

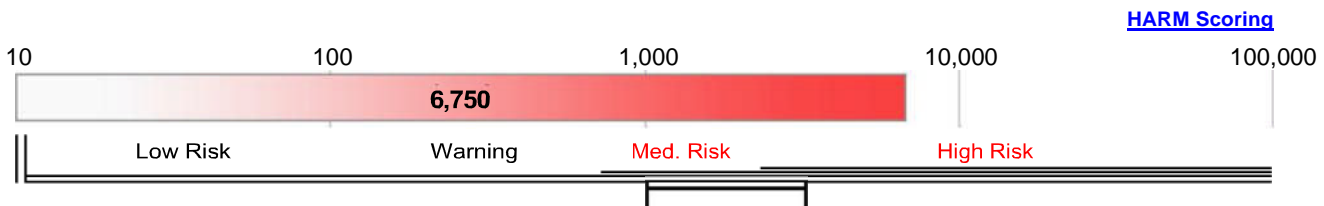
Assessment Report

Date Range: All

Application(s) Assessed: Online Payment

Summary

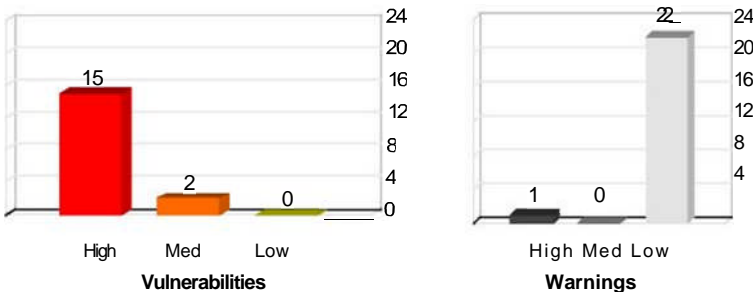
An assessment was performed on the 'Online Payment' application, using 7 SmartAttacks™ to identify vulnerabilities. As shown below, a large number of issues were found with the application that resulted in a **very high HARM™ score of 6750**, which is commonly seen when there is at least one broadly repeated significant vulnerability. Typical HARM scores for complete assessments of individual non-remediated applications range from 1000 to 4500. **It is recommended that action be taken to remediate these vulnerabilities.** The tests performed, as well as specific vulnerabilities to be remediated, and their contribution to the total HARM score, can be viewed in the "SmartAttack Results (by HARM)" section of this report below.



Total HARM™ Score: 6750 = 6750 (Raw Scores) x 1.0 (App Risk Factor)

Common Range For Unremediated Applications

The '**Total HARM Score**', above, is a sum of the HARM scores for all the SmartAttack assessments included in this report. SmartAttacks have different HARM scores based on the risks associated with each kind of vulnerability. The charts reflect the raw HARM scores without application specific risk adjustments.



Severity of Findings

[Severity Drill Down](#) [Severity Drill-down w/Info Items](#)

Pages Tested	49
Attack Count	1809
Informational Items	2

0 Note: **High, Med. & Low** relate to the severity of the findings. **Warnings** are findings for which there is less confidence of accuracy. These items may or may not be real vulnerabilities.

SmartAttack.	High Severity		Medium and Low Severity	
	Vuln.	Warn.	Vuln.	Warn.
Cross-Site Scripting	11	0	SQL Error Message	2 0
SQL Disclosure	3	0	Web Server Version Vulnerabilities	0 22
Blind SQL Injection	1	0		
Buffer Overflow	0	1		

SmartAttack Results (by HARM) [SmartAttack Drill-down](#) [SmartAttack Drill-down w/Info Items](#)

SmartAttack	Status	Severity	HARM	Vuln	Warning	Info	Attacks	Pages	Doc
Cross-Site Scripting	Alert	High	3520	11	0	0	370	55	Doc
SQL Disclosure	Alert	High	2304	3	0	0	349	55	Doc
Blind SQL Injection	Note	High	230	1	0	0	490	49	Doc
Buffer Overflow	Note	High	192	0	1	0	101	49	Doc
Windows Command Injection	Ok	High	0	0	0	0	329	6	Doc
SQL Error Message	Note	Medium	240	2	0	0	121	49	Doc
Web Server Version Vulnerabilities	Alert	Low	264	0	22	2	49	49	Doc

Detail (by SmartAttack / Report Item Type) [High Detail](#) [HighDetail w/Info Items](#) [\(Condensed Format\)](#)

Testing Summary (by Job Run)

Application: Online Payment

Job	Start Time	Duration	Pages	Attacks	HARM
test job localhost-	2/28/2007 11:35:46AM	00:04:46	6	826	2496
Demo (2)	11/1/2007 7:41:44AM	00:04:21	49	983	4254

Note: Detailed individual findings start on the next page