2DrEUaelbvqhSlBl5qakY"; e_fb_builduser="
AcJcFkpkztCvvuxrZG7Sjj46TzQnAYbLrvd5f28nx1NcRnLbRW1lmdnrHxJN-w"; e_fb_binaryversion="AcKVczh0BGxGH4Q0cjDPKYdTT8O3Kj3A_oCewnfh02JSUqfppMSa
pQHDADWO8G6d4olTHjKb3RJ5S8Hy4p24S7f8NgMaerXner8"; e_proxy="AcKOKclYVj496x2MWFc7PsjuBdadMkj1bGfGscWo6fQopwJcyN2Xg_R2qndgx_DH_tqxCPFMhn-Be-
l3"
+ 7785 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-10-04 06:13:11 (GMT0) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Q-2) Perform Curl Operation on any five websites.

```
200420116059@kali:~$ curl -I google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Tue, 04 Oct 2022 06:46:16 GMT
Expires: Thu, 03 Nov 2022 06:46:16 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

```
200420116059@kali:~$ curl -I gmail.com
HTTP/1.1 301 Moved Permanently
Location: https://www.google.com/gmail/
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: sffe
Content-Length: 226
X-XSS-Protection: 0
Date: Tue, 04 Oct 2022 06:42:45 GMT
Expires: Tue, 04 Oct 2022 07:12:45 GMT
Cache-Control: public, max-age=1800
Content-Type: text/html; charset=UTF-8
Age: 367
```

```
200420116059@kali:~$ curl -I youtube.com
HTTP/1.1 301 Moved Permanently
Content-Type: application/binary
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Tue, 04 Oct 2022 06:50:04 GMT
Location: https://youtube.com/
Content-Length: 0
Server: ESF
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

```
200420116059@kali:~$ curl -I netflix.com
HTTP/1.1 403 Forbidden
Via: 1.1 i-049f5ceb125898412 (us-east-1)
Server: nq_website_nonmember-prod-release UNKNOWN
X-Xss-Protection: 1; mode=block; report=https://www.netflix.com/ichnaea/log/freeform/xssreport
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Originating-URL: http://netflix.com/
Set-Cookie: nfvdid=BQFmAAEBEFtlb9nmgoc6iREp-0vrPqpAC1ju8YIUJ8W5A6q_KcIgIIThtzfn5fzrkJK45RB7HzxHM5NdEsO-yaTm0jXCMi49UgheOSklDAgAsqgMg7C9rw
%3D%3D; Domain=.netflix.com; Path=/; Max-Age=31536000
X-Netflix.nfstatus: 1_2
X-Netflix-Error-Cause: SpeedbumpV2 (nq_website_nonmember-prod-release; us-east-1)
Set-Cookie: memclid=d4f93a98-2c12-4565-88f2-03cd3eec2551; Max-Age=31536000; Expires=Wed, 04 Oct 2023 06:50:37 GMT; Path=/; Domain=.netfli
x.com
X-Netflix.proxy.execution-time: 2
transfer-encoding: chunked
```

```
200420116059@kali:~$ curl -I jaiminmalaviya.ml
HTTP/1.1 301 Moved Permanently
Location: https://jaiminmalaviya.ml/
Server: Netlify
X-Nf-Request-Id: 01GEGW6N0P7X1FBSM7S3VSHQEW
Date: Tue, 04 Oct 2022 06:51:16 GMT
```

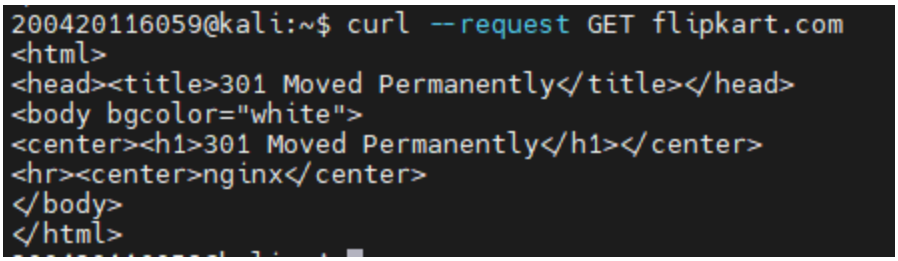
Q-3) Perform Curl Operation on any five websites with request method GET.

```
200420116059@kali:~$ curl --request GET google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

