



# OWASP Honeytrap

## Honeypot Threat Intelligence

Base around OWASP Honeypot-Project

**Pituphong Yavirach, CPTe**  
Founder – Debug Consulting

Ref. Anglia Ruskin University, OWASP Cambridge Chapter



# Honeypots

ระบบที่ใช้ล่อลวงผู้โจมตี

- ประเภทของ Honeypot
  - ตรวจจับ
  - ล่อลวง (วิจัย)
- ระดับการนำมาใช้ตามความเสี่ยงของการใช้ Honeypot
  - ต่ำ – จำลองระบบ, ไม่มีการเข้าสู่ระบบจริง
  - กลาง - จำลองระบบ, มีการเข้าสู่ระบบแบบจำลอง
  - สูง – ระบบบริการจริง มีมีการเข้าสู่ระบบจริง

# OWASP Web Honeypots

- เน้นตรวจจับบน protocol HTTP(s)
- 92% ของช่องโหว่เกิดขึ้นบน Application (NIST/GARTNER)
- สถาปัตยกรรมเว็บมีความซับซ้อน
- กรโจอมติที่ซับซ้อนและมีการพัฒนา



# จะต้องตรวจจับอะไร?

- ตรวจจับรูปแบบเครื่องมือโจมตีอัตโนมัติ
- พัฒนาจากระบบที่มีอยู่ แล้วตัดทอนความสามารถต่าง ๆ รวมถึงสร้างเป้าหมายลวง

# แล้วทำไมไม่ใช้ WAF – Web Application Firewall

- WAF มีเทคโนโลยีที่หลากหลาย
- สามารถติดตั้งได้หลายรูปแบบ
  - inline
  - mirroring
  - load balance mirror port
  - Web server module
- วิธีการตรวจจับที่แตกต่าง
  - รูปแบบซีกเนเจอร์
  - เรียนรู้แบบฮิวริสติกส์

