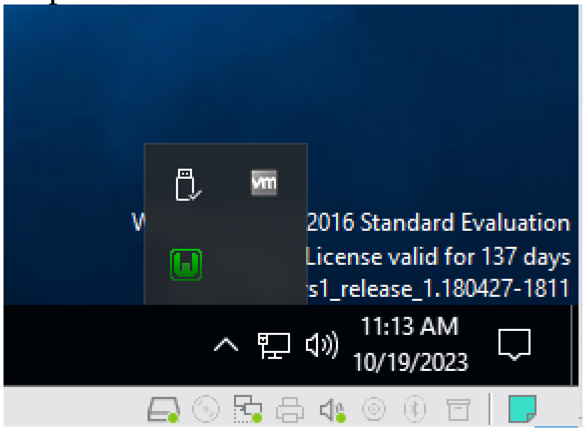
Lab 12: Hacking Web Applications

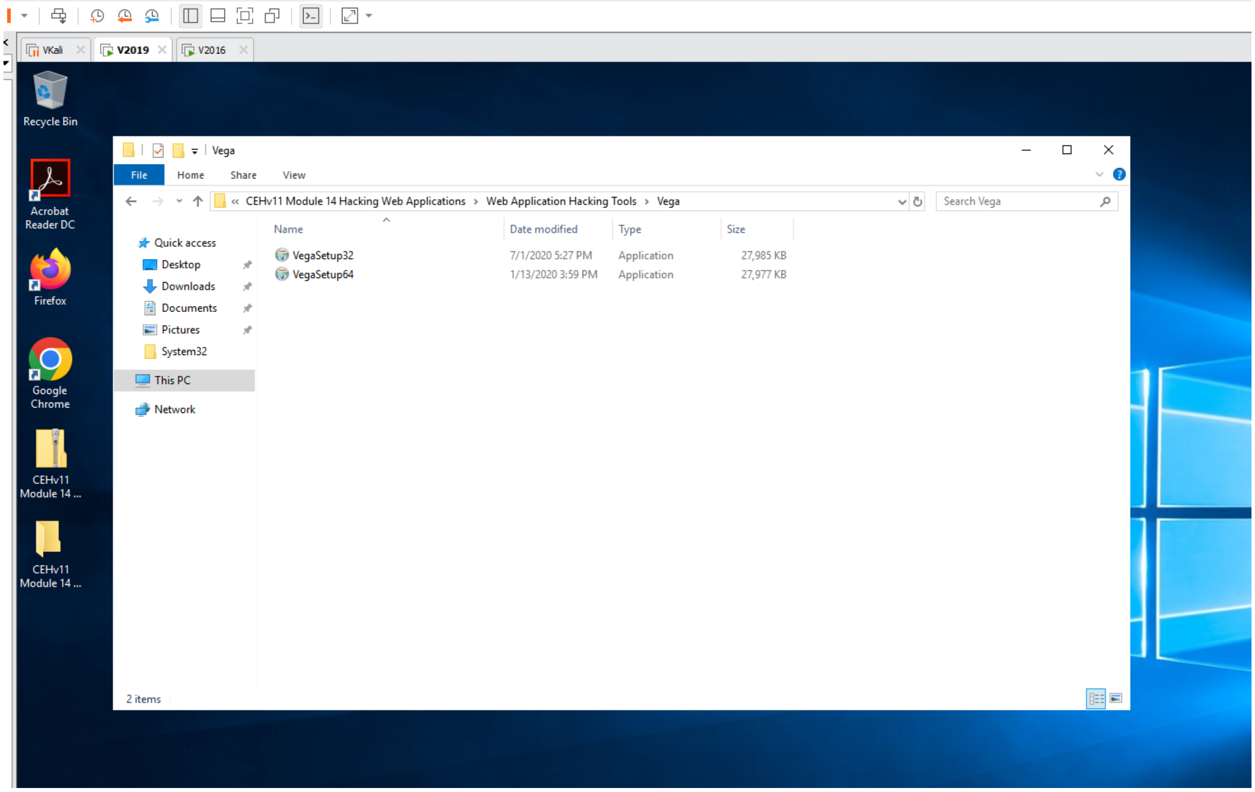
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 21/10/2023

1. Footprint the Web Infrastructure

1.6 Perform Web Application Vulnerability Scanning using Vega

- Open Windows Server 2016 and Windows 2010

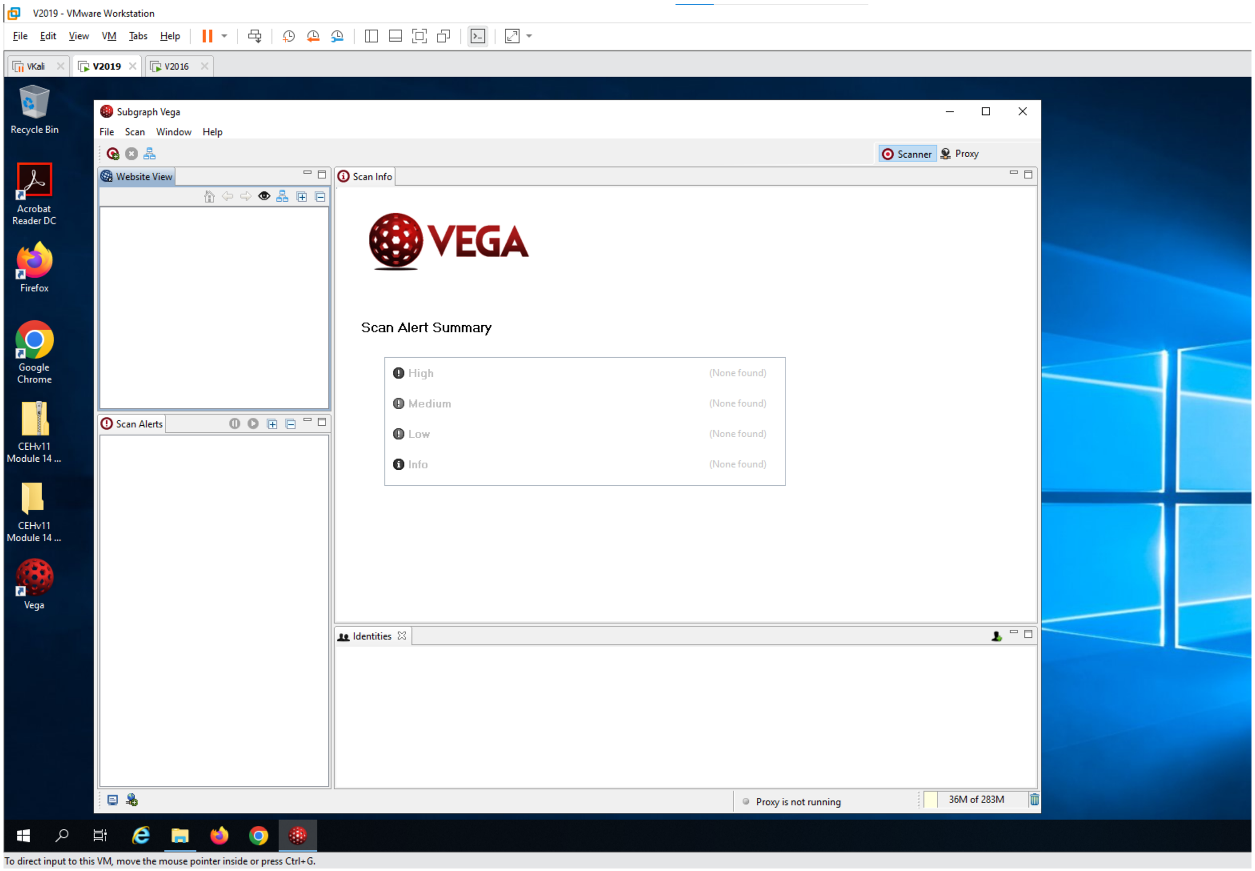

W 2016 Standard Evaluation
License valid for 137 days
s1_release_1.180427-1811
11:13 AM
10/19/2023



« CEHv11 Module 14 Hacking Web Applications › Web Application Hacking Tools › Vega

Name	Date modified	Type	Size
VegaSetup32	7/1/2020 5:27 PM	Application	27,985 KB
VegaSetup64	1/13/2020 3:59 PM	Application	27,977 KB

2 items



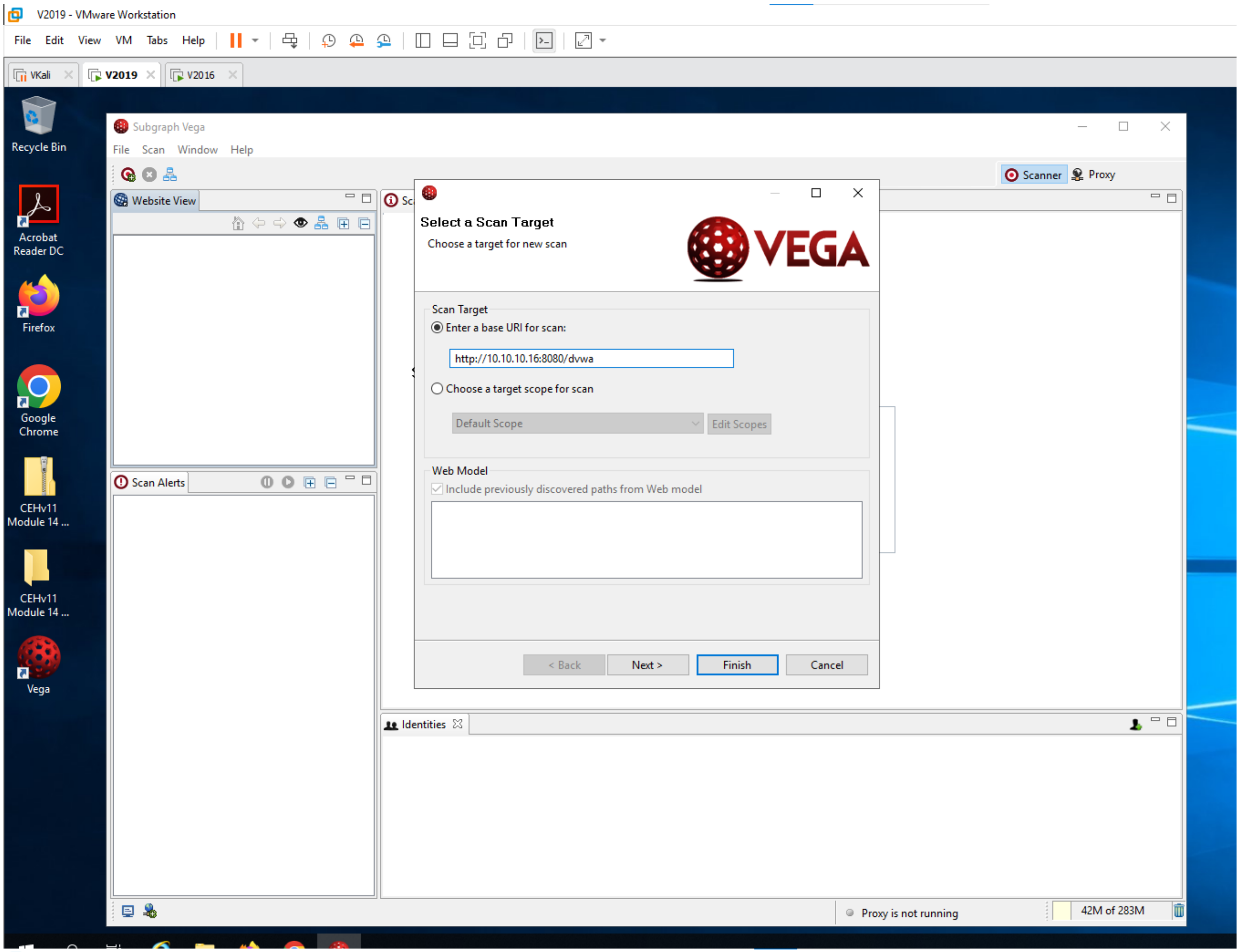
Scan Alert Summary

High	(None found)
Medium	(None found)
Low	(None found)
Info	(None found)

Proxy is not running

36M of 283M

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Select a Scan Target

Choose a target for new scan

Scan Target

● Enter a base URI for scan:

http://10.10.10.16:8080/dvwa

○ Choose a target scope for scan

Default Scope | Edit Scopes

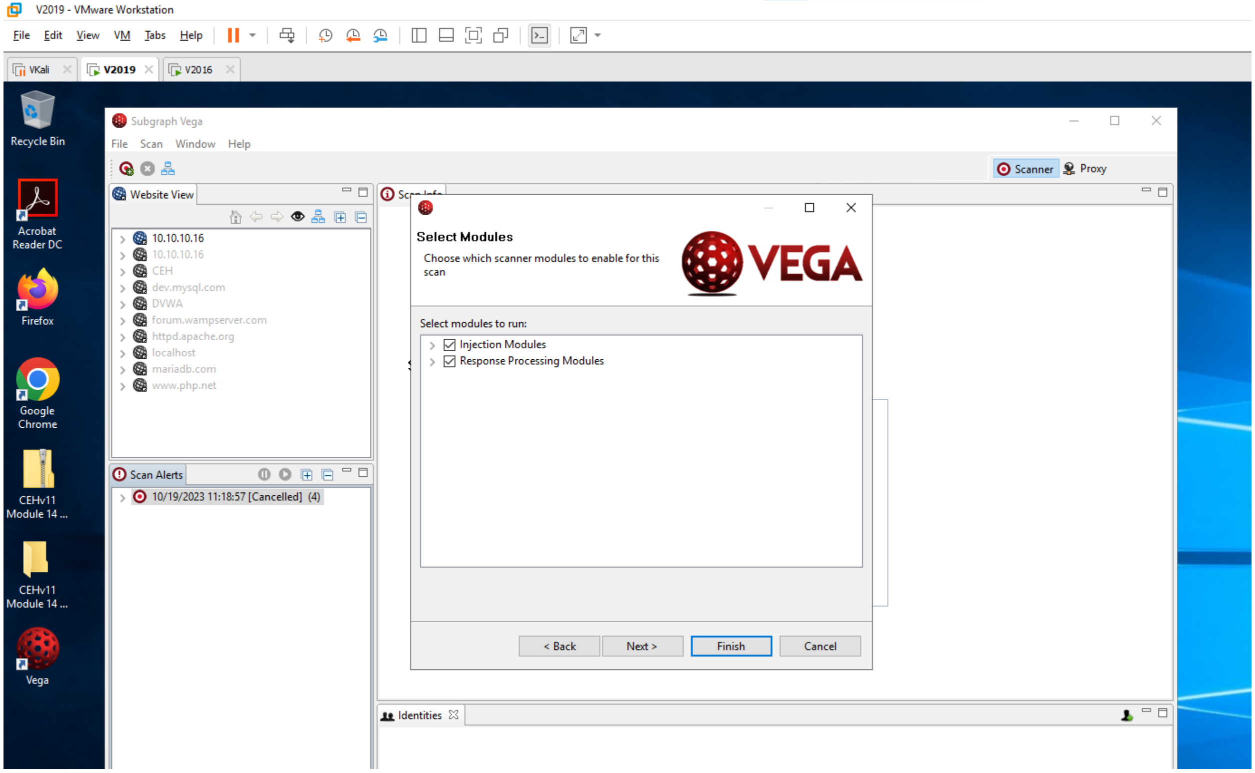
Web Model

☑ Include previously discovered paths from Web model

< Back | Next > | Finish | Cancel

Proxy is not running

42M of 283M



10.10.10.16
10.10.10.16
CEH
dev.mysql.com
DVWA
forum.wampserver.com
httpd.apache.org
localhost
mariadb.com
www.php.net

