

SE CREA UN NUEVO USUARIO Y DEVUELVE LA CONTRASEÑA TAMBIEN SE INTERSEPTA EL PAQUETE CON **Burp Suite** Y SE OBTINE TODOS LOS DDTOS YSE REALIZA MODIFICACIONES PARA CAMBIAR EL PAQUETE DE RETORNO

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.12.3 Security Level: 0 (Hosed) Hints: Enabled Logged In Admin: admin

Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

OWASP 2017 OWASP 2013 OWASP 2010 OWASP 2007 Web Services Others Labs Documentation Resources

Donate Want to Help? Video Tutorials Announcements Getting Started

Hints and Videos

TIP: Click [Hint and Videos](#) on each page

What Should I Do? Help Me! Listing of vulnerabilities Video Tutorials Release Announcements Latest Version Helpful Hints and scripts Mutillidae LDIF File

User Lookup (SQL)

Back Help Me!

Switch to SOAP Web Service version Switch to XPath version

Please enter username and password to view account details

Username Password View Account Details

Don't have an account? Please register here

Results for "pikachu": 1 records found.

First Name: perez
Last Name: perez
Username: pikachu
Password: holamundo
Signature:
Client ID: 63a5ce9b20e1666ea5bc6b9ab77bc046
Client Secret: e94b6ced22e7f0015965e447e394816ef9b09388e2e344197e09b554782669ff



Switch to XPath version

Authentication Error: Bad user name or password

Please enter username and password
to view account details

Username

Password

View Account Details

Dont have an account? [Please register here](#)

Response

Pretty Raw Hex Render

```
1287 </tr>
1288 <tr><td></td></tr>
1289 <tr>
1290   <td colspan="2" style="text-align:center;">
1291     <input name="user-info-php-submit-button" class="button" type="submit" value="
View Account Details" />
1292   </td>
1293 </tr>
1294 <tr><td></td></tr>
1295 <tr>
1296   <td colspan="2" style="text-align:center; font-style: italic;">
1297     Dont have an account? <a href="?page=register.php">Please register here</a>
1298   </td>
1299 </tr>
1300 </table>
1301 </form>
1302
1303 <div class="report-header">
1304   Results for &quot;<span style="color:#770000;">poquemon</span>&quot;; 0 records
found.
1305 </div><script>document.getElementById("id-bad-cred-tr").style.display=""</script>
1306 <!-- I think the database password is set to blank or perhaps samurai.
1307 It depends on whether you installed this web app from irongeeks site or
1308 are using it inside Kevin Johnsons Samurai web testing framework.
1309 It is ok to put the password in HTML comments because no user will ever see
1310 this comment. I remember that security instructor saying we should use the
1311 framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
1312 rather than HTML comments, but we all know those
1313 security instructors are just making all this up. --> <!-- End Content -->
1314 </td>
1315 </tr>
1316 <tr class="main-table-frame-dark">
1317   <td colspan="2">
1318     Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/136.0.0.0 Safari/537.36 <br/>
1319     PHP Version: 8.2.12 </td>
1320 </tr>
```

1  Switch to XPath version

Authentication Error: Bad user name or password

Please enter username and password
to view account details

Username

Password

View Account Details

Dont have an account? [Please register here](#)

Results for "poquemon". 0 records found.

User Lookup (SQL)



Back



Help Me!



Switch to SOAP Web Service version



Switch to XPath version

Please enter username and password
to view account details

Username

Password

View Account Details

Dont have an account? [Please register here](#)

Results for "pikachu". 1 records found.

First Name: perez

Last Name: perez

Username: pikachu

Password: holamundo

Signature:

Client ID: 63a5ce9bb0e1666ea5bcb69ab73bc046

Client Secret: e94b6ced22e7f0015965e447e394616e9bd09388e2e344b97e09b554782b69ff

Request cookies			4	^
Name	Value			
PHPSESSID	jqvu3rombgr1eggiltcglhg8vq		>	
showhints	0		>	
username	admin		>	
uid	1		>	
			🗑️	⌵ ⌶ ⌷ +

Request headers

Request headers			17	^
Name	Value			
Host	127.0.0.1		>	
Cookie	PHPSESSID=jqvu3rombgr1eggiltcglhg8vq; showhints=0...		>	
Sec-Ch-Ua	"Not.A/Brand";v="99", "Chromium";v="136"		>	
Sec-Ch-Ua-Mobile	?0		>	
Sec-Ch-Ua-Platform	"Windows"		>	
Accept-Language	es-ES,es;q=0.9		>	
Upgrade-Insecure-Requests	1		>	
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit...		>	
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,i...		>	
Sec-Fetch-Site	same-origin		>	
Sec-Fetch-Mode	navigate		>	
Sec-Fetch-User	?1		>	
Sec-Fetch-Dest	document		>	
Referer	https://127.0.0.1/mutillidae-main/src/index.php?page=...		>	
Accept-Encoding	gzip, deflate, br		>	
Priority	u=0, i		>	
Connection	keep-alive		>	
			🗑️	⌵ ⌶ ⌷ +