acunetix

Nuri Hosting

웹취약점점검 결과 리포트

Acunetix 웹취약점점검

24 April 2017

http://testhtml5.vulnweb.com 스캔결과

스캔 상세정보

스캔 정보	
시작시간	24/04/2017, 13:30:38
대상 URL	http://testhtml5.vulnweb.com
Host	http://testhtml5.vulnweb.com
소요시간	16 minutes, 8 seconds
Profile	Full Scan

위험수준

취약점 위험도 Level 3

취약점점검에서 하나이상의 높은 위험도의 취약점이 발견되었습니다. 악의적인 사용자가 발견된 취약점을 이용하여 웹사이트나 데이터베이스에 영향을 줄 수 있습니다.

취약점 현황

Total	19
High	9
Medium	3
Low	6
Informational	1

취약점 요약정보

AngularJS client-side template injection

분류		
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None	
CWE	CWE-79	
영향을받은 항목		Variation
/contact		2

Cross site scripting

분류		
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None	
CWE	CWE-79	

영향을받은 항목	Variation
Web Server	1

DOM-based cross site scripting

분류	
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

영향을받은 항목	Variation
Web Server	3

nginx SPDY heap buffer overflow

분류	
CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2014-0133
CWE	CWE-122

영향을받은 항목	Variation
Web Server	1

Weak password

분류	
CVSS2	Base Score: 7.5 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

영향을받은 항목	Variation
/admin	1

XML external entity injection via external file

분류	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: High
CWE	CWE-611

영향을받은 항목	Variation
/forgotpw	1

Basic authentication over HTTP

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

영향을받은 항목	Variation
/admin	1

HTML form without CSRF protection

분류	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352

영향을받은 항목	Variation
Web Server	1

User credentials are sent in clear text

분류	
	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None

CVSS2	Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

영향을받은 항목	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

분류	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

영향을받은 항목	Variation
Web Server	1

Cookie(s) without HttpOnly flag set

분류	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CWE	CWE-16
영향을받은 항목	Variation
Web Server	1

Login page password-guessing attack

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

영향을받은 항목	Variation
/login	1

OPTIONS method is enabled

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200

영향을받은 항목	Variation
Web Server	1

Possible sensitive directories

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

영향을받은 항목	Variation
/admin	1

Possible virtual host found

분류	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High

	Integrity Impact: None Availability Impact: None
CWE	CWE-200

영향을받은 항목	Variation
Web Server	1

Password type input with auto-complete enabled

분류	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

영향을받은 항목	Variation
Web Server	1

취약점 세부정보

AngularJS client-side template injection

위험도	**High**
Reported by module	Scripting (XSS.script)

설명

이 웹 응용프로그램은 클라이언트측에 AngularJS템플릿 주입 취약점에 취약합니다. 클라이언트측에 AngularJS템플릿 주입 취약점은 사용자 입력이 클라이언트측에 AngularJS템플릿이 사용되는 페이지에 동적으로 포함될 때 발생합니다. 중괄호를 사용하면 응용 프로그램에서 사용중인 클라이언트측 AngularJS템플릿에 AngularJS 표현식을 주입할 수 있습니다. 이러한 표현식은 AngularJS가 클라이언트측에서 평가하며 샌드박스 이스케이프와 함께 사용하면 공격자가 임의의 자바 스크립트 코드를 실행할 수 있습니다.

영향

공격자는 클라이언트측에서 평가할 AngularJS식을 주입할 수 있습니다. 일반적으로 AngularJS 표현은 위험하지 않지만 샌드박스 이스케이프와 결합하면 공격자가 임의의 JavaScript 코드를 실행할 수 있습니다.

조치사항

공격자가 중괄호를 사용하여 AngularJS식을 주입하는 것은 불가능해야 합니다. 애플리케이션은 사용자 입력에서 중괄호를 매우 위험한 것으로 취급하거나 서버측에서 사용자 입력을 완전히 반영하지 않아야합니다.

