# ISS/NASA Prototype Dev Report w/ Database

## Sites: https://tracking-protection.cdn.mozilla.net https://content-signature-2.cdn.mozilla.net https://cdn.jsdelivr.net https://shavar.services.mozilla.com http://127.0.0.1:8000 https://location.services.mozilla.com https://firefox.settings.services.mozilla.com

### Generated on Tue, 11 Apr 2023 06:21:21

### Summary of Alerts

| Risk Level | Number of Alerts |
|---|---|
| High | 1 |
| Medium | 3 |
| Low | 5 |
| Informational | 5 |

### Alerts

| Name | Risk Level | Number of Instances |
|---|---|---|
| Cross Site Scripting (Reflected) | High | 2 |
| Content Security Policy (CSP) Header Not Set | Medium | 21 |
| Cross-Domain Misconfiguration | Medium | 6 |
| Hidden File Found | Medium | 4 |
| Cookie No HttpOnly Flag | Low | 5 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 51 |
| Strict-Transport-Security Header Not Set | Low | 18 |
| Timestamp Disclosure - Unix | Low | 21 |
| X-Content-Type-Options Header Missing | Low | 27 |
| Information Disclosure - Suspicious Comments | Informational | 6 |
| Re-examine Cache-control Directives | Informational | 4 |
| Retrieved from Cache | Informational | 23 |
| User Agent Fuzzer | Informational | 96 |
| User Controllable HTML Element Attribute (Potential XSS) | Informational | 14 |

### Alert Detail

| High | Cross Site Scripting (Reflected) |
|---|---|
| | Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within |

| | |
|---|---|
| Description | WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.<br><br>When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.<br><br>There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based.<br><br>Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash.<br><br>Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code. |
| URL | http://127.0.0.1:8000/login |
| Method | POST |
| Attack | <scrIpt>alert(1);</scRipt> |
| Evidence | <scrIpt>alert(1);</scRipt> |
| URL | http://127.0.0.1:8000/login |
| Method | POST |
| Attack | <scrIpt>alert(1);</scRipt> |
| Evidence | <scrIpt>alert(1);</scRipt> |
| Instances | 2 |
| | Phase: Architecture and Design<br><br>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.<br><br>Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.<br><br>Phases: Implementation; Architecture and Design<br><br>Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.<br><br>For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. |

| | |
|---|---|
| Solution | Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.<br><br>Phase: Architecture and Design<br><br>For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.<br><br>If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.<br><br>Phase: Implementation<br><br>For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.<br><br>To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.<br><br>Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.<br><br>When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."<br><br>Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere. |
| Reference | http://projects.webappsec.org/Cross-Site-Scripting<br>http://cwe.mitre.org/data/definitions/79.html |
| CWE Id | 79 |
| WASC Id | 8 |
| Plugin Id | 40012 |

| **Medium** | **Content Security Policy (CSP) Header Not Set** |
|---|---|
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. |
| URL | http://127.0.0.1:8000 |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/ |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/create-report |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/export-report |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/favicon.ico |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/robots.txt |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | |
| URL | http://127.0.0.1:8000/sitemap.xml |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/css |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/js |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/missions |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/missions/images |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | POST |
| Attack | |
| Evidence | |

| | |
|---|---|
| Instances | 21 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. |
| Reference | https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy<br>https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html<br><br>http://www.w3.org/TR/CSP/<br>http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html<br>http://www.html5rocks.com/en/tutorials/security/content-security-policy/<br>http://caniuse.com/#feat=contentsecuritypolicy<br>http://content-security-policy.com/ |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10038 |

| **Medium** | **Cross-Domain Misconfiguration** |
|---|---|
| Description | Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server |
| URL | https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/partitioning-exempt-urls/changeset?_expected=1675943045406 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/query-stripping/changeset?_expected=1678736907773 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=partitioning-exempt-urls&bucket=main&_expected=0 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=query-stripping&bucket=main&_expected=0 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| URL | https://location.services.mozilla.com/v1/country?key=91e66841-a83b-487f-9b5d-e460f5225ebf |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | Access-Control-Allow-Origin: * |
| Instances | 6 |
| Solution | Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).<br><br>Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner. |
| Reference | https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy |
| CWE Id | 264 |
| WASC Id | 14 |
| Plugin Id | 10098 |

