# Securing Synoptic

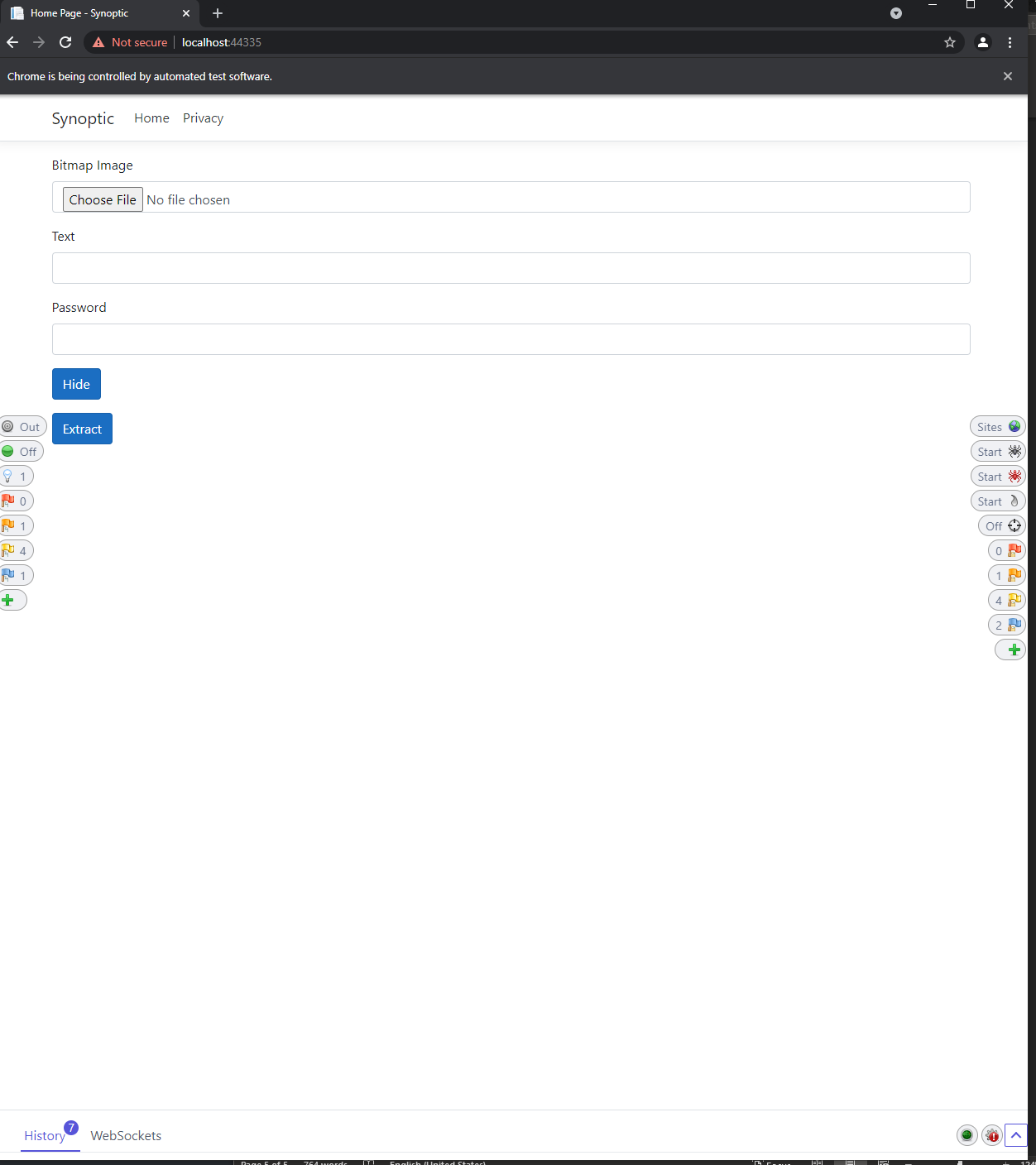
### Threats

|  |  |
| --- | --- |
| Id | TR1 |
| Name | Adversary tries to upload a very large file |
| Description | Adversary tries to upload a very large file, above 28.6 MB. This causes an HTTP error to be thrown, as the global upload size limit for IIS Express 7 is 28.6MB. Using this, an attacker can determine what server the website is using, and using this information, can discover more dangerous attacks. |
| Stride | Using Components with Known Vulnerabilities |
| Entry Points | Index form |
| Assets | Server |
| Mitigation Strategy | Changing Error page to not show any server information |