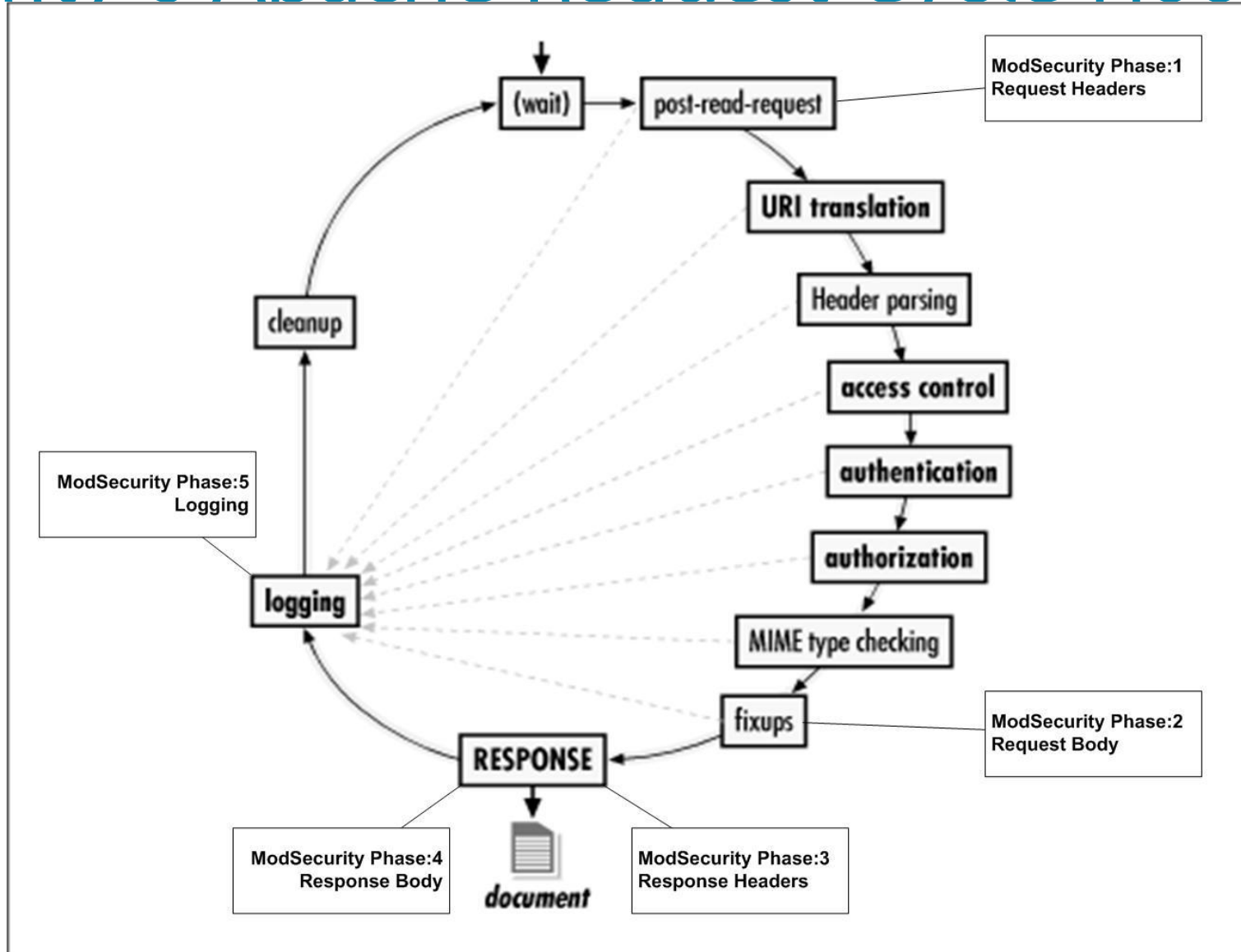
# modsecurity

## Open Source Web Application Firewall

- Open-source Web Application Firewall ที่ได้รับความนิยมมากที่สุด
  - พัฒนาตั้งแต่ ค.ศ. 2002
  - รุ่นปัจจุบัน 3.0.9 (<https://github.com/SpiderLabs/ModSecurity>)
- ออกแบบรองรับ OWASP Core Rules Set
  - พัฒนาตั้งแต่ ค.ศ. 2009
  - รุ่นปัจจุบัน 3.3.4 และกำลังจะออกรุ่นใหม่



# ModSecurity's Apache Request Cycle Hooks



# OWASP Core Rule Set (CRS)

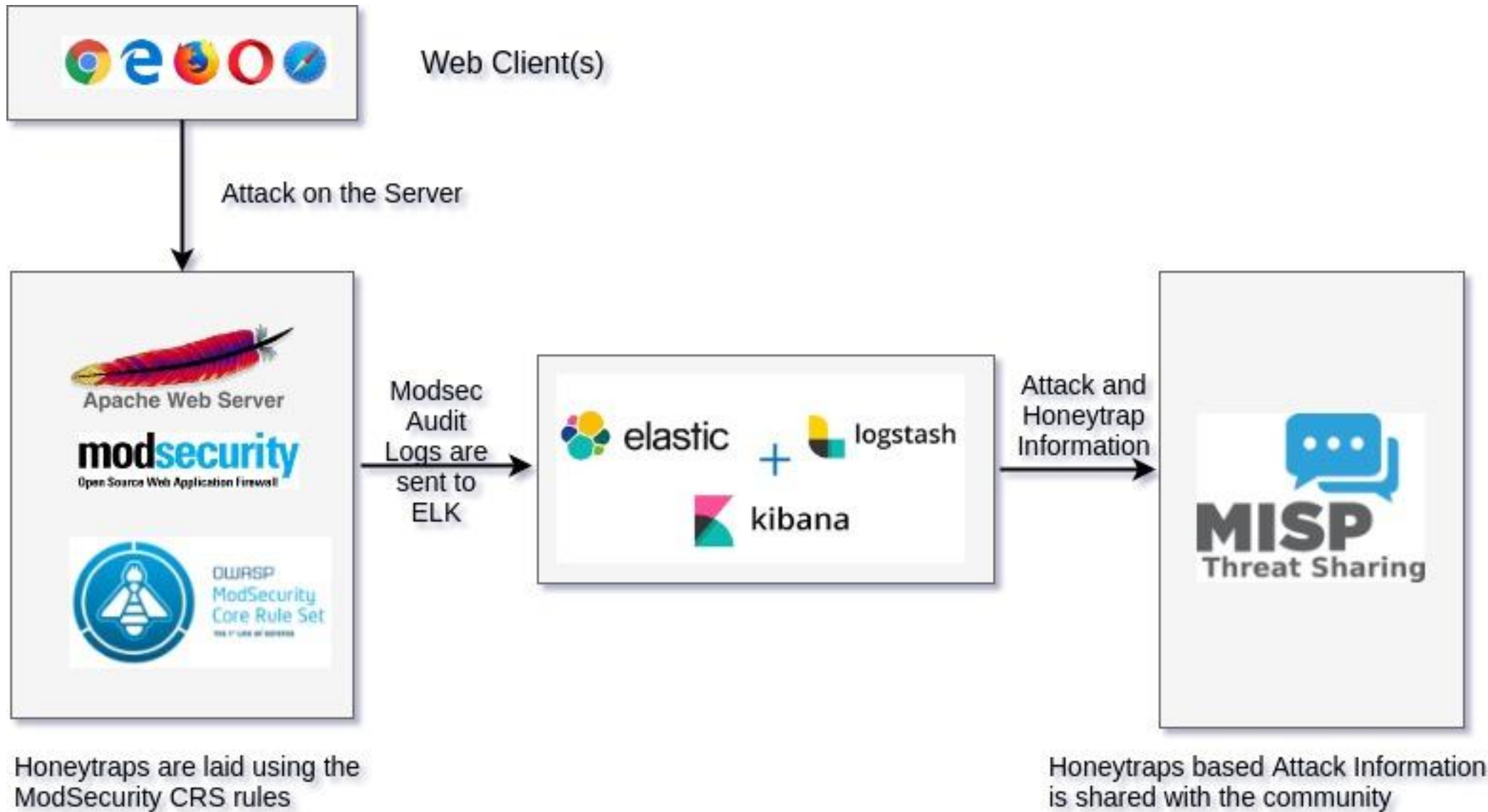
- ชุดกฎการตรวจจับสำเร็จรูป
- มีหลากหลายรูปแบบการตรวจจับ
  - ทั่วไป/คะแนนความผิดปกติ
- หมวดหมู่การตรวจจับที่หลากหลาย
  - Protocol Validation
  - Malicious Client Identification
  - Generic Attack Signatures
  - Known Vulnerabilities Signatures
  - Trojan/Backdoor Access
  - Outbound Data Leakage
  - Anti-Virus and DoS utility scripts





