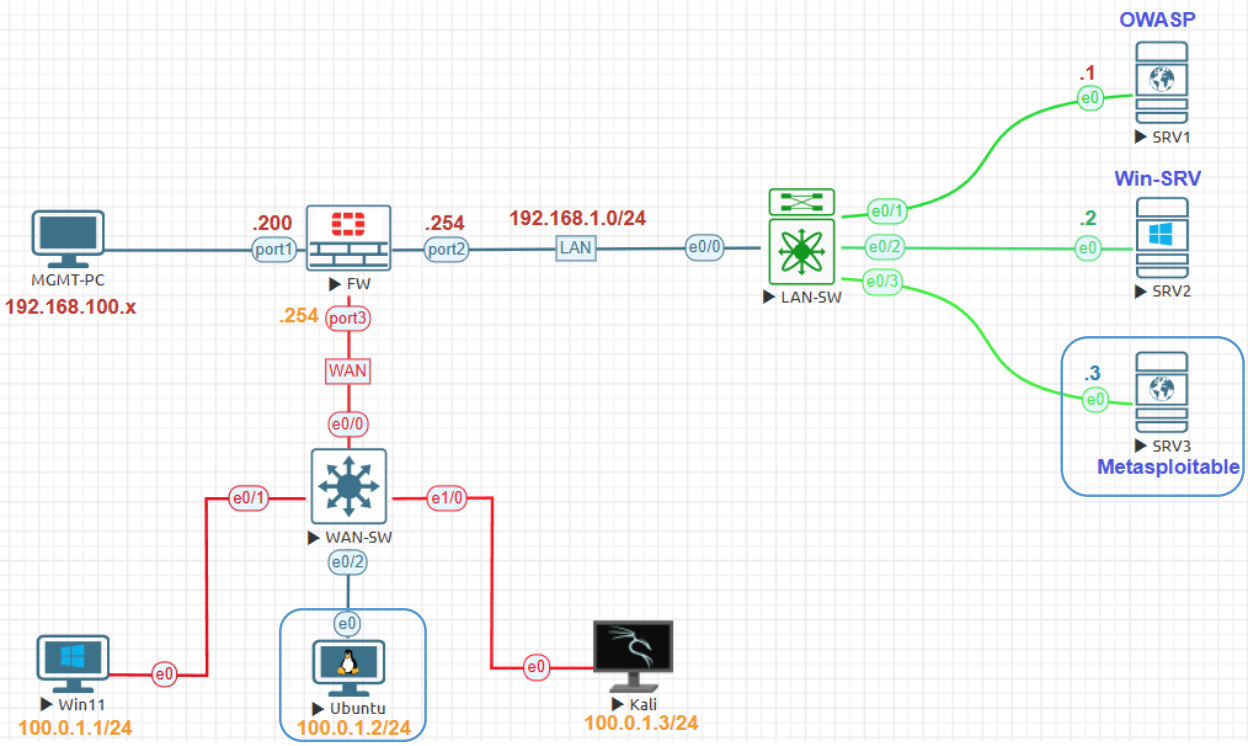
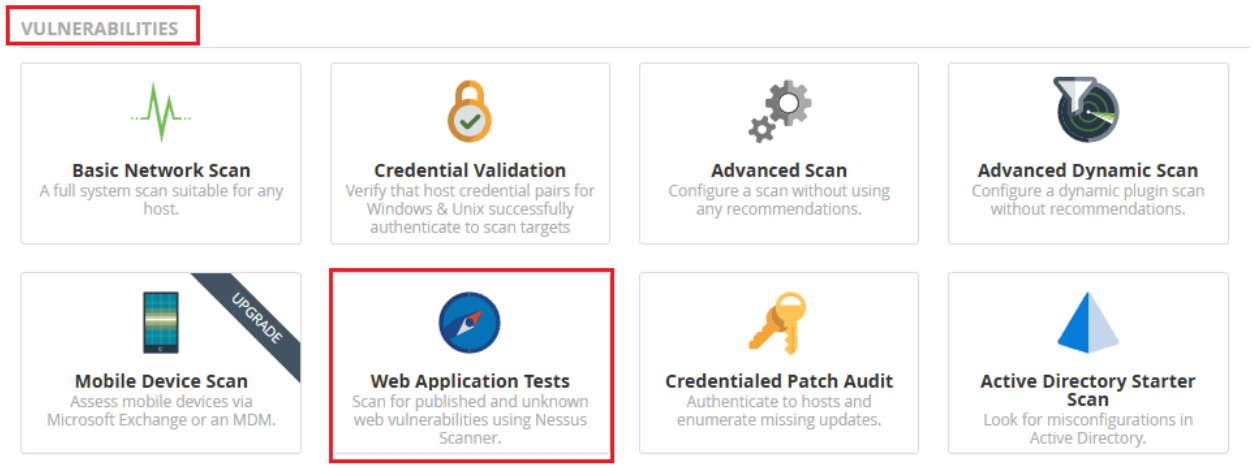
Web Application Test Lab:



