ExploitMe: Free Firefox Plug-Ins Test Web Apps

Tools run directly on the browser and target pervasive XSS, SQL injection vulnerabilities in Web apps

OCTOBER 24, 2007 | 5:40 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

Canadian researchers have built a set of free exploit tools for Web applications that run as Firefox browser plug-ins; the so-called ExploitMe suite includes tools for cross-site scripting (XSS) and SQL injection, two of the most common vulnerabilities found on Websites.

Nishchal Bhalla, founder of Security Compass, and his fellow researchers at the firm will demonstrate and release the new exploit tools -- aimed at facilitating penetration testing of Web applications -- at next month's SecTor security conference in Toronto. The tools let researchers, Web app developers, and quality assurance staffers "fuzz" their Web apps for vulnerabilities to XSS and SQL injection attacks.

"We actually plugged it [the tools] right into the browser logic so it sees things the way the browser does," says Oliver Lavery, principal consultant with Security Compass and one of the developers of the ExploitMe tools.

And having the exploit, or penetration testing, tool inside the browser is especially helpful when it comes to detecting bugs, such as XSS, which actually gets exploited via the browser. "Because cross-site scripting exists within the browser, it's harder to detect" with other tools that run outside the browser, Lavery says.

There are other handy Web app hacking tools available for free today, such as Paros Proxy, Burp Suite, and WebScarab, but unlike ExploitMe, they are basically proxy tools that emulate the browser. "They intercept requests, and tend to do XSS on the basis of the data they collect," SecurityCompass' Bhalla says. "They emulate a browser, which is where problems happen with detection. Ours is tied into the browser." (See Weaponizing All Browsers.)

Renowned researcher HD Moore, creator of the popular Metasploit pen-testing tool, says the browser-based exploit approach indeed makes it easier for security researchers to detect bugs in sites that are "heavy on client-side scripting," such as XSS.

The tool also reaps the home-field advantage benefits of being on the browser: "The browser already does the hard work of processing JavaScript, negotiating SSL, loading Flash, and handling authentication. All the plug-in needs to do is leverage the existing data," says Moore, director of security research for BreakingPoint Systems. "Stand-alone Web assessment tools have to re-invent the wheel when it comes to processing Web pages and acting like a 'real' user. This is a hard job, and because of it, many of the stand-alone tools do a poor job when the site in question is heavy on client-side scripting."

But there are risks, too, in embedding an exploit tool into the browser, Moore says. "It becomes really easy for a malicious operator to subvert your tool for their own use. Any hacking-specific extensions should be kept disabled, it's just too easy to make a mistake," he says.

Moore says other tradeoffs include limitations with how it interacts with other services, such as a central database. "Additionally, automation is difficult when the entire toolkit lives within a browser. A single, unhandled JavaScript alert could stall the tool indefinitely," he says.

The ExploitMe tools -- which are in currently in beta form -- include SQL Inject-Me, which lets you right-click on an HTML field in your Firefox browser and inject it with SQL injection payloads, and XSS-Me, which works the same way, but with XSS. The tools developers also plan to release Web services exploit tools as well. They chose Firefox mainly due to its interface for writing plug-ins, Bhalla says. "It lets you write

- DISCUSS
- EMAIL
- PRINT
- LINK/REPRINT
- SHARE
- RSS

RELATED

VIDEO

Dan Kaminsky, Director - Penetration Testing, IOActive
PLAY (06:49)
Flaws: Back to the Future

Jennifer Granick, Director - Cyberlaw Clinic, Stanford Law School
PLAY (05:33)
Is That Legal?

NEWS ANALYSIS
- Bots Rise in the Enterprise 10/29/2007
- Researchers Fear Reprisals From Storm 10/29/2007

RESEARCH
- Web App Firewalls: Who's Doing What
- Web Services & Grid Computing: Synergy Rules
- MicroTCA & AdvancedMC: Delivering on the Promise
- Service Delivery and XML: The Path to Carrier SOA
- Mobile Malware: The Enterprise at Risk

WEBINAR ARCHIVE
- Security Update: eCards, Email Threats and Compliance 10/24/2007
- The Impact of Wireless LAN Technology on Compliance to the PCI Data Security Standard* 11/8/2006

COLUMNS
- Phishing's Future Scapegoats 10/17/2007
- Online Games &

US Cybersecurity Policy Advisers Named
Credit Card Holders Suffer for Their Art
Feds: 30 Security Incidents per Day
MORE KEYHOLE

BUGS

ENTERPRISE VULNERABILITIES

Vulnerability: phpBasic phpBasic
Published: 2007-10-30
Severity: MEDIUM
Description: php remote file inclusion vulnerability in includes.php in phpbasic allows remote attackers to execute arbitrary php code via a url in the root parameter, possibly related to the music module.

