

Forum:[Hack Forums](#)

Thread: [This Password Authentication Backdoor Won a DEFCON 23 Contest. Can You Figure it Out?](#)

sarciszewski - January 8, 2016, 5:40 pm

The challenge:

Spoiler ([Click to View](#))

To clarify the usability, assume that your document root is set to public/, such that <http://somedomain.com/foo.php> resolves to public/foo.php, not foo.php.

autoload.php

PHP Code

```
<?php
```

```
/**
 * Too lazy to do a PSR-4 autoloader using spl_autoload(), we only have one
 * class anyway.
 *
 *
 *                                     Scott Arciszewski
 */
require_once "TimingSafeAuth.php";
```

```
/**
 * Generate a random string with our specific charset, which conforms to the
 * RFC 4648 standard for BASE32 encoding.
 *
 * @return string
 */
function noise()
{
    return substr(
        str_shuffle(str_repeat('abcdefghijklmnopqrstuvwxyz234567', 16)),
        0,
        32
    );
}
```

TimingSafeAuth.php:

PHP Code

```
<?php
```

```
/**
 * A password_* wrapper that is proactively secure against user enumeration from
 * the timing difference between a valid user (which runs through the
 * password_verify() function) and an invalid user (which does not).
 */
class TimingSafeAuth
{
    private $db;
```

```

public function __construct(\PDO $db)
{
    $this->db = $db;
    $this->dummy_pw = password_hash(noise(), PASSWORD_DEFAULT);
}

/**
 * Authenticate a user without leaking valid usernames through timing
 * side-channels
 *
 * @param string $username
 * @param string $password
 * @return int|false
 */
public function authenticate($username, $password)
{
    $stmt = $this->db->prepare("SELECT * FROM users WHERE username = :username");
    if ($stmt->execute(['username' => $username])) {
        $row = $stmt->fetch(\PDO::FETCH_ASSOC);
        // Valid username
        if (password_verify($password, $row['password'])) {
            return $row['userid'];
        }
        return false;
    } else {
        // Returns false
        return password_verify($password, $this->dummy_pw);
    }
}
}

```

public/index.php:

PHP Code

```

<?php
require_once dirname(__DIR__).'/autoload.php';
$db = new \PDO('sqlite:'. dirname(__DIR__) . '/database.sql');
session_start();

if (!isset($_SESSION['userid'])) {
    if (!empty($_POST['csrf']) && !empty($_COOKIE['csrf'])) {
        if (hash_equals($_POST['csrf'], $_COOKIE['csrf'])) {
            $auth = new TimingSafeAuth($db);
            $userid = (int) $auth->authenticate($_POST['username'], $_POST['password']);
            if ($userid) {
                // Success!
                $_SESSION['userid'] = $userid;
                header("Location: /");
                exit;
            }
        }
    }
}
require_once dirname(__DIR__).'/secret/login_form.php';
} else {

```

```
require_once dirname(__DIR__).'secret/login_successful.php';
}
```

secret/login_form.php

PHP Code

```
<?php
if (!isset($_COOKIE['csrf'])) {
    $csrf = noise();
    setcookie('csrf', $csrf);
} else {
    $csrf = $_COOKIE['csrf'];
}
?>
<!DOCTYPE html>
<html>
<head>
    <title>Log In</title>
    <link rel="stylesheet" href="/style.css?<?=rand(); ?>" type="text/css" /><?php
/* cache-busting random query string */ ?>
</head>
<body>
<form method="post" action="/">
    <input type="hidden" name="csrf" value="<?=htmlentities($csrf, ENT_QUOTES | ENT_HTML5,
'UTF-8'); ?>" />
    <table>
        <tr>
            <td>
                <fieldset>
                    <legend>Username</legend>
                    <input type="text" name="username" required="required" />
                </fieldset>
            </td>
            <td>
                <fieldset>
                    <legend>Password</legend>
                    <input type="password" name="password" required="required" />
                </fieldset>
            </td>
        </tr>
        <tr>
            <td colspan="2">
                <button type="submit">
                    Log In
                </button>
            </td>
        </tr>
    </table>
</form>
</body>
</html>
```

secret/login_successful.php

PHP Code

```

<?php
<!DOCTYPE html>
<html>
<head>
    <title>Welcome</title>
    <link rel="stylesheet" href="/style.css?<?=rand(); ?>" type="text/css" /><?php
/* cache-busting random query string */ ?>
</head>
<body><?php
if ($_SESSION['userid'] == 1) {
    echo "Welcome great leader!\n";
    echo "<hr />";
    echo "Administrative features: ...";
    /**
     * @todo make the admin account actually useful ;)
     */
} else {
    echo "Welcome, peon.\n";
}
?></body>
</html>

```

The full write-up is available online. Don't feel bad if you can't figure it out at first glance.