10/19/2023 11:18:57 [Cancelled] (4)

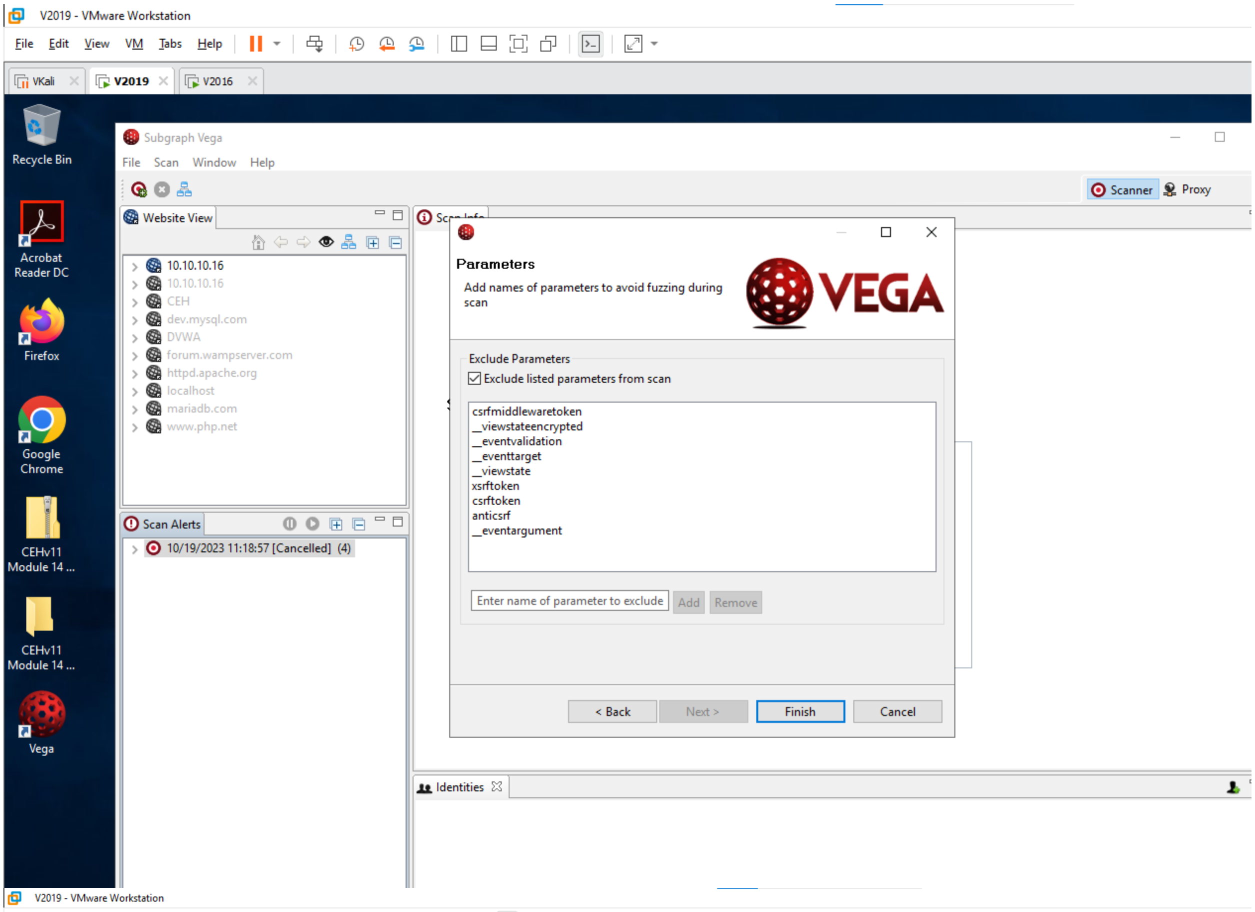
Select Modules

Choose which scanner modules to enable for this scan

Select modules to run:

☑ Injection Modules
☑ Response Processing Modules

< Back | Next > | Finish | Cancel



```
10.10.10.16
10.10.10.16
CEH
dev.mysql.com
DVWA
forum.wampserver.com
httpd.apache.org
localhost
mariadb.com
www.php.net
```

```
10/19/2023 11:18:57 [Cancelled]  (4)
```

Parameters

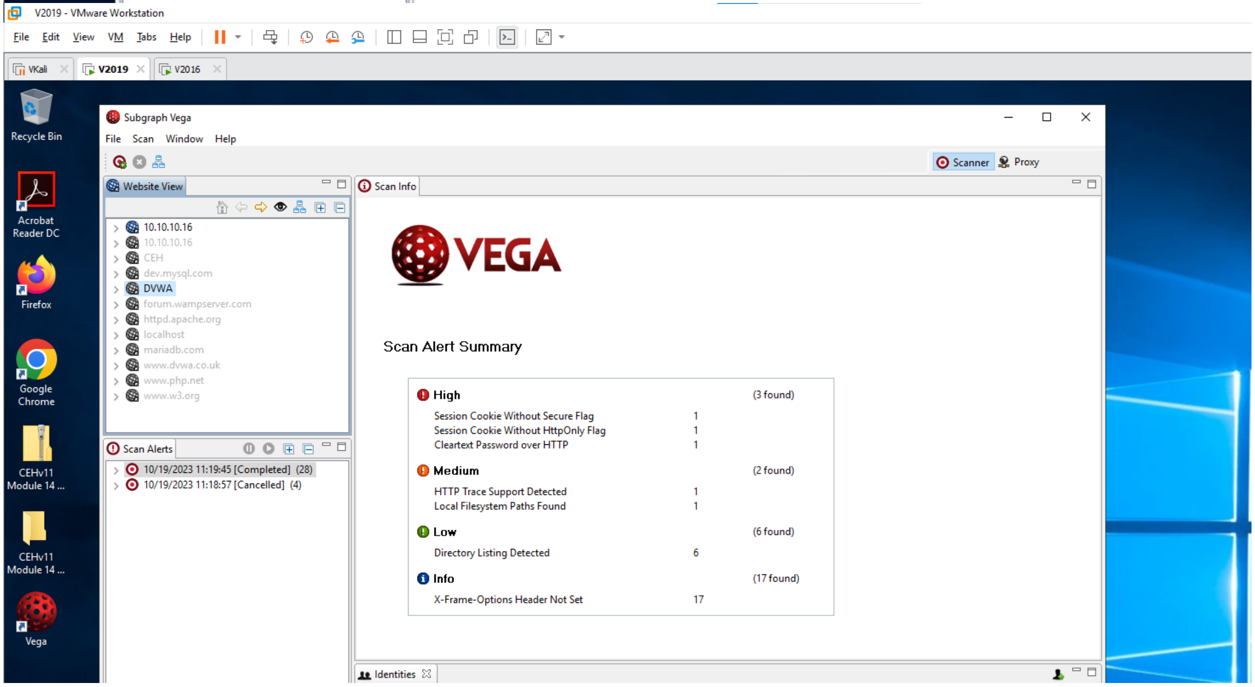
Add names of parameters to avoid fuzzing during scan

Exclude Parameters

☑ Exclude listed parameters from scan

```
csrfmiddlewaretoken
__viewstateencrypted
__eventvalidation
__eventtarget
__viewstate
xsrftoken
csrftoken
anticsrf
__eventargument
```

Enter name of parameter to exclude

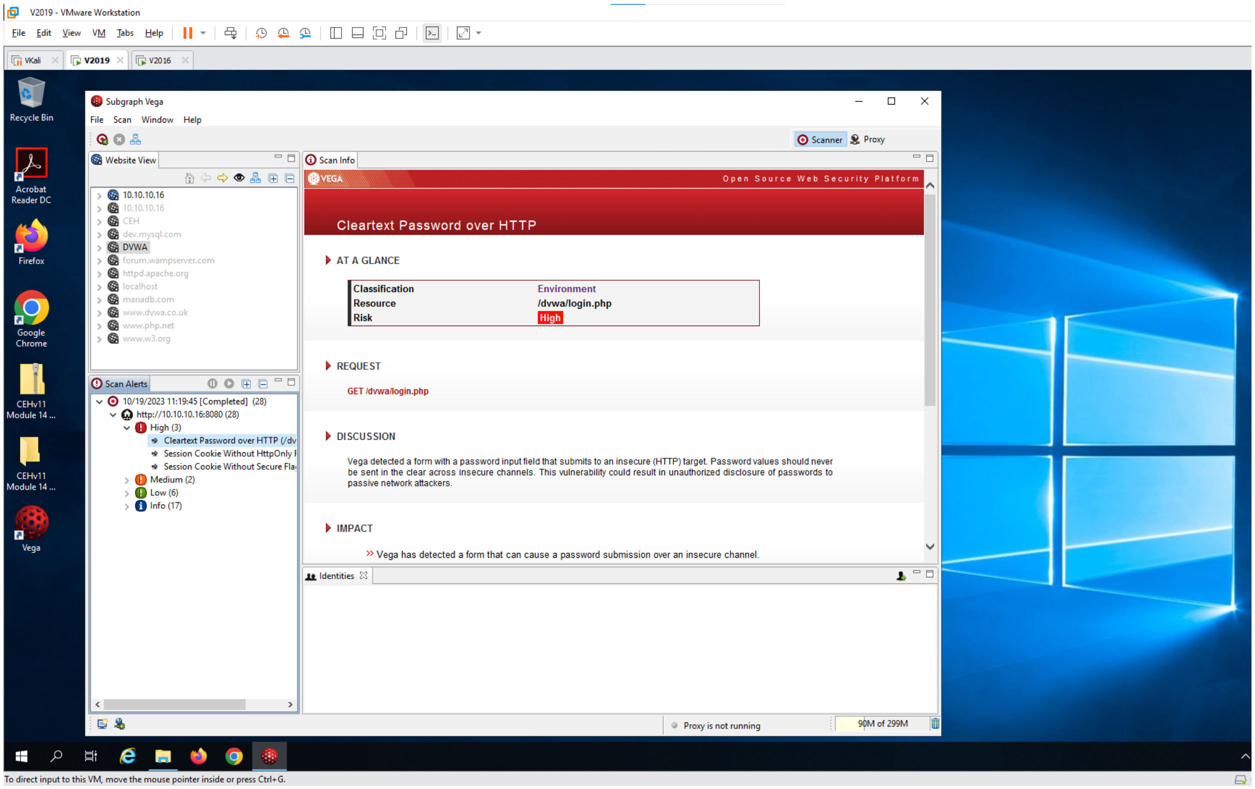


```
10.10.10.16
10.10.10.16
CEH
dev.mysql.com
DVWA
forum.wampserver.com
httpd.apache.org
localhost
mariadb.com
www.dvwa.co.uk
www.php.net
www.w3.org
```

```
10/19/2023 11:19:45 [Completed]  (28)
10/19/2023 11:18:57 [Cancelled]  (4)
```

Scan Alert Summary

```
High                                               (3 found)
    Session Cookie Without Secure Flag          1
    Session Cookie Without HttpOnly Flag        1
    Cleartext Password over HTTP                1
Medium                                             (2 found)
    HTTP Trace Support Detected                 1
    Local Filesystem Paths Found                1
Low                                                (6 found)
    Directory Listing Detected                  6
Info                                               (17 found)
    X-Frame-Options Header Not Set              17
```



Website View:

- 10.10.10.16
- 10.10.10.16
- CEH
- dev.mysql.com
- DVWA
- forum.wampserver.com
- httpd.apache.org
- localhost
- mariadb.com
- www.dvwa.co.uk
- www.php.net
- www.w3.org

Scan Alerts:

```
10/19/2023 11:19:45 [Completed]  (28)
  http://10.10.10.16:8080 (28)
    High (3)
      Cleartext Password over HTTP (/dv
      Session Cookie Without HttpOnly F
      Session Cookie Without Secure Fla
    Medium (2)
    Low (6)
    Info (17)
```

Cleartext Password over HTTP

AT A GLANCE

Classification	Environment
Resource	/dvwa/login.php
Risk	High

REQUEST

GET /dvwa/login.php

DISCUSSION

Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.

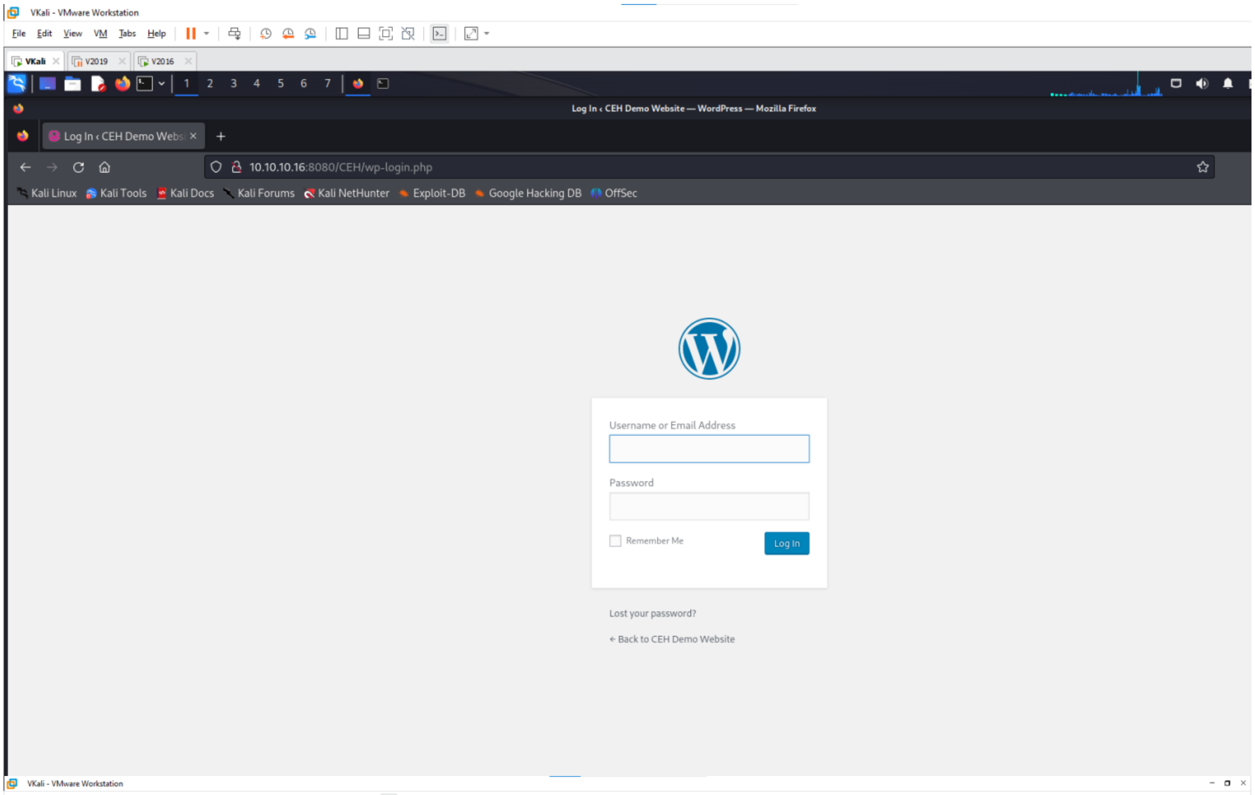
IMPACT

» Vega has detected a form that can cause a password submission over an insecure channel.