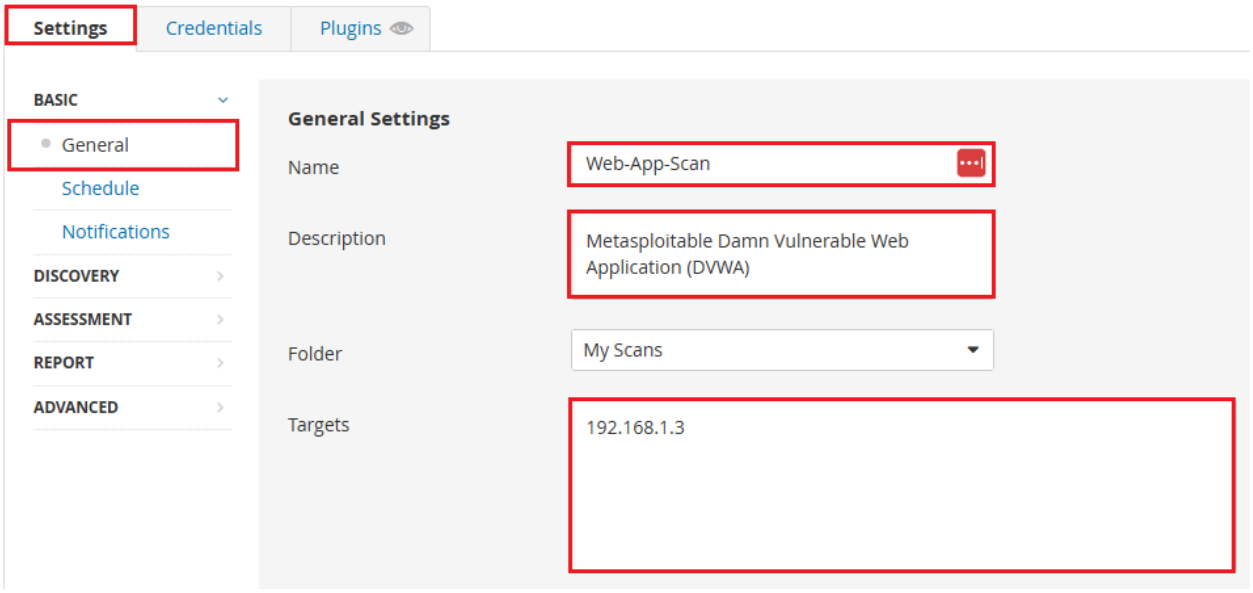
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 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

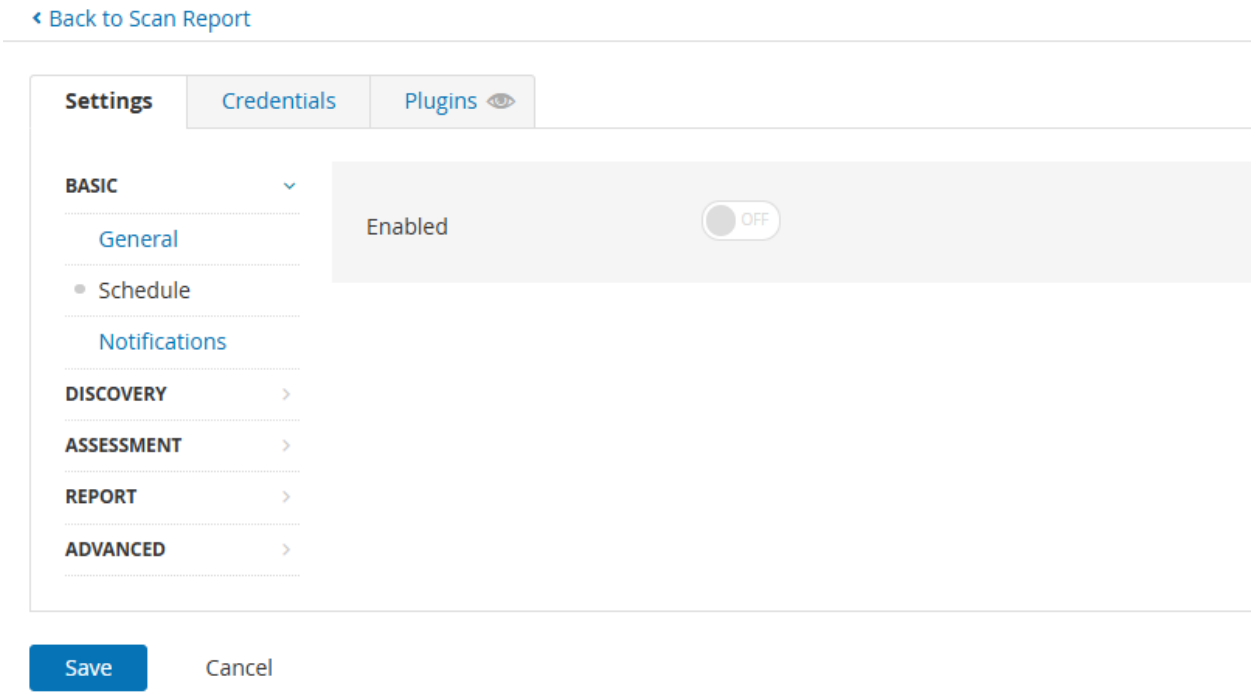
Go to Scans > New Scan. Choose Web Application Tests to open.



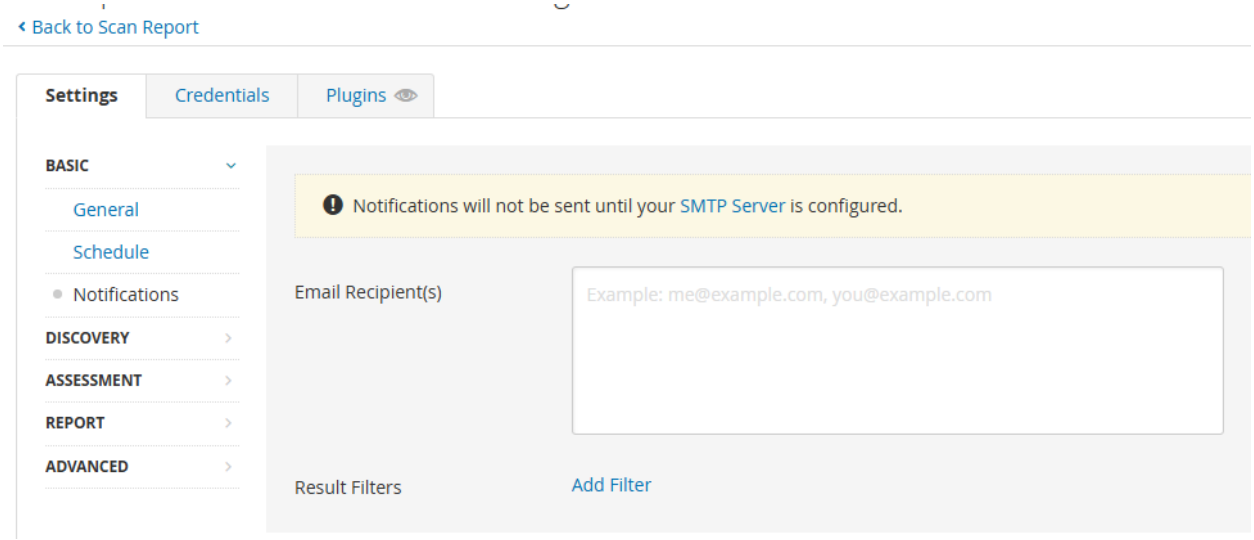
Name: Web-App-Scan. Targets: IP address of target 192.168.1.3 the IP Address of Metasploitable 2 where Damn Vulnerable Web Application DVWA to test.