```
200420116059@kali:~$ curl --request GET gmail.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/gmail/">here</A>.
</BODY></HTML>
```

```
200420116059@kali:~$ curl --request GET gtu.ac.in



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>
        Gujarat Technological University
</title>

    <!-- Meta line commented & added by Vishwa - 05/09/2022-->

    <meta charset="utf-8" name="viewport" content="width=device-width, initial-scale=1.0" />
    <!-- Responsive css -->
<link rel="stylesheet" href="assets/css/responsive.css" /><link rel="shortcut icon" type="image/x-icon" href="assets/img/favicon.ico" /><
link rel="stylesheet" href="assets/css/odometer-theme-default.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/font-awes
ome/css/font-awesome.min.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/themify-icons/css/themify-icons.css" /><link r
el="stylesheet" type="text/css" href="assets/vendor/animate/animate.min.css" /><link rel="stylesheet" type="text/css" href="assets/vendor
/fancybox/css/jquery.fancybox.min.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/owlcarousel/css/owl.carousel.min.css"
 /><link rel="stylesheet" type="text/css" href="assets/vendor/swiper/css/swiper.min.css" /><link rel="stylesheet" type="text/css" href="a
ssets/vendor/swiper/css/swiper.css" /><link href="https://fonts.googleapis.com/css2?family=Nunito:wght@300;400;600;700&amp;display=swap"
rel="stylesheet" /><link href="css/lightgallery.css" rel="stylesheet" /><link rel="stylesheet" href="assets/css/style.css" /><link rel="s
tylesheet" href="assets/css/responsive.css" />

    <style type="text/css">
        table, th
        {
            border: 1px solid black;
            color:#424242;
        }
        td
        {
            vertical-align: middle;
```

```
200420116059@kali:~$ curl --request GET amazon.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>Server</center>
</body>
</html>
```


200420116059@kali:~$ curl --request GET flipkart.com
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<h1>301 Moved Permanently</h1>
<hr> nginx
</body>
</html>

Q-4) Perform Curl Operation on any five websites with request method POST.

```
200420116059@kali:~$ curl --request POST google.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max
-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;pa
dding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:77
2px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1
x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.goo
gle.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/ima
ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:u
rl(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{displ
ay:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That’s an error.</ins>
  <p>POST requests require a <code>Content-length</code> header.  <ins>That’s all we know.</ins>
```

```
200420116059@kali:~$ curl --request POST gmail.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max
-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;pa
dding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:77
2px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1
x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.goo
gle.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/ima
ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:u
rl(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{displ
ay:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That’s an error.</ins>
  <p>POST requests require a <code>Content-length</code> header.  <ins>That’s all we know.</ins>
```

```
200420116059@kali:~$ curl --request POST youtube.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max
-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;pa
dding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:77
2px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1
x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.goo
gle.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/ima
ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:u
rl(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{displ
ay:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That’s an error.</ins>
  <p>POST requests require a <code>Content-length</code> header.  <ins>That’s all we know.</ins>
```

```
200420116059@kali:~$ curl --request POST amazon.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>Server</center>
</body>
</html>
```

```
200420116059@kali:~$ curl --request POST drive.google.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max
-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;pa
dding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:77
2px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1
x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.goo
gle.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/ima
ges/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:u
rl(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{displ
ay:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That’s an error.</ins>
  <p>POST requests require a <code>Content-length</code> header.  <ins>That’s all we know.</ins>
```