# โหมดการตรวจจับแบบดั้งเดิมของ CRS

- IDS/IPS Mode ด้วยกฎเกณฑ์ที่ “มีอยู่ในตัว”
- Stateless rule
- ผู้ใช้มือใหม่สามารถเข้าใจได้ง่าย
- อาจจัดการกฎได้ยาก
  - ไม่ใช่ทุกไซต์จะยอมรับความเสี่ยงได้เท่ากัน
  - การแจ้งเตือนระดับความรุนแรงต่ำจะถูกละเว้นเป็นส่วนใหญ่



# MISP?

- MISP เป็นแพลตฟอร์มแบ่งปันข้อมูลภัยคุกคามที่เป็นซอฟต์แวร์โอเพ่นซอร์ส
- เครื่องมือที่รวบรวมข้อมูลจากพันธมิตร นักวิเคราะห์ เครื่องมือ และ ฟีด
- ทำให้เป็นบรรทัดฐาน หากความสัมพันธ์ เสริมสร้างข้อมูล
- ช่วยให้ทีม และชุมชนทำงานร่วมกันได้
- ป้อนข้อมูลให้เครื่องมือป้องกันอัตโนมัติ และเครื่องมือวิเคราะห์

<https://github.com/coolacid/docker-misp>



# วัตถุประสงค์การใช้งานจากกลุ่มผู้ใช้

- แบ่งปันตัวอย่างสำหรับเรื่องการตรวจจับ
  - มีระบบที่ติดไวรัสในโครงสร้างพื้นฐาน หรือที่กำลังใช้งานอยู่หรือไม่?
- แบ่งปันตัวอย่างชี้การเพื่อทำการบล็อก
  - นำใช้คุณลักษณะมาใช้เพื่อบล็อก หลอกล่อ หรือเปลี่ยนเส้นทาง
- แบ่งปันตัวอย่างชี้เพื่อดำเนินการทางกลยุทธ์
  - รวบรวมข้อมูลเกี่ยวกับขบวนการการโจมตี มีความเกี่ยวข้องกันหรือไม่? ใครกำลังตกเป็นเป้าหมาย? ใครคือผู้โจมตี?
- ข้อมูลขัดแย้งต่าง ๆ (เช่น ผลบวกเท็จที่มีผลกระทบต่างไป)

# กลุ่มผู้ใช้งาน MISP

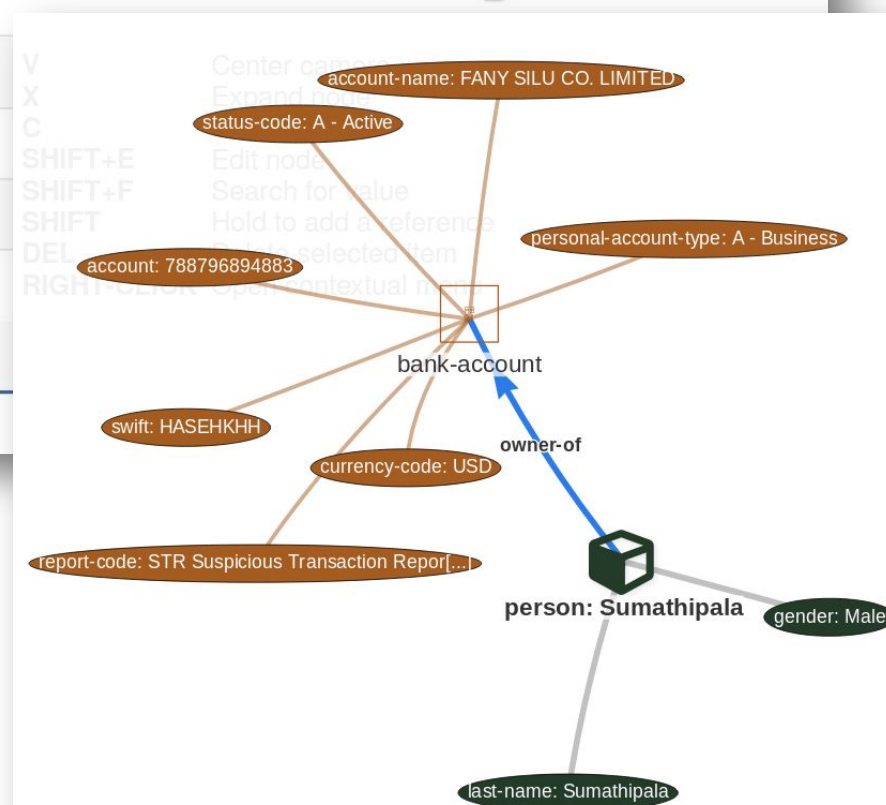
- กลุ่มที่มีการแบ่งปันข้อมูลด้วยวัตถุประสงค์เฉพาะ
- CIRCL ที่ดำเนินงานดูแล MISP จำนวนมาก (มากกว่า 1,200 องค์กร ที่มีผู้ใช้งานมากกว่า 4,000 คน)
- กลุ่มที่เชื่อมโยงกันระหว่างกลุ่มอุตสาหกรรม
- ภาคการเงิน (ธนาคาร, ISACs, องค์กรรับชำระเงิน) ใช้ MISP เป็นขั้นตอนในการแลกเปลี่ยนข่าวสาร
- หน่วยงานทหารหรือหน่วยงานระหว่างประเทศ (NATO, Military CSIRTs, n/g CERT and etc.)
- ผู้ให้บริการด้านความปลอดภัย ที่ก่อตั้งกลุ่มขึ้นร่วมกัน หรือเชื่อมต่อกับกลุ่มผู้ใช้งาน
- ชุมชนเฉพาะที่จัดตั้งขึ้นเพื่อจัดการกับปัญหาเฉพาะกิจ (COVID-19 MISP)

