		STI3					
			Done	52			
			Missing	0			
ID	Code	Name	Status				
4							
4.1							
4.1.1	WSTG-INFO-01	Conduct Search Engine Discovery Reconnaissance for Inforr	☑	not aplicable			
4.1.2	WSTG-INFO-02	Fingerprint Web Server	☑	applicable			
4.1.3	WSTG-INFO-03	Review Webserver Metafiles for Information Leakage	☑	applicable			
4.1.4	WSTG-INFO-04	Enumerate Applications on Webserver	☑	applicable			\
4.1.5	WSTG-INFO-05	Review Webpage Comments and Metadata for Information	☑	applicable			
4.1.6	WSTG-INFO-06	Identify Application Entry Points	☑	applicable			
4.1.7	WSTG-INFO-07	Map Execution Paths Through Application	☑	applicable			
4.1.8	WSTG-INFO-08	Fingerprint Web Application Framework	☑	applicable			
4.1.9	WSTG-INFO-09	Fingerprint Web Application	☑	not aplicable(ish)			
4.1.10	WSTG-INFO-10	Map Application Architecture	☑	applicable			
4.2							
4.2.1	WSTG-CONF-01	Test Network Infrastructure Configuration	☑	applicable			
4.2.2	WSTG-CONF-02	Test Application Platform Configuration	☑	applicable			
4.2.3	WSTG-CONF-03	Test File Extensions Handling for Sensitive Information	☑	applicable			
4.2.4	WSTG-CONF-04	Review Old Backup and Unreferenced Files for Sensitive Info	☑	applicable			
4.2.5	WSTG-CONF-05	Enumerate Infrastructure and Application Admin Interfaces	☑	not applicable			
4.2.6	WSTG-CONF-06	Test HTTP Methods	☑	applicable			
4.2.7	WSTG-CONF-07	Test HTTP Strict Transport Security	☑	not applicable			
4.2.8	WSTG-CONF-08	Test RIA Cross Domain Policy	☑	not applicable			
4.2.9	WSTG-CONF-09	Test File Permission	☑	applicable(ish)			
4.2.10	WSTG-CONF-10	Test for Subdomain Takeover	☑	not applicable			
4.2.11	WSTG-CONF-11	Test Cloud Storage	☑	not applicable			
4.3							
4.3.1	WSTG-IDNT-01	Test Role Definitions	☑	applicable			
4.3.2	WSTG-IDNT-02	Test User Registration Process	☑	applicable			
4.3.3	WSTG-IDNT-03	Test Account Provisioning Process	☑	applicable			
4.3.4	WSTG-IDNT-04	Testing for Account Enumeration and Guessable User Accou	☑	applicable			
4.3.5	WSTG-IDNT-05	Testing for Weak or Unenforced Username Policy	☑	not applicable			
4.4							
4.4.1	WSTG-ATHN-01	Testing for Credentials Transported over an Encrypted Chan	☑	not applicable			
4.4.2	WSTG-ATHN-02	Testing for Default Credentials	☑	applicable			
4.4.3	WSTG-ATHN-03	Testing for Weak Lock Out Mechanism	☑	applicable			