2. Perform Web Application Attacks

2.1 Perform a Brute-force Attack using Burp Suite

- Open Parrot, Windows Server 2016, Windows 10



10.10.10.16:8080/CEH/wp-login.php

Username or Email Address

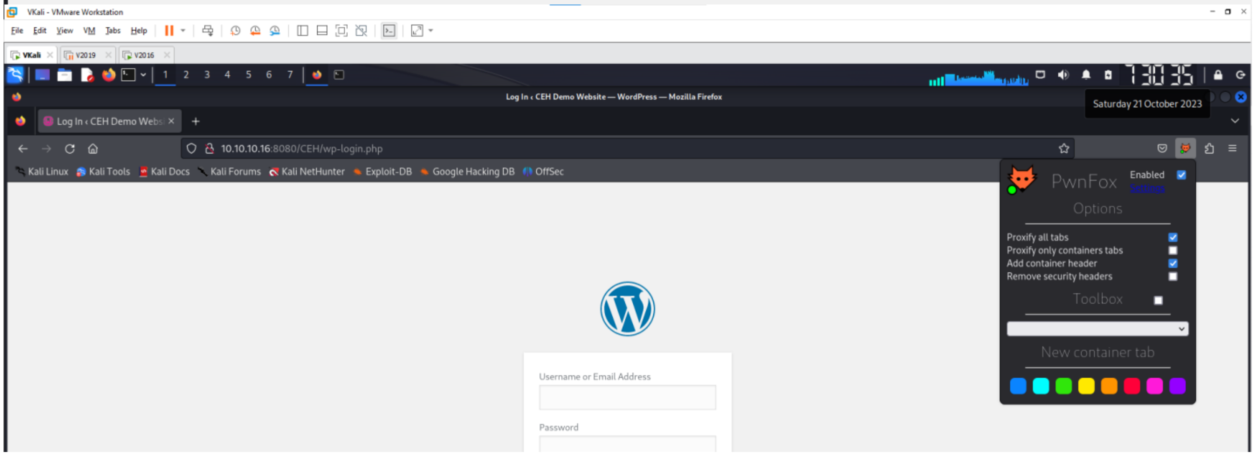
Password

□ Remember Me

Log In

Lost your password?

← Back to CEH Demo Website



10.10.10.16:8080/CEH/wp-login.php

PwnFox

Enabled ☑

Settings

Options

Proxify all tabs ☑

Proxify only containers tabs □

Add container header ☑

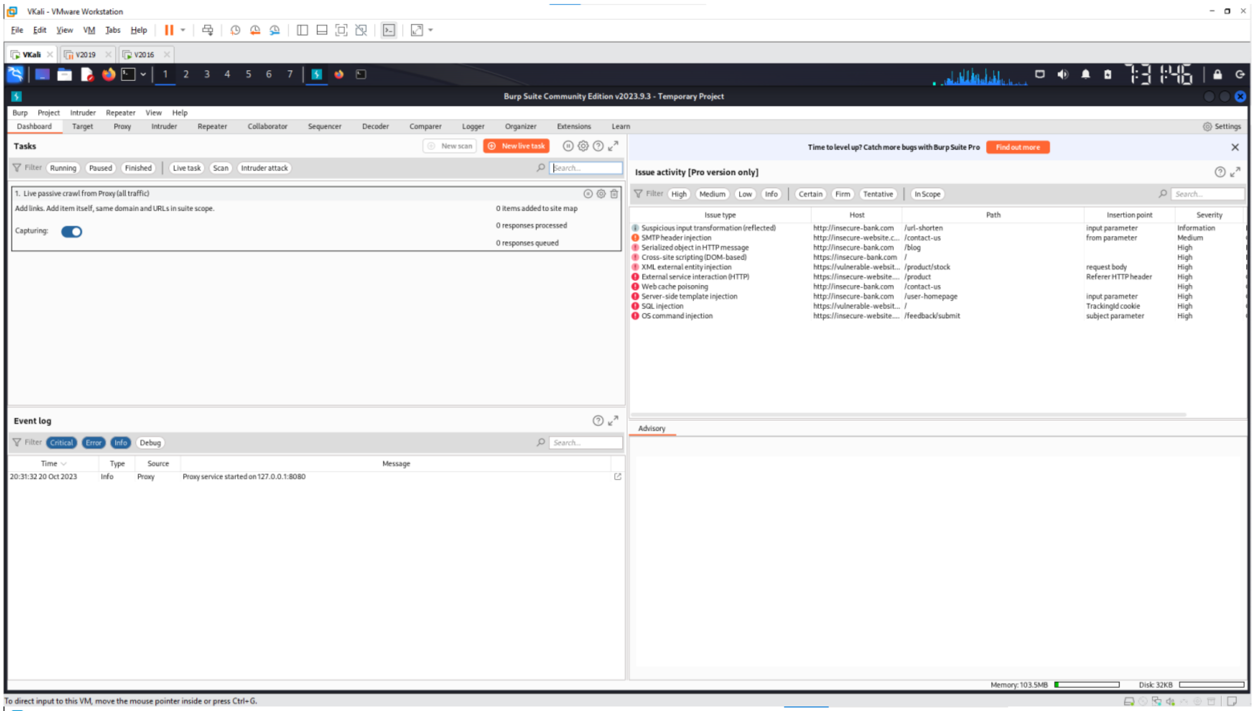
Remove security headers □

Toolbox □

New container tab

Username or Email Address

Password



VKali - VMware Workstation

Burp Suite Community Edition v2023.9.3 - Temporary Project

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Filter High Medium Low Info Certain Firm Tentative In Scope
Advisory

Tasks

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

Issue activity [Pro version only]

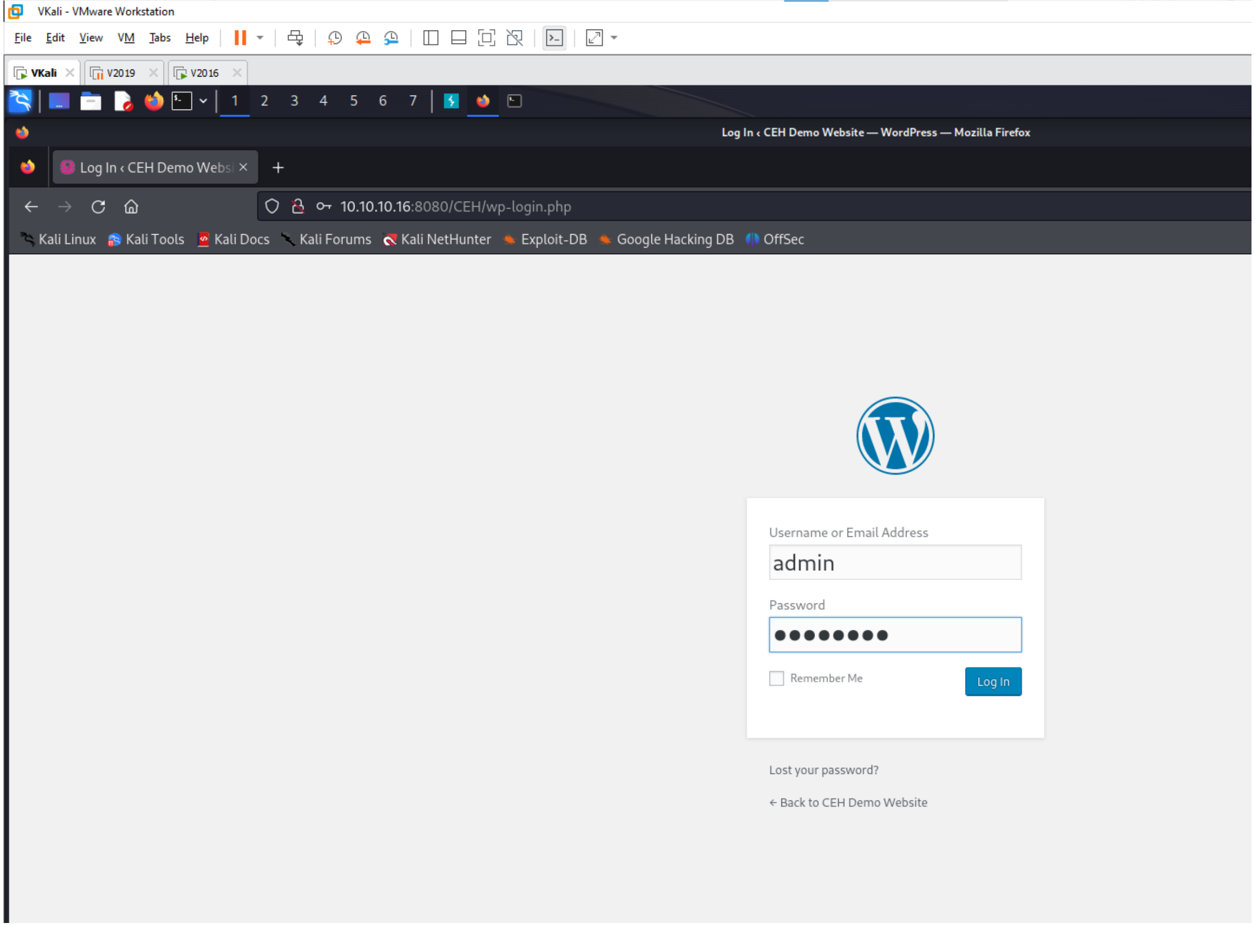
Issue type	Host	Path	Insertion point	Severity
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten	input parameter	Information
SMTP header injection	http://insecure-website.c...	/contact-us	from parameter	Medium
Serialized object in HTTP message	http://insecure-bank.com	/blog		High
Cross-site scripting (DOM-based)	https://insecure-bank.com	/		High
XML external entity injection	https://vulnerable-websit...	/product/stock	request body	High
External service interaction (HTTP)	https://insecure-website....	/product	Referer HTTP header	High
Web cache poisoning	http://insecure-bank.com	/contact-us		High
Server-side template injection	http://insecure-bank.com	/user-homepage	input parameter	High
SQL injection	https://vulnerable-websit...	/	TrackingId cookie	High
OS command injection	https://insecure-website....	/feedback/submit	subject parameter	High

Event log

```
Time                  Type   Source   Message
20:31:32 20 Oct 2023  Info   Proxy    Proxy service started on 127.0.0.1:8080
```

Memory: 103.5MB   Disk: 32KB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



VKali - VMware Workstation

Log In ‹ CEH Demo Website — WordPress — Mozilla Firefox

10.10.10.16:8080/CEH/wp-login.php

Username or Email Address

admin

Password

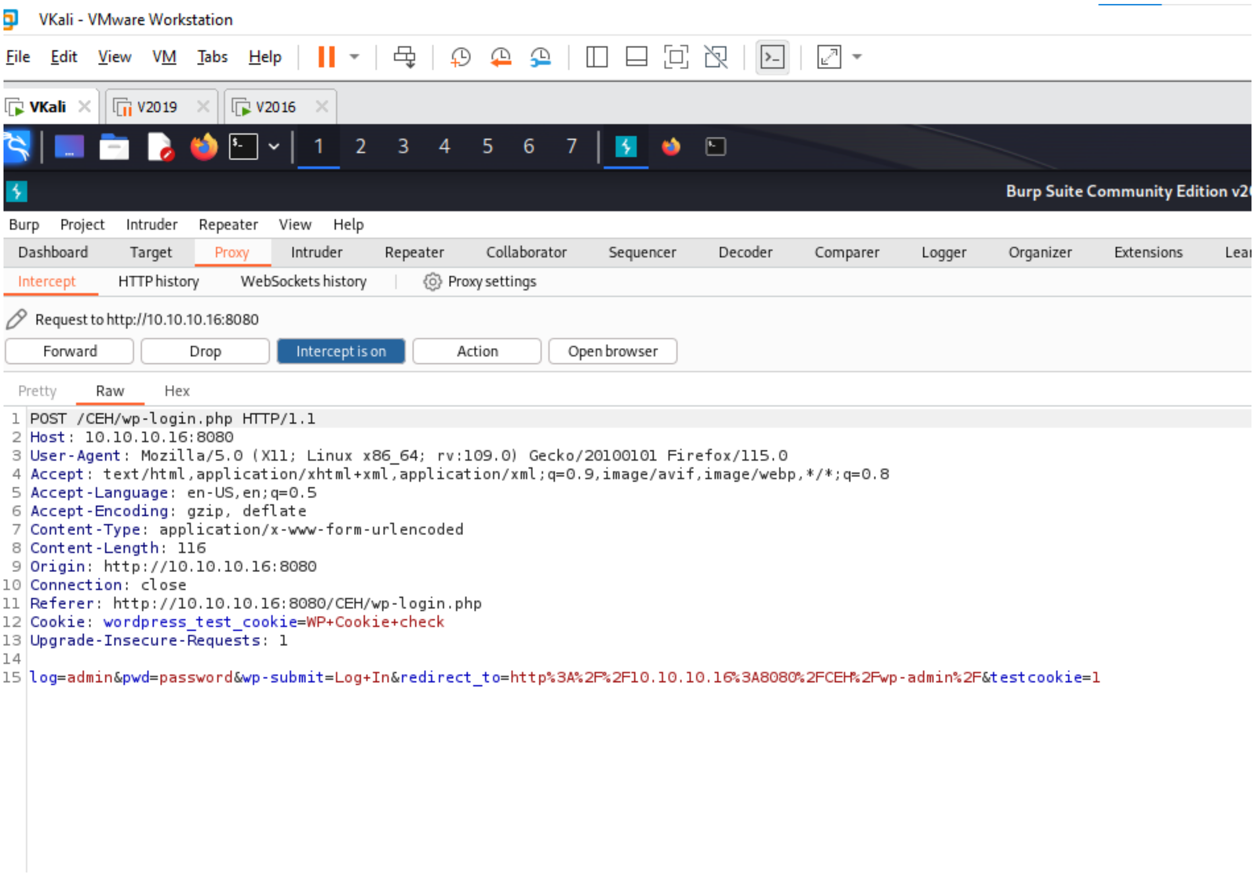
••••••••

□ Remember Me

Log In

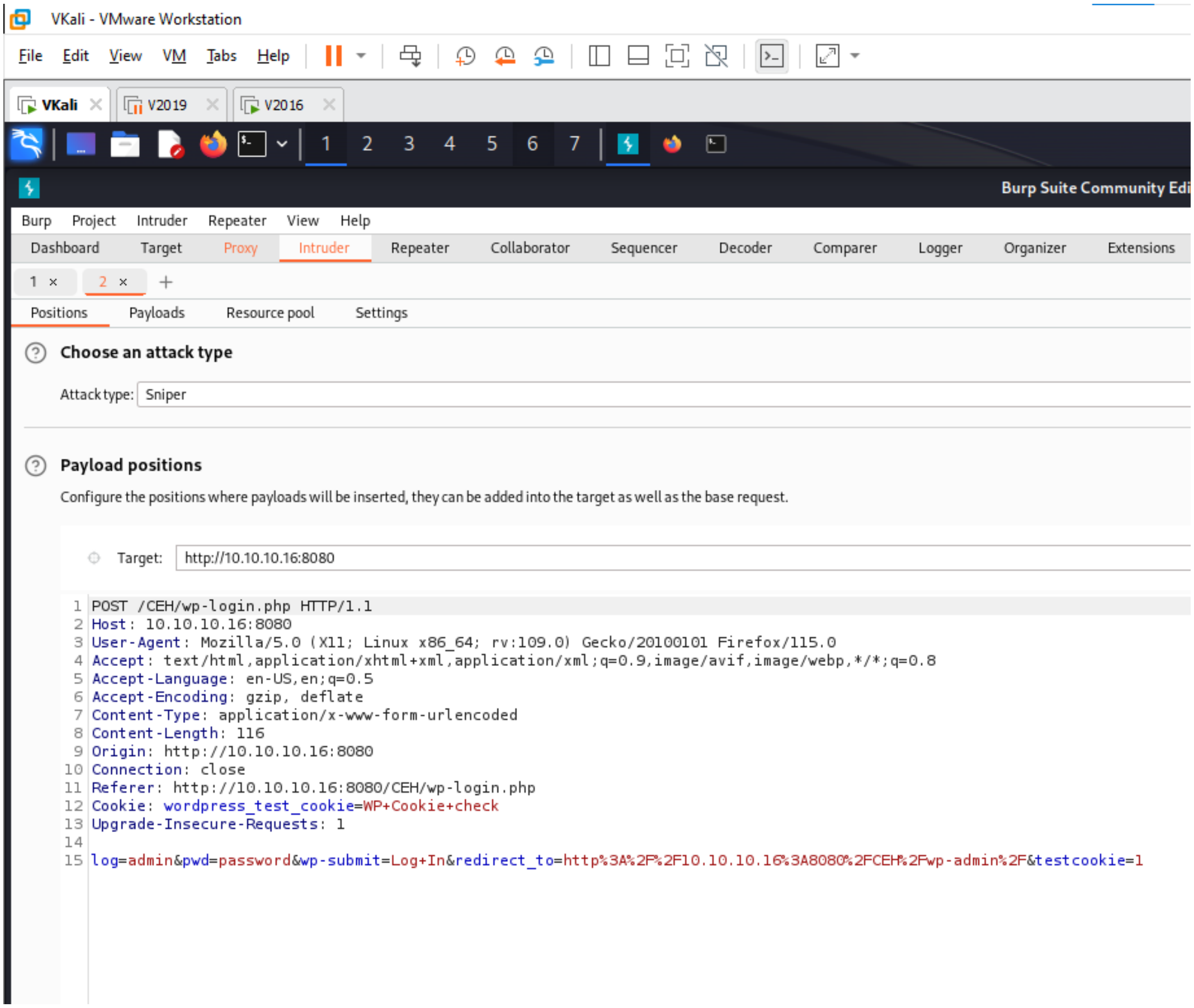
Lost your password?