| **Medium** | **Hidden File Found** |
|---|---|
| Description | A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts. |
| URL | http://127.0.0.1:8000/admin/login/._darcs |
| Method | GET |
| Attack | |
| Evidence | HTTP/1.1 302 Found |
| URL | http://127.0.0.1:8000/admin/login/.bzr |
| Method | GET |
| Attack | |
| Evidence | HTTP/1.1 302 Found |
| URL | http://127.0.0.1:8000/admin/login/.hg |
| Method | GET |
| Attack | |
| Evidence | HTTP/1.1 302 Found |
| URL | http://127.0.0.1:8000/admin/login/BitKeeper |
| Method | GET |
| Attack | |
| Evidence | HTTP/1.1 302 Found |
| Instances | 4 |
| Solution | Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc. |
| Reference | https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html |
| CWE Id | 538 |
| WASC Id | 13 |
| Plugin Id | 40035 |

| **Low** | **Cookie No HttpOnly Flag** |
|---|---|
| Description | A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible. |

| | |
|---|---|
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: csrftoken |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: csrftoken |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: csrftoken |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | Set-Cookie: csrftoken |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | Set-Cookie: csrftoken |
| Instances | 5 |
| Solution | Ensure that the HttpOnly flag is set for all cookies. |
| Reference | https://owasp.org/www-community/HttpOnly |
| CWE Id | 1004 |
| WASC Id | 13 |
| Plugin Id | 10010 |

| **Low** | **Server Leaks Version Information via "Server" HTTP Response Header Field** |
|---|---|
| Description | The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to. |
| URL | http://127.0.0.1:8000 |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/ |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/create-report |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/export-report |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/export-report/1 |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/favicon.ico |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |

| | |
|---|---|
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/robots.txt |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/sitemap.xml |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css/base.css |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css/dark_mode.css |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css/login.css |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css/nav_sidebar.css |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/css/responsive.css |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/js |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/js/nav_sidebar.js |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/admin/js/theme.js |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/missions |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/missions/images |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/static/missions/images/nasa-logo.png |
| Method | GET |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-05-20-17-04-38.chain |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/ads-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/102.0/1657213547 |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/content-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/102.0/1657213547 |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/social-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| URL | http://127.0.0.1:8000/login |
| Method | POST |
| Attack | |
| Evidence | WSGIServer/0.2 CPython/3.11.2 |
| Instances | 51 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. |
| Reference | http://httpd.apache.org/docs/current/mod/core.html#servertokens<br>http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007<br>http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx<br>http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10036 |

| Low | Strict-Transport-Security Header Not Set |
| --- | --- |
| Description | HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797. |
| URL | https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-05-20-17-04-38.chain |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/ads-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/content-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| Instances | 18 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. |

| | |
|---|---|
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html<br>https://owasp.org/www-community/Security_Headers<br>http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security<br>http://caniuse.com/stricttransportsecurity<br>http://tools.ietf.org/html/rfc6797 |
| CWE Id | 319 |
| WASC Id | 15 |
| Plugin Id | 10035 |

| **Low** | **Timestamp Disclosure - Unix** |
|---|---|
| Description | A timestamp was disclosed by the application/web server - Unix |
| URL | https://tracking-protection.cdn.mozilla.net/ads-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | 1490633678 |
| URL | https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | 1604686195 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | 1604686195 |
| URL | https://tracking-protection.cdn.mozilla.net/content-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | 1604686195 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | 1490633678 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265 |
| Method | GET |
| Attack | |
| Evidence | 1517935265 |
| URL | https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/social-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | 1657213547 |
| URL | https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=102.9&pver=2.2 |
| Method | POST |

| | |
|---|---|
| Attack | |
| Evidence | 1490633678 |
| URL | https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=102.9&pver=2.2 |
| Method | POST |
| Attack | |
| Evidence | 1517935265 |
| URL | https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=102.9&pver=2.2 |
| Method | POST |
| Attack | |
| Evidence | 1604686195 |
| URL | https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=102.9&pver=2.2 |
| Method | POST |
| Attack | |
| Evidence | 1657213547 |
| Instances | 21 |
| Solution | Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns. |
| Reference | http://projects.webappsec.org/w/page/13246936/Information%20Leakage |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10096 |

| **Low** | **X-Content-Type-Options Header Missing** |
|---|---|
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
| URL | http://127.0.0.1:8000/static/admin/css/base.css |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/css/dark_mode.css |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/css/login.css |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/css/nav_sidebar.css |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/css/responsive.css |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/js/nav_sidebar.js |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/admin/js/theme.js |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/static/missions/images/nasa-logo.png |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-05-20-17-04-38.chain |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/ads-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| | https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/102.0 |

| | |
|---|---|
| URL | /1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/content-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/102. |

| | |
|---|---|
| URL | 0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | |
| URL | https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=102.9&pver=2.2 |
| Method | POST |
| Attack | |
| Evidence | |
| Instances | 27 |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.<br><br>If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing. |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br>https://owasp.org/www-community/Security_Headers |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10021 |