참조사이트

AngularJS security features and best practices (https://docs.angularjs.org/guide/security)
XSS without HTML: Client-Side Template Injection with AngularJS (http://blog.portswigger.net/2016/01/xss-without-html-client-side-template.html)

영향받은 항목

/contact

세부정보

URL encoded POST input **firstName** was set to **paqeobhpktsxm{{1==1}}l6fus**.
The input was reflected inside an AngularJS template.

요청 headers

```
POST /contact HTTP/1.1
Content-Length: 107
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
address=3137%20Laguna%20Street&firstName=paqeobhpktsxm{{1==1}}l6fus&lastName=iqijwkvx&messag
e=20&subject=na
```

/contact

세부정보

URL encoded POST input **lastName** was set to **iqijwkvxcmbpy{{1==1}}vxov0**.
The input was reflected inside an AngularJS template.

요청 headers

```
POST /contact HTTP/1.1
```

```
Content-Length: 107
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
address=3137%20Laguna%20Street&firstName=bwwwuaib&lastName=iqijwkvxcmbpy{{1==1}}vxov0&messag
e=20&subject=na
```

Cross site scripting

위험도	**High**
Reported by module	Scripting (XSS.script)

설명

이 스크립트는 Cross Site Scripting (XSS)공격 가능성이 있는 취약점이 있습니다.

Cross Site Scripting (XSS)는 공격자가 다른 사용자에게 악의적이 코드(보편적으로 Javascript)를 보낼수 있도록 하는 취약점입니다.만약 브라우저가 스크립트의 안정성을 확인할 수 없을때 사용자의 컨텍스트에서 공격자에게 쿠키 및 세션에 접근할 수 있도록 하는 스크립트가 실행될 수 있습니다.

영향

악의적인 사용자가 취약한 어플리케이션에 JavaScript, VBScript, ActiveX, HTML 또는 Flash를 삽입하여 사용자 몰래 데이터를 가져갈 수 있습니다.공격자는 세션쿠키를 훔쳐서 사용자의 계좌 및 명의를 도용할 수 있습니다.또한, 사용자에게 보여지는 페이지를 수정하는것도 가능합니다.

조치사항

스크립트에서 사용자 입력의 메타케릭터를 필터링하여야 합니다.

참조사이트

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

영향받은 항목

Web Server
세부정보
Cookie input **username** was set to **1<script>5daH(9403)</script>** The input is reflected inside a text element.
요청 headers

```
GET / HTTP/1.1
Cookie: username=1<script>5daH(9403)</script>
Referer: http://testhtml5.vulnweb.com
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

DOM-based cross site scripting

위험도	**High**
Reported by module	DeepScan

설명

이 스크립트는 Cross Site Scripting (XSS)공격에 취약합니다.

Cross Site Scripting (XSS)는 공격자가 다른 사용자에게 악의적이 코드(보편적으로 Javascript)를 보낼수 있도록 하는 취약점입니다.만약 브라우저가 스크립트의 안정성을 확인 할수 없을때 사용자의 컨텍스트에서 공격자에게 쿠키 및 세션에 접근할수 있도록 하는 스크립트가 실행될수 있습니다.

전형적인 cross-site scripting 취약점은 서버 측 코드에서 발생 하지만, document object model based cross-site scripting은 클라이언트 브라우저의 스크립트 코드에 영향을 미치는 취약점 유형입니다.

영향

악의적인 사용자가 취약한 어플리케이션에 JavaScript, VBScript, ActiveX, HTML 또는 Flash를 삽입하여 사용자 몰래 데이터를 가져갈수 있습니다.공격자는 세션쿠키를 훔쳐서 사용자의 계좌 및 명의를 도용할수 있습니다.또한, 사용자에게 보여지는 페이지를 수정하는것도 가능합니다.

조치사항

스크립트의 사용자 입력에서 메타케릭터를 필터링하여야 합니다.

참조사이트

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

영향받은 항목

Web Server

세부정보

Source: window.name
window.name: javascript:domxssExecutionSink(2,"'\"><xsstag>()wildxss")
Execution Sink: evaluate code (eval/setTimeout/setInterval/...)
Evaluated code:

```
this.myObj=javascript:domxssExecutionSink(2,"'\"><xsstag>()wildxss") ...
```

Stack Trace:

- toObject@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:105:17
- init@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:76:36
- http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:202:13
- global code@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:204:2

요청 headers

Web Server

세부정보

Source: Referrer Header
Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"'\"><xsstag>()refdxss")
Execution Sink: set HTML code (innerHTML/outerHTML/...)
HTML code set:

```
unknown is coming from <b>http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,
"'\"><xsstag>()refdxss")</xsstag></b> and has visited this page <b>1</b> times. ...
```

Stack Trace:

- http://code.jquery.com/jquery-1.9.1.min.js:4:27657
- access@http://code.jquery.com/jquery-1.9.1.min.js:3:6852
- html@http://code.jquery.com/jquery-1.9.1.min.js:4:27282
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182
- global code@http://testhtml5.vulnweb.com/static/app/post.js:114:17

요청 headers

Web Server

세부정보

Source: location.hash
location.hash: #/latest/page/javascript:domxssExecutionSink(1,"'\"><xsstag>()hashxss")
Execution Sink: set HTML code (innerHTML/outerHTML/...)
HTML code set:

```
javascript:domxssExecutionSink(1,"'\"><xsstag>()hashxss")</xsstag> ...
```

Stack Trace:

- http://code.jquery.com/jquery-1.9.1.min.js:4:27657
- access@http://code.jquery.com/jquery-1.9.1.min.js:3:6852
- html@http://code.jquery.com/jquery-1.9.1.min.js:4:27282
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:142:173
- $digest@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:86:339
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:61:148
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:85
- forEach@[native code]
- n@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:6:199
- h@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:69
- dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590
- handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295

요청 headers

nginx SPDY heap buffer overflow

위험도	**High**
Reported by module	Scripting (Version_Check.script)

설명

1.3.15 이전 1.4.7 및 1.5.x 이전 1.5.12버전의 nginx의 SPDY구현하는 heap-based buffer overflow에서 원격 공격자 가 조작 된 요청을 통해 임의의 코드를 실행할 수 있습니다.만약 설정파일에서 SPDY옵션이 listen으로 설정되어 있으면, ngx_http_spdy_module module을 컴파일한것 과 --with-debug configure option없이 컴파일한 nginx에 영향을 줍니다.

영향

공격자는 잠재적으로 특수하게 조작 된 요청을 사용하여 작업자 프로세스 에서 heap memory buffer overflow가 발생 하도록 임의의 코드 실행할 수 있습니다.

조치사항

공급 업체 에서 제공하는 패치를 최신 버전으로 nginx를 업그레이드합니다.

참조사이트

nginx security advisory (CVE-2014-0133) (http://mailman.nginx.org/pipermail/nginx-announce/2014/000135.html)
nginx patch (http://nginx.org/download/patch.2014.spdy2.txt)
CVE-2014-0133 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0133)

영향받은 항목

Web Server
세부정보
Current version is : nginx/1.4.1.
요청 headers

Weak password

위험도	**High**
Reported by module	Scripting (Weak_Password_Basic_Auth.script)

설명

이 페이지는 쉬운 비밀번호를 사용합니다.Acunetix WVS에서 이 페이지에 접근하기 위한 권한을 추정할 수 있었습니다. 쉬운 암호는 짧거나, 기본 프로그램 비밀번호로 자동으로 사전의 단어, 사용자 이름, 기본적인 패턴들을 대입하여 공격하는 것에 약합니다.

영향

공격자는 비밀번호로 보호된 페이지에 접근할 수 있습니다.

조치사항

어려운 암호로 변경 하시기 바랍니다.쉬운 암호나 사전에 나오는 단어로 암호를 계속 사용하시면 안됩니다.

참조사이트

Wikipedia - Password strength (http://en.wikipedia.org/wiki/Password_strength)
Authentication Hacking Attacks (http://www.acunetix.com/websitesecurity/authentication/)

영향받은 항목

/admin
세부정보
Username: **admin**, Password: **secret**.
요청 headers

