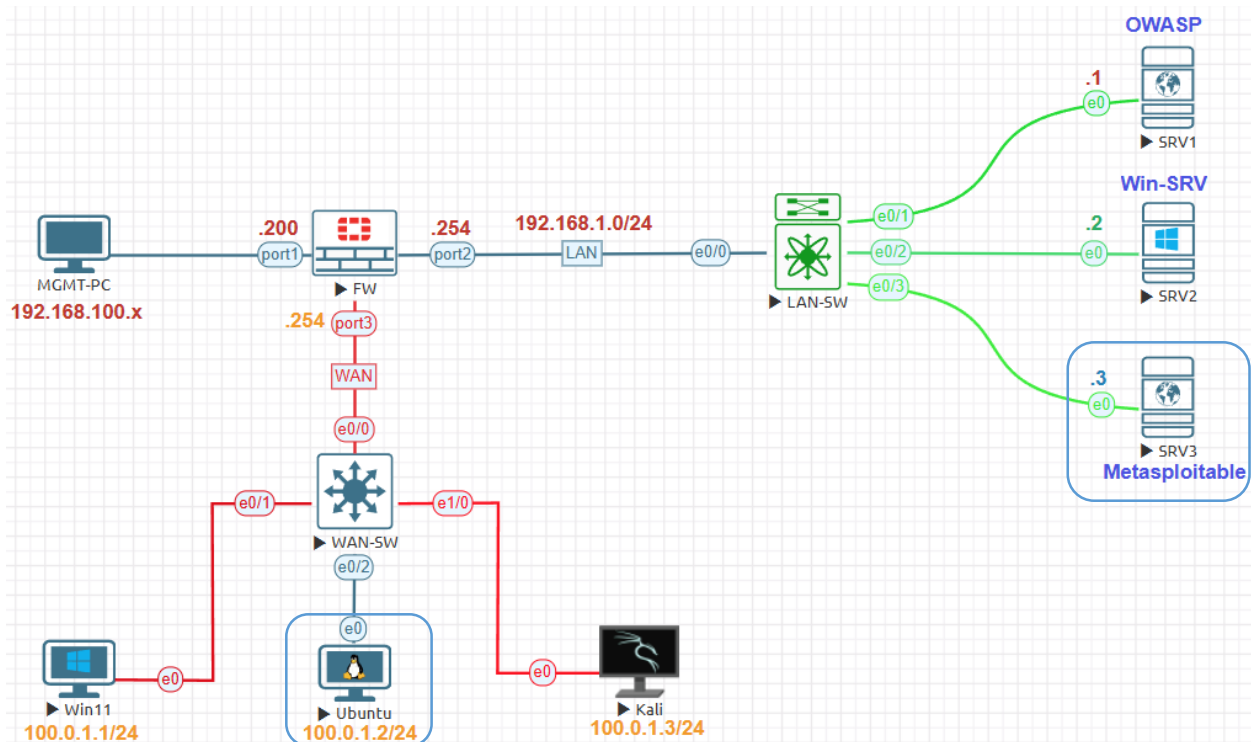


Web Application Test Lab:











| | |
|--------------------------------|------------------|
| Management Subnet | 192.168.100.0/24 |
| FortiGate Management IP | 192.168.100.200 |
| Internal Servers Subnet | 192.168.1.0/24 |
| FortiGate Firewall External | 100.0.1.0/24 |
| FortiGate Firewall Internal IP | 192.168.1.254 |
| FortiGate Firewall External IP | 100.0.1.254 |
| SRV1 IP Address | 192.168.1.1 |
| SRV2 IP Address | 192.168.1.2 |
| SRV3 IP Address | 192.168.1.3 |
| External Win11 IP Address | 100.0.1.1 |
| External Ubuntu IP Address | 100.0.1.2 |
| External Kali IP Address | 100.0.1.3 |

| Devices | Username | Password |
|----------------------------|---------------------|----------|
| FortiGate 7.0.9 | Admin | 123 |
| Linux Kali 2025.1c | kali | kali |
| Linux Ubuntu 22.04 Desktop | user | Test123 |
| Windows 11 x64 SE | user(Administrator) | Test123 |
| Linux Metasploitable 2.0 | msfadmin | msfadmin |
| Linux-OWASP | root | owaspbwa |
| Windows Server 2012 | Administrator | Test123 |

Go to **Scans > New Scan**. Choose **Web Application Tests** to open.