Spoiler: [On The Design and Implementation of a Stealth Backdoor for Web Applications](#)

?Criminal - January 8, 2016, 5:45 pm

the backdoor involves the str_shuffle() function, it can easily be guessed since the entropy is not that secure and did you get this from the reddit article on r/netsec/? they explain in detail how it works.

sarciszewski - January 8, 2016, 5:46 pm

(Jan 8, 2016 06:45 PM)?Criminal Wrote: [\[CITE\]](#) the backdoor involves the str_shuffle() function, it can easily be guessed since the entropy is not that secure and did you get this from the reddit article on r/netsec/? they explain in detail how it works.

Nope. I didn't get it from there.

I'm the author of both the UnderCrypto submission as well as the write-up on Paragon Initiative Enterprises' blog. (I also submitted it to /r/netsec.)

I'm Scott, nice to meet you. :)

?Criminal - January 8, 2016, 5:50 pm

(Jan 8, 2016 06:46 PM)sarciszewski Wrote: [\[CITE\]](#) Nope. I didn't get it from there.

I'm the author of both the UnderCrypto submission as well as the write-up on Paragon Initiative Enterprises' blog. (I also submitted it to /r/netsec.)

I'm Scott, nice to meet you. :)

Nice to meet you as well and im subscribed to the latest feeds I remember when webRTC first came out on there and 2-3 weeks later everyone was making their own variations of it in IP loggers although im sure people were aware of the flaw way before it was publicized. But on topic yeah its a pretty interesting backdoor I think from an attackers perspective the idea of intentional honeypotting stuff is a smart idea especially if its a big web app alot of people use.

sarciszewski - January 8, 2016, 5:58 pm

(Jan 8, 2016 06:50 PM)?Criminal Wrote: [\[CITE\]](#) Nice to meet you as well and im subscribed to the latest feeds I remember when webRTC first came out on there and 2-3 weeks later everyone was making their own variations of it in IP loggers although im sure people were aware of the flaw way before it was publicized. But on topic yeah its a pretty interesting backdoor I think from an attackers perspective the idea of intentional honeypotting stuff is a smart idea especially if its a big web app alot of people use. Thanks :)

The [Underhanded Crypto Contest](#) is pretty neat. I highly encourage everyone to look into entering the one at DEFCON 24 if they're going. (Even if you're not, the organizers might open it up to the Internet again.)

Fleckens - January 8, 2016, 6:01 pm

I don't know anything about this topic but I find it highly interesting

sinmar - January 8, 2016, 6:04 pm

(Jan 8, 2016 06:46 PM)sarciszewski Wrote: [\[CITE\]](#) Nope. I didn't get it from there.

I'm the author of both the UnderCrypto submission as well as the write-up on Paragon Initiative Enterprises' blog. (I also submitted it to /r/netsec.)

I'm Scott, nice to meet you. :)

what happened to the awesome group you were gonna start on voodooKobra man ??

sarciszewski - January 8, 2016, 6:06 pm

(Jan 8, 2016 07:04 PM)sinmar Wrote: [\[CITE\]](#) what happened to the awesome group you were gonna start on voodooKobra man ??

I vaguely recall expressing interest in starting a group years ago, but there was no real interest in it from the rest of the community-- probably because I don't regularly engage in attention-seeking behavior and most people have me beat in experience there.

(Jan 8, 2016 07:01 PM)Fleckens Wrote: [\[CITE\]](#) I don't know anything about this topic but I find it highly interesting

It's a fun topic. Cryptography is fascinating as hell. (Don't let the depressing droll of the "crack this hash plz?" of the crypto forum here discourage you!)

sinmar - January 8, 2016, 6:12 pm

(Jan 8, 2016 07:06 PM)sarciszewski Wrote: [\[CITE\]](#) I vaguely recall expressing interest in starting a group years ago, but there was no real interest in it from the rest of the community-- probably because I don't regularly engage in attention-seeking behavior and most people have me beat in experience there.

idk i spoke w/ our man J.C. of ic.fbi.gov recently and had some good laughs

sarciszewski - January 8, 2016, 6:14 pm

(Jan 8, 2016 07:12 PM)sinmar Wrote: [\[CITE\]](#) idk i spoke w/ our man J.C. of ic.fbi.gov recently and had some good laughs

Huh. Those initials don't ring a bell.

Anyway, I'm an appsec/crypto consultant these days. Occasionally some troll tries to incite me to commit a high crime and I just shake my head and ignore them.

Spooky White - January 8, 2016, 6:15 pm

Nope, can't tend to figure it out.

hugsyou - January 8, 2016, 6:17 pm

what are all those letters and why are they together

sarciszewski - January 8, 2016, 6:20 pm

(Jan 8, 2016 07:15 PM)MagicFlakes Wrote: [\[CITE\]](#) Nope, can't tend to figure it out.