```
GET /admin/ HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
Authorization: Basic YWRtaW46c2VjcmV0
```

XML external entity injection via external file

위험도	**High**
Reported by module	Scripting (XML_External_Entity_Injection.script)

설명

XML은 특정 외부 URI에 위치한 XML의 인라인 포함을 검색하고 수행하도록 XML 프로세서에 지시하는 "외부 엔티티 (external entities)"로 알려진 기능을 지원한다. 외부 XML 엔티티를 사용하여 XML문서와 연관된 document type declaration (DTD)을 추가하거나 수정 할 수 있습니다. 외부 XML 엔티티를 사용하여 XML 문서의 내용에 XML을 포함시킬 수도 있습니다.

이제 XML 처리기가 공격자 제어하에있는 출처의 데이터를 구문 분석한다고 가정합니다. 대부분 프로세서는 유효성을 검사하지 않지만 대체 텍스트를 포함하여 예상치 못한 파일 열기 작업 또는 HTTP 전송을 시작하거나 XML 프로세스가 스시템 ID 접근을 알 수 있습니다.

다음은이 기능을 사용하여 로컬 파일 (/ etc / passwd)의 내용을 포함하는 샘플 XML 문서입니다.

```
<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE acunetix [

  <!ENTITY acunetixent SYSTEM "file:///etc/passwd">

]>

<xxx>&acunetixent;</xxx>
```

영향

공격에는 암호 또는 개인 사용자 데이터와 같은 중요한 데이터가 포함될 수 있는 로컬파일공개, 시스템 식별자의 파일과 스키마 또는 상대 경로가 포함될 수 있습니다. 공격은 XML 문서를 처리하는 응용 프로그램과 관련하여 발생하기 때문에 공격자는 이 신뢰할 수있는 응용 프로그램을 사용하여 다른 내부 시스템으로 피벗 할 수 있으며 http 요청을 통해 다른 내부 내용을 공개할 수 있습니다.

조치사항

가능한 경우 XML 외부엔터티의 구문분석을 사용하지 않는 것이 좋습니다.

참조사이트

CWE-611: Information Exposure Through XML External Entity Reference (http://cwe.mitre.org/data/definitions/611.html)
XXE (Xml eXternal Entity) attack (http://archive.cert.uni-stuttgart.de/bugtraq/2002/10/msg00421.html)
XML External Entity (XXE) Processing (https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)

영향받은 항목

/forgotpw
세부정보

Custom POST input **text/xml** was set to **<?xml version="1.0" encoding="utf-8"?> <!DOCTYPE acunetix [<!ENTITY acunetixent SYSTEM "http://hitHnO48AOCjZ.bxss.me/">]> <xxx>&acunetixent;</xxx>**
 	
An HTTP request was initiated for the domain **hitHnO48AOCjZ.bxss.me** which indicates that this script is vulnerable to XXE injection.
 	
HTTP request details:
 	
`IP address: 176.28.50.165`
`User agent: Python-urllib/1.17`

요청 headers