← Back to CEH Demo Website


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
V2019
V2016
1 2 3 4 5 6 7
Burp Suite Community Edition v2
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Lea
Intercept HTTP history WebSockets history Proxy settings
Request to http://10.10.10.16:8080
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.10.16:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Origin: http://10.10.10.16:8080
Connection: close
Referer: http://10.10.10.16:8080/CEH/wp-login.php
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.10.16%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali V2019 V2016
1 2 3 4 5 6 7
Burp Suite Community Edi
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
1 × 2 × +
Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

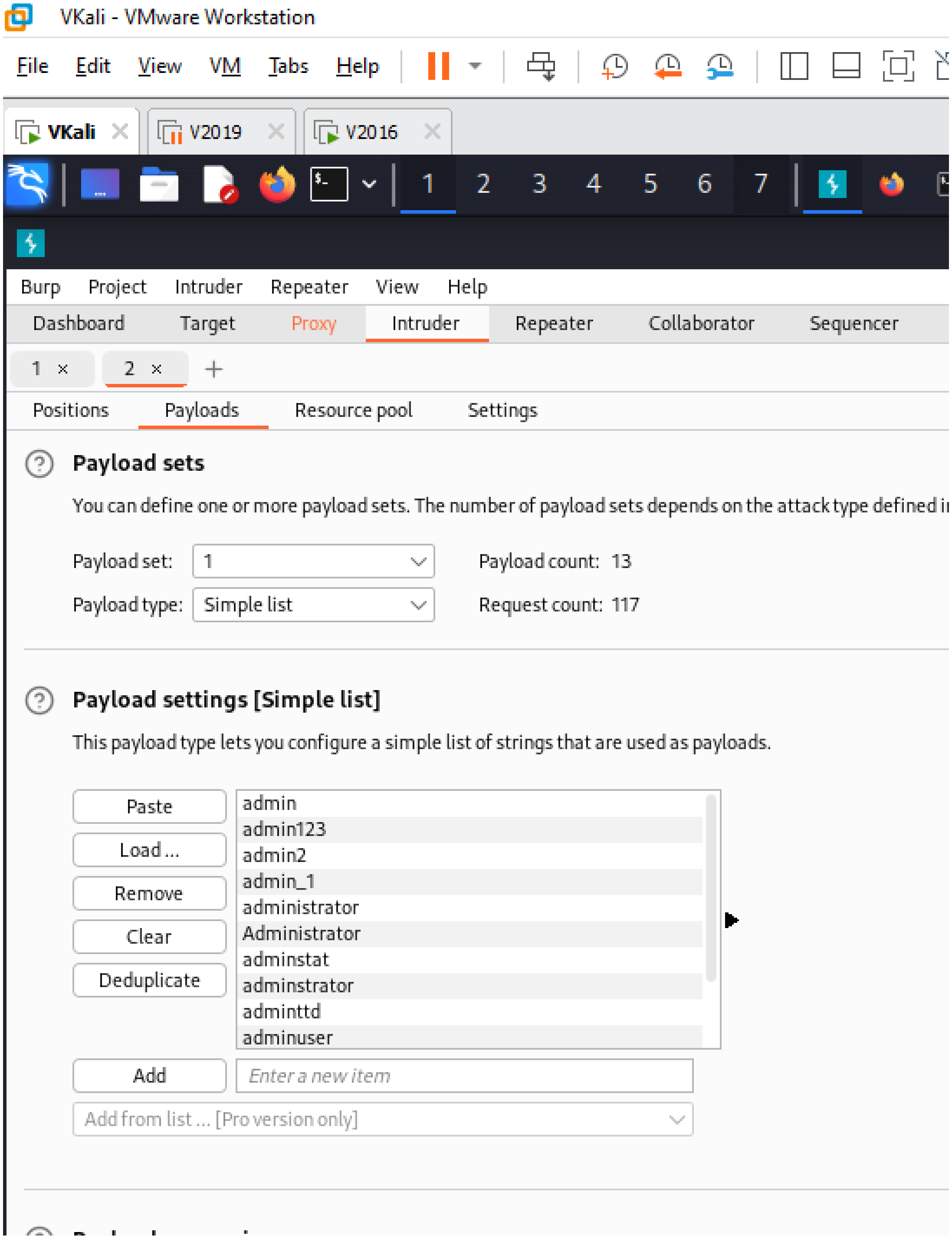
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.10.16:8080

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.10.16:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Origin: http://10.10.10.16:8080
Connection: close
Referer: http://10.10.10.16:8080/CEH/wp-login.php
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.10.16%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali V2019 V2016
1 2 3 4 5 6 7
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer
1 × 2 × +
Positions Payloads Resource pool Settings
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined i

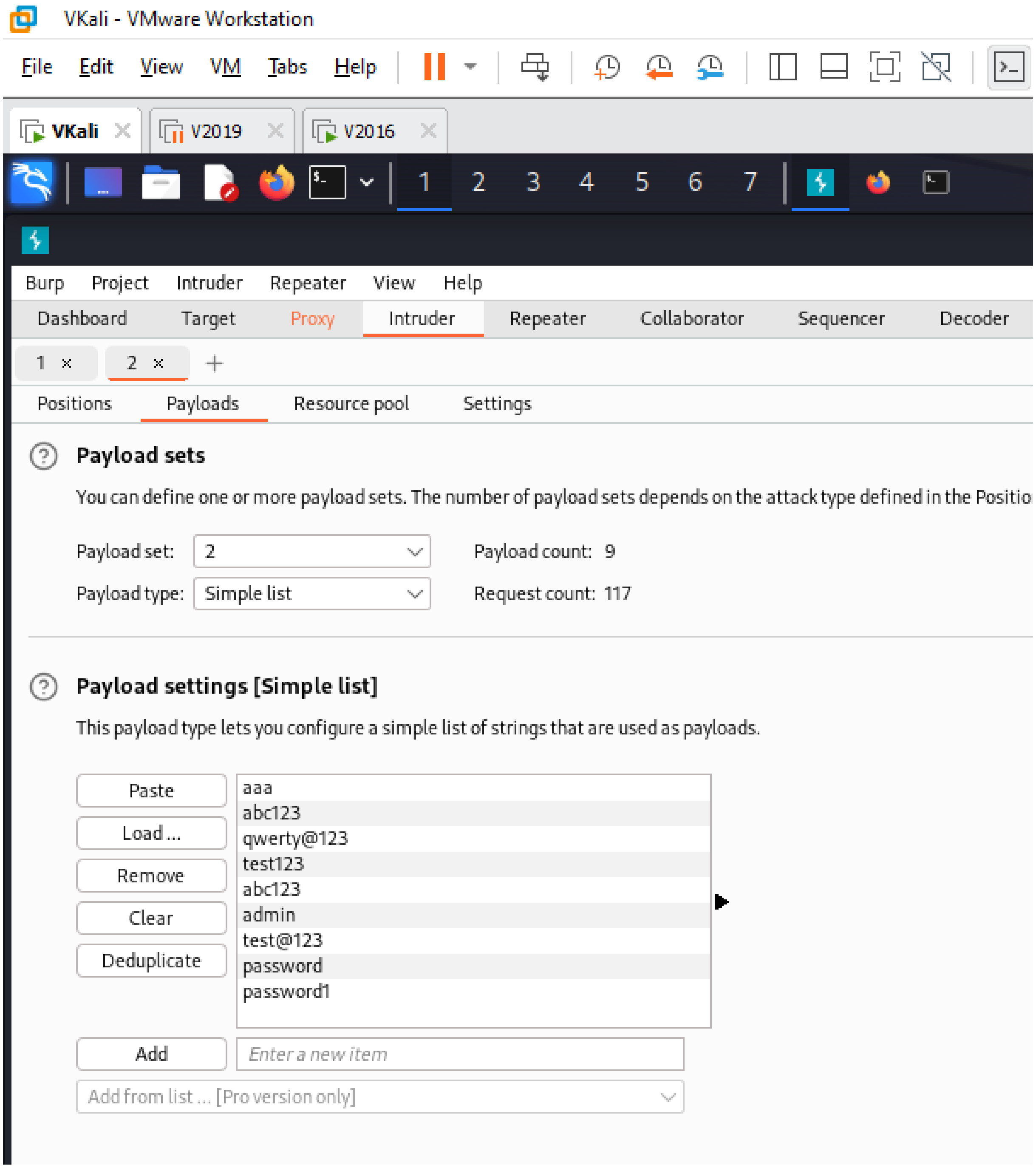
Payload set: 1 Payload count: 13

Payload type: Simple list Request count: 117

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
admin123
admin2
admin_1
administrator
Administrator
adminstat
adminstrator
adminttd
adminuser
```


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
V2019
V2016
1 2 3 4 5 6 7
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
1 × 2 × +
Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positio

Payload set: 2

Payload count: 9

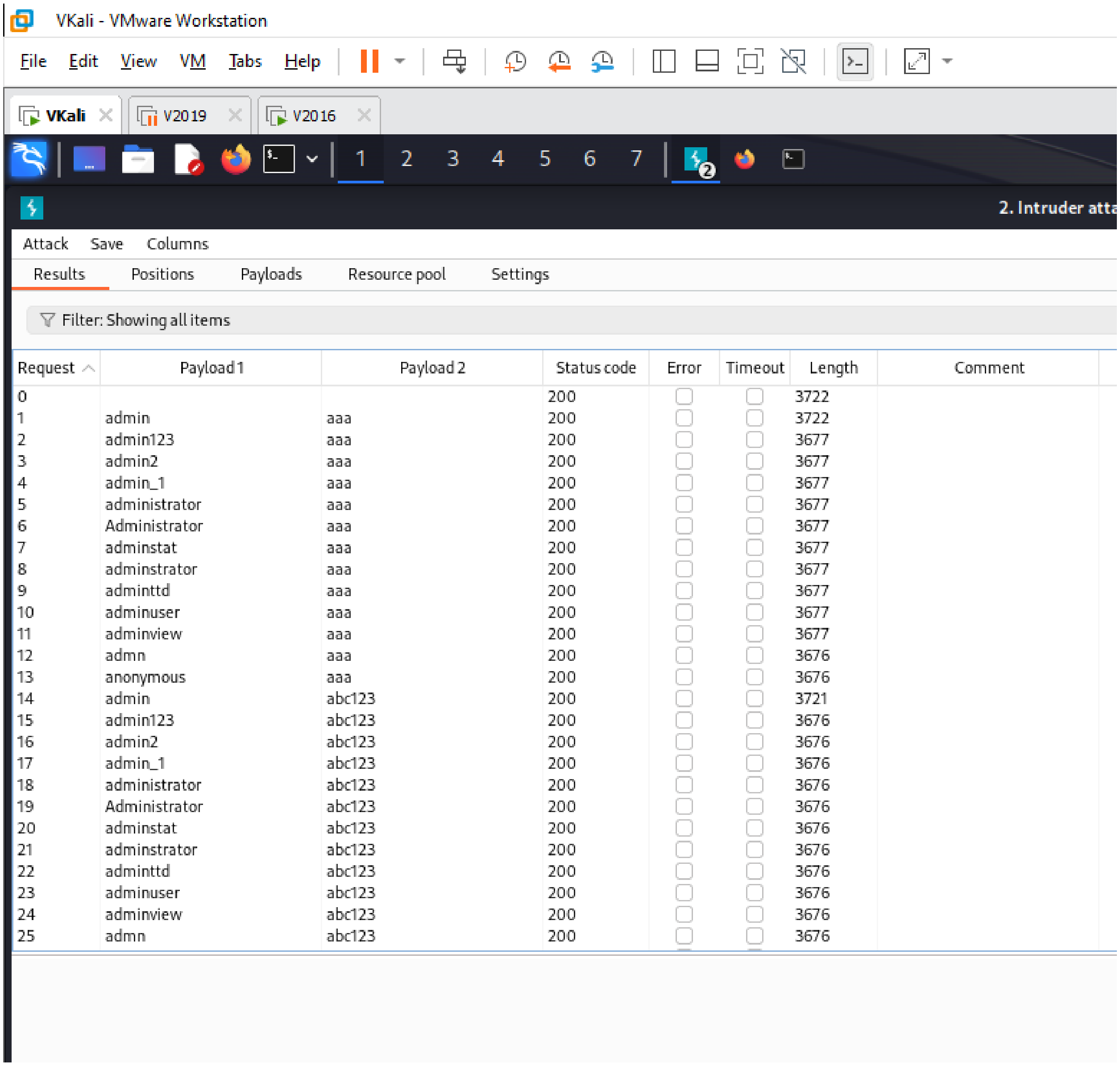
Payload type: Simple list

Request count: 117

Payload settings [Simple list]

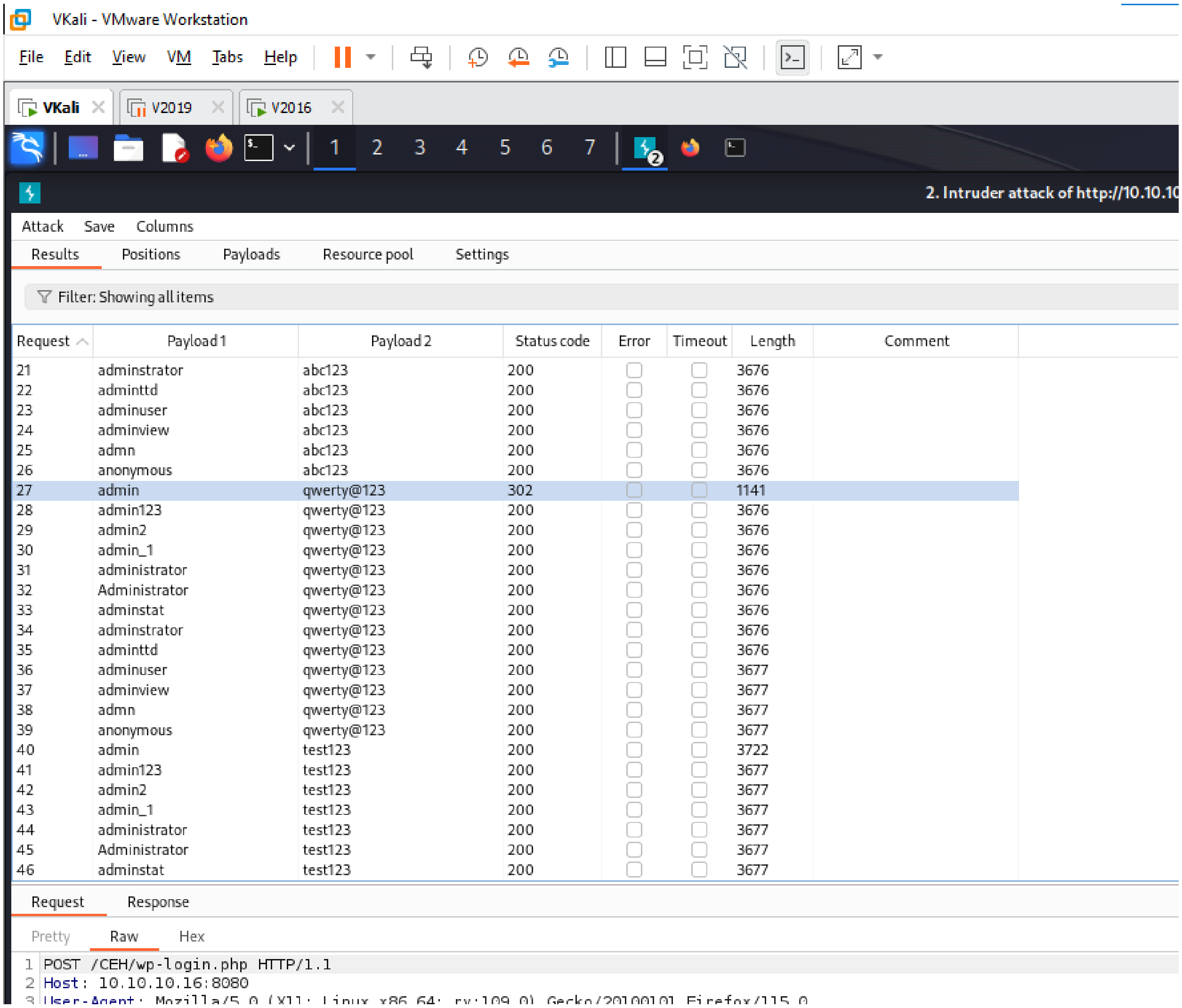
This payload type lets you configure a simple list of strings that are used as payloads.