# ความท้าทายในการแบ่งปันข่าวสาร

- ความยากลำบากในการแบ่งปันไม่ใช่ปัญหาทางเทคนิค แต่มักเป็นเรื่องของสังคมหรือธุรกิจ (เช่น ความไว้วางใจ)
- ข้อกำหนดทางกฎหมาย
  - กรอบกฎหมาย ไม่อนุญาตให้แบ่งปันข้อมูล
  - ความเสี่ยงจากการรั่วไหลของข้อมูลสูงเกินไป และเสี่ยงเกินไปสำหรับองค์กรหรือพันธมิตร
- ข้อจำกัดในทางปฏิบัติ
  - ไม่มีข้อมูลที่จะแบ่งปัน
  - ไม่มีเวลาประมวลผลหรือมีส่วนร่วมกับตัวชี้วัด
  - แบบจำลองการจัดประเภทมีความไม่เข้ากัน
  - เครื่องมือสำหรับการแบ่งปันข้อมูลมีการเชื่อมโยงเป็นรูปแบบเฉพาะ หรือใช้รูปแบบที่แตกต่างกัน

# ตัวอย่าง : โมเดลข้อมูล

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28				<b>Name:</b> bank-account			References: 0		
2018-09-28		Other	<b>status-code:</b> text	A - Active	+	Add		<input type="checkbox"/>	
2018-09-28		Other	<b>report-code:</b> text	STR Suspicious Transaction Report	+	Add		<input type="checkbox"/>	
2018-09-28		Other	<b>personal-account-type:</b> text	A - Business	+	Add			
2018-09-28		Financial fraud	<b>swift:</b> bic	HASEHKHH	+	Add			
2018-09-28		Financial fraud	<b>account:</b> bank-account-nr	788796894883	+	Add			
2018-09-28		Other	<b>account-name:</b> text	FANY SILU CO. LIMITED	+	Add			
2018-09-28		Other	<b>currency-code:</b> text	USD	+	Add			



# บริบทและการจับกลุ่มข้อมูล

- MISP ทำงานร่วมกันในระดับ Event และระดับแอดทริบิวต์ MITRE's Adversarial Tactics, Techniques และ Common Knowledge (ATT&CK)