```
POST /forgotpw HTTP/1.1
Content-Type: text/xml
Content-Length: 156
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE acunetix [
<!ENTITY acunetixent SYSTEM "http://hitHnO48AOCjZ.bxss.me/">
]>
<xxx>&acunetixent;</xxx>
```

Basic authentication over HTTP

위험도	**Medium**
Reported by module	Scripting (Basic_Auth_Over_HTTP.script)

설명

HTTP 트랜젝션의 콘텍스트에서 기본 엑세스 인증은 HTTP 사용자 에이젼트가 요청을 만들때 이름과 암호를 입력하는 방법입니다.

이 디렉토리는 HTTP연결을 통해 기본인증을 사용하여 보호됩니다. 기본 인증을 사용할때 HTTPS를 사용하지 않아 사용자의 인증정보가 평문으로 정송되어 HTTP sniffing 취약점이 있습니다.

영향

사용자 자격 증명이 일방 텍스트로 전송되어 packet sniffing에 취약합니다.

조치사항

기본인증을 HTTPS 연결에서 사용하시기 바랍니다.

참조사이트

Basic access authentication (http://en.wikipedia.org/wiki/Basic_access_authentication)

영향받은 항목

/admin
세부정보
요청 headers

HTML form without CSRF protection

위험도	**Medium**
Reported by module	Crawler

설명

이 경고는 오탐일수 있으며, 수동으로 확인이 필요합니다.

크로스 사이트 요청 위조는 사용자의 권한을 무단 명령으로 전송하여 악용하는 것으로 one-click 공격또는 세션 갈아타기로도 알려져 있으며, CSRF 및 XSRF 약자를 사용합니다.

Acunetix WVS에서 명백한 CSRF 보호 HTML약식을 발견하였습니다. 영향을 받는 HTML양식에 대한 더 자세한 내용은 세부 사항을 참조하시기 바랍니다.,

영향

공격자는 공격자가 선택한 사용자의 행동을 강제로 실행할 수 있습니다.성공적인 CSRF는 일반적으로 최종 사용자 데이터 및 동작을 손상 시킬수 있습니다. 타겟이 된 엔드 사용자가 관리자이면, 웹 어플리케이션의 모든 부분을 타협할 수 있습니다.

조치사항

CSRF 보호 및 대책 구현이 필요할 경우 이 양식을 확인 하시기 바랍니다.

영향받은 항목

Web Server
세부정보
Form name: <empty> Form action: http://testhtml5.vulnweb.com/login Form method: POST Form inputs: • username [Text] • password [Password]
요청 headers

`GET / HTTP/1.1`
`Pragma: no-cache`
`Cache-Control: no-cache`
`Host: testhtml5.vulnweb.com`
`Connection: Keep-alive`
`Accept-Encoding: gzip,deflate`
`User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21`
`Accept: */*`

User credentials are sent in clear text

위험도	**Medium**
Reported by module	Crawler

설명

사용자 자격증명은 암호화 되지 않은 채널에서 전송됩니다. 이 정보는 항상 암호화 된 채널 (HTTPS)을 악의적인 사용자에 의해 차단 되는 것을 방지하기위해 전송 해야합니다

영향

제 3자가 암호화되지 않은 HTTP 연결을 차단 하여 사용자 자격 증명을 읽을 수 있습니다 .

조치사항

사용자 자격 증명이 민감한 정보로 간주 되기 때문에 , 항상 암호화된 연결 (HTTPS)을 통해 서버로 전송 해야합니다.

영향받은 항목

Web Server

세부정보

Form name: <empty>
Form action: http://testhtml5.vulnweb.com/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

요청 headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Clickjacking: X-Frame-Options header missing

위험도	**Low**
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

설명

클릭 재킹 (사용자 인터페이스 교정 공격, UI 구제 공격, UI 교정)은 웹 사용자를 클릭하여 사용자가 클릭 한 것과 다른 것을 클릭하여 기밀 정보를 공개하거나 컴퓨터를 제어하는 악의적 인 기법입니다. 겉보기에 무해한 웹 페이지를 클릭하십시오.

서버가 **X-Frame-Options** 헤더를 반환하지 않았으므로이 웹 사이트가 클릭 공격의 위험에 노출 될 수 있습니다. **X-Frame-Options HTTP** 응답 헤더는 브라우저가 프레임 또는 **iframe** 내에 페이지를 렌더링 할 수 있어야하는지 여부를 나타내는 데 사용할 수 있습니다. 사이트는이를 통해 다른 사이트에 콘텐츠가 삽입되지 않도록함으로써 클릭 공격을 피할 수 있습니다.

영향

영향을받는 웹 응용 프로그램에 따라 다릅니다.

조치사항

X-Frame-Options 헤더를 포함하도록 웹 서버를 구성하십시오. 이 머리글에 사용할 수있는 값에 대한 자세한 정보는 참조사이트를 참고하십시오.

참조사이트

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive
(https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

영향받은 항목

Web Server
세부정보
요청 headers

```
GET / HTTP/1.1
Cookie: username=admin
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cookie(s) without HttpOnly flag set

위험도	Low
Reported by module	Crawler

설명

쿠키에 **HTTPOnly flag set**이 설정되어 있지 않습니다. **HTTPOnly flag set**이 설정되어 있어야, 브라우저에 지시하여 쿠키가 클라이언트측 스크립트가 아닌 서버에서 접근할 수 있습니다. 세션 쿠키를 위해 중요한 보안성 보호입니다.

영향

None

조치사항

가능하다면, **HttpOnly flag**를 설정하시기 바랍니다.