Vulnerability: SiteBar SiteBar
Published: 2007-10-30
Severity: MEDIUM
Description: command.php in sitebar 3.3.8 allows remote attackers to redirect users to arbitrary web sites via the forward parameter in a log in action.

Vulnerability: SiteBar SiteBar
Published: 2007-10-30
Severity: MEDIUM
Description: absolute path traversal vulnerability in the translation module (translator.php) in sitebar 3.3.8 allows remote authenticated users to read arbitrary files via an absolute path in the dir parameter, a different vulnerability than cve-2007-5491.

Vulnerability: SiteBar SiteBar
Published: 2007-10-30
Severity: MEDIUM
Description: eval injection vulnerability in the translation module (translator.php) in sitebar 3.3.8 allows remote authenticated users to execute arbitrary php code via the edit parameter in an

plug-ins to it more easily."

Security Compass' Lavery says unlike full-blown commercial penetration testing tools, ExploitMe is Web application-specific. And ExploitMe is all about making life easier for the security testers and developers, he says. "We were scratching our own itch when we developed this."

"This looks to me to be more of a convenience tool... That's what these types of tools should be designed for -- saving pen-testers time," says Jeremiah Grossman, CTO and founder of WhiteHat Security.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, send us a message.

- BreakingPoint Systems
- WhiteHat Security

DISCUSS EMAIL PRINT LINK/REPRINT SHARE

MESSAGE BOARDS

Discuss this story >

the Law 10/11/2007

REPORTS

- Security's School of Hard Knocks 9/21/2007
- Five Signs That You're Under a Targeted Attack 9/20/2007

upd cmd action, a different vulnerability than cve-2007-5492.

Vulnerability: SiteBar SiteBar
Published: 2007-10-30
Severity: MEDIUM
Description: multiple cross-site scripting (xss) vulnerabilities in sitebar 3.3.8 allow remote attackers to inject arbitrary web script or html via (1) the lang parameter to integrator.php; (2) the token parameter in a new password action, (3) the nid_acl parameter in a <b...

TAG CLOUD

Application scanning | Application Security | Attacks / Exploits / Threats | Authentication | Botnets | Browser security | Computer crime | Consultants | Content filtering | Cross-site

scripting | DOS | Encryption | End-user monitoring | Host Protection | Identity management | Industry Trends | IPS | Law enforcement | Legal & Regulatory Topics | Legislation | Malware | Managed services | Market Research | Messaging Security | Microsoft | PCI | Penetration testing | Penetration testing | Perimeter Security | Phishing | Policy management | Rootkits | Security Administration / Management | Security Industry | Security Services | Social engineering | Spam | Spyware | SQL injection | Storage Security | Stored data losses | Trojans | User privacy | Viruses | Vulnerabilities | Vulnerability assessment | Vulnerability management | Vulnerability Management | Web services security | Worms

Companies
3Com (14), Aventail (7), CA (13), Check Point (26), Cisco (116), Enterasys (5), F-Secure (6), F5 (3), HP (13), IBM (87), Intel (6), ISS (28), Juniper (32), Alcatel-Lucent (1), McAfee (131), Microsoft (958), NetIQ (2), Nokia (3), Nortel (6), Oracle (30), Qualys (2), RSA (35), Secure Computing (14), Sun (6), Symantec (221), Trend Micro (16), VeriSign (30)

