



# 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 the DVWA interface with the 'Command Injection' vulnerability selected. The 'Ping a device' section shows the command 'cat /etc/passwd' entered in the input field. The output displays the contents of the /etc/passwd file, listing system users and their home directories. The 'More Information' section provides links to related resources.

**Vulnerability: Command Injection**

**Ping a device**

Enter an IP address:

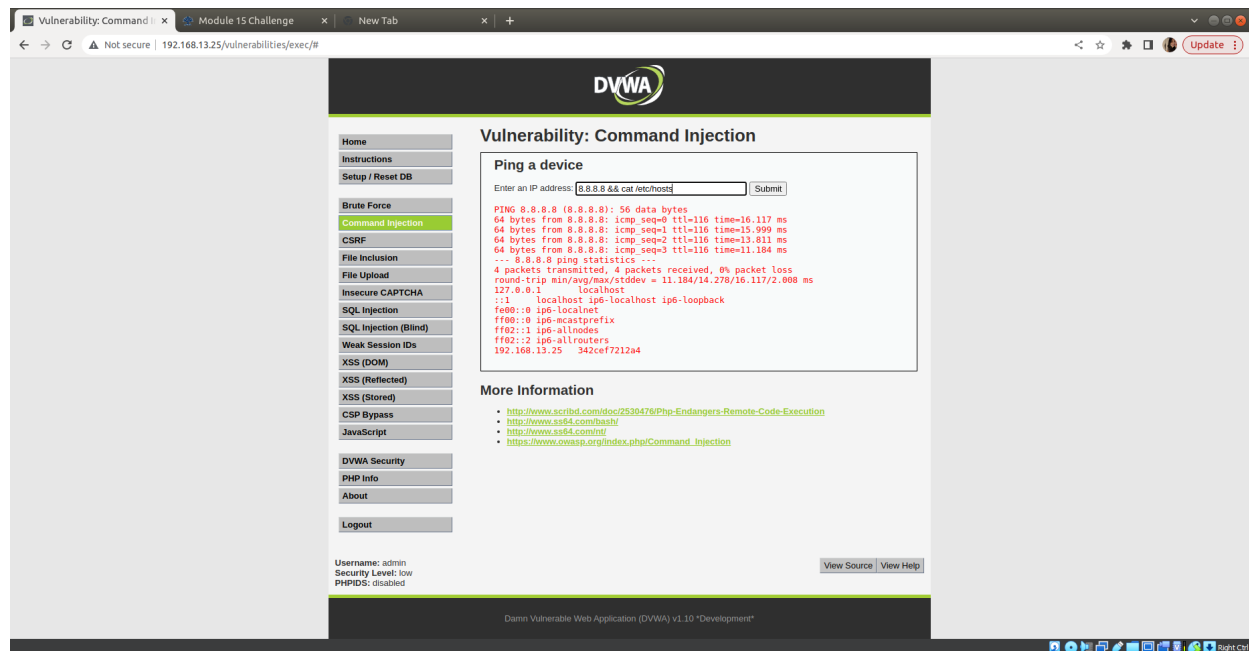
PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: icmp\_seq=0 ttl=116 time=17.047 ms  
64 bytes from 8.8.8.8: icmp\_seq=1 ttl=116 time=14.893 ms  
64 bytes from 8.8.8.8: icmp\_seq=2 ttl=116 time=13.543 ms  
64 bytes from 8.8.8.8: icmp\_seq=3 ttl=116 time=15.446 ms  
... 8.8.8.8 ping statistics ...  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 13.543/15.032/17.047/1.354 ms  
root:x:0:root:/root:/bin/bash  
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/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:MailList 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/sbin/nologin  
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

**More Information**

- <http://www.scribd.com/doc/2530470/Php-Endangers-Remote-Code-Execution>
- <http://www.as64.com/haash/>
- <http://www.as64.com/nll/>
- [https://www.owasp.org/index.php/Command\\_Injection](https://www.owasp.org/index.php/Command_Injection)

Username: admin  
Security Level: low

[View Source](#) [View Help](#)



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

This vulnerability of Command Injection can be mitigated by avoiding to run the system Commands with User-Supplied Input. Additionally, it is viable to use strong Commands that will validate the passed input data and to make sure that we test our applications and patch any errors and vulnerabilities on a daily basis.