영향받은 항목

Web Server
세부정보
Cookies found: • **Name: username, Domain: testhtml5.vulnweb.com**
요청 headers

```
OPTIONS / HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Login page password-guessing attack

위험도	Low
Reported by module	Scripting (Html_Authentication_Audit.script)

설명

웹 개발자가 공통으로 직면하는 위협은 **brute force**공격으로 알려진 암호 추측 공격입니다. 무차별 대입공격은 작동하는 하나의 올바른 조합을 찾을때까지 체계적으로 문자, 숫자 및 기호의 가능한 모든 조합을 시도하여 암호를 발견하는 공격입니다.

이 로그인 페이지는 무차별 대입공격에 대한 아무 보호책을 가지고 있지 않습니다.여러 차례 잘못된 암호를 시도할때 계정이 잠기는 유형을 구현하는것이 좋습니다.이 프로그램을 보완하는데 더 자세한 내용은 웹 참조를 참고하시기 바랍니다.

영향

공격자는 동작하는 하나의 조합을 발견할때까지 체계적으로 문자, 숫자 및 기호의 가능한 모든 조합을 사용하여 약한 암호를 발견할때 까지 시도합니다.

조치사항

여러 차례 잘못된 암호를 시도할때 계정이 잠기는 유형을 구현하는것이 좋습니다.

참조사이트

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

영향받은 항목

/login
세부정보
The scanner tested 10 invalid credentials and no account lockout was detected.
요청 headers
POST /login HTTP/1.1 Content-Length: 35 Content-Type: application/x-www-form-urlencoded Referer: http://testhtml5.vulnweb.com Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */* password=oVz28hgb&username=HpjQrFNM

OPTIONS method is enabled

위험도	Low
Reported by module	Scripting (Options_Server_Method.script)

설명

웹 사이트에서 HTTP OPTIONS method가 활성화 되어 있습니다. OPTIONS method는 Request-URI가 식별하는 요청 / 응답 체인에서 사용할 수 있는 통신 선택 사항에 관한 정보 요청을 표시하는 method의 목록을 제공합니다.

영향

OPTIONS method는 악의적인 사용자가 더 고급화된 공격을 준비할 수 있는 민감한 정보들을 보여줍니다.

조치사항

웹 사이트에서 OPTIONS method를 비활성화 하는 것을 권장합니다.

참조사이트

Testing for HTTP Methods and XST (OWASP-CM-008)
(https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008))

영향받은 항목

Web Server
세부정보
Methods allowed: HEAD, OPTIONS, GET.

요청 headers
OPTIONS / HTTP/1.1 Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

Possible sensitive directories

위험도	Low
Reported by module	Scripting (Possible_Sensitive_Directories.script)

설명

민감한 디렉토리를 발견 하였습니다. 이 디렉토리는 직접적으로 웹사이트에 연결은 되어 있지 않습니다.이 검사는 백업, 데이터베이스, 관리 페이지, 임시 디렉토리 같은 일반적인 민감한 자원들을 확인 합니다. 각 각의 디렉토리들은 공격자가 대상의 대하여 더 알수 있도록 도와 줄수 있습니다.

영향

이 디렉토리는 악의적인 사용자가 공격을 준비하는데 도움이 될 수 있는 정보가 노출 될 수 있습니다.

조치사항

디렉토리의 접근을 제한 하거나 웹 사이트에서 제거합니다.

참조사이트

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

영향받은 항목

/admin
세부정보

요청 headers
GET /admin HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Possible virtual host found

위험도	Low
Reported by module	Scripting (VirtualHost_Audit.script)

설명

가상 호스팅은 하나의 서버(또는 서버의 풀)에 여러 도메인 이름(각 이름을 별도로 처리)을 호스팅 하기 위한 방법입니다.모든 서비스에서 같은 호스트 네임을사용할 필요 없이 하나의 서버의 메모리와 프로세스 사이클 같은 자원을 공유할 수 있습니다.

이 웹 서버는 호스트 헤더를 조작하거나 여러 일반적인 호스트를 테스트 했을때 응답이 달랐습니다. 가상 호스트의 존재가 나타 날 수 있습니다.

영향

민감한 정보가 노출될 수 있습니다.

조치사항

가상 호스트 설정을 확인하고, 공개적으로 접근이 가능한지 확인하여야 합니다.

참조사이트

Virtual hosting (http://en.wikipedia.org/wiki/Virtual_hosting)

영향받은 항목

Web Server
세부정보