VULNERABILITIES

| | | | |
|---|---|--|---|
|  Basic Network Scan A full system scan suitable for any host. |  Credential Validation Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets |  Advanced Scan Configure a scan without using any recommendations. |  Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations. |
|  Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. |  Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner. |  Credentialed Patch Audit Authenticate to hosts and enumerate missing updates. |  Active Directory Starter Scan Look for misconfigurations in Active Directory. |

Name: **Web-App-Scan**. Targets: IP address of target **192.168.1.3** the IP Address of Metasploitable 2 where Damn Vulnerable Web Application DVWA to test.

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

General Settings

Name: Web-App-Scan

Description: Metasploitable Damn Vulnerable Web Application (DVWA)

Folder: My Scans

Targets: 192.168.1.3

Settings>Basic>Schedule keep default disable.

[← Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule**
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Enabled OFF

Save Cancel

Settings>Basic>Notification keep default disable.

[← Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule
- Notifications**

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Notifications will not be sent until your SMTP Server is configured.

Email Recipient(s)

Result Filters [Add Filter](#)

Settings>Discovery keep scan type Port scan (common ports)

Settings | Credentials | Plugins

BASIC >
DISCOVERY v
ASSESSMENT >
REPORT >
ADVANCED >

Scan Type: Port scan (common ports)

General Settings:
Always test the local Nessus host
Use fast network discovery

Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:
TCP
ARP
ICMP (2 retries)

Settings>Assessment keep default no changes Scan for all web vulnerabilities (quick)

Web-App-Scan / Configuration

[Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT v
REPORT >
ADVANCED >

Scan Type: Scan for all web vulnerabilities (quick)

General Settings:
Avoid potential false alarms
Enable CGI scanning

Web Applications:
Start crawling from "/"
Crawl 1000 pages (max)
Traverse 6 directories (max)
Test for known vulnerabilities in commonly used web applications
Perform each generic web app test for 5 minutes (max)

Settings>Reports keep the default no changes.

Web-App-Scan / Configuration

[Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the 'Reports' section. The left sidebar has 'REPORT' highlighted. The main content area is titled 'Processing' and contains the following options:

- Override normal verbosity
- I have limited disk space. Report as little information as possible
- Report as much information as possible
- Show missing patches that have been superseded
When enabled, includes superseded patch information in the scan report.
- Hide results from plugins initiated as a dependency
When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disal

Settings>Advanced keep default no changes.

Web-App-Scan / Configuration

[Back to Scan Report](#)

The screenshot shows the 'Settings' tab selected in the 'Advanced' section. The left sidebar has 'ADVANCED' highlighted. The main content area shows the 'Scan Type' dropdown menu set to 'Default' and the 'Performance options' section with the following values:

- 30 simultaneous hosts (max)
- 4 simultaneous checks per host (max)
- 5 second network read timeout

Under Credentials Tab. Choose HTTP.

The screenshot shows the 'Credentials' tab selected. The 'CATEGORIES' dropdown is set to 'Plaintext Authentication'. Below it is a search box labeled 'Filter Credentials'. A table lists the categories, with 'HTTP' highlighted and a count of '1' next to it.

| CATEGORIES | Count |
|------------|-------|
| HTTP | 1 |

Authentication method: **HTTP login form**

Username/Password of DVWA



Username

Password

Login

Login page: **/dvwa/login.php**

Login submission page: **login.php**

```
<body>
  <div align="center">
    <br>
    <p>...</p>
    <br>
    <form action="login.php" method="post">
      <fieldset overflow>
        <label for="user">Username</label>
        <input class="loginInput" type="text" size="20" name="username">
        <br>
```



| Status | Method | Domain | File | Initiator | Type | Transferred | Size |
|--------|--------|-------------|-------------|----------------------------|--------|-------------|---------|
| 302 | POST | 192.168.1.3 | login.php | document | html | 4.98 kB | 4.59 kB |
| 200 | GET | 192.168.1.3 | index.php | document | html | 4.94 kB | 4.59 kB |
| 200 | GET | 192.168.1.3 | main.css | stylesheet | css | cached | 3.95 kB |
| 200 | GET | 192.168.1.3 | dvwaPage.js | script | js | cached | 775 B |
| 200 | GET | 192.168.1.3 | favicon.ico | FaviconLoader.sys.mjs:1... | x-icon | cached | 1.41 kB |

