

EXPERIMENT 04

VIRUSTOTAL :

Not Vulnerable :

http://testphp.vulnweb.com/

Q

↑

☰

Sign in

0 / 89

Community Score

✓ No security vendors flagged this URL as malicious

⌂

http://testphp.vulnweb.com/
testphp.vulnweb.com

200
Status

2022-10-07 11:24:50 UTC
3 days ago

🌐

DETECTION

DETAILS

LINKS

COMMUNITY 1

Security Vendors' Analysis

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
Avira	✓ Clean	BADWARE.INFO	✓ Clean
benkow.cc	✓ Clean	Bfore AI PreCrime	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean

Vulnerable:

aa1b94c74a936791b118b9f6de9fdceeb02ab3715b738bdb2e30bb49a775ff00

Q

↑

☰

Sign in

17 / 63

Community Score

ⓘ 17 security vendors and no sandboxes flagged this file as malicious

⌂

aa1b94c74a936791b118b9f6de9fdceeb02ab3715b738bdb2e30bb49a775ff00
370dc901f07621fdeb64e4d61d7431ac5ac86aff5c0b6b05dcbdc1998abfd3072e676f.zip

1.38 KB
Size

2022-09-22 01:34:17 UTC
19 days ago

📁
ZIP

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Security Vendors' Analysis

Arcabit	ⓘ Trojan.Bat.1	Avast	ⓘ Other:Malware-gen [Trj]
AVG	ⓘ Other:Malware-gen [Trj]	BitDefender	ⓘ Gen:Heur.Bat.1
DrWeb	ⓘ BAT.Renamer.62	Emsisoft	ⓘ Gen:Heur.Bat.1 (B)
ESET-NOD32	ⓘ BAT/Agent.PLJ	Fortinet	ⓘ BAT/Renamer.5478tr
GData	ⓘ Gen:Heur.Bat.1	Google	ⓘ Detected
Ikarus	ⓘ Gen.Bat	MAX	ⓘ Malware (ai Score=82)
McAfee-GW-Edition	ⓘ Artemis	NANO-Antivirus	ⓘ Trojan.Script.Renamer.jpdsf
Sangfor Engine Zero	ⓘ Malware.Generic-Script.Save.96b62b42	Trellix (FireEye)	ⓘ Gen:Heur.Bat.1

Netsparker:

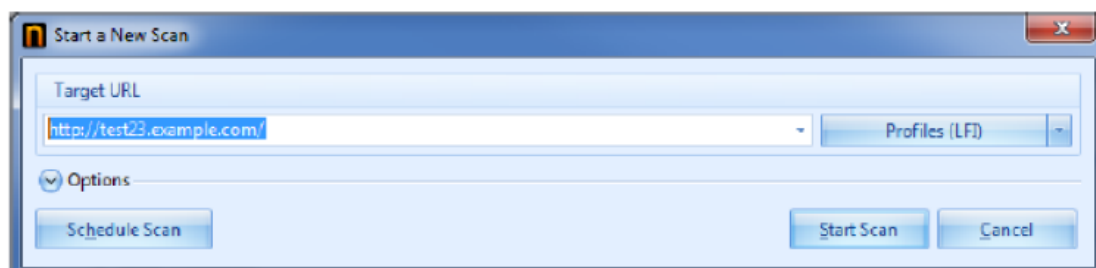
Sample Usages:

Scan `http://test23.example.com` and save the report to `C:\reports\report.pdf`.

Netsparker /a /url `http://test23.example.com` /rf pdf /r `C:\reports\scanreport.pdf`

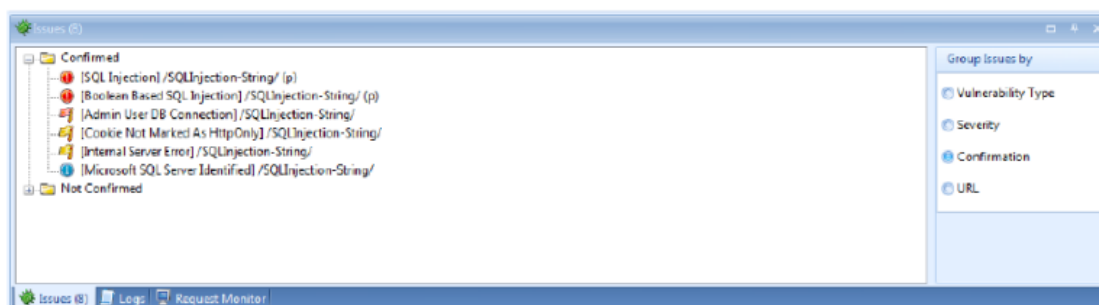
Launch a new scan parameter with a custom profile and URL:

Netsparker /url `http://test23.example.com` /p LFI



SQL INJECTION:

You can exploit the Error Based or Boolean Based SQL Injection vulnerabilities identified in the web application and run custom SQL queries in the application's database via Netsparker's SQL Injection panel.



From the issues in the Issues panel choose a confirmed “SQL Injection” or “Boolean Based SQL Injection” issue, click the Execute SQL Commands button and the SQL Injection panel will appear where you can run custom SQL queries.



Fig: Running Custom SQL Queries in SQL Injection Panel

Afterwards, you can type an SQL query and run the query with the **Run Query** button. Response of the query will be displayed in the panel.

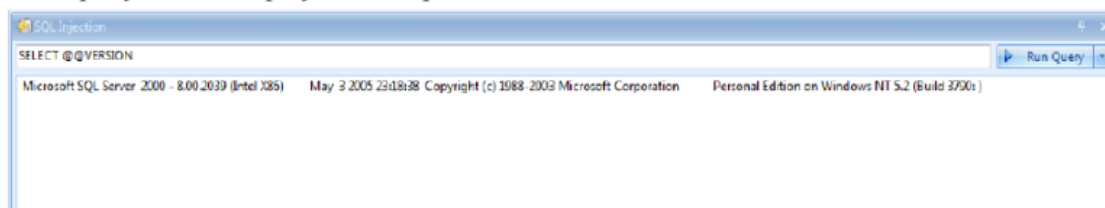


Fig:Sample Custom SQL Query Output