Virtual host: localhost **Response:** `<!DOCTYPE html>` `<html>` `<head>` `<title>Welcome to nginx!</title>` `<style>` `body {` `width: 35em;` `margin: 0 auto;` `font-family: Tahoma, Verdana, Arial, sans-serif;` `}` `</style>` `</head>` `<body>` `<h1>Welcome to nginx!</h1>` `<p>If you see this page, the nginx web server is successfully installed and` `working. Further configuration is required.</p>` `<p>For online documentation and support please refer to` `<a href="http://nginx.org/">nginx.org</a>. ` `Commercial support is available at` `<a href`
요청 headers

Password type input with auto-complete enabled

위험도	Informational
Reported by module	Crawler

설명

새로운 이름과 암호를 입력하여 양식이 제출되면 브라우저는 저장할것인지 물어봅니다.그후, 양식이 표시될때 자동으로 이름과 암호가 입력이 되거나, 이름을 입력하면 완성인됩니다. 로컬 접근을 할 수 있는 공격자는 브라우저 캐시에서 일반 텍스트 암호를 얻을 수 있습니다.

영향

민감한 정보가 노출될수 있습니다.

조치사항

암호 자동 완성은 민감한 어플리케이션에서는 비활성화를 하여야 합니다.
자동 완성을 비활성화 하기 위해서는 아래와 같은 코드를 사용하면 됩니다.**[pre][code]<INPUT TYPE="password" AUTOCOMPLETE="off">[/code][/pre]**

영향받은 항목

Web Server
세부정보
Password type input(s): password from form with ID loginForm with action /login have autocomplete enabled.
요청 **headers**
GET / HTTP/1.1 **Pragma: no-cache** **Cache-Control: no-cache** **Host: testhtml5.vulnweb.com** **Connection: Keep-alive** **Accept-Encoding: gzip,deflate** **User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21** **Accept: */***

스캔 항목 (coverage report)

http://testhtml5.vulnweb.com/
http://testhtml5.vulnweb.com/admin
http://testhtml5.vulnweb.com/ajax
http://testhtml5.vulnweb.com/ajax/archive
http://testhtml5.vulnweb.com/ajax/latest
http://testhtml5.vulnweb.com/ajax/popular
http://testhtml5.vulnweb.com/contact
http://testhtml5.vulnweb.com/favicon.ico
http://testhtml5.vulnweb.com/forgotpw
http://testhtml5.vulnweb.com/login
http://testhtml5.vulnweb.com/logout
http://testhtml5.vulnweb.com/static
http://testhtml5.vulnweb.com/static/app
http://testhtml5.vulnweb.com/static/app/app.js
http://testhtml5.vulnweb.com/static/app/controllers
http://testhtml5.vulnweb.com/static/app/controllers/controllers.js
http://testhtml5.vulnweb.com/static/app/libs
http://testhtml5.vulnweb.com/static/app/libs/sessvars.js
http://testhtml5.vulnweb.com/static/app/partials
http://testhtml5.vulnweb.com/static/app/partials/about.html
http://testhtml5.vulnweb.com/static/app/partials/archive.html
http://testhtml5.vulnweb.com/static/app/partials/carousel.html
http://testhtml5.vulnweb.com/static/app/partials/contact.html
http://testhtml5.vulnweb.com/static/app/partials/itemsList.html
http://testhtml5.vulnweb.com/static/app/partials/latest.html
http://testhtml5.vulnweb.com/static/app/partials/popular.html
http://testhtml5.vulnweb.com/static/app/post.js
http://testhtml5.vulnweb.com/static/app/services
http://testhtml5.vulnweb.com/static/app/services/itemsService.js
http://testhtml5.vulnweb.com/static/css
http://testhtml5.vulnweb.com/static/css/style.css
http://testhtml5.vulnweb.com/static/img