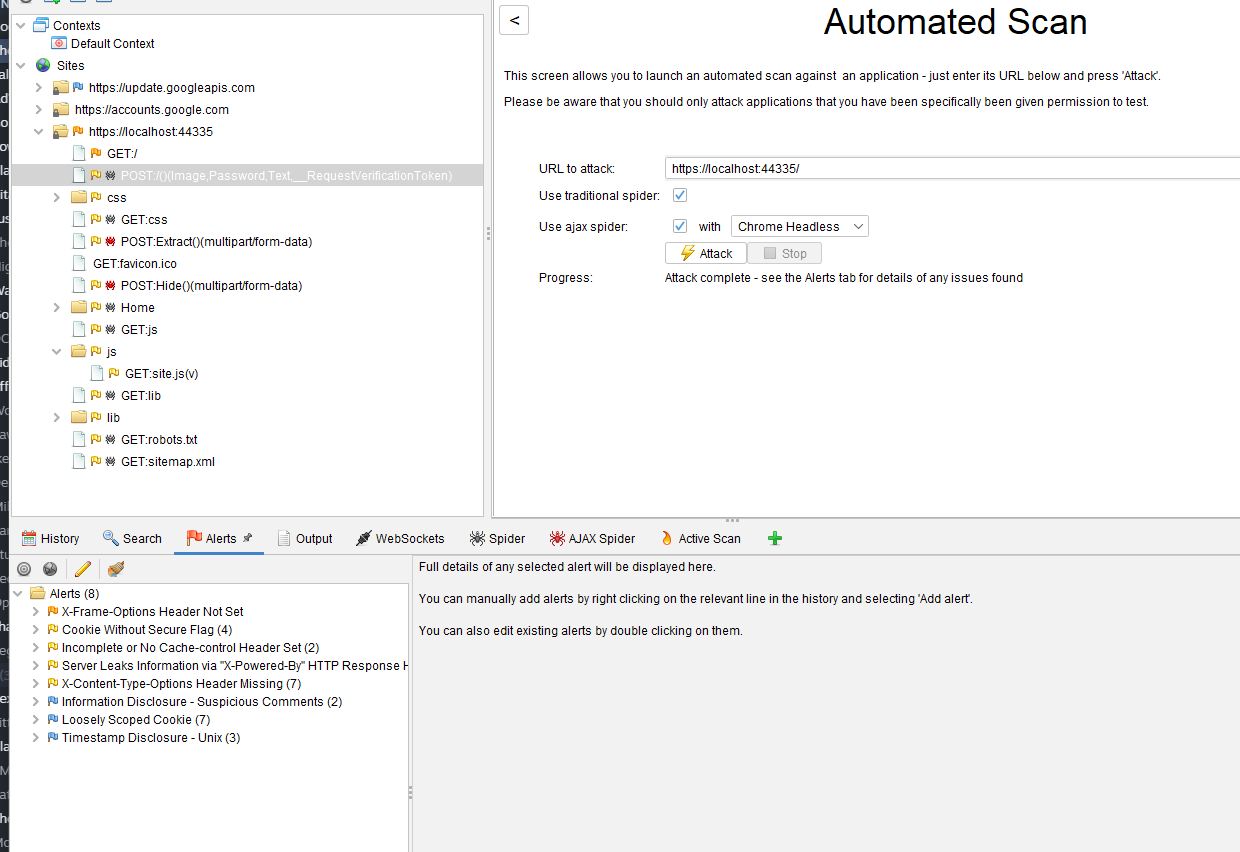
|  |  |
| --- | --- |
| Id | TR2 |
| Name | Adversary tries to supply malicious data inside bitmap file |
| Description | Adversary tries to upload bitmap image with malicious code hidden inside |
| Stride | Tampering, Injection |
| Entry Points | Index form |
| Assets | Server |
| Mitigation Strategy | Even further checks to make sure that the data uploaded is not malicious |

### ZAP Attack

Started in Manual mode to load website in ZAP



Did an automated attack to get more information on the site



Put a breakpoint on the site to grab all changes, and sent a small file to have its text extracted to see how the body is changed