[All](#) | [HTML](#) | [CSS](#) | [JS](#) | [XHR](#) | [Fonts](#) | [Images](#) | [Media](#) | [WS](#) | [Other](#) | Disable Cache | No Throttling ⌵ |

[▶](#) Headers | Cookies | **Request** | Response | Timings

Filter Request Parameters

Form data Raw

username: "admin"
 password: "password"
 Login: "Login"

| File | Initiator | Type | ▶ Headers | Cookies | Request | Response | Timings | |
|-------------|----------------------------|--------|---------------------------|--|----------------|----------|---------|--|
| login.php | document | html | Filter Request Parameters | | | | | |
| index.php | document | html | Request payload | | | | | |
| main.css | stylesheet | css | 1 | username=admin&password=password&Login=Login | | | | |
| dwvaPage.js | script | js | | | | | | |
| favicon.ico | FaviconLoader.sys.mjs:1... | x-icon | | | | | | |

Settings | **Credentials** | Plugins

CATEGORIES: All

Filter Credentials

HTTP Method: HTTP login form, User: admin

Authentication method: HTTP login form

Username: admin

Password (unsafe!):

Login page: /dwva/login.php

Login submission page: login.php

Login parameters: username=admin&password=password&L.....
If the keywords %USER% and %PASS% are used, they will be substituted

Check authentication on page: /dwva/login.php

Regex to verify successful authentication: Welcome

Global Credential Settings

Login method: POST

The screenshot shows the Network tab in a browser's developer tools. A 302 status code is highlighted in blue, indicating a redirect. The method is POST, and the domain is 192.168.1.3. The file being redirected to is index.php. A red box highlights the 302 status code, the POST method, and the index.php file. A red arrow points from the login.php file to the index.php file, with the text "Redirect from login.php to index.php" next to it. Other resources like main.css, dvwaPage.js, logo.png, and favicon.ico are also listed.

| Status | Method | Domain | File | Initiator |
|--------|--------|-------------|-------------|-------------|
| 302 | POST | 192.168.1.3 | login.php | document |
| 200 | GET | 192.168.1.3 | index.php | document |
| 200 | GET | 192.168.1.3 | main.css | stylesheet |
| 200 | GET | 192.168.1.3 | dvwaPage.js | script |
| 200 | GET | 192.168.1.3 | logo.png | img |
| 200 | GET | 192.168.1.3 | favicon.ico | FaviconLoad |

Global Credential Settings

Login method:

Re-authenticate delay (seconds):
The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.

Follow 30x redirections (# of levels):
If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.

Under **Plugins** Tab no changes require keep the default.