```
aaa
abc123
qwerty@123
test123
abc123
admin
test@123
password
password1
```



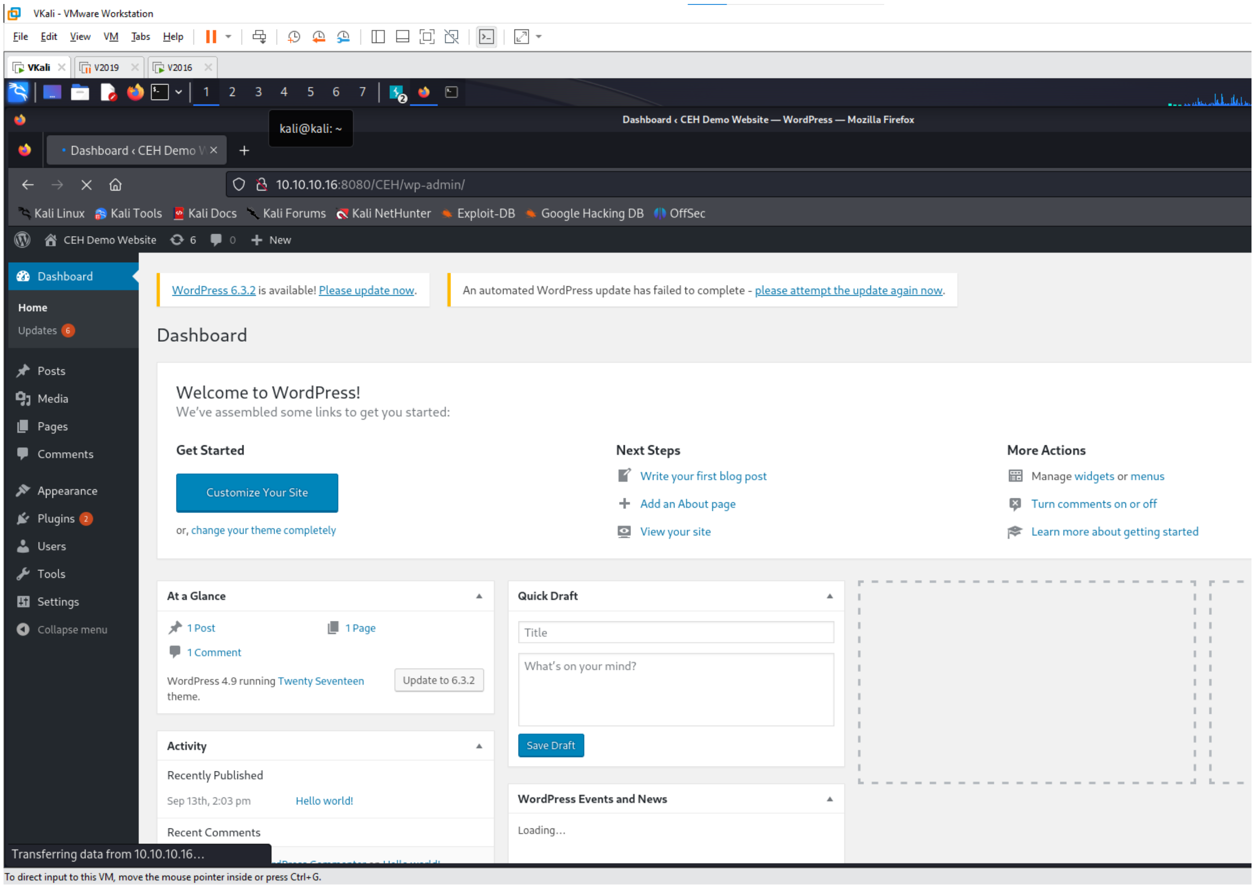
VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
V2019
V2016
1 2 3 4 5 6 7
2. Intruder atta
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	☐	☐	3722	
1	admin	aaa	200	☐	☐	3722	
2	admin123	aaa	200	☐	☐	3677	
3	admin2	aaa	200	☐	☐	3677	
4	admin_1	aaa	200	☐	☐	3677	
5	administrator	aaa	200	☐	☐	3677	
6	Administrator	aaa	200	☐	☐	3677	
7	adminstat	aaa	200	☐	☐	3677	
8	adminstrator	aaa	200	☐	☐	3677	
9	adminttd	aaa	200	☐	☐	3677	
10	adminuser	aaa	200	☐	☐	3677	
11	adminview	aaa	200	☐	☐	3677	
12	admn	aaa	200	☐	☐	3676	
13	anonymous	aaa	200	☐	☐	3676	
14	admin	abc123	200	☐	☐	3721	
15	admin123	abc123	200	☐	☐	3676	
16	admin2	abc123	200	☐	☐	3676	
17	admin_1	abc123	200	☐	☐	3676	
18	administrator	abc123	200	☐	☐	3676	
19	Administrator	abc123	200	☐	☐	3676	
20	adminstat	abc123	200	☐	☐	3676	
21	adminstrator	abc123	200	☐	☐	3676	
22	adminttd	abc123	200	☐	☐	3676	
23	adminuser	abc123	200	☐	☐	3676	
24	adminview	abc123	200	☐	☐	3676	
25	admn	abc123	200	☐	☐	3676	



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
21	adminstrator	abc123	200	☐	☐	3676	
22	adminttd	abc123	200	☐	☐	3676	
23	adminuser	abc123	200	☐	☐	3676	
24	adminview	abc123	200	☐	☐	3676	
25	admn	abc123	200	☐	☐	3676	
26	anonymous	abc123	200	☐	☐	3676	
27	admin	qwerty@123	302	☐	☐	1141	
28	admin123	qwerty@123	200	☐	☐	3676	
29	admin2	qwerty@123	200	☐	☐	3676	
30	admin_1	qwerty@123	200	☐	☐	3676	
31	administrator	qwerty@123	200	☐	☐	3676	
32	Administrator	qwerty@123	200	☐	☐	3676	
33	adminstat	qwerty@123	200	☐	☐	3676	
34	adminstrator	qwerty@123	200	☐	☐	3676	
35	adminttd	qwerty@123	200	☐	☐	3676	
36	adminuser	qwerty@123	200	☐	☐	3677	
37	adminview	qwerty@123	200	☐	☐	3677	
38	admn	qwerty@123	200	☐	☐	3677	
39	anonymous	qwerty@123	200	☐	☐	3677	
40	admin	test123	200	☐	☐	3722	
41	admin123	test123	200	☐	☐	3677	
42	admin2	test123	200	☐	☐	3677	
43	admin_1	test123	200	☐	☐	3677	
44	administrator	test123	200	☐	☐	3677	
45	Administrator	test123	200	☐	☐	3677	
46	adminstat	test123	200	☐	☐	3677	

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.10.16:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```



WordPress 6.3.2 is available! Please update now.

An automated WordPress update has failed to complete - please attempt the update again now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

WordPress 4.9 running Twenty Seventeen theme.

Sep 13th, 2:03 pm Hello world!

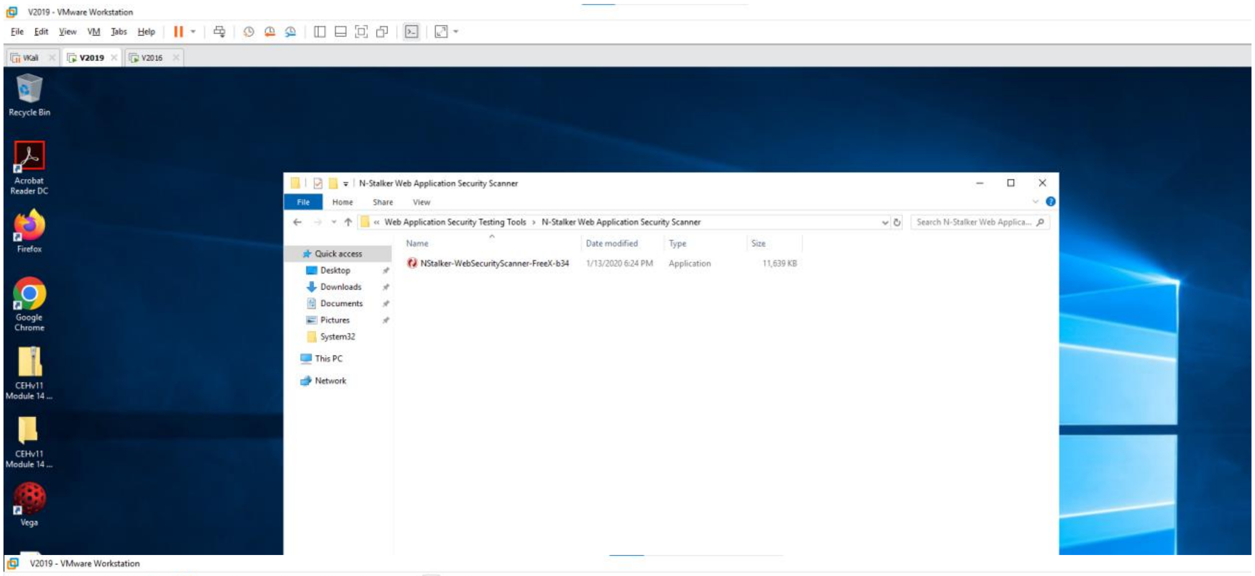
Transferring data from 10.10.10.16…

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

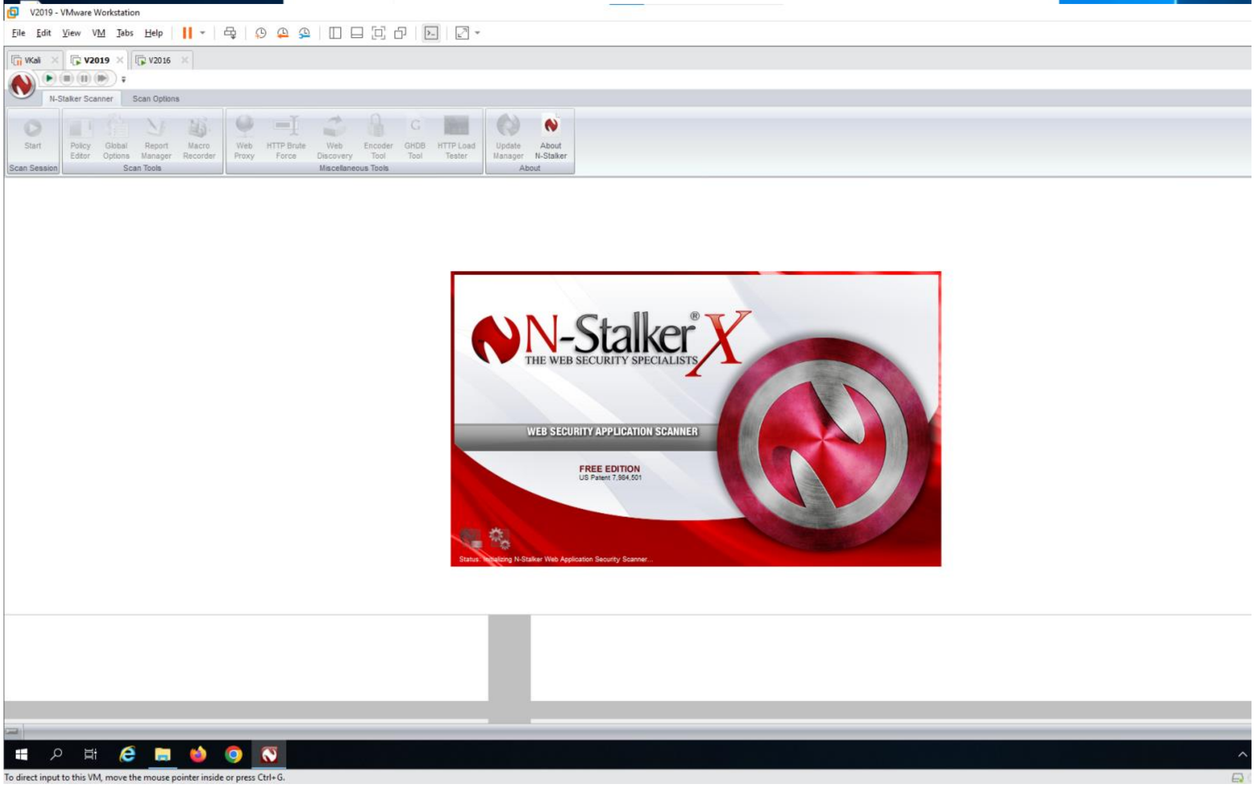
3. Detect Web Application Vulnerabilities using Various Web Application Security Tools

3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

- Open Windows 10 and Windows Server 2019

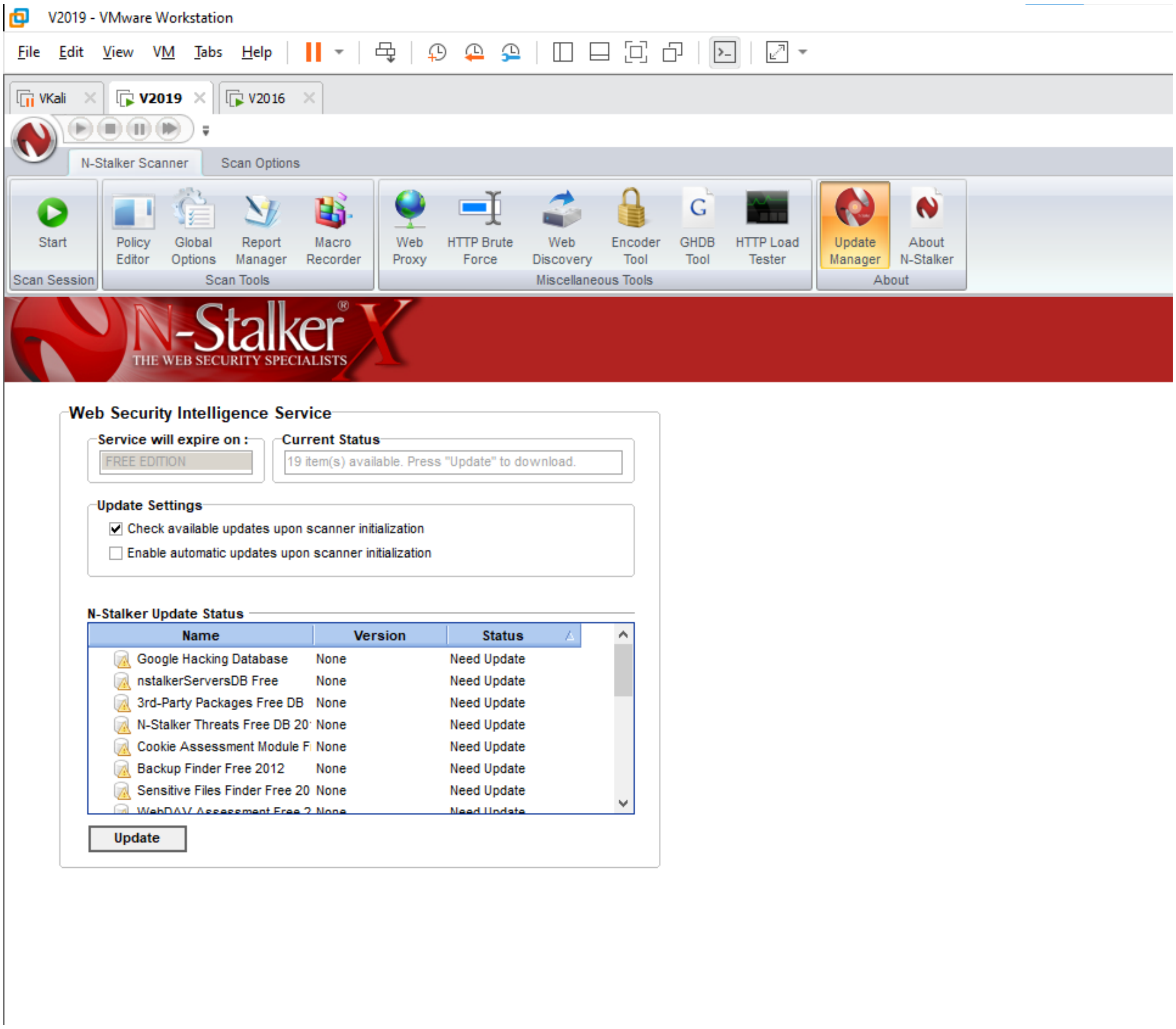

V2019 - VMware Workstation
File Edit View VM Tabs Help
VKali
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module 14 ...
CEHv11 Module 14 ...
Vega
N-Stalker Web Application Security Scanner
File
Home
Share
View
« Web Application Security Testing Tools › N-Stalker Web Application Security Scanner
Search N-Stalker Web Applica...
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network

Name	Date modified	Type	Size
NStalker-WebSecurityScanner-FreeX-b34	1/13/2020 6:24 PM	Application	11,639 KB



Status: Initializing N-Stalker Web Application Security Scanner...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: 19 item(s) available. Press "Update" to download.

Update Settings

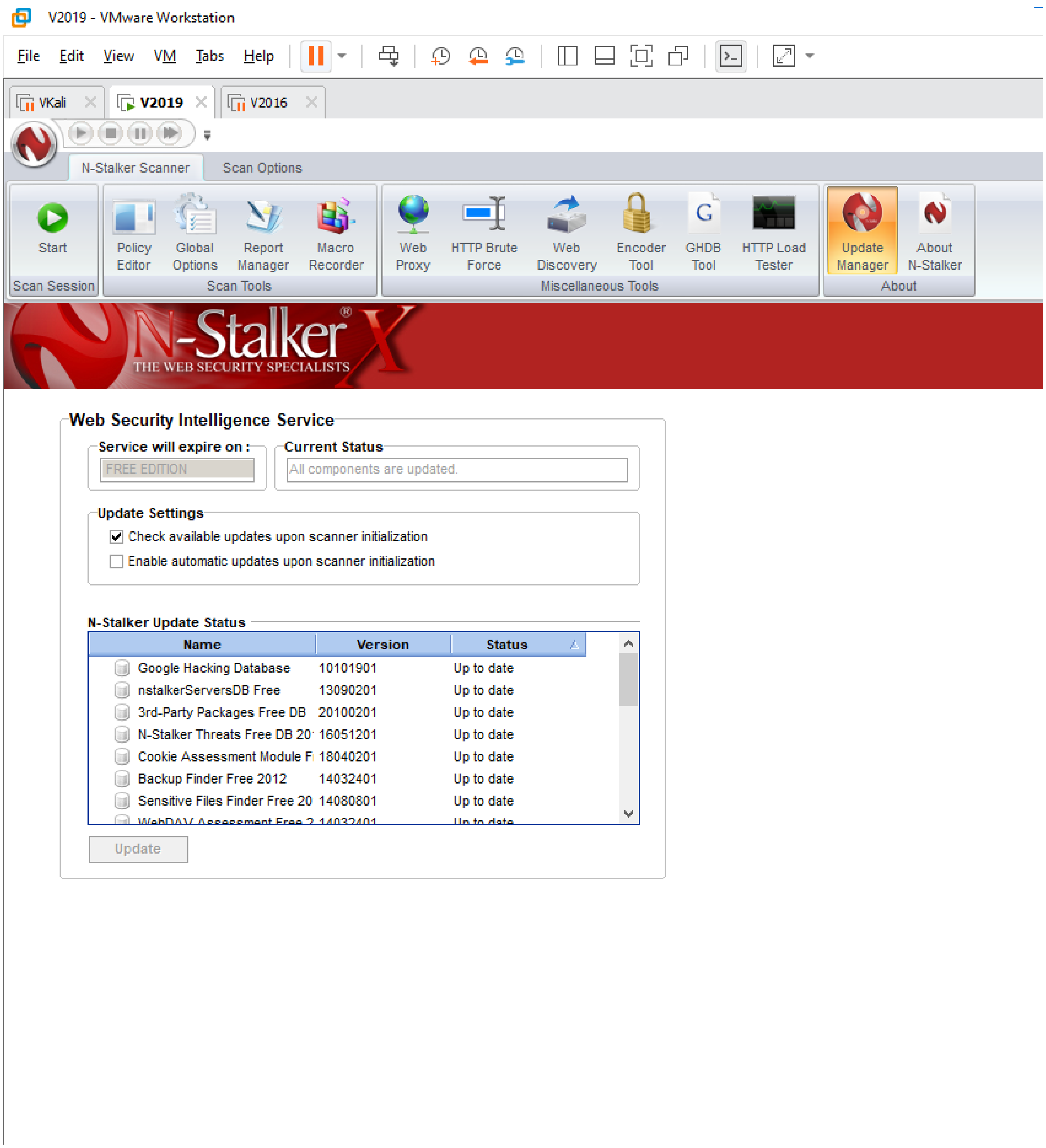
☑ Check available updates upon scanner initialization

□ Enable automatic updates upon scanner initialization

N-Stalker Update Status

Name	Version	Status
Google Hacking Database	None	Need Update
nstalkerServersDB Free	None	Need Update
3rd-Party Packages Free DB	None	Need Update
N-Stalker Threats Free DB 20	None	Need Update
Cookie Assessment Module F	None	Need Update
Backup Finder Free 2012	None	Need Update
Sensitive Files Finder Free 20	None	Need Update
WebDAV Assessment Free 2	None	Need Update

Update



Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: All components are updated.

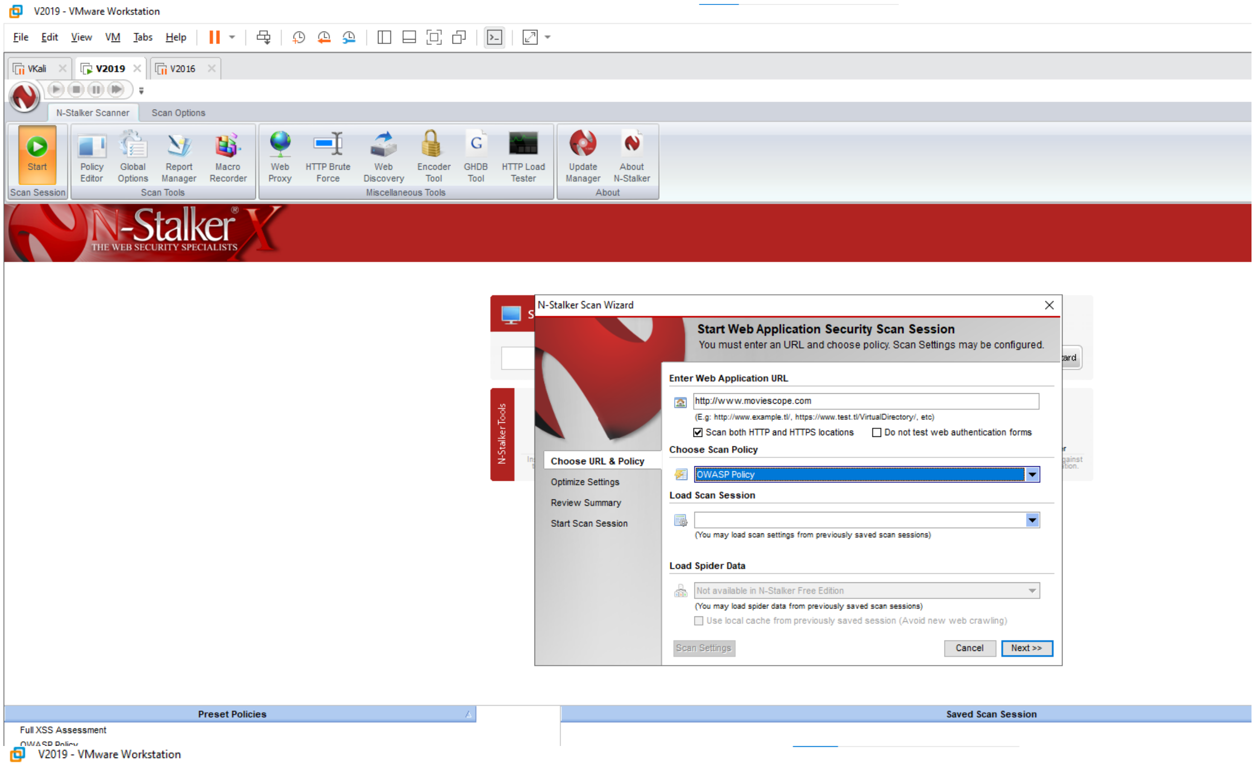
Update Settings

☑ Check available updates upon scanner initialization

☐ Enable automatic updates upon scanner initialization

N-Stalker Update Status

Name	Version	Status
Google Hacking Database	10101901	Up to date
nstalkerServersDB Free	13090201	Up to date
3rd-Party Packages Free DB	20100201	Up to date
N-Stalker Threats Free DB 20	16051201	Up to date
Cookie Assessment Module F	18040201	Up to date
Backup Finder Free 2012	14032401	Up to date
Sensitive Files Finder Free 20	14080801	Up to date
WebDAV Assessment Free 2	14032401	Up to date



