Incident Response Report

1. Alert Analysis

The simulated log file was analyzed to identify potential security events.
Key alerts observed:
- Multiple failed login attempts from the same IP.
- Successful login after several failed attempts.
- Privilege escalation activity detected.

These indicators suggest a possible brute-force attack followed by privilege escalation.

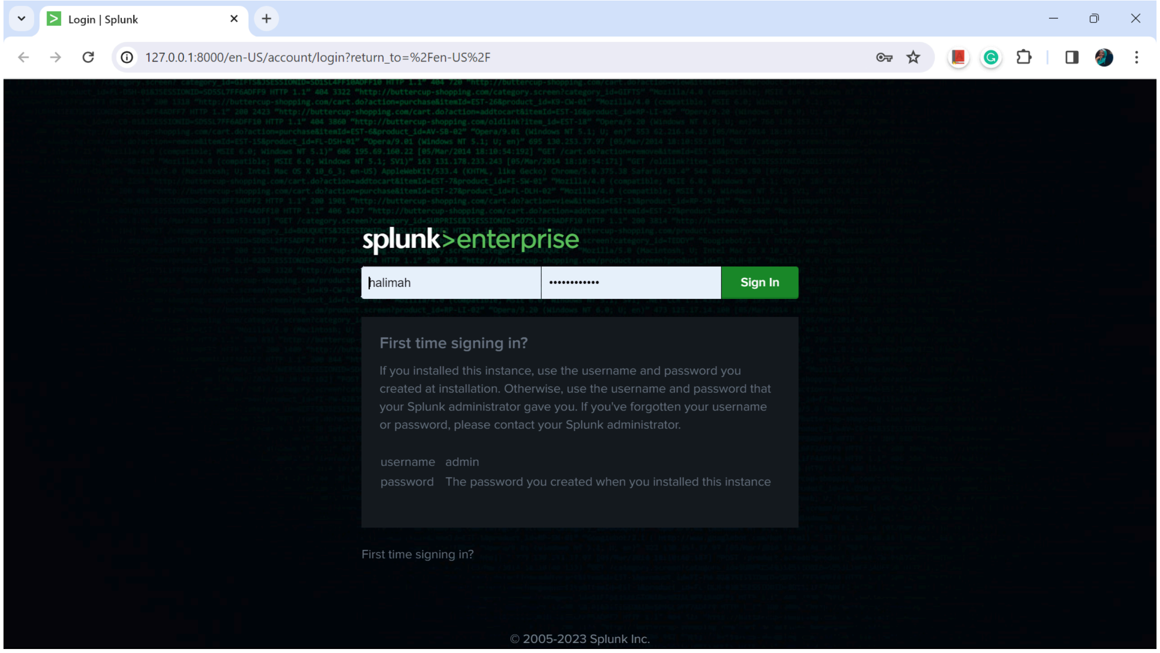
2. Incident Classification

Incident Type	Severity	Reason
Failed login attempts	Medium	Could indicate brute force attempt
Successful login after multiple failed attempts	High	Possible account compromise
Privilege escalation attempt	High	Indicates post-compromise activity

3. Remediation Recommendations

- Enforce strong password policies and enable MFA.
- Block suspicious IPs and monitor login attempts.
- Investigate compromised accounts and reset credentials.
- Review privilege escalation logs and patch vulnerabilities.

- Implement continuous monitoring via SIEM tools (Splunk / ELK).



127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F

splunk>enterprise

halimah ············ Sign In

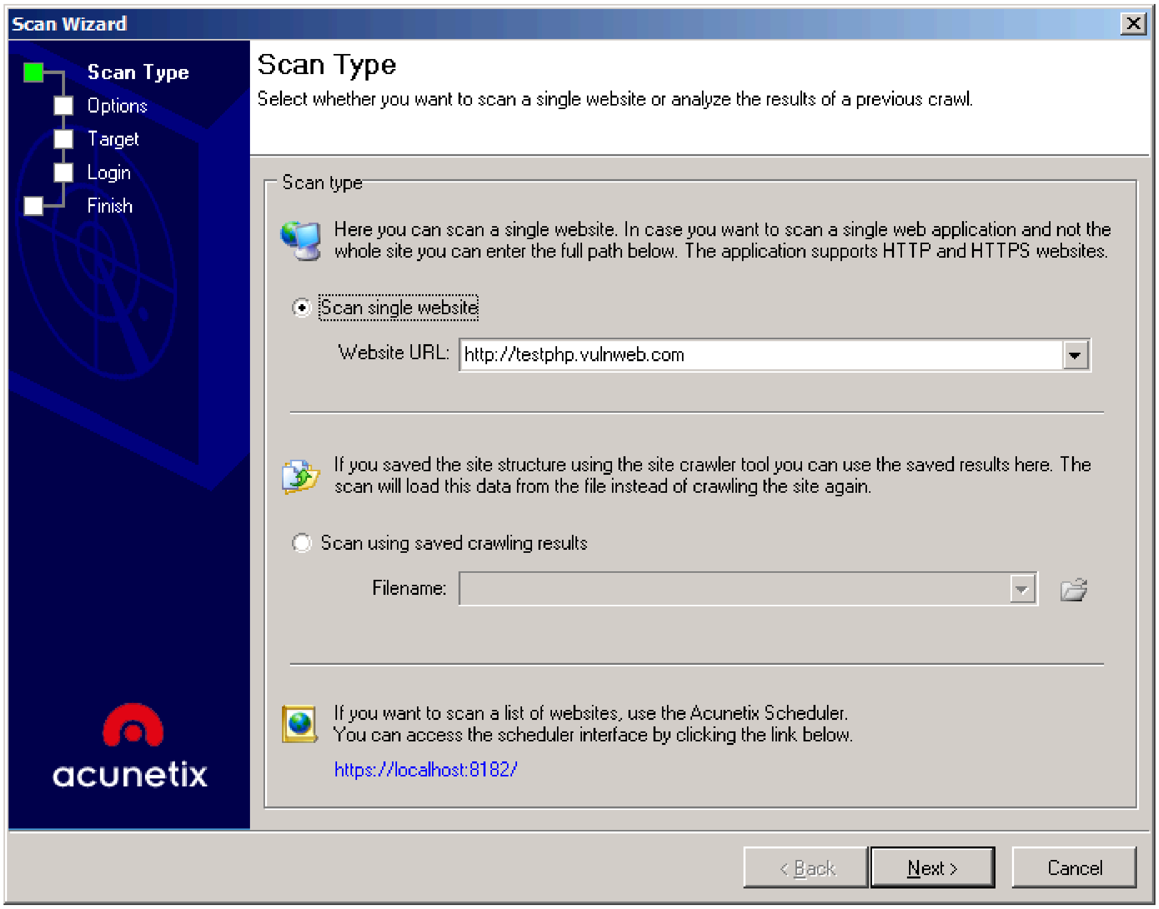
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2023 Splunk Inc.



Scan Type

Select whether you want to scan a single website or analyze the results of a previous crawl.

Scan type

Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites.

● Scan single website

Website URL: http://testphp.vulnweb.com

If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again.

○ Scan using saved crawling results

Filename:

If you want to scan a list of websites, use the Acunetix Scheduler. You can access the scheduler interface by clicking the link below.

https://localhost:8182/