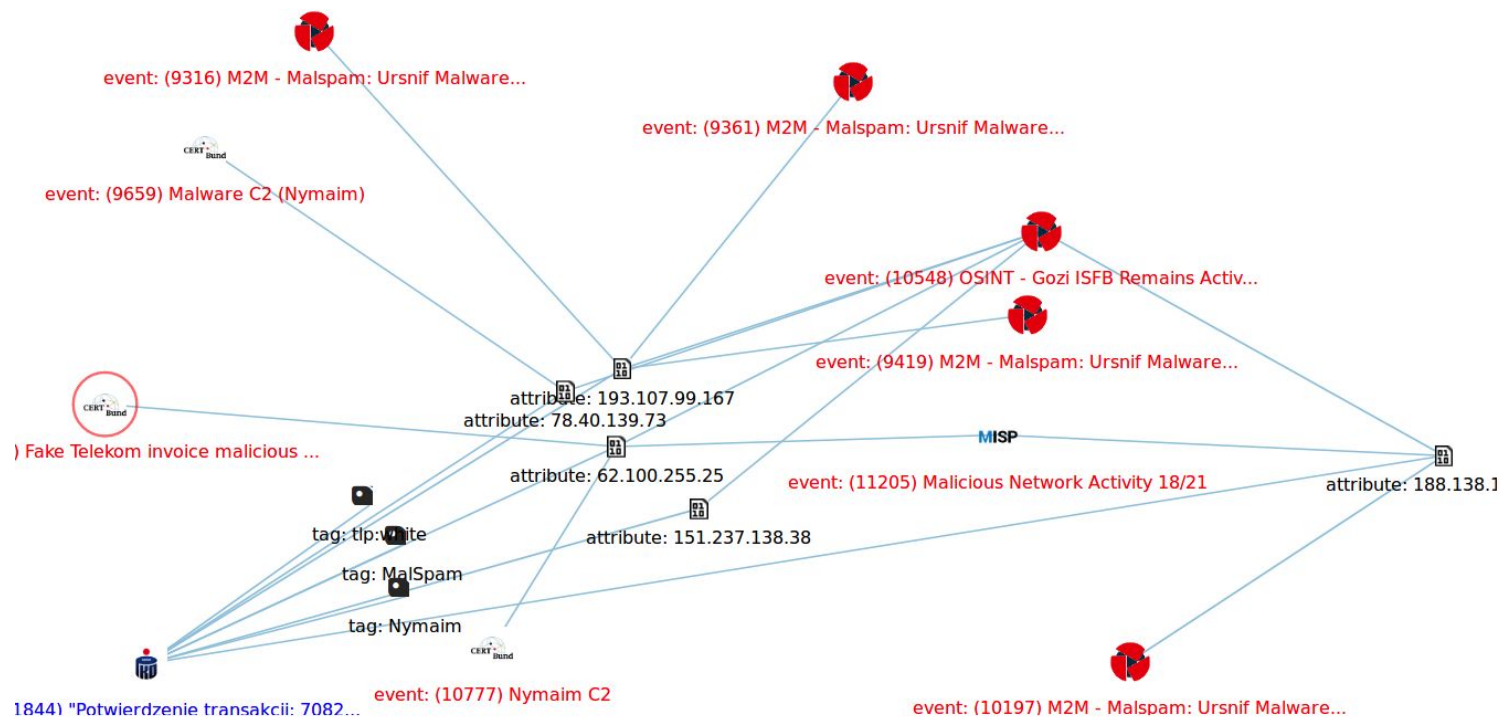
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Exfiltration Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Exfiltration	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
Spearphishing Link	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänger	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestomp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obfuscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modify Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software	Data from Local System		Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding





# คุณสมบัติความสัมพันธ์ : เครื่องมือสำหรับนักวิเคราะห์

เพื่อยืนยันการค้นพบ (เช่น นี่เป็นแคมเปญเดียวกันหรือไม่) เสริมการวิเคราะห์ (เช่น นักวิเคราะห์คนอื่นๆ มีสมมติฐานเหมือนกันหรือไม่) ยืนยันลักษณะเฉพาะ (เช่น ที่อยู่ IP ที่ได้จากการดักใช้สำหรับแคมเปญเดียวหรือไม่) หรือแค่ค้นหาว่า ภัยคุกคามนี้เป็นของใหม่หรือไม่เคยเจอในกลุ่มของคุณ



# รองรับ Sightings

- เราหรือกลุ่มได้พบ/เคยพบ ตามชุดข้อมูลดังกล่าวมาก่อนหรือไม่
- นอกจากนี้ ระบบ sighting ยังรองรับการตรวจพบเชิงลบ (FP) และ sighting หมดอายุ
- sighting สามารถทำได้ผ่าน API หรือ UI
- หลายกรณี การให้คะแนนตัวบ่งชี้ (scoring indicators) สามารถพิจารณาได้จาก sighting จากผู้ใช้
- สำหรับข้อมูลปริมาณมาก สามารถใช้ SightingDB โดย Devo



> Search... (e.g. status:200 AND extension:PHP)