N-Stalker Scan Wizard

Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Enter Web Application URL

http://www.moviescope.com

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

☑ Scan both HTTP and HTTPS locations ☐ Do not test web authentication forms

Choose Scan Policy

OWASP Policy

Load Scan Session

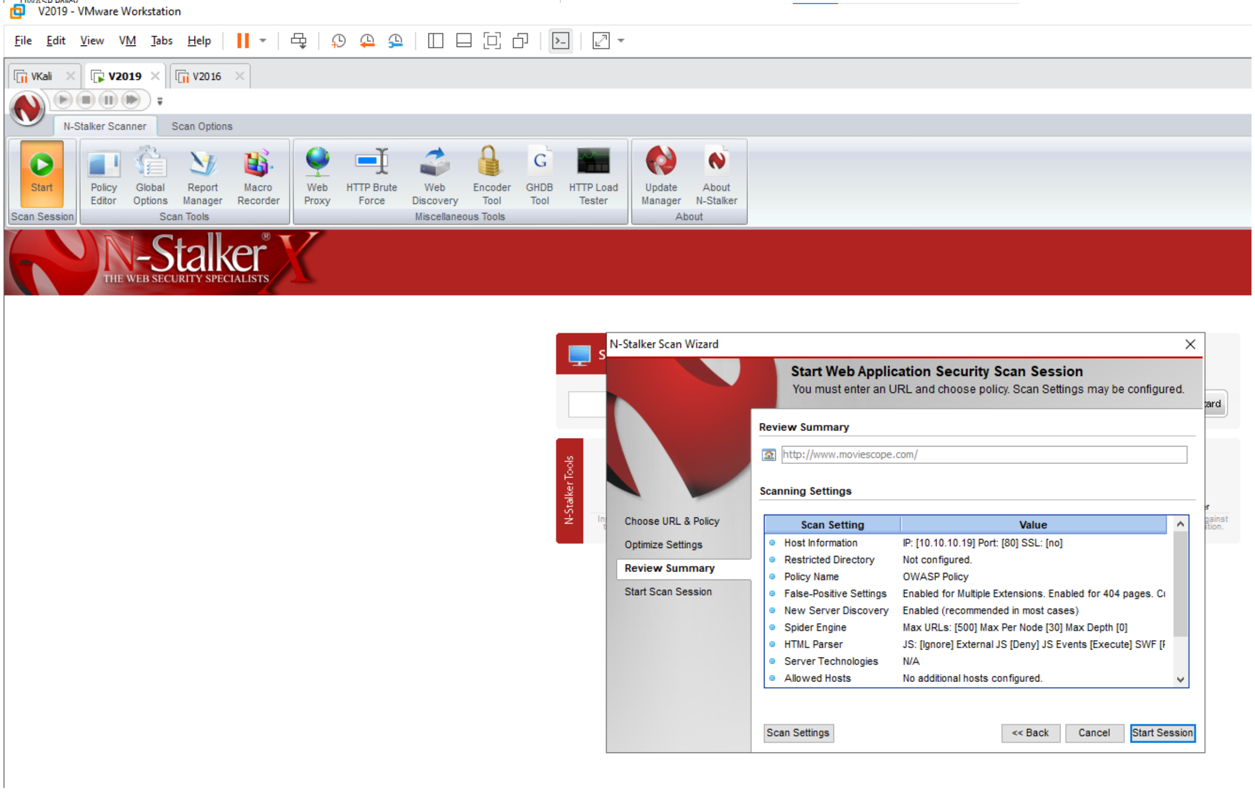
(You may load scan settings from previously saved scan sessions)

Load Spider Data

Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

☐ Use local cache from previously saved session (Avoid new web crawling)



N-Stalker Scan Wizard

Start Web Application Security Scan Session

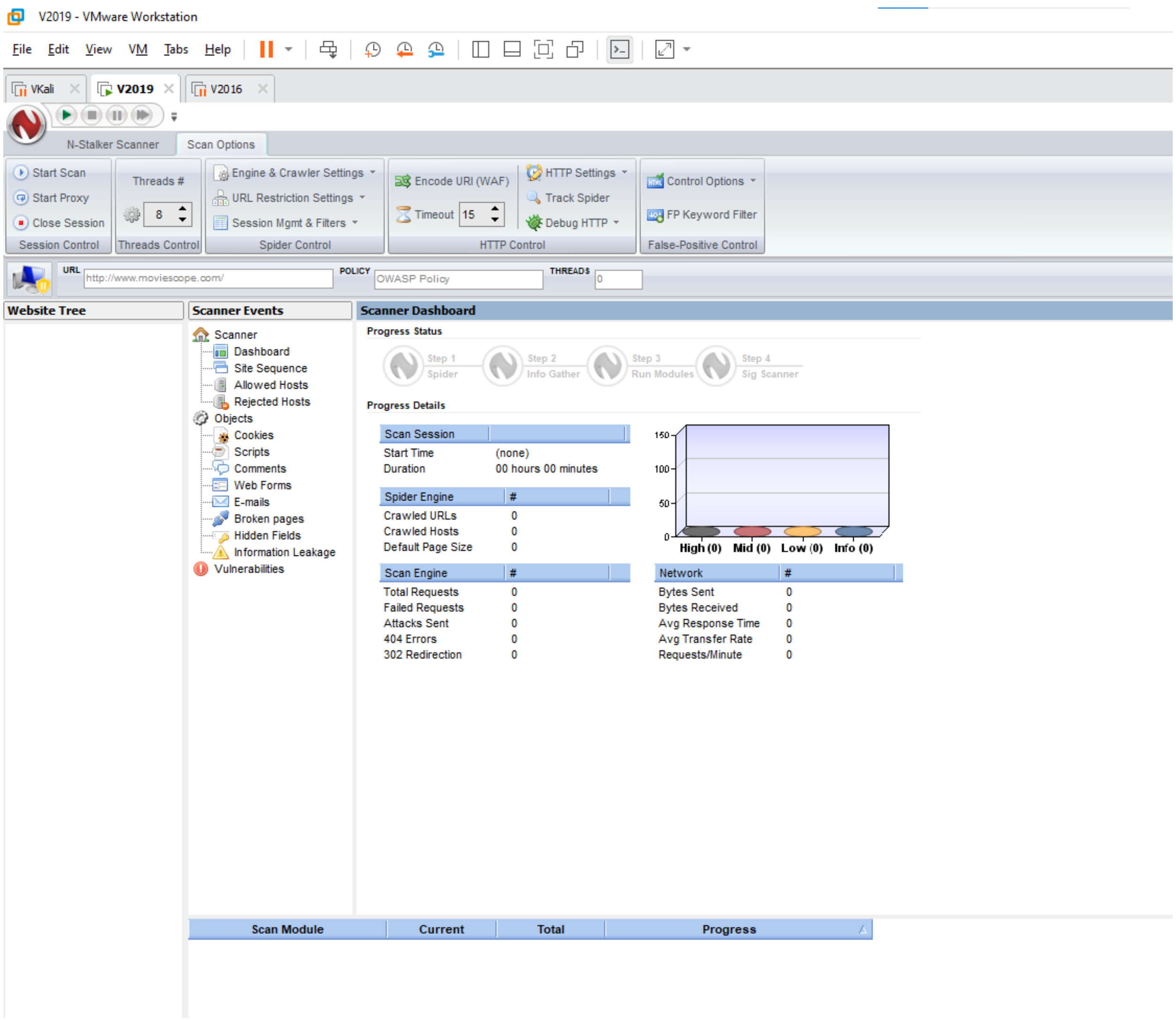
You must enter an URL and choose policy. Scan Settings may be configured.

Review Summary

http://www.moviescope.com/

Scanning Settings

Scan Setting	Value
Host Information	IP: [10.10.10.19] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	OWASP Policy
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. C
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Ignore] External JS [Deny] JS Events [Execute] SWF [F
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.



Threads # 8

Timeout 15

URL http://www.moviescope.com/

POLICY OWASP Policy

THREADS 0

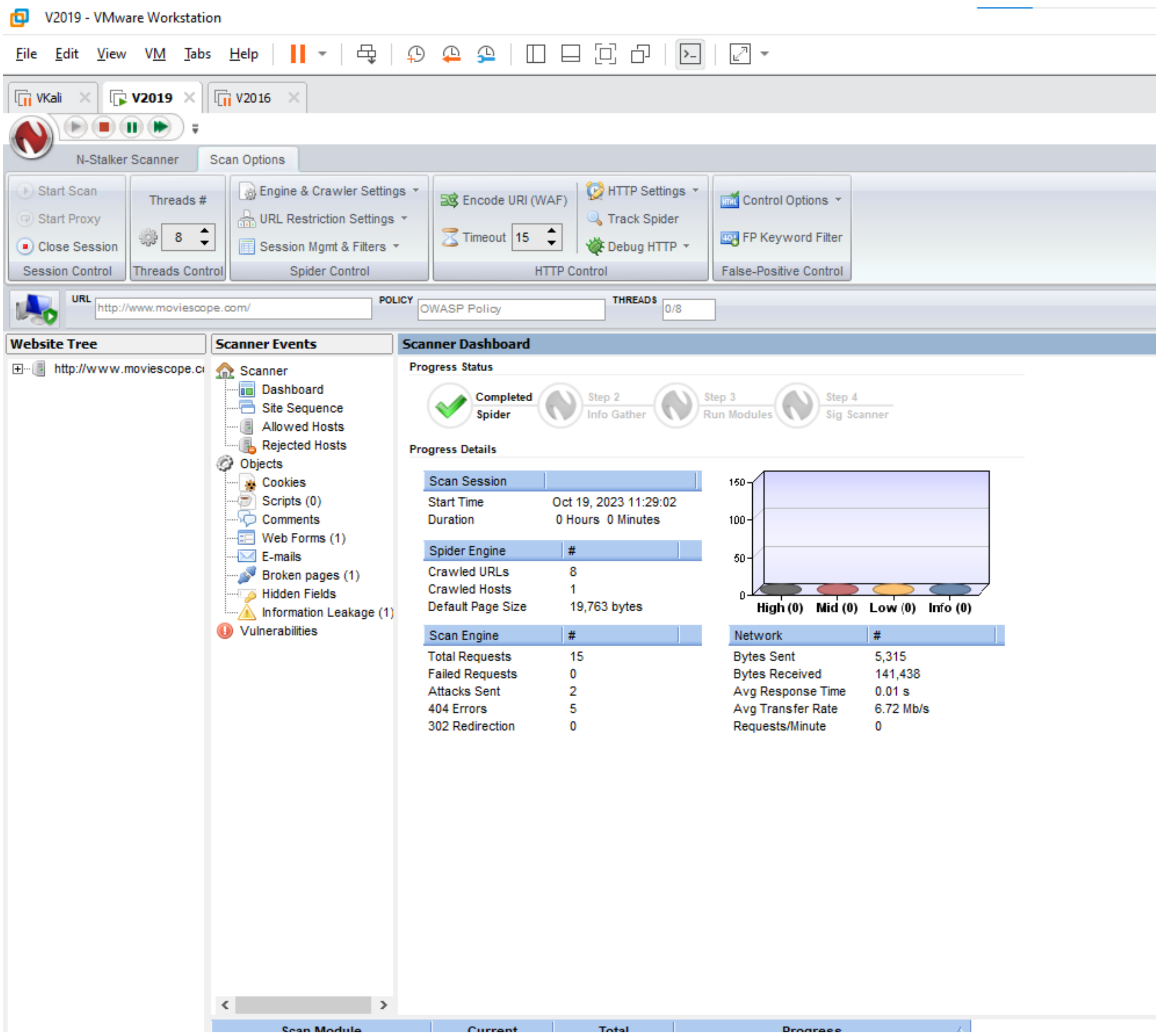
Scan Session	
Start Time	(none)
Duration	00 hours 00 minutes

Spider Engine	#
Crawled URLs	0
Crawled Hosts	0
Default Page Size	0

Scan Engine	#
Total Requests	0
Failed Requests	0
Attacks Sent	0
404 Errors	0
302 Redirection	0

Network	#
Bytes Sent	0
Bytes Received	0
Avg Response Time	0
Avg Transfer Rate	0
Requests/Minute	0

Scan Module	Current	Total	Progress



Threads #: 8

Timeout: 15

URL: http://www.moviescope.com/

POLICY: OWASP Policy

THREADS: 0/8

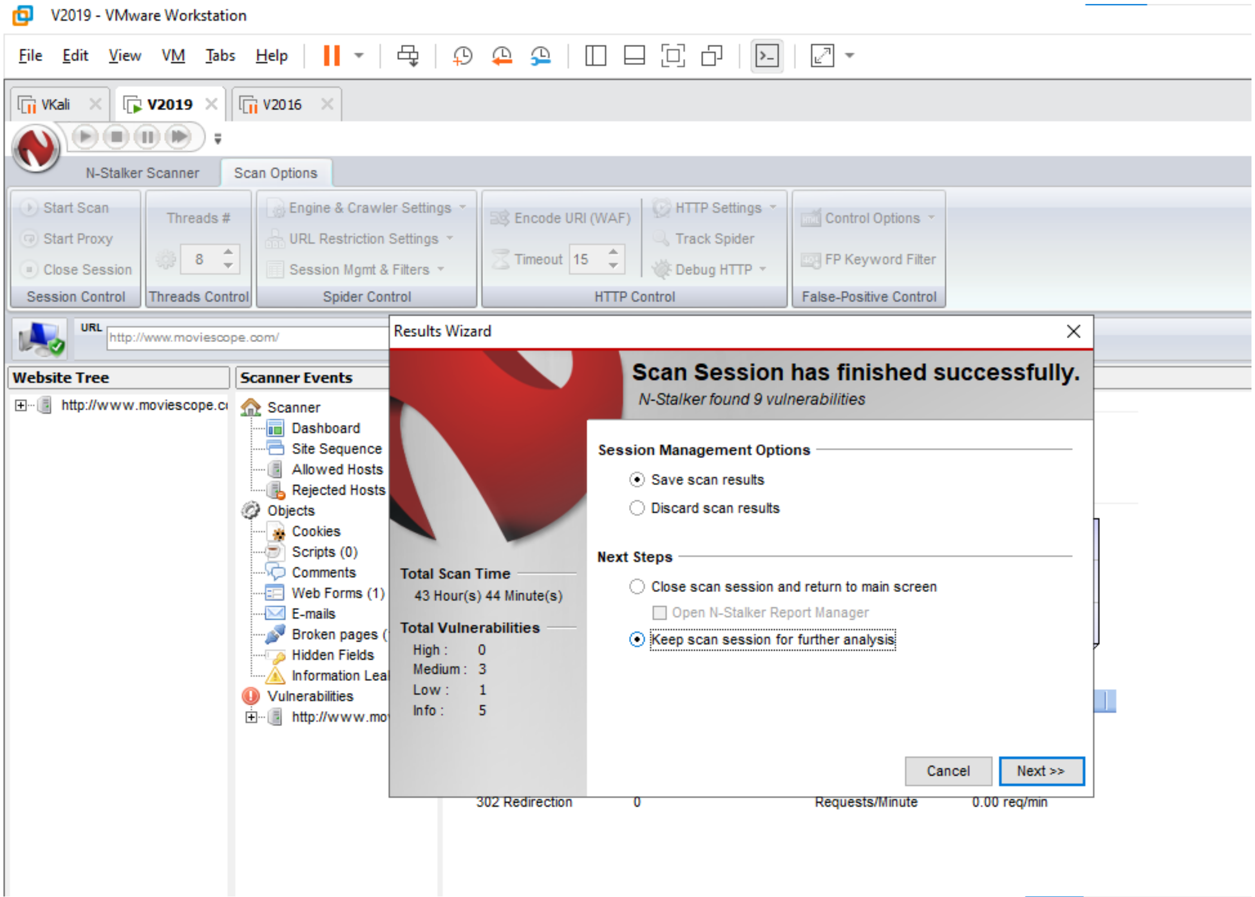
http://www.moviescope.c

Scan Session	
Start Time	Oct 19, 2023 11:29:02
Duration	0 Hours 0 Minutes

Spider Engine	#
Crawled URLs	8
Crawled Hosts	1
Default Page Size	19,763 bytes

Scan Engine	#
Total Requests	15
Failed Requests	0
Attacks Sent	2
404 Errors	5
302 Redirection	0

Network	#
Bytes Sent	5,315
Bytes Received	141,438
Avg Response Time	0.01 s
Avg Transfer Rate	6.72 Mb/s
Requests/Minute	0


V2019 - VMware Workstation
File Edit View VM Tabs Help
VKali V2019 V2016
N-Stalker Scanner Scan Options
Start Scan Start Proxy Close Session Session Control
Threads # 8 Threads Control
Engine & Crawler Settings URL Restriction Settings Session Mgmt & Filters Spider Control
Encode URI (WAF) Timeout 15 HTTP Settings Track Spider Debug HTTP HTTP Control
Control Options FP Keyword Filter False-Positive Control
URL http://www.moviescope.com/
Website Tree
http://www.moviescope.c
Scanner Events
Scanner Dashboard Site Sequence Allowed Hosts Rejected Hosts
Objects Cookies Scripts (0) Comments Web Forms (1) E-mails Broken pages (Hidden Fields Information Lea
Vulnerabilities http://www.mo
302 Redirection 0 Requests/Minute 0.00 req/min

Results Wizard

Scan Session has finished successfully.

N-Stalker found 9 vulnerabilities

Total Scan Time

43 Hour(s) 44 Minute(s)

Total Vulnerabilities

High :	0
Medium :	3
Low :	1
Info :	5

Session Management Options

● Save scan results

○ Discard scan results

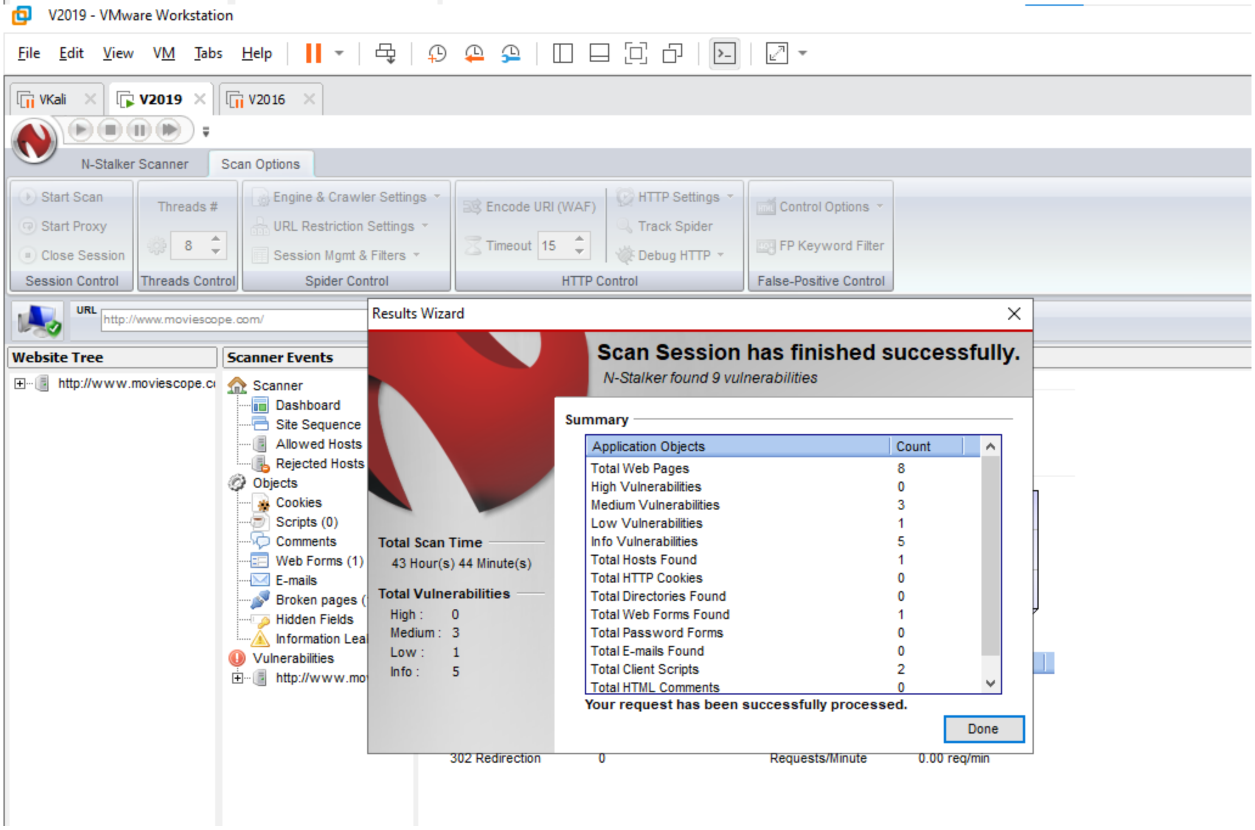
Next Steps

○ Close scan session and return to main screen

□ Open N-Stalker Report Manager

● Keep scan session for further analysis

Cancel Next >>


V2019 - VMware Workstation
File Edit View VM Tabs Help
VKali V2019 V2016
N-Stalker Scanner Scan Options
Start Scan Start Proxy Close Session Session Control
Threads # 8 Threads Control
Engine & Crawler Settings URL Restriction Settings Session Mgmt & Filters Spider Control
Encode URI (WAF) Timeout 15 HTTP Settings Track Spider Debug HTTP HTTP Control
Control Options FP Keyword Filter False-Positive Control
URL http://www.moviescope.com/
Website Tree
http://www.moviescope.c
Scanner Events
Scanner Dashboard Site Sequence Allowed Hosts Rejected Hosts
Objects Cookies Scripts (0) Comments Web Forms (1) E-mails Broken pages (Hidden Fields Information Lea
Vulnerabilities http://www.mo
302 Redirection 0 Requests/Minute 0.00 req/min

Results Wizard

Scan Session has finished successfully.

N-Stalker found 9 vulnerabilities

Total Scan Time

43 Hour(s) 44 Minute(s)

Total Vulnerabilities

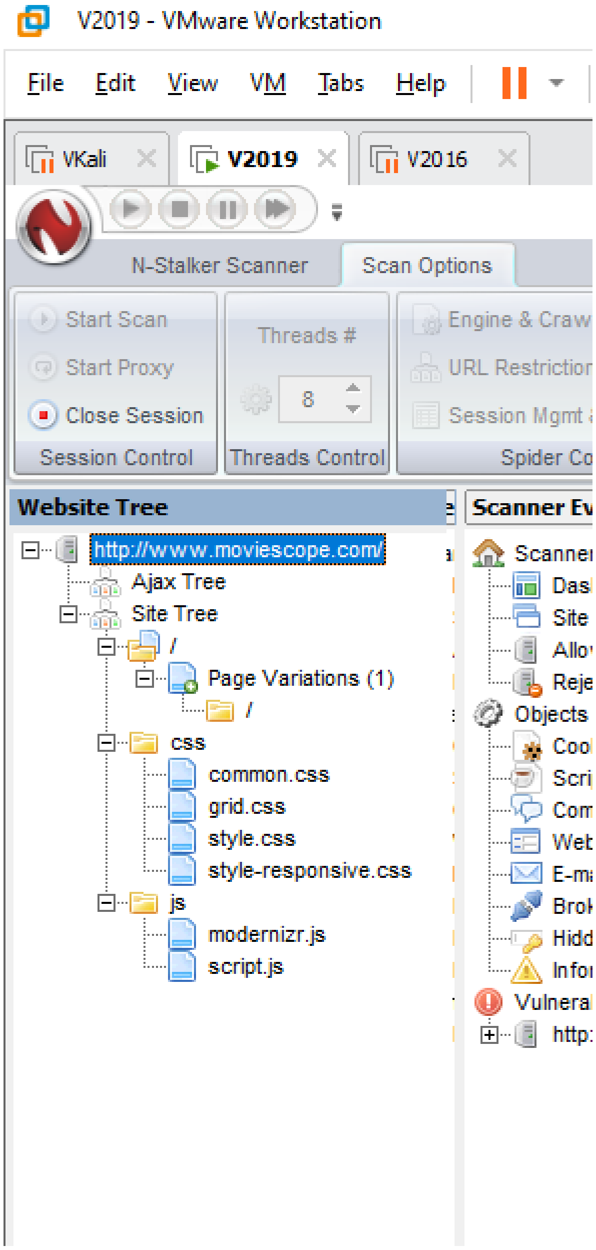
High :	0
Medium :	3
Low :	1
Info :	5

Summary

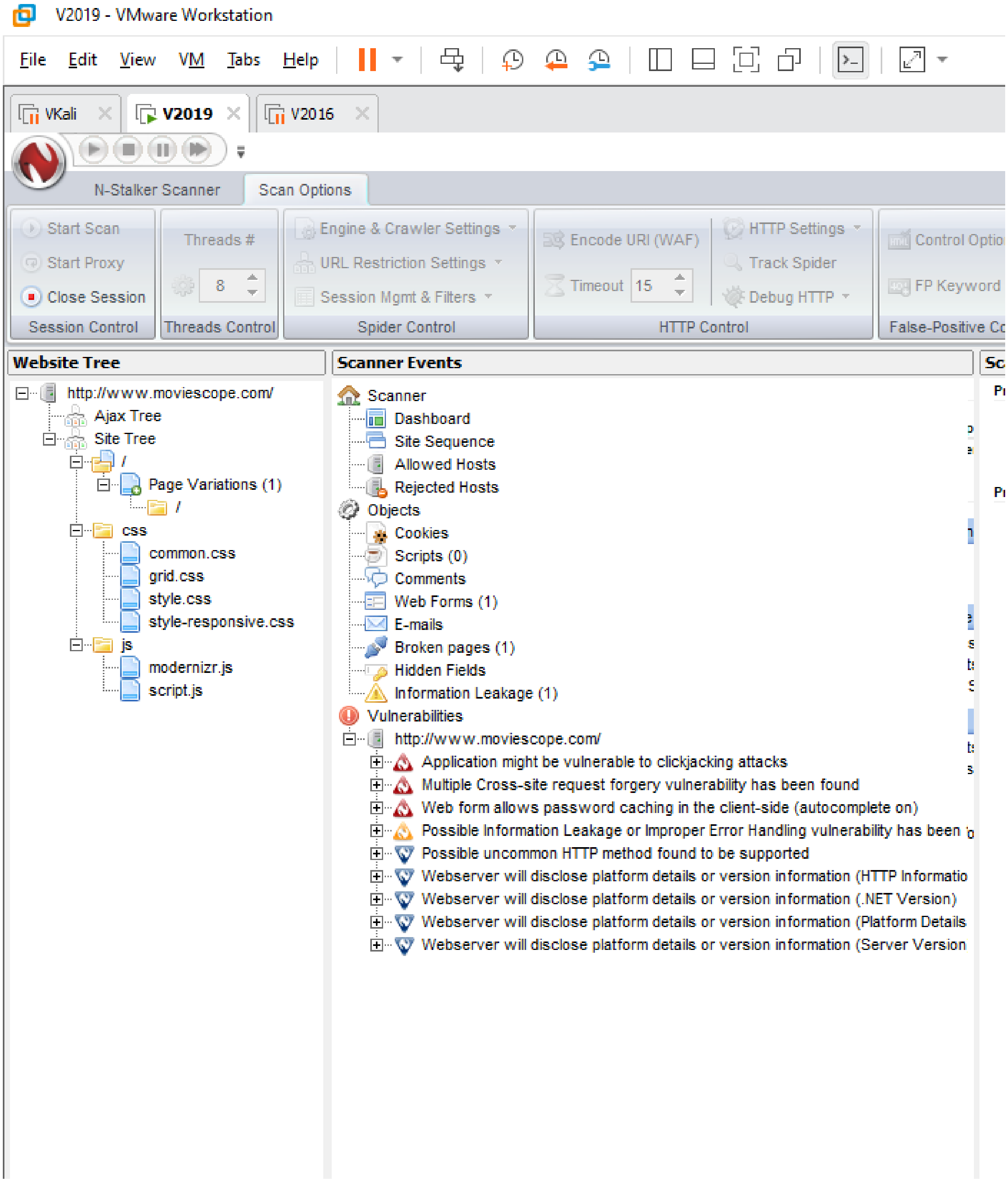
Application Objects	Count
Total Web Pages	8
High Vulnerabilities	0
Medium Vulnerabilities	3
Low Vulnerabilities	1
Info Vulnerabilities	5
Total Hosts Found	1
Total HTTP Cookies	0
Total Directories Found	0
Total Web Forms Found	1
Total Password Forms	0
Total E-mails Found	0
Total Client Scripts	2
Total HTML Comments	0

Your request has been successfully processed.

Done



