



Public Penetration Testing Assessment Report



Date: 01-19-2023

High Bit Security performed a baseline penetration test for Action Verb, LLC (DBA Files.com) on 10-17-2022 encompassing the scope described below.

Hosts in Scope (By IP Address or Canonical Name)	
ec2-18-233-135-177.compute-1.amazonaws.com	
ec2-34-204-150-23.compute-1.amazonaws.com	
ec2-34-204-153-236.compute-1.amazonaws.com	
ec2-34-204-236-250.compute-1.amazonaws.com	
ec2-35-170-226-161.compute-1.amazonaws.com	
ec2-35-182-68-20.ca-central-1.compute.amazonaws.com	
ec2-52-23-22-134.compute-1.amazonaws.com	
ec2-52-60-148-20.ca-central-1.compute.amazonaws.com	
ec2-52-71-236-198.compute-1.amazonaws.com	
ec2-54-175-149-222.compute-1.amazonaws.com	
wsip-98-191-176-224.ph.ph.cox.net	
bird29.ganijon-afandi.info	
files-production-proxy-ftp.services.avr53.com	
Applications in Scope (By URL)	
http(s)://pentest.files.com	(primary testing was on this site)
http(s)://pentest1.files.com	(testing on this site was limited to horizontal access control boundary testing)
Test Limitations	
No intentional Denial of Service, memory corruption tests or social engineering.	
Exceptions	
None.	

The penetration test was conducted by High Bit Security's certified security engineers. If we identified security vulnerabilities we provided remediation advice. High Bit Security performed a remediation test (if required), or a regularly scheduled monthly test, on 01-19-2023 and confirmed that all previously identified vulnerabilities were either corrected, or had been adequately addressed through other controls, or are listed as exceptions on this report.

High Bit Security used both automated and manual efforts in penetration testing. Subject to any limitations given above, web applications received testing for all vulnerabilities defined in the current OWASP testing guide, not just the OWASP top ten. Any firewalls, other network devices or supporting hosts identified by IP above were evaluated for common misconfiguration and conformance to security best practices.

High Bit Security clients are required to correct **all identified faults**, including low severity faults, before we will issue this report with a site seal. While no application or system can be 100% secure, all of our security findings were corrected or addressed and it is our opinion that the applications tested are reasonably well written from a security perspective and the applications and supporting systems are deployed, configured and implemented in a secure manner.

Disclaimer

High Bit Security conducted this testing on the applications and systems that existed as of 10-17-2022. Information security threats are continually changing, with new vulnerabilities discovered on a daily basis, and no application can ever be 100% secure no matter how much security testing is conducted. This report is intended only to provide documentation that Action Verb, LLC (DBA Files.com) has corrected all findings noted by High Bit Security as of 01-19-2023. This report cannot and does not protect against personal or business loss as the result of use of the applications or systems described. High Bit Security offers no warranties, representations or legal certifications concerning the applications or systems we test. All software includes defects: nothing in this document is intended to represent or warrant that security testing was complete and without error, nor does this document represent or warrant that the application tested is suitable to task, free of other defects than reported, fully compliant with any industry standards, or fully compatible with any operating system, hardware, or other application. By using this information you agree that High Bit Security shall be held harmless.