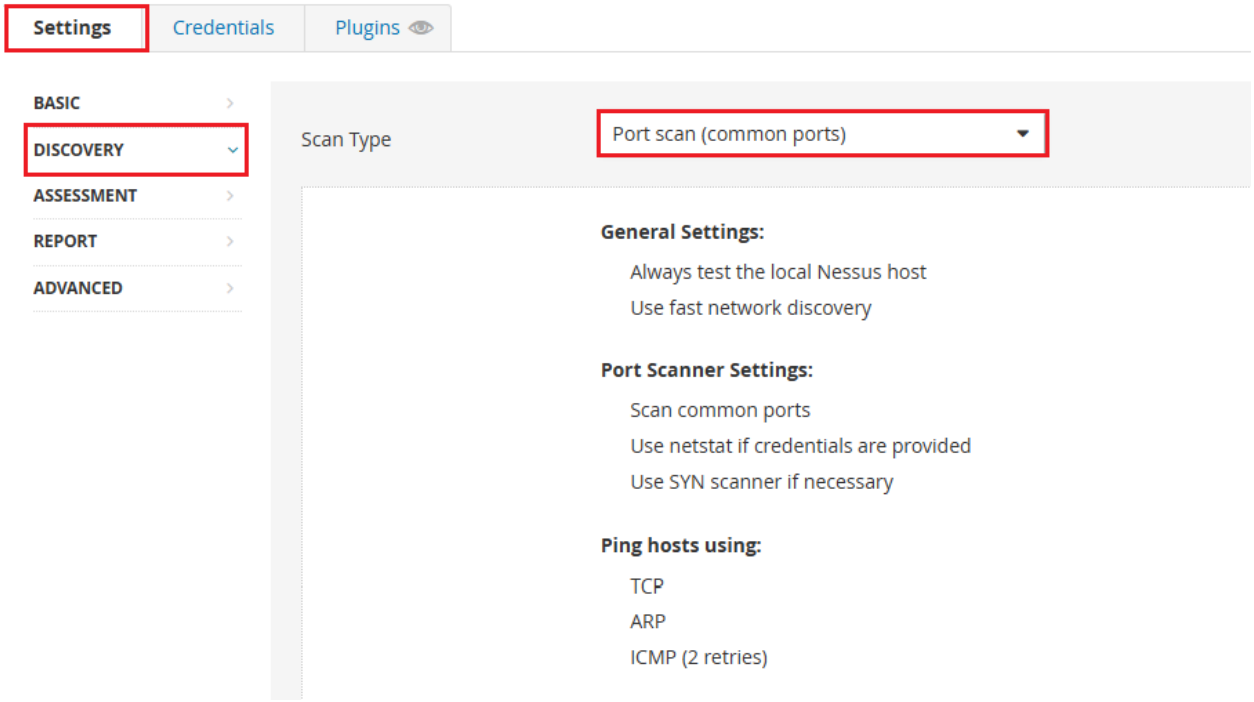
Settings>Basic>Schedule keep default disable.



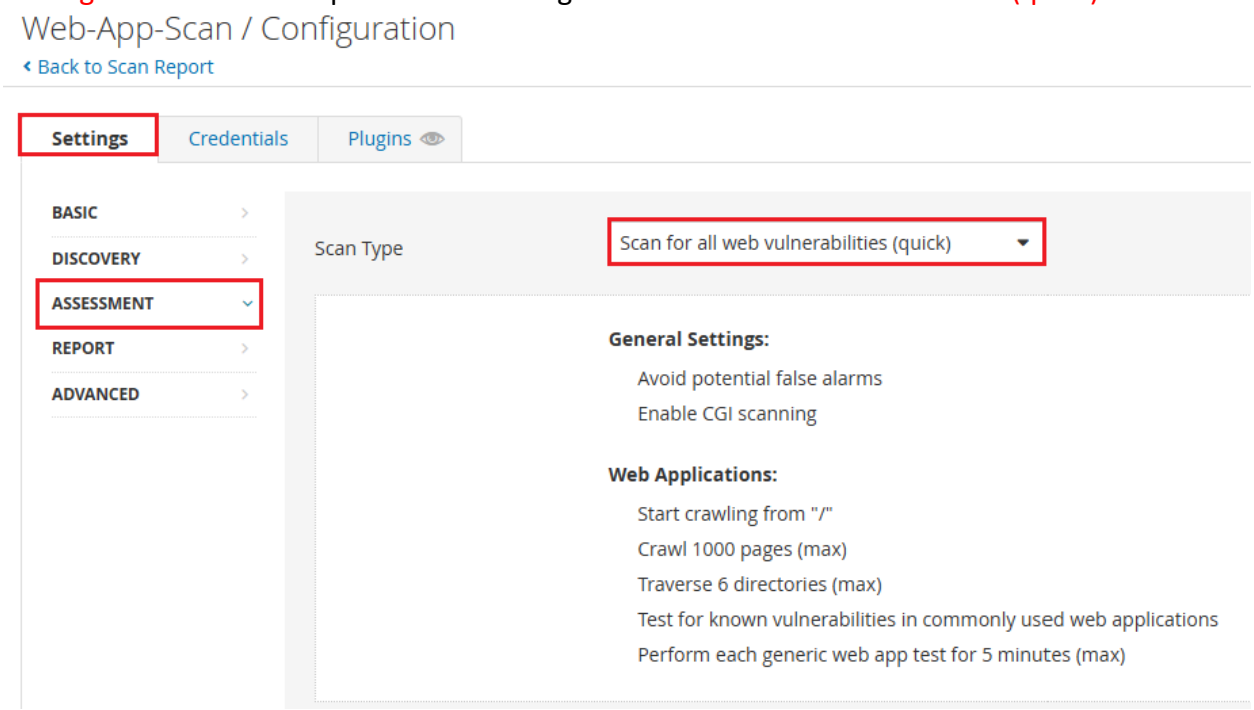
Settings>Basic>Notification keep default disable.