```
http://www.moviescope.com/
    Ajax Tree
    Site Tree
        /
            Page Variations (1)
                /
        css
            common.css
            grid.css
            style.css
            style-responsive.css
        js
            modernizr.js
            script.js
```

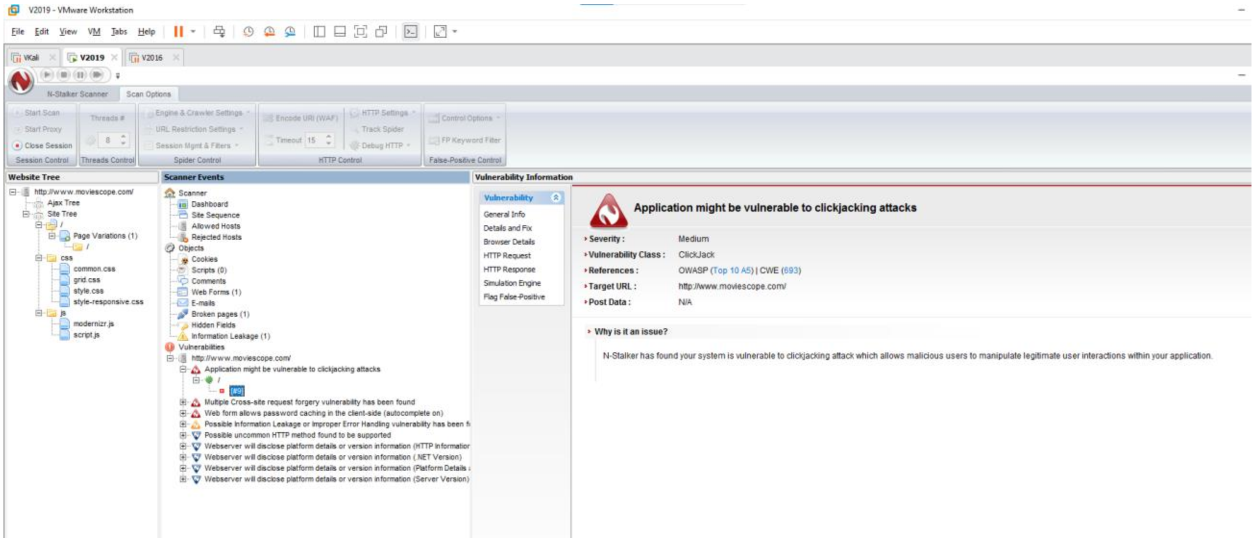


Website Tree

- http://www.moviescope.com/
  - Ajax Tree
  - Site Tree
    - /
      - Page Variations (1)
        - /
    - css
      - common.css
      - grid.css
      - style.css
      - style-responsive.css
    - js
      - modernizr.js
      - script.js

Scanner Events

- Scanner
  - Dashboard
  - Site Sequence
  - Allowed Hosts
  - Rejected Hosts
- Objects
  - Cookies
  - Scripts (0)
  - Comments
  - Web Forms (1)
  - E-mails
  - Broken pages (1)
  - Hidden Fields
  - Information Leakage (1)
- Vulnerabilities
  - http://www.moviescope.com/
    - Application might be vulnerable to clickjacking attacks
    - Multiple Cross-site request forgery vulnerability has been found
    - Web form allows password caching in the client-side (autocomplete on)
    - Possible Information Leakage or Improper Error Handling vulnerability has been
    - Possible uncommon HTTP method found to be supported
    - Webserver will disclose platform details or version information (HTTP Informatio
    - Webserver will disclose platform details or version information (.NET Version)
    - Webserver will disclose platform details or version information (Platform Details
    - Webserver will disclose platform details or version information (Server Version



Website Tree