| **Informational** | **Information Disclosure - Suspicious Comments** |
|---|---|
| Description | The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments. |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | admin |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | admin |
| URL | http://127.0.0.1:8000/static/admin/js/nav_sidebar.js |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | admin |
| URL | http://127.0.0.1:8000/static/admin/js/theme.js |
| Method | GET |
| Attack | |
| Evidence | from |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | admin |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | admin |
| Instances | 6 |
| Solution | Remove all comments that return information that may help an attacker and fix any underlying problems they refer to. |
| Reference | |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10027 |

| **Informational** | **Re-examine Cache-control Directives** |
|---|---|
| Description | The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached. |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/partitioning-exempt-urls/changeset?_expected=1675943045406 |
| Method | GET |
| Attack | |
| Evidence | max-age=3600,public |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/query-stripping/changeset?_expected=1678736907773 |
| Method | GET |
| Attack | |
| Evidence | max-age=3600,public |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=partitioning-exempt-urls&bucket=main&_expected=0 |
| Method | GET |
| Attack | |
| Evidence | max-age=3600,public |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=query-stripping&bucket=main&_expected=0 |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | max-age=3600,public |
| Instances | 4 |
| Solution | For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable". |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching<br>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control<br>https://grayduck.mn/2021/09/13/cache-control-recommendations/ |
| CWE Id | 525 |
| WASC Id | 13 |
| Plugin Id | 10015 |

| **Informational** | **Retrieved from Cache** |
|---|---|
| Description | The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance. |
| URL | https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css |
| Method | GET |
| Attack | |
| Evidence | HIT |
| URL | https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-05-20-17-04-38.chain |
| Method | GET |
| Attack | |
| Evidence | Age: 1574 |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/partitioning-exempt-urls/changeset?_expected=1675943045406 |
| Method | GET |
| Attack | |
| Evidence | Age: 3546 |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/query-stripping/changeset?_expected=1678736907773 |
| Method | GET |
| Attack | |
| Evidence | Age: 2250 |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=partitioning-exempt-urls&bucket=main&_expected=0 |
| Method | GET |
| Attack | |
| Evidence | Age: 1030 |
| URL | https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=query-stripping&bucket=main&_expected=0 |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | Age: 103 |
| URL | https://tracking-protection.cdn.mozilla.net/ads-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 32648 |
| URL | https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |
| Evidence | Age: 27212 |
| URL | https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 5350 |
| URL | https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 74271 |
| URL | https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 61723 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | Age: 8286 |
| URL | https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | Age: 3291 |
| URL | https://tracking-protection.cdn.mozilla.net/content-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 84636 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1604686195 |
| Method | GET |
| Attack | |
| Evidence | Age: 11182 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678 |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | Age: 73173 |
| URL | https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265 |
| Method | GET |
| Attack | |
| Evidence | Age: 11825 |
| URL | https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 11242 |
| URL | https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 62648 |
| URL | https://tracking-protection.cdn.mozilla.net/social-track-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 41808 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 70179 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 2834 |
| URL | https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/102.0/1657213547 |
| Method | GET |
| Attack | |
| Evidence | Age: 63791 |
| Instances | 23 |
| Solution | Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:<br><br>Cache-Control: no-cache, no-store, must-revalidate, private<br><br>Pragma: no-cache<br><br>Expires: 0<br><br>This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request. |
| | https://tools.ietf.org/html/rfc7234 |

| | |
|---|---|
| Reference | https://tools.ietf.org/html/rfc7231<br>http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234) |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10050 |

| **Informational** | **User Agent Fuzzer** |
|---|---|
| Description | Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response. |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |

| | |
|---|---|
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |

| | |
|---|---|
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/ |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |

| | |
|---|---|
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |

| | |
|---|---|
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |

| | |
|---|---|
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| | |

| | |
|---|---|
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/login |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |

| | |
|---|---|
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/mission |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) |

| | |
|---|---|
| Attack | Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/missions |
| Method | GET |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| | |

| | |
|---|---|
| Method | POST |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |

| | |
|---|---|
| Instances | 96 |
| Solution | |
| Reference | https://owasp.org/wstg |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10104 |

| **Informational** | **User Controllable HTML Element Attribute (Potential XSS)** |
|---|---|
| Description | This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability. |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | GET |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |

| | |
|---|---|
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/ |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | |
| URL | http://127.0.0.1:8000/admin/login/?next=/admin/login |
| Method | POST |
| Attack | |
| Evidence | |
| Instances | 14 |
| Solution | Validate all input and sanitize output it before writing to any HTML attributes. |
| Reference | http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute |
| CWE Id | 20 |
| WASC Id | 20 |
| Plugin Id | 10031 |