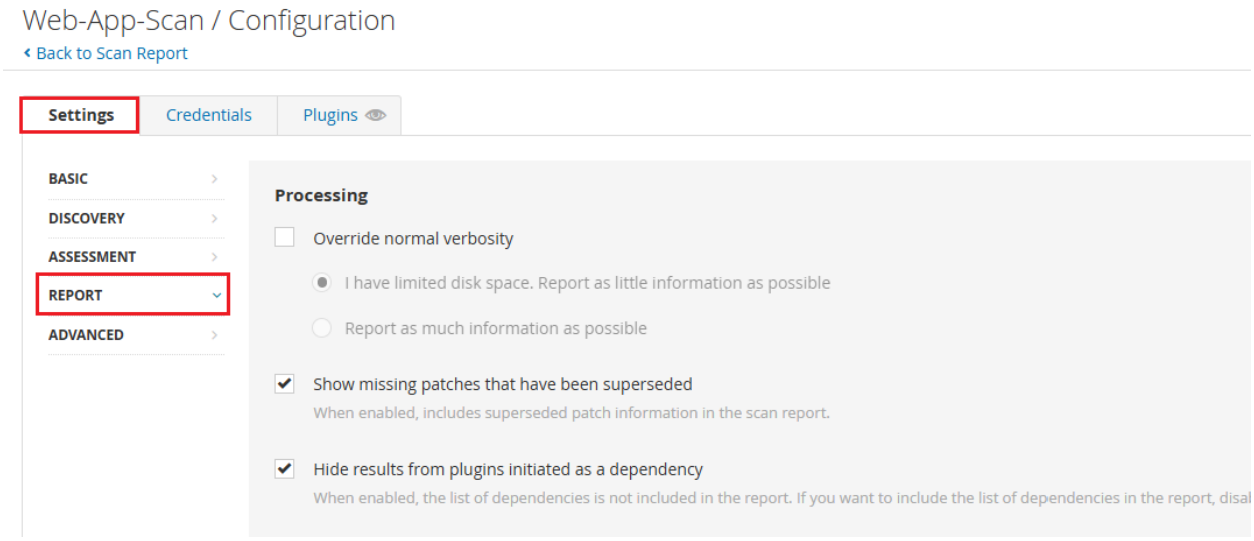
Settings>Discovery keep scan type Port scan (common ports)



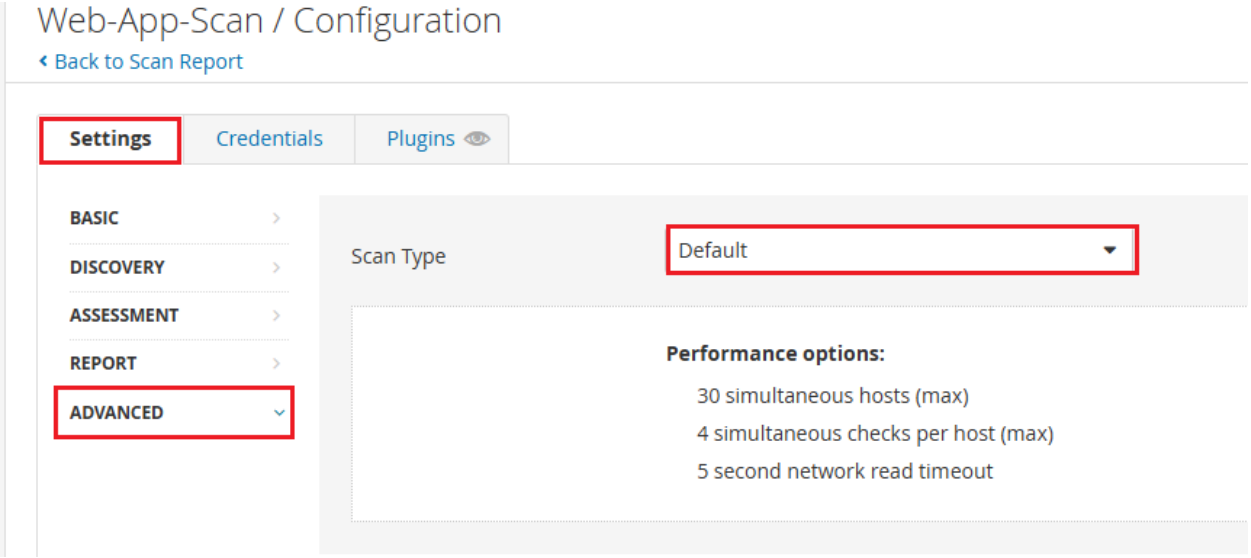
Settings>Assessment keep default no changes Scan for all web vulnerabilities (quick)



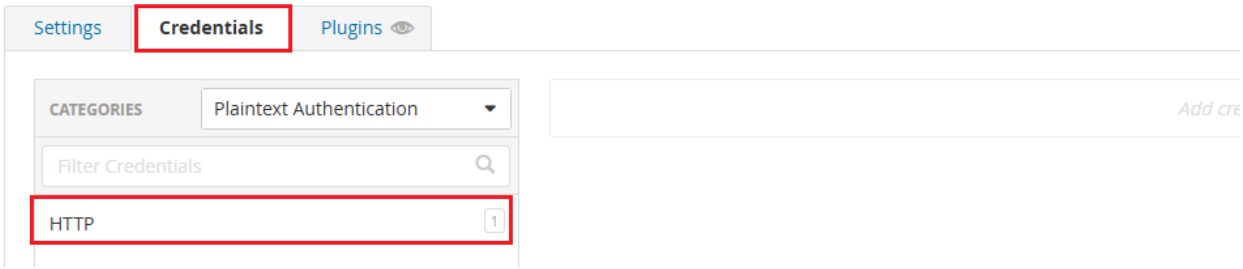
Settings>Reports keep the default no changes.