Add a filter +

Honeytrap Ports Used



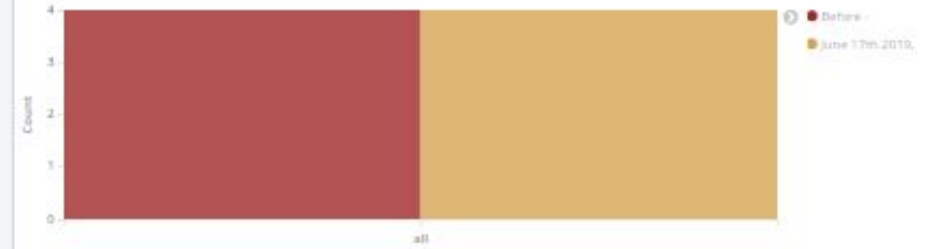
Honeytrap Remote IP Addresses



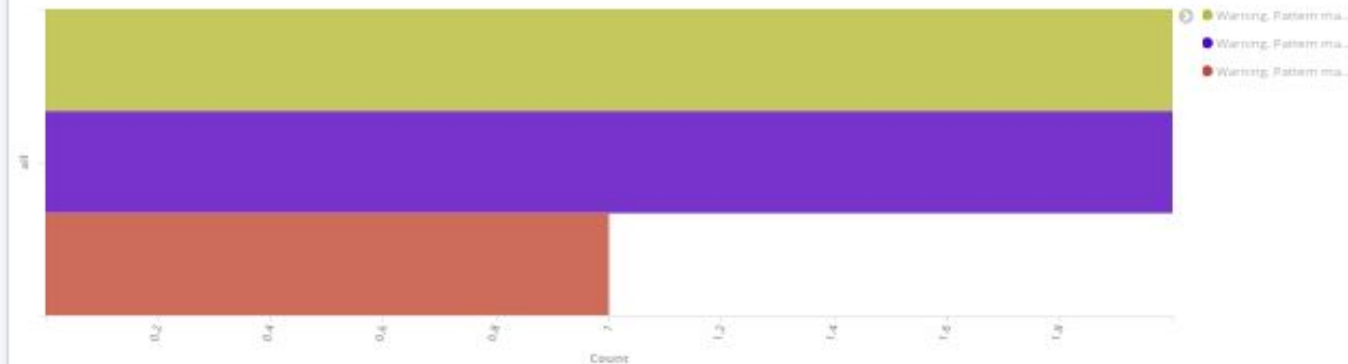
User Agents used in Honeytraps



Honeytrap Events Count



Honeytrap SecRule Events



# Events

« previous next »



My Events Org Events

Enter value to search

Filter

<input type="checkbox"/>	Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	Email	Date	Info	Distribution	Actions
<input type="checkbox"/>	x	ORNAME	ORNAME	45		<b>AutoGenerated</b> <b>HoneytrapEvent</b> <b>ModSecurity</b>	0	admin@admin.test	2019-07-23	Attack identified from the "172.17.0.1" at timestamp "23/Jul/2019:12:06:24 +0000" ["Warning. Pattern match \"^(8000 8080 8888)\$\" at SERVER_PORT. [file \"/etc/modsecurity.d/modsecurity.conf\" [line \"237\" [id \"999004\" [msg \"HoneyTrap Alert: Traffic Received on Fake Port.\"]] This information is generated from [\"ModSecurity for Apache/2.9.3 (http://www.modsecurity.org)\", \"OWASP_CRS/3.1.0\"]	Organisation <	
<input type="checkbox"/>	x	ORNAME	ORNAME	44		<b>AutoGenerated</b> <b>HoneytrapEvent</b> <b>ModSecurity</b>	0	admin@admin.test	2019-07-23	Attack identified from the "172.17.0.1" at timestamp "23/Jul/2019:12:06:21 +0000" ["Warning. Pattern match \"^(8000 8080 8888)\$\" at SERVER_PORT. [file \"/etc/modsecurity.d/modsecurity.conf\" [line \"237\" [id \"999004\" [msg \"HoneyTrap Alert: Traffic Received on Fake Port.\"]] This information is generated from [\"ModSecurity for Apache/2.9.3 (http://www.modsecurity.org)\", \"OWASP_CRS/3.1.0\"]	Organisation <	
<input type="checkbox"/>	x	ORNAME	ORNAME	43		<b>AutoGenerated</b> <b>HoneytrapEvent</b> <b>ModSecurity</b>	0	admin@admin.test	2019-07-23	Attack identified from the "172.17.0.1" at timestamp "23/Jul/2019:12:05:32 +0000" ["Warning. Pattern match \"~/db_backup.\\\\\\\\d{10}\" at REQUEST_FILENAME. [file \"/etc/modsecurity.d/modsecurity.conf\" [line \"250\" [id \"999006\" [msg \"HoneyTrap Alert: Disallowed robots.txt Entry Accessed.\"]] Idata	Organisation <	



# OWASP / Honeypot-Project / honeytraps

<https://github.com/OWASP/Honeypot-Project>

POC Pre-require

- Docker engine
- RAM > 8GB
- ตรวจสอบ port ที่ต้องใช้ใน file “docker-compose.yml” ว่าพร้อมใช้หรือไม่ หากไม่ ต้องทำการเปลี่ยน
  - 9091 – เว็บที่ถูกจำลอง เข้าได้โดยไม่เก็บ log
  - 8000,8080,8888 – มีการตั้งกฎการตรวจจับ
  - 9200,9300 – Elasticsearch
  - 5601 – Kibana
  - 5044 – Logstash
  - 443 – MISP