4.4.4	WSTG-ATHN-04	Testing for Bypassing Authentication Schema	☑	applicable			
4.4.5	WSTG-ATHN-05	Testing for Vulnerable Remember Password	☑	applicable			
4.4.6	WSTG-ATHN-06	Testing for Browser Cache Weaknesses	☑	applicable			
4.4.7	WSTG-ATHN-07	Testing for Weak Password Policy	☑	applicable			
4.4.8	WSTG-ATHN-08	Testing for Weak Security Question Answer	☑	applicable			
4.4.9	WSTG-ATHN-09	Testing for Weak Password Change or Reset Functionalities	☑	applicable			
4.4.10	WSTG-ATHN-10	Testing for Weaker Authentication in Alternative Channel	☑	applicable			
4.5							
4.5.1	WSTG-ATHZ-01	Testing Directory Traversal File Include	☑	applicable			
4.5.2	WSTG-ATHZ-02	Testing for Bypassing Authorization Schema	☑	applicable			
4.5.3	WSTG-ATHZ-03	Testing for Privilege Escalation	☑	applicable			
4.5.4	WSTG-ATHZ-04	Testing for Insecure Direct Object References	☑	applicable			
4.6							
4.6.1	WSTG-SESS-01	Testing for Session Management Schema	☑	applicable			
4.6.2	WSTG-SESS-02	Testing for Cookies Attributes	☑	applicable			
4.6.3	WSTG-SESS-03	Testing for Session Fixation	☑	applicable			
4.6.4	WSTG-SESS-04	Testing for Exposed Session Variables	☑	applicable			
4.6.5	WSTG-SESS-05	Testing for Cross Site Request Forgery	☑	applicable			
4.6.6	WSTG-SESS-06	Testing for Logout Functionality	☑	applicable			
4.6.7	WSTG-SESS-07	Testing Session Timeout	☑	not applicable			
4.6.8	WSTG-SESS-08	Testing for Session Puzzling	☑	not applicable			
4.7							
4.7.1	WSTG-INPV-01	Testing for Reflected Cross Site Scripting		applicable			
4.7.2	WSTG-INPV-02	Testing for Stored Cross Site Scripting					
4.7.3	WSTG-INPV-03	4.7.3 Testing for HTTP Verb Tampering					
4.7.4	WSTG-INPV-04	4.7.4 Testing for HTTP Parameter Pollution					
4.7.5	WSTG-INPV-05	4.7.5 Testing for SQL Injection		applicable			
4.7.5.1	-	Testing for Oracle					
4.7.5.2	-	Testing for MySQL					
4.7.5.3	-	Testing for SQL Server					
4.7.5.4	-	Testing PostgreSQL					
4.7.5.5	-	Testing for MS Access					
4.7.5.6	-	Testing for NoSQL Injection					
4.7.5.7	-	Testing for ORM Injection					
4.7.5.8	-	Testing for Client Side					
4.7.6	WSTG-INPV-06	Testing for LDAP Injection					
4.7.7	WSTG-INPV-07	Testing for XML Injection					
4.7.8	WSTG-INPV-08	Testing for SSI Injection	☑				
4.7.9	WSTG-INPV-09	Testing for XPath Injection					

4.7.10	WSTG-INPV-10	Testing for IMAP SMTP Injection					
4.7.11	WSTG-INPV-11	Testing for Code Injection					
4.7.11.1	-	Testing for Local File Inclusion					
4.7.11.2	-	Testing for Remote File Inclusion					
4.7.12	WSTG-INPV-12	Testing for Command Injection					
4.7.13	WSTG-INPV-13	Testing for Buffer Overflow					
4.7.13.1	-	Testing for Heap Overflow					
4.7.13.2	-	Testing for Stack Overflow					
4.7.13.3	-	Testing for Format String					
4.7.14	WSTG-INPV-14	Testing for Incubated Vulnerability					
4.7.15	WSTG-INPV-15	Testing for HTTP Splitting Smuggling					
4.7.16	WSTG-INPV-16	Testing for HTTP Incoming Requests					
4.7.17	WSTG-INPV-17	Testing for Host Header Injection					
4.7.18	WSTG-INPV-18	Testing for Server Side Template Injection					
4.8							
4.8.1	WSTG-ERRH-01	Testing for Error Code	☑	applicable			
4.8.2	WSTG-ERRH-02	Testing for Stack Traces	☑	applicable			
4.9							
4.9.1	WSTG-CRYP-01	-					
4.9.2	WSTG-CRYP-02	-					
4.9.3	WSTG-CRYP-03	-					
4.9.4	WSTG-CRYP-04	-					
4.10							
4.10.1	WSTG-BUSL-01	-					
4.10.2	WSTG-BUSL-02	-					
4.10.3	WSTG-BUSL-03	-					
4.10.4	WSTG-BUSL-04	-					
4.10.5	WSTG-BUSL-05	-					
4.10.6	WSTG-BUSL-06	-					
4.10.7	WSTG-BUSL-07	-					
4.10.8	WSTG-BUSL-08	-					
4.10.9	WSTG-BUSL-09	-					
4.11							
4.11.1	WSTG-CLNT-01	Testing for DOM-Based Cross Site Scripting					
4.11.2	WSTG-CLNT-02	Testing for JavaScript Execution					
4.11.3	WSTG-CLNT-03	Testing for HTML Injection					
4.11.4	WSTG-CLNT-04	Testing for Client Side URL Redirect					
4.11.5	WSTG-CLNT-05	Testing for CSS Injection					
4.11.6	WSTG-CLNT-06	Testing for Client Side Resource Manipulation					

4.11.7	WSTG-CLNT-07	Testing Cross Origin Resource Sharing	☑				
4.11.8	WSTG-CLNT-08	Testing for Cross Site Flashing					
4.11.9	WSTG-CLNT-09	Testing for Clickjacking					
4.11.10	WSTG-CLNT-10	Testing WebSockets					
4.11.11	WSTG-CLNT-11	Testing Web Messaging					
4.11.12	WSTG-CLNT-12	Testing Browser Storage					
4.11.13	WSTG-CLNT-13	Testing for Cross Site Script Inclusion					