Settings>Advanced keep default no changes.



Under Credentials Tab. Choose HTTP.



Authentication method: HTTP login form

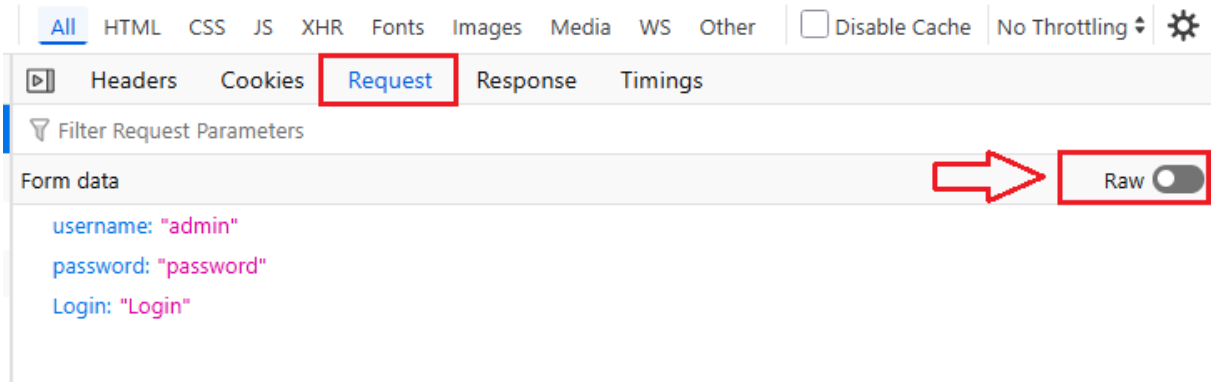
Username/Password of DVWA

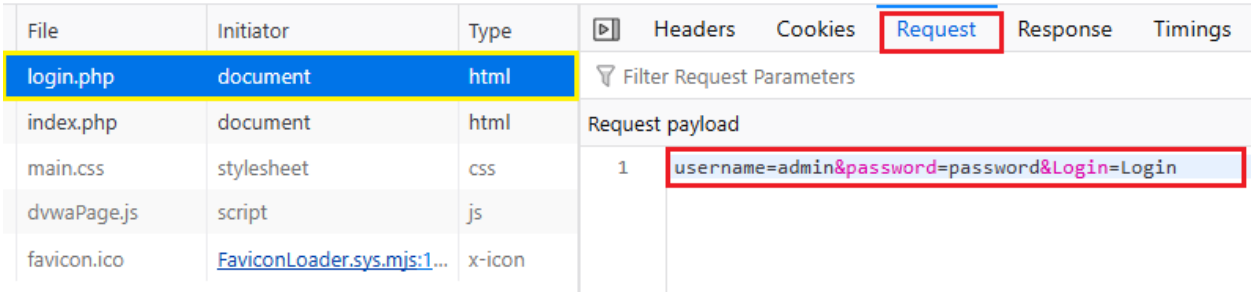
Login page: /dvwa/login.php

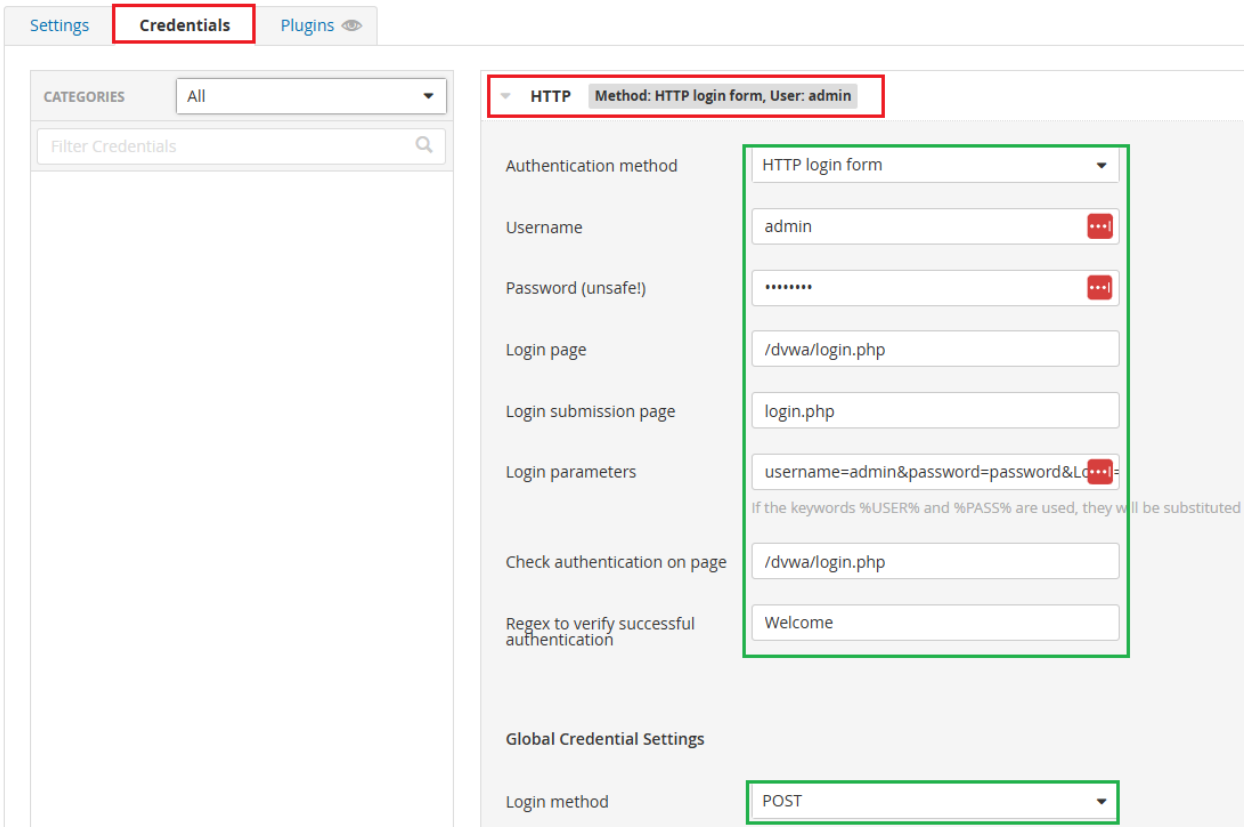
Login submission page: login.php

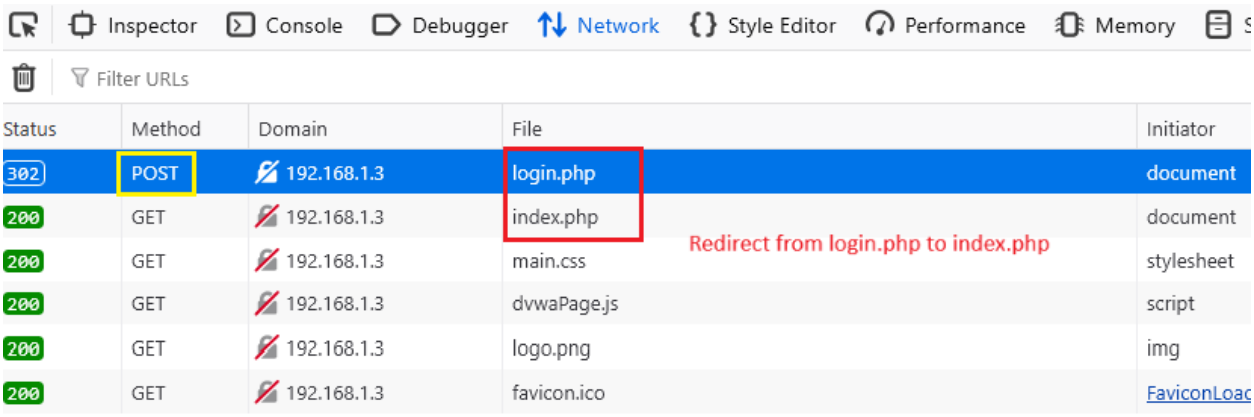
```
<body>
  <div align="center">
    <br>
    <p> ... </p>
    <br>
    <form action="login.php" method="post">
      <fieldset> overflow