```
http://www.moviescope.com/
  Ajax Tree
  Site Tree
    /
      Page Variations (1)
        /
    css
      common.css
      grid.css
      style.css
      style-responsive.css
    js
      modernizr.js
      script.js
```

Scanner Events

```
Scanner
  Dashboard
  Site Sequence
  Allowed Hosts
  Rejected Hosts
Objects
  Cookies
  Scripts (0)
  Comments
  Web Forms (1)
  E-mails
  Broken pages (1)
  Hidden Fields
  Information Leakage (1)
Vulnerabilities
  http://www.moviescope.com/
    Application might be vulnerable to clickjacking attacks
      /
        [#9]
    Multiple Cross-site request forgery vulnerability has been found
    Web form allows password caching in the client-side (autocomplete on)
    Possible Information Leakage or Improper Error Handling vulnerability has been fi
    Possible uncommon HTTP method found to be supported
    Webserver will disclose platform details or version information (HTTP Informatior
    Webserver will disclose platform details or version information (.NET Version)
    Webserver will disclose platform details or version information (Platform Details :
    Webserver will disclose platform details or version information (Server Version)
```

Vulnerability Information

Application might be vulnerable to clickjacking attacks

Severity :	Medium
Vulnerability Class :	ClickJack
References :	OWASP (Top 10 A5) | CWE (693)
Target URL :	http://www.moviescope.com/
Post Data :	N/A

Why is it an issue?

N-Stalker has found your system is vulnerable to clickjacking attack which allows malicious users to manipulate legitimate user interactions within your application.