



# Cybersecurity

## Module 15 Challenge Submission File

### Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

#### Web Application 1: Your Wish is My Command Injection

Provide a screenshot confirming that you successfully completed this exploit:

The screenshot shows a web browser displaying the DVWA Command Injection page. The URL is 192.168.13.25/vulnerabilities/exec/. The left sidebar lists various vulnerabilities, with 'Command Injection' highlighted. The main content area has a title 'Vulnerability: Command Injection' and a sub-section 'Ping a device'. A form asks 'Enter an IP address:' with a text input field containing '192.168.13.25' and a 'Submit' button. Below the form is a red terminal-style output window showing the results of a ping command:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.041 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.033/0.036/0.041/0.000 ms
127.0.0.1      localhost
::1      localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.13.25 ed693af6f40b
```

At the bottom, there's a 'More Information' section with a link: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>.

The screenshot shows a web browser window for the DVWA Command Injection vulnerability. The URL is 192.168.13.25/vulnerabilities/exec/. The title bar says "Vulnerability: Command Injection". On the left, there's a sidebar menu with various exploit categories: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (which is highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, and PHP Info. The main content area has a heading "Ping a device" and a form where you can enter an IP address and click "Submit". Below the form, the terminal output of the ping command is displayed in red text:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.041 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.035/0.040/0.044/0.000 ms
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

Write two or three sentences outlining mitigation strategies for this vulnerability:

Input validation is a great technique to protect web security to prevent attackers from exploiting vulnerabilities. Input validation checks and sanitizes the data that users or other sources provide to your web application. Also, separating sensitive data from this server to a more secure location would prevent unauthorized users from obtaining sensitive information.

## Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

3. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
70	henryhacker	Courage is immortal	200			11801	
71	superman	I am Iron Man	200			11801	
72	isolane	I am Iron Man	200			11801	
73	spiderman	I am Iron Man	200			11801	
74	jennymcros	I am Iron Man	200			11801	
75	tony Stark	I am Iron Man	200			11827	
76	tintom	I am Iron Man	200			11801	
77	peterparker	I am Iron Man	200			11801	
78	darkknight	I am Iron Man	200			11801	
79	mysticsmith	I am Iron Man	200			11800	
80	henryhacker	I am Iron Man	200			11801	
81	superman	His Past. Our future	200			11801	
82	isolane	His Past. Our future	200			11801	

Request Response

Pretty Raw Hex Render

```
80
81    <br>
82
83    <font color="green">
84        Successful login! You really are Iron Man :)
85    </font>
86
87    </div>
88
89    <div id="side">
90
91        <a href="http://itsecgames.blogspot.com" target="blank_" class="button">
92            
93        </a>
94        <a href="http://de.linkedin.com/in/malikmeselen" target="blank_" class="button">
95            
96        </a>
97        <a href="http://twitter.com/MME_IT" target="blank_" class="button">
98            
99        </a>
100       <a href="http://www.facebook.com/pages/MME-IT-Audits-Security/104159019664877" target="blank_" class="button">
101           
102       </a>
103   </div>
104
105   <div id="disclaimer">
106
107       <p>
108           MME IT is for educational purposes only / Follow <a href="http://twitter.com/MME_IT" target="_blank">
109               @MME_IT
110           </a>
111           on Twitter and help our shout shout shout containning #IT educational ! And as we know it's time now it's time to add some more like #audits #IT audits
112       </p>
113   </div>
```

0 matches

Write two or three sentences outlining mitigation strategies for this vulnerability:

Multi-factor authentication helps to reduce the risk of account attacks and provides additional security for users with their accounts. Forcing more complex passwords and multifactor authentication helps to mitigate this vulnerability.

## Web Application 3: Where's the BeEF?

Provide a screenshot confirming that you successfully completed this exploit:

Screenshot of DVWA XSS (Stored) vulnerability demonstration.

**Browser Headers:**

```
Not secure | 192.168.13.25/vulnerabilities/xss_s/
```

**DVWA Navigation Bar:**

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)**
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

**Vulnerability: Stored Cross Site Scripting (XSS) Form:**

Name \*

Message \*

**Sign Guestbook** **Clear Guestbook**

**Guestbook Comments:**

- Name: test  
Message: This is a test comment.
- Name: Allison  
Message:

**Developer Tools - Elements Tab:**

```
<tr>
  <td width="100">Name *</td>
  <td><input name="txtName" type="text" size="30" maxlength="10"></td>
</tr>
<tr>
  <td width="100">Message *</td>
  <td><textarea name="mtxMessage" cols="50" rows="3" maxlength="100"></textarea> == $0</td>
</tr>
</tbody>
</table>
</form>
</div>
<br>
<div id="guestbook_comments"></div>
<div id="guestbook_comments"></div>
</div>
</div>
```

**Developer Tools - Styles Tab:**

```
element.style { }
input, textarea, select {
  font: 100% arial,sans-serif;
  vertical-align: middle;
}
textarea {
  writing-mode: horizontal-tb !important;
  font-style: ;
  font-variant: ligatures;
  font-variant: caps;
  font-variant: numeric;
  font-variant: east-asian;
  font-weight: ;
  font-stretch: ;
}
```

Screenshot of DVWA XSS (Stored) vulnerability demonstration with a session timeout overlay.

**Browser Headers:**

```
Not secure | 192.168.13.25/vulnerabilities/xss_s/
```

**DVWA Navigation Bar:**

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)**
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

**Vulnerability: Stored Cross Site Scripting (XSS) Form:**

Name \*

Message \*

**Sign Guestbook** **Clear Guestbook**

**Guestbook Comments:**

- Name: test  
Message: This is a test comment.
- Name: Allison  
Message:

**Facebook Session Timed Out Overlay:**

Your session has timed out due to inactivity.  
Please re-enter your username and password to login.

Email:   
Password:   
**Log In**

The screenshot shows a Linux desktop environment with two browser windows open:

- DVWA (Top Window):** Displays the "Vulnerability: Stored Cross Site Scripting (XSS)" page. On the left is a sidebar with various security modules. The "XSS (Stored)" module is highlighted. The main form has fields for "Name" and "Message". Below the form, a guestbook entry from "Allison" is shown.
- BeEF Control Panel (Bottom Window):** Shows a list of "Hooked Browsers" (192.168.13.1) and "Offline Browsers" (127.0.1). The "Commands" tab is selected, displaying a "Module Tree" with categories like Debug, Exploits, Host, and Network. A "Module Results History" table lists a single command entry from April 7, 2024. The "Command results" pane shows a JSON response containing geographical and organizational information.

Write two or three sentences outlining mitigation strategies for this vulnerability:

Input validation minimizes cross-site scripting. This will make it harder for people to put webhooks into your browser. Additionally, outputting coding stops browsers from running scripts in message boxes.