        <label for="user ">Username</label>
        <input class="loginInput" type="text" size="20" name="username">
        <br>
```

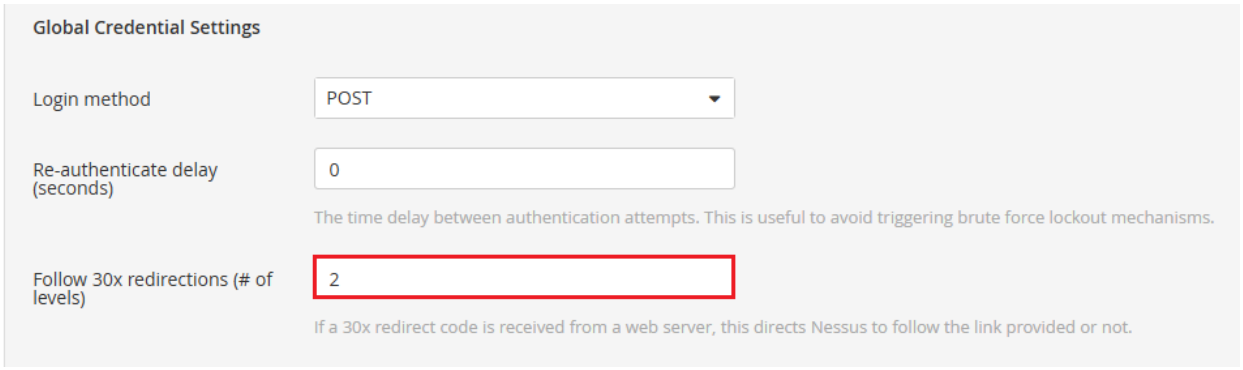
Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	192.168.1.3	login.php	document	html	4.98 kB	4.59 kB
200	GET	192.168.1.3	index.php	document	html	4.94 kB	4.59 kB
200	GET	192.168.1.3	main.css	stylesheet	css	cached	3.95 kB
200	GET	192.168.1.3	dvwaPage.js	script	js	cached	775 B
200	GET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