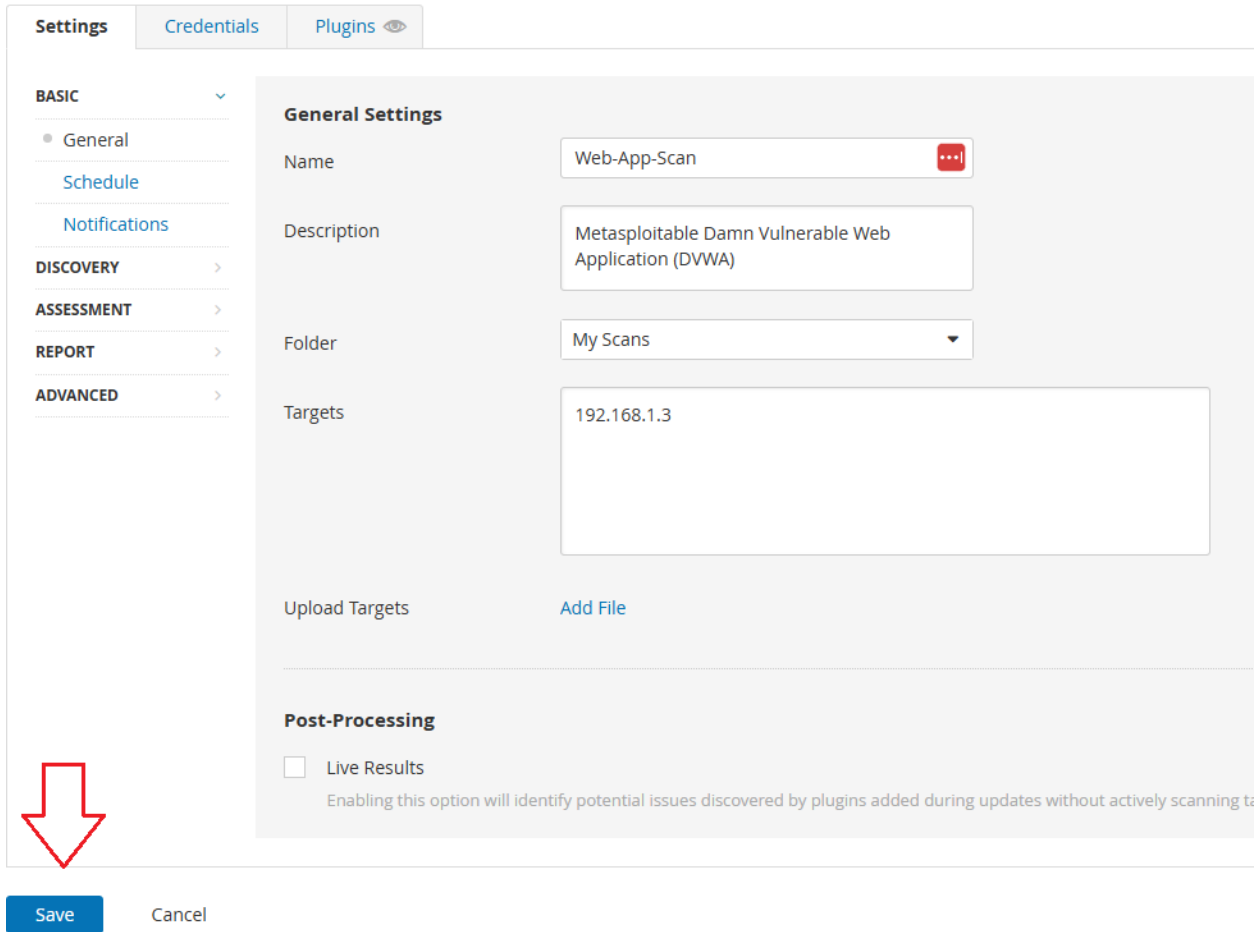
Web-App-Scan / Configuration

[← Back to Scan Report](#)

Settings | Credentials | **Plugins**

| PLUGIN FAMILY | TOTAL |
|------------------|-------|
| CGI abuses | 6412 |
| CGI abuses : XSS | 711 |
| Settings | 2 |
| Web Servers | 1925 |

Click **Save** Then **Launch**. Wait for the scan to complete.



Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

General Settings

Name: Web-App-Scan

Description: Metasploitable Damn Vulnerable Web Application (DVWA)