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

Provide a screenshot confirming that you successfully completed this exploit:

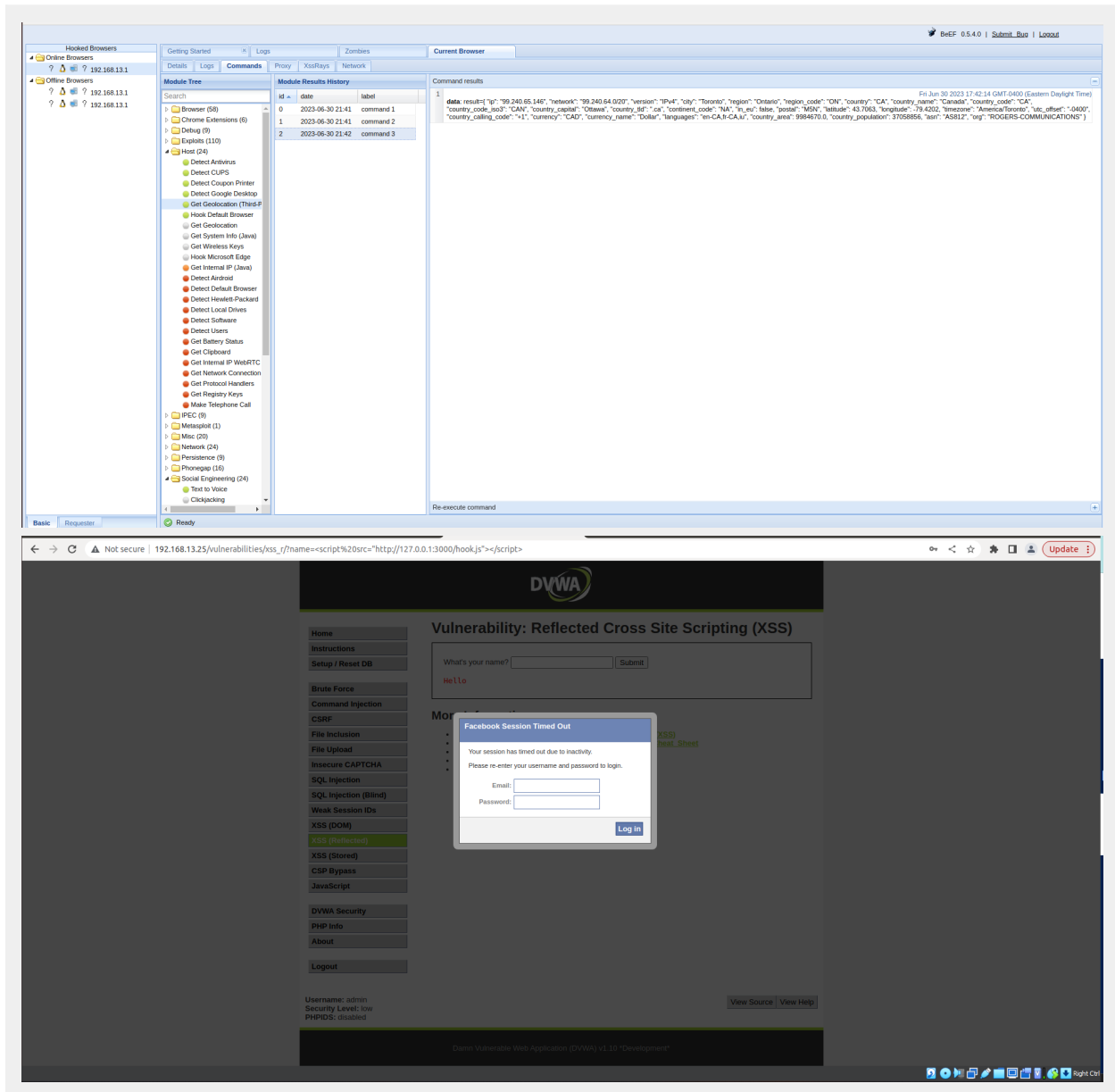
The screenshot displays a web application security tool interface. The top section shows a list of requests with columns for Request ID, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The requests are numbered 57 to 83. The bottom section shows the response of the selected request (ID 83), which is a 200 status code. The response content is a login form for 'bWAPP' with the title 'Broken Auth - Insecure Login Forms'. The form includes fields for 'Login:' and 'Password:', a 'Login' button, and a message 'Successful login! You really are Iron Man :)'. The page also features a navigation bar with links like 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. A footer note states: 'bWAPP is for educational purposes only / Follow @0x000000 on Twitter and ask for our cheat sheet containing all solutions / Need a license? / © 2014 MORE BVBA'.

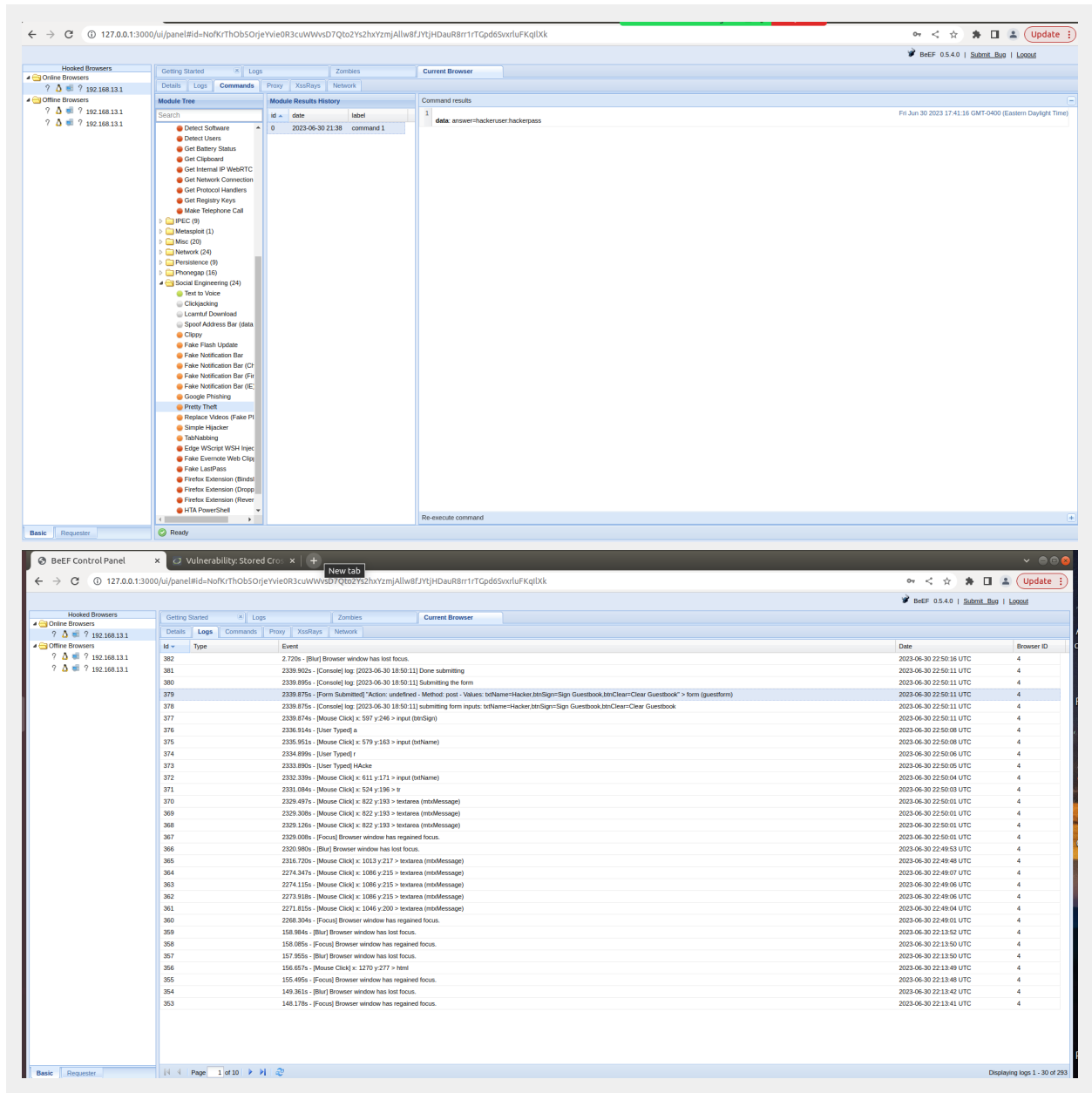
Write two or three sentences outlining mitigation strategies for this vulnerability:

The Brute Force attacks are the most common and harmful types of attacks. One of the most commonly used methods of mitigation is to lock out accounts after a defined number of incorrect password attempts and another is to Employ CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), this will prevent from brute force attack and will make sure that it is a human/user attempting to login.

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

Provide a screenshot confirming that you successfully completed this exploit:





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

To prevent this XSS attacks, it is extremely recommended to make sure that the application validates all and any kind of data imputed, making sure that the data which is being processed is amongst the allowlisted data. This will also make sure that all variable output in a page which has been returned to the user is encoded.