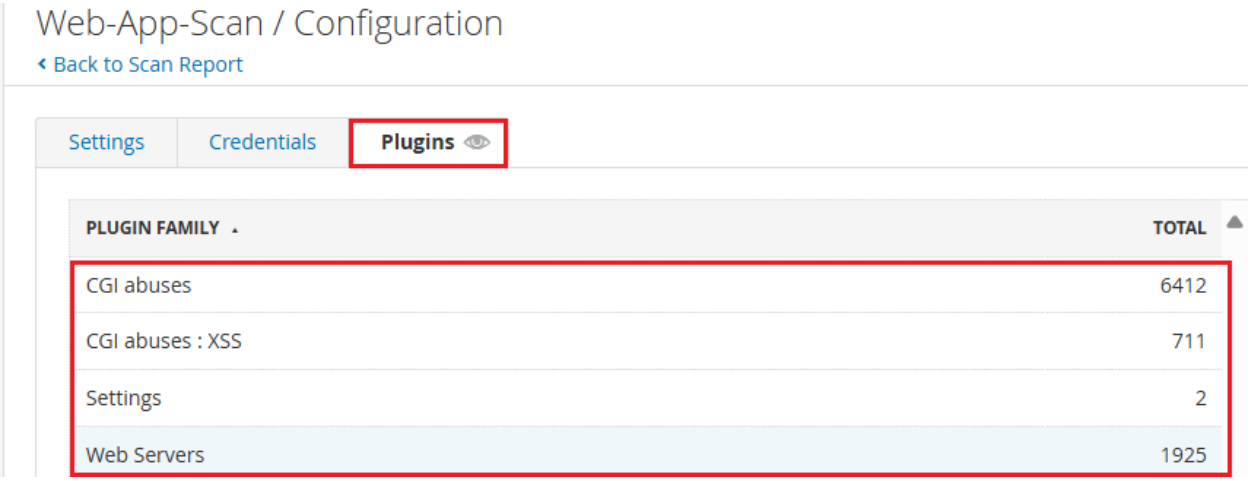




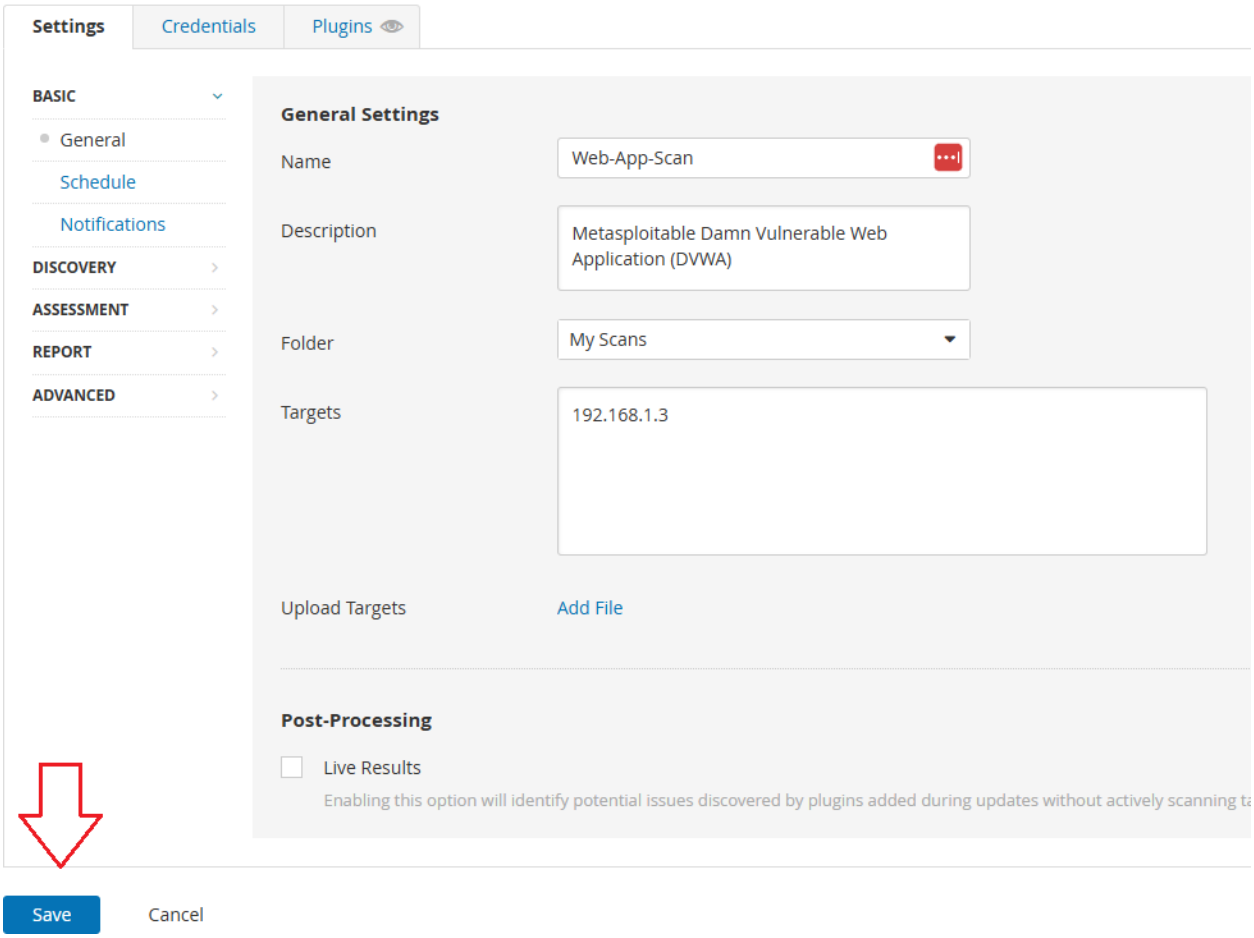




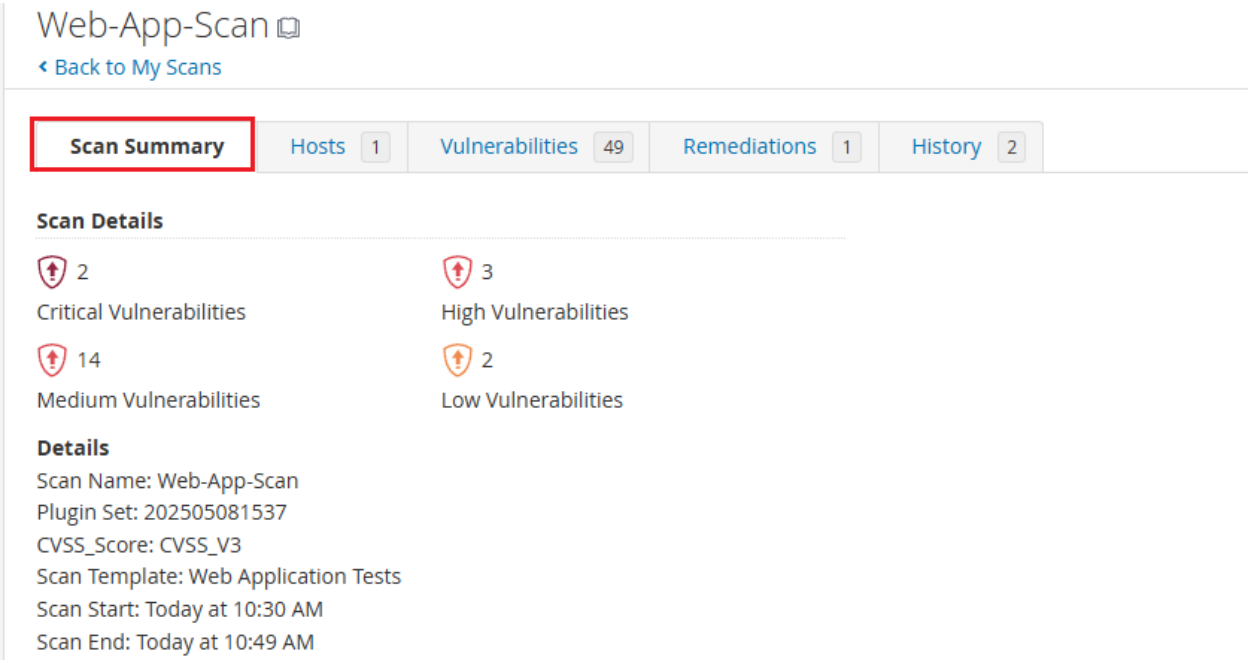
Under Plugins Tab no changes require keep the default.