Folder: My Scans

Targets: 192.168.1.3

Upload Targets: Add File

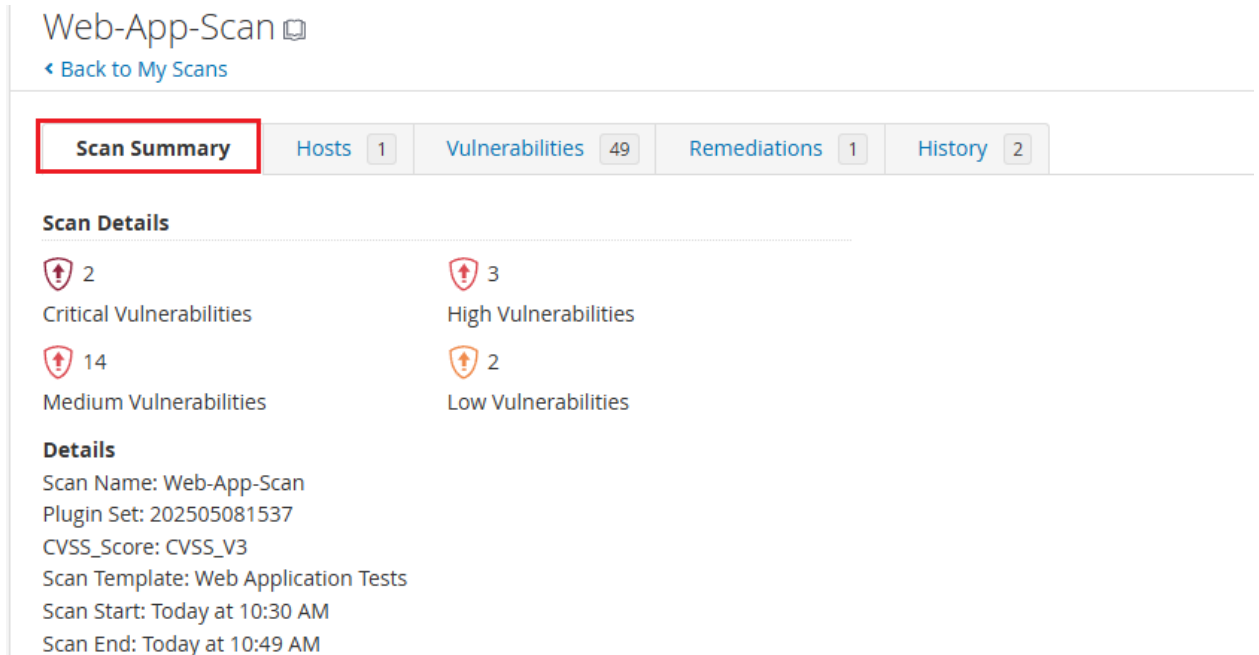
Post-Processing

Live Results

Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets.

Save Cancel

After complete the **Scan Summary**.



Web-App-Scan

[Back to My Scans](#)

Scan Summary | Hosts 1 | Vulnerabilities 49 | Remediations 1 | History 2

Scan Details

| | |
|----------------------------|------------------------|
| 2 Critical Vulnerabilities | 3 High Vulnerabilities |
| 14 Medium Vulnerabilities | 2 Low Vulnerabilities |

Details

Scan Name: Web-App-Scan
Plugin Set: 202505081537
CVSS_Score: CVSS_V3
Scan Template: Web Application Tests
Scan Start: Today at 10:30 AM
Scan End: Today at 10:49 AM


Vulnerabilities Tab provide information about the scan.

Web-App-Scan 

[← Back to My Scans](#)

| Scan Summary | Hosts 1 | Vulnerabilities 49 | Remediations 1 | History 2 | |
|-----------------------------------|---|---------------------------|--------------------|---|-------------|
| Filter | Search Vulnerabilities <input type="text"/> | | 49 Vulnerabilities | | |
| <input type="checkbox"/> Sev | CVSS | VPR | EPSS | Name | Family |
| <input type="checkbox"/> CRITICAL | 9.8 | 8.9 | 0.9447 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers |
| <input type="checkbox"/> CRITICAL | 9.8 | 5.9 | 0.0172 | phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3) | CGI abuses |
| <input type="checkbox"/> HIGH | 8.8 | 7.4 | 0.8167 | TWiki 'rev' Parameter Arbitrary Command Execution | CGI abuses |
| <input type="checkbox"/> HIGH | 7.5 * | 6.7 | 0.0116 | phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP C... | CGI abuses |
| <input type="checkbox"/> HIGH | 7.5 * | | | CGI Generic Remote File Inclusion | CGI abuses |
| <input type="checkbox"/> MEDIUM | 6.8 * | | | CGI Generic Local File Inclusion (2nd pass) | CGI abuses |
| <input type="checkbox"/> MEDIUM | 5.3 | 4.0 | 0.8269 | HTTP TRACE / TRACK Methods Allowed | Web Servers |

Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0 
Scanner: Local Scanner
Start: Today at 10:30 AM
End: Today at 10:49 AM
Elapsed: 19 minutes

Vulnerabilities



Under Remediation Tab.

Web-App-Scan 

[← Back to My Scans](#)

| Scan Summary | Hosts 1 | Vulnerabilities 49 | Remediations 1 | History 2 |
|----------------|---|--------------------|-----------------------|-----------|
| Search Actions | <input type="text"/> | | 1 Action | |
| Action | phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the advisories. | | | |