# HoneyTrap-1 (Adding Fake HTTP Ports for Listening)

- ขั้นตอนทดสอบ

```
curl <Host-IP>:8888/index.html
```

- ผลลัพธ์

```
t message  🔍 📄 * {"transaction":{"time":"15/Jun/2019:16:17:48 +0000","transaction_id":"XQUaLIYqPyL9jSkciTxejQAAAAE","remote_address":"192.168.112.210","remote_port":40356,"local_address":"172.17.0.3","local_port":8888},"request":{"request_line":"GET / HTTP/1.1","headers":{"Host":"192.168.136.88:8888","Connection":"keep-alive","Upgrade-Insecure-Requests":"1","User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36","Accept":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3","Accept-Encoding":"gzip, deflate","Accept-Language":"en-GB,en;q=0.9,en-US;q=0.8,te;q=0.7"},"response":{"protocol":"HTTP/1.1","status":200,"headers":{"Last-Modified":"Sun, 23 Jul 2017 17:50:26 GMT","ETag":"\"b-554ffb2bc80\"","Accept-Ranges":"bytes","Content-Length":"11","Keep-Alive":"timeout=5, max=100","Connection":"Keep-Alive","Content-Type":"text/html; charset=UTF-8"},"body":"hello world"},"audit_data":{"messages":["Warning. Pattern match \"^[\\\\\\\\d.]+$\" at REQUEST_HEADERS:Host. [file \"/etc/httpd/modsecurity.d/owasp-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf \"] [line \"810\"] [id \"920350\"] [rev \"2\"] [msg \"Host header is a numeric IP address\"] [data \"192.168.136.88:8888\"] [severity \"WARNING\"] [ver \"OWASP_CRS/3.0.0\"] [maturity \"9\"] [accuracy \"9\"] [tag \"application-multi\"] [tag \"language-multi\"] [tag \"platform-multi\"] [tag \"attack-protocol\"] [tag \"OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST\"] [tag \"WASCTC/WASC-21\"] [tag \"OWASP_TOP_10/A7\"] [tag \"PCI/6.5.10\"],\"Warning. Pattern match \"^(8000|8080|8888)$\" at SERVER_PORT. [file \"/etc/httpd/modsecurity.d/modsecurity.conf\"] [line \"237\"] [id \"999004\"] [msg \"HoneyTrap Alert: Traffic Received on Fake Port.\""],"error_messages":["[file \"apache2_util.c\"] [line 273] [level 3] [client %s] ModSecurity: %s% [uri \"%s\"]%s\"],[file \"apache2_util.c\"] [line 273] [level 3] [client %s] ModSecurity: %s% [uri \"%s\"]%s\""],"stopwatch":{"p1":511,"p2":814,"p3":43,"p4":139,"p5":109,"sr":88,"sw":67,"l":0,"gc":0},"response_body_dechunked":true,"producer":["ModSecurity for Apache/2.9.1 (http://www.modsecurity.org/)", "OWASP_CRS/3.0.2"],"server":"Apache/2.4.27 (Fedora)","engine_mode":"ENABLED"}}
```



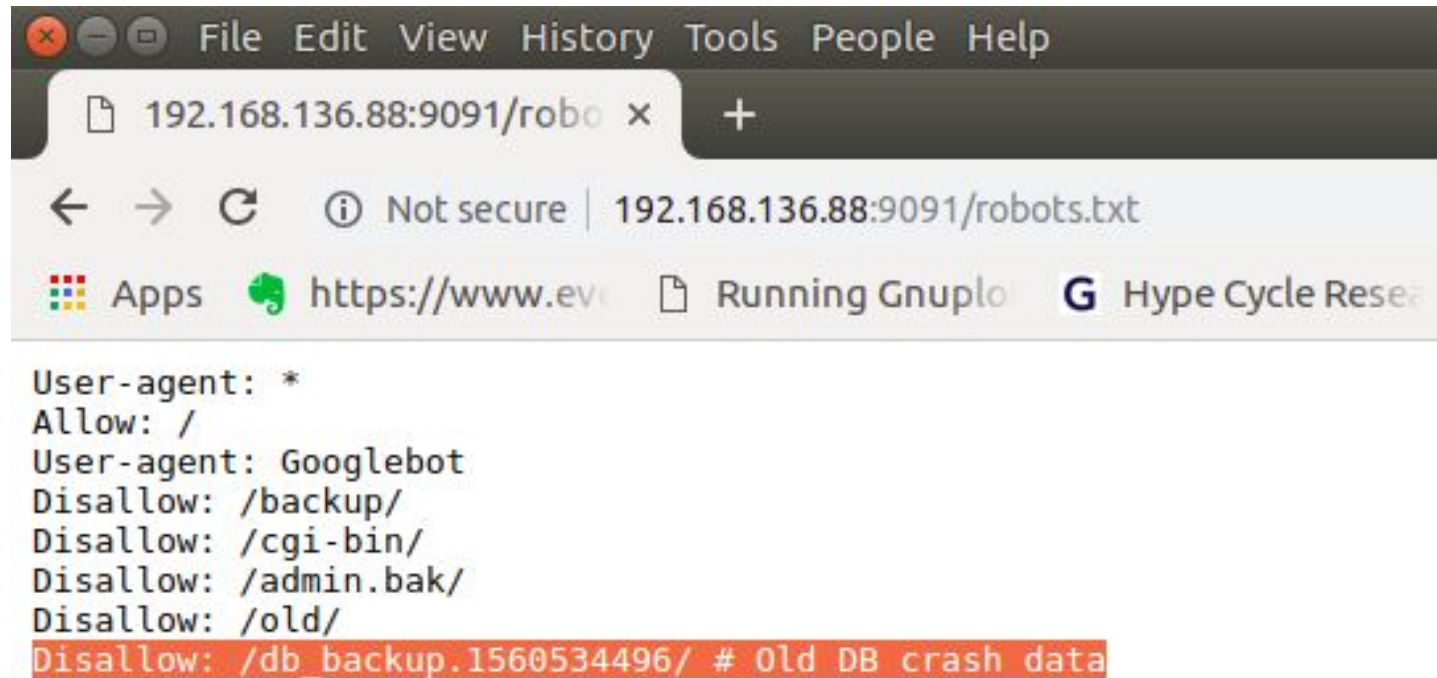
# HoneyTrap-1 (Adding Fake HTTP Ports for Listening)

```
# # Generate Alerts for all requests that we receive and
# set a variable in the IP Collection to mark the client
# as malicious.
#
SecRule SERVER_PORT "(8000|8080|8888)" \

"id:'999004',phase:2,t:none,log,block,msg:'HoneyTrap
Alert: Traffic Received on Fake
Port.',setvar:ip.malicious_client=1"
```