Peep the [write-up \(contains spoilers\)](#) then. :)

(Jan 8, 2016 07:17 PM)hugsyou Wrote: [\[CITE\]](#) what are all those letters and why are they together
You mean this?

PHP Code

```
<?php
/**
 * Generate a random string with our specific charset, which conforms to the
 * RFC 4648 standard for BASE32 encoding.
 *
 * @return string
 */
function noise()
{
    return substr(
        str_shuffle(str_repeat('abcdefghijklmnopqrstuvwxyz234567', 16)),
        0,
        32
    );
}
```

The string (which is 32 characters long) is repeated 16 times, then shuffled, and the first 32 characters of the shuffled output are returned.

Any arbitrary string would work here, I just chose base32 because it's the easiest to read at a glance.

D?ath - January 8, 2016, 6:34 pm

[Video: <https://www.youtube.com/watch?v=Ccoj5lhLmSQ>]

hugsyou - January 8, 2016, 6:34 pm

(Jan 8, 2016 07:34 PM)D?ath Wrote: [\[CITE\]](#) [Video:

<https://www.youtube.com/watch?v=Ccoj5lhLmSQ>] (Jan 8, 2016 07:17 PM)hugsyou Wrote: [\[CITE\]](#)

what are all those letters and why are they together

LOL exactly what I was thinking

sarciszewski - January 8, 2016, 6:37 pm

(Jan 8, 2016 07:34 PM)hugsyou Wrote: [\[CITE\]](#) LOL exactly what I was thinking

Well, if anything was confusing, please do tell me what parts need clarification.

D?ath - January 8, 2016, 6:38 pm

(Jan 8, 2016 07:37 PM)sarciszewski Wrote: [\[CITE\]](#) Well, if anything was confusing, please do tell me what parts need clarification.

nah you see, most of us here understand a little bit about everything here. we arent necessarily experts. So seeing something like this is kind of what the youtube reaction is like hahaha

sarciszewski - January 8, 2016, 7:11 pm

(Jan 8, 2016 07:38 PM)D?ath Wrote: [\[CITE\]](#) nah you see, most of us here understand a little bit about everything here. we arent necessarily experts. So seeing something like this is kind of what the youtube reaction is like hahaha

Oh, well, if anyone is interested in catching up sometime, start here:

<https://github.com/paragonie/awesome-appsec>

Fleckens - January 9, 2016, 8:55 am

I see, how to get knowledge of it?

sarciszewski - January 9, 2016, 1:12 pm

(Jan 9, 2016 09:55 AM)Fleckens Wrote: [\[CITE\]](#) I see, how to get knowledge of it?

Knowledge of what? The write-up I linked to in OP explains the vulnerability, the reasoning behind its design and implementation, and how to exploit it.

<https://paragonie.com/blog/2016/01/on-design-and-implementation-stealth-backdoor-for-web-applications>

?Criminal - January 9, 2016, 2:34 pm

(Jan 9, 2016 02:12 PM)sarciszewski Wrote: [\[CITE\]](#) Knowledge of what? The write-up I linked to in OP explains the vulnerability, the reasoning behind its design and implementation, and how to exploit it.

<https://paragonie.com/blog/2016/01/on-design-and-implementation-stealth-backdoor-for-web-applications>

Other sections are better suited then the lounge most people are gonna be like "lol wtf is this".

sarciszewski - January 9, 2016, 2:53 pm

Which sections would you recommend in particular? I've always sort of just saw this place as the "if it doesn't fit anywhere else" dumping ground.

?Criminal - January 10, 2016, 8:56 am

(Jan 9, 2016 03:53 PM)sarciszewski Wrote: [\[CITE\]](#) Which sections would you recommend in particular? I've always sort of just saw this place as the "if it doesn't fit anywhere else" dumping ground.

Either cryptography or the php section.

sarciszewski - March 13, 2016, 5:23 pm

(Jan 10, 2016 09:56 AM)?Criminal Wrote: [\[CITE\]](#) Either cryptography or the php section. Cryptography is full of cancer. "Crack this hash plz?"

I started a few threads hoping to spark positive discussion, but they got buried under the bullshit.

At least [Taylor Swift](#) liked my post :(

WOLGA - March 13, 2016, 5:42 pm

Hey OP! If you made this, please consider yourself one of the top (PHP) programmers on this site.

sarciszewski - March 13, 2016, 9:45 pm

(Mar 13, 2016 05:42 PM)Qwertyuiopasdfghjklzxc Wrote: [CITE](#) Hey OP! If you made this, please consider yourself one of the top (PHP) programmers on this site.

Hey, thanks. Yeah, this was my UCC entry and subsequent write-up.