Application and Perimeter Security
802.11x (44), Anomaly detection (57), Anti-spam (110), Application quality assurance (20), Application scanning (73), Auditing (25), AVDL (1), Buffer overflows (83), CERT (7), Consultants (93), Cross-site scripting (120), CVE (7), Database encryption (51), Digital vaults (7), DOS (141), EAP/LEAP (1), Email gateways (69), Encryption (91), Filtering (45), Firewalls (223), FIRST (1), HIPAA (74), Host-based IDS (38), Host/server configuration (14), Host/server encryption (6), IDS (11), IDS (130), IM (49), IPS (213), ISO 17799 (8), Key management (52), Least-privilege user (37), License management (27), Malware (869), NAC (222), Network IDS (30), NIST (16), OWASP (12), OWASP (6), Patch management (227), PCI (118), Penetration testing (119), Phishing (453), PKI (37), Rootkits (83), SAML (2), Software metering (3), Source-code auditing (53), SOX (73), SSL (148), Systems integrators (7), VPNs (212), Vulnerability assessment (415), Web App Security Consortium (6), Web App Security Consortium (13), Web application firewall (61), Web services security (280), WLANs (263), Worms (224), WPA (12), XML (26)

Desktop Security
Anti-spam (110), Antivirus (255), Application Security (821), Attacks / Exploits / Threats (1346), Authentication (568), Browser security (505), Digital certificates (47), Digital signatures (33), Disk encryption (41), DRM (45), Encryption (437), File/folder encryption (28), Identity management (212), IM (49), Malware (869), Messaging Security (405), PGP (4), Phishing (453), Rootkits (83), S/MIME (2), Security Administration / Management (1224), Social engineering (226), Spam (431), Spyware (190), Tokens (59), Trojans (237), User privacy (954), Viruses (275), VOIP security (90), Vulnerabilities (1915), Vulnerability Management (339), Worms (224)

Discovery and management
Anomaly detection (57), Application scanning (73), AVDL (1), Black Hat (94), COBIT (8), Consultants (93), Content filtering (109), CVE (7), End-user monitoring (168), Filtering (45), FISMA (17), HIPAA (74), Host intrusion prevention (93), Host-based IDS (38), IDS (130), IDS (11), IPS (213), ISACA (1), ISO 17799 (8), Log aggregation (30), Network IDS (30), OWASP (6), OWASP (12), PCI (118), Penetration testing (114), Penetration testing (119), SAML (2), SIM/SEM (131), Source-code auditing (53), SOX (73), Vulnerability assessment (415), Vulnerability management (554), Web App Security Consortium (6)

Host security
802.11x (44), Application quality assurance (20), Authentication (568), Backup security (49), Biometrics (123), Buffer overflows (83), Digital certificates (47), Disk encryption (41), Encryption (437), End-user monitoring (168), HIPAA (74), Host anti-spam (60), Host anti-spyware (82), Host antivirus (79), Host intrusion prevention (93), Host Protection (305), Host-based IDS (38), Host/server configuration (14), Host/server encryption (6), Host/server patching (9), IDS (11), IEEE (4), ISO 17799 (8), Least-privilege user (37), License management (27), NAC (222), P2P management (21), Patch management (227), PGP (10), Port control (10), Single sign-on (49), Smart cards (60), Software metering (3), SOX (73), Systems integrators (7), TCG (17), Tokens (59), User privacy (954), Vulnerability Management (339), WPA (12)

Security services
Agency application (2), Application quality assurance (20), Application scanning (73), AVDL (1), COBIT (8), Consultants (93), FISMA (17), HIPAA (74), ISO 17799 (8), Managed services (209), PCI (118), Penetration testing (114), PKI (37), Policy management (300), SIM/SEM (131), Source-code auditing (53), SOX (73), Systems integrators (7)

Storage Security
AES (10), Backup security (49), COBIT (8), Database encryption (51), DES (3), Digital vaults (7), Disk encryption (41), Encryption (91), File/folder encryption (28), FIPS-140-2 (1), FISMA (17), Hashing algorithms (12), HIPAA (74), Host/server encryption (6), Identity management (72), ISO 17799 (8), Key management (52), Law enforcement (593), Legislation (192), Offsite backup (19), PCI (118), PKI (37), SOX (73), Stored data losses (222), Systems integrators (7), Triple DES (3), User privacy (954)

Wireless Security
802.11x (44), AES (10), Auditing (25), COBIT (8), Credential service provider (6), DES (3), Digital certificates (47), Digital signatures (33), DOS (141), EAP/LEAP (1), FISMA (17), Hashing algorithms (12), HIPAA (74), Host/server encryption (6), IEEE (4), IETF (9), ISO 17799 (8), Key management (52), NAC (222), Network IDS (30), PCI (118), Penetration testing (114), PKI (37), Port control (10), Tokens (59), Triple DES (3), VPNs (212), Vulnerability assessment (415), WLANs (263), WPA (12)