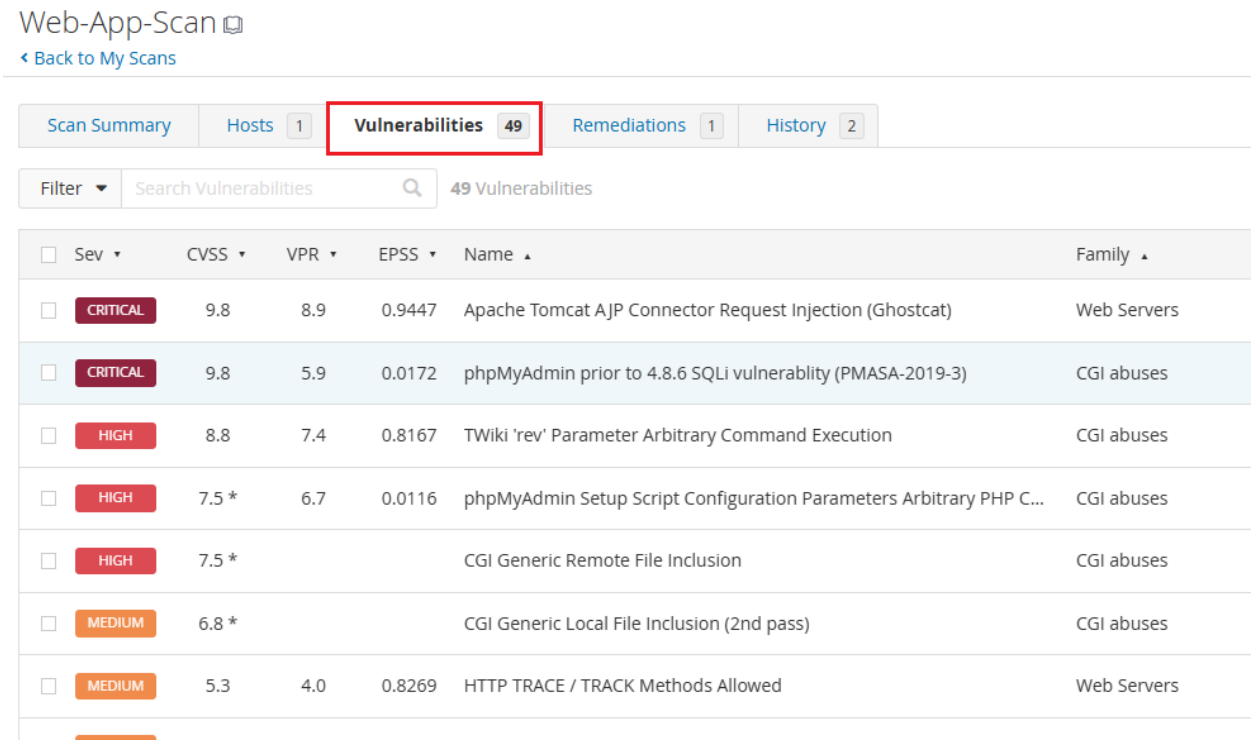
Click Save Then Launch. Wait for the scan to complete.

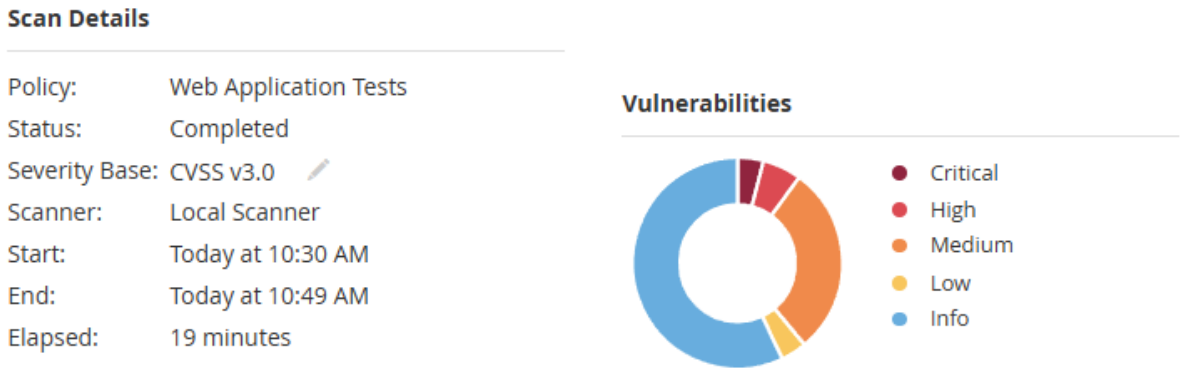


After complete the Scan Summary.



Vulnerabilities Tab provide information about the scan.





Under Remediation Tab.