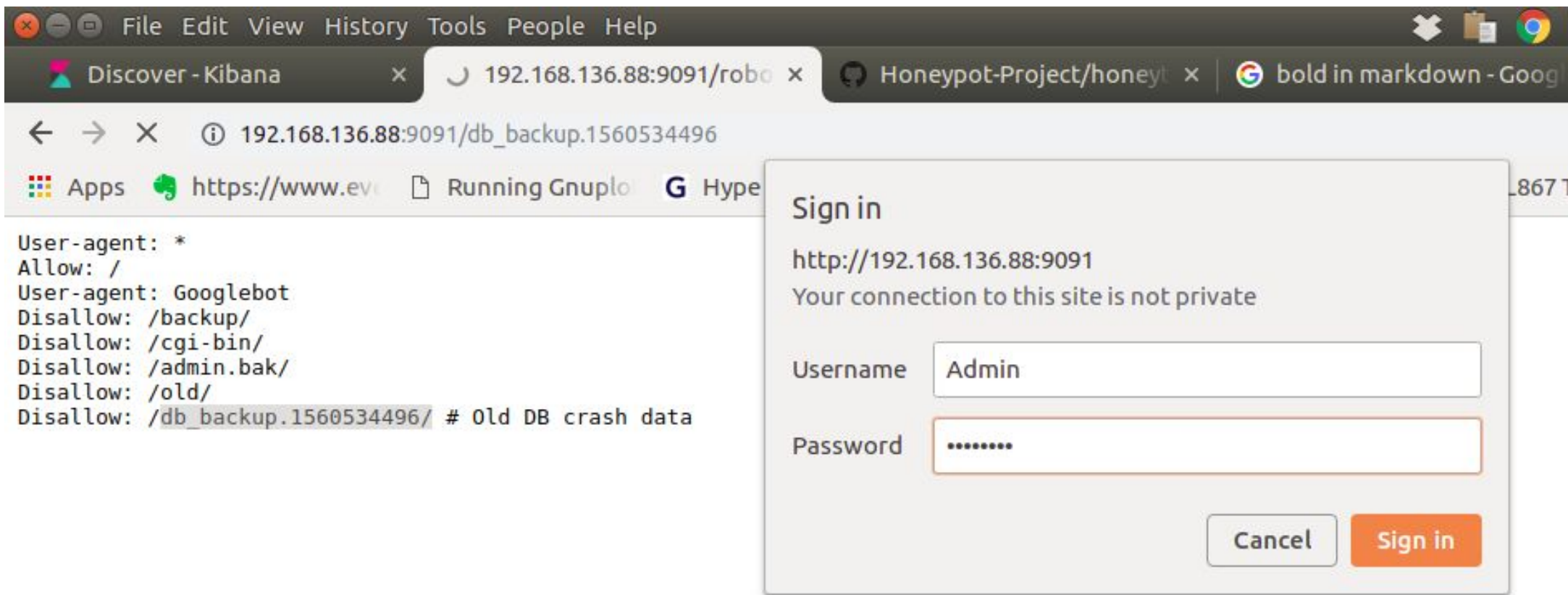
# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)



```
File Edit View History Tools People Help
192.168.136.88:9091/robo x +
Not secure | 192.168.136.88:9091/robots.txt
Apps https://www.ev Running Gnuplo Hype Cycle Resea
User-agent: *
Allow: /
User-agent: Googlebot
Disallow: /backup/
Disallow: /cgi-bin/
Disallow: /admin.bak/
Disallow: /old/
Disallow: /db backup.1560534496/ # Old DB crash data
```



# