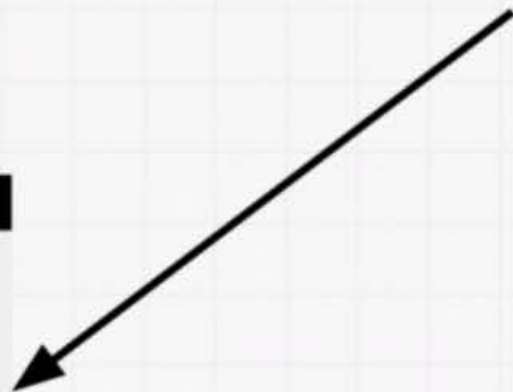


1.



HTML
CODE



1.

INPUT YOUR FIRST NAME

TOM

HELLO TOM!

1.

<H1>TEST</H1>



```
<div class="vulnerable_code_area">  
  <form name="HTMLi" action="#" method="GET">  
    <p>What's your name?</p>  
    <input type="text" name="name">  
    <input type="submit" value="Submit">  
  </form>  
  <pre>Hello Tom</pre>  
</div>
```

1.

<H1>TEST</H1>



```
<div class="vulnerable_code_area">  
  <form name="HTMLi" action="#" method="GET">  
    <p>What's your name?</p>  
    <input type="text" name="name">  
    <input type="submit" value="Submit">  
  </form>  
  <pre>Hello <h1>TEST</h1></pre>  
</div>
```

YEP, THIS IS HTML!



Get Started

Learn with structured pathways or individuals rooms



Pathways

Enroll in a pathway and get structured learning



Series

Complete sets of fun security challenges

Welcome Tasks

- ✔ Join a room
- ✔ Connect to our network
- 🔄 Complete a room



Learning Path

Learn by following a structured learning path

0 Questions

Answered this week

0 🟢



Access via OpenVPN

To access machines, you will need to connect to our network.

OpenVPN Access Details

VPN Server Name

Server Status

Connected

Internal Virtual IP Address



0.0.0.0

Opening printmrhacker.ovpn

You have chosen to open:

printmrhacker.ovpn

which is: ovpn File (8.0 KB)

from: https://tryhackme.com

Would you like to save this file?

Cancel Save File

you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Download My Configuration File

Regenerate

To hack machines on TryHackMe you need to connect to our network

You can connect through OpenVPN, or a Kali Linux machine controlled in your browser.



File Actions Edit View Help

(mrhacker@kali) - [~]

\$ cd /home/mrhacker/Downloads

(mrhacker@kali) - [~/Downloads]

\$ ls

cacert.der printmrhacker.ovpn 11.0.10 from Debian

(mrhacker@kali) - [~/Downloads]

\$ sudo openvpn printmrhacker.ovpn

WARNING: Please consider reporting this to the maintainers of burp.g2k

We trust you have received the usual lecture from the local System

Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

[sudo] password for mrhacker:

```
(mrhacker@kali) - [~/Downloads]
```

- ```
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```

2021-03-11 03:17:29 WARNING: Compression for receiving enabled. Compression

```
2021-03-11 03:17:29 DEPRECATED OPTION: --cipher set to --cipher-suite=TLS_AES_128_GCM_SHA256 is deprecated, please use --cipher-suite=TLS_AES_128_GCM_SHA256 --ssl-mode=REQUIRED instead
```

```
2021-03-11 03:17:29 OpenVPN 2.5.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Oct 28 2020
```

```
2021-03-11 03:17:29 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
```

```
2021-03-11 03:17:29 TCP/UDP: Preserving recently used remote address: [AF_INET]18.202.129.195:1194
```

```
2021-03-11 03:17:29 UDP link local: (not bound)
```

```
2021-03-11 03:17:29 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=1499cdf4 cdabbee2
```

2021-03-11 03:17:29 VERIFY KU OK

```
2021-03-11 03:17:29 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
```

```
2021-03-11 03:17:29 VERIFY OK: depth=0, CN=server
```

```
2021-03-11 03:17:29 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:1194
```





1861



# OWASP Top 10

Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.

[Start AttackBox](#)[Awards](#)[Help](#)[Options](#)

## Active Machine Information

Title  
Injection v4

IP Address  
10.10.168.40

Expires  
58m 49s

[?](#)[Add 1 hour](#)[Terminate](#)

0%

Task 1 ☐ Introduction



Task 2 ☐ Accessing machines



Task 3 ☐ [Severity 1] Injection



Task 4 ☐ [Severity 1] OS Command Injection



File Actions Edit View Help

(mrhacker@kali) - [~]

\$ ping 10.10.168.40

PING 10.10.168.40 (10.10.168.40) 56(84) bytes of data.

64 bytes from 10.10.168.40: icmp\_seq=1 ttl=63 time=124 ms

64 bytes from 10.10.168.40: icmp\_seq=2 ttl=63 time=87.8 ms

64 bytes from 10.10.168.40: icmp\_seq=3 ttl=63 time=130 ms

64 bytes from 10.10.168.40: icmp\_seq=4 ttl=63 time=84.7 ms

64 bytes from 10.10.168.40: icmp\_seq=5 ttl=63 time=125 ms

64 bytes from 10.10.168.40: icmp\_seq=6 ttl=63 time=81.3 ms

64 bytes from 10.10.168.40: icmp\_seq=7 ttl=63 time=124 ms

64 bytes from 10.10.168.40: icmp\_seq=8 ttl=63 time=91.0 ms

OWASP Top 10

Learn about and exploit each of the OWASP Top 10 vulnerabilities.

Error! User **test** was not found on the system

# Directory Search

Submit

**Error!** User **test** was not found on the **system**

# Directory Search

`<h1>TEST</h1>`|  
I

Submit

Error! User

TEST

was not found on the system

# Directory Search

Submit



- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

  
**Getting Started:  
Project  
Whitepaper**

  
**Release  
Announcements**

 **Back**     **Help Me!**

 **Hints**

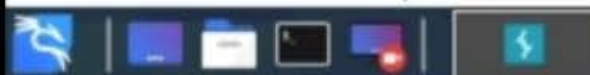
|                           |                                                                      |
|---------------------------|----------------------------------------------------------------------|
| <b>Client IP</b>          | 192.168.1.4                                                          |
| <b>Client Hostname</b>    | 192.168.1.4                                                          |
| <b>Operating System</b>   | Linux                                                                |
| <b>User Agent String</b>  | Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 |
| <b>Referrer</b>           | http://192.168.1.5/mutillidae/                                       |
| <b>Remote Client Port</b> | 33488                                                                |

```
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#

#
Query terms are ambiguous. The query is assumed to be:
"n 192.168.1.4"
#
Use "?" to get help
```

Kali 2021 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



Burp Suite Community E...

Mozilla Firefox

qterminal

Burp Suite Community Edition v...

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.1.5:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw In Actions

```
1 GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
2 Host: 192.168.1.5
3 User-Agent: <h1><u>TEST</u></h1>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.5/mutillidae/
8 Connection: close
9 Cookie: showhints=1; PHPSESSID=5bh3blpvjo06fn8fcav7up04m7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

 Request to http://192.168.1.5:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw In Actions ▾

```
1 GET /mutillidae/index.php?page=capture-data.php HTTP/1.1
2 Host: 192.168.1.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.5/mutillidae/
8 Connection: close
9 Cookie: showhints=1; PHPSESSID=<meta http-equiv="refresh" content="5; URL=https://www.google.com" /> acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```



# OWASP Mutillidae II: Web P

Version: 2.6.24

Security Level: 0 (Hosed)

Hints: Enab

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [E](#)[OWASP 2013](#)[OWASP 2010](#)[OWASP 2007](#)[Web Services](#)[HTML 5](#)[Others](#)[Documentation](#)[Resources](#)

## Discussion o

**Back****Help Me!****Hints**

## Discussion o

The large back button image appears on the site. If the image is clicked the user is redirected to the previous page. The button works by executing a javascript: document.location.href equal to the

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

InterceptHTTP historyWebSockets historyOptions

Request to http://192.168.1.5:80

ForwardDropIntercept is onActionOpen Browser

PrettyRawInActions

1 GET /mutillidae/index.php?page=html5-storage.php HTTP/1.1  
2 Host: 192.168.1.5  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Referer: http://192.168.1.5/mutillidae/index.php?page=back-button-discussion.php  
9 Cookie: shdwhints=1; PHPSESSID=5d1062dec3482uvun5llgaltt0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada  
10 Upgrade-Insecure-Requests: 1  
11  
12



```
<a onclick="document.location.href='<h1>TEST</h1>';">
```

```
<h1>TEST</h1>';">
```

```
"><h1>TEST</h1>
```

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

HTML5

Others

Documentation

Back

Help Me!

Hints

Discussion of Back But

Discussion of Back Button

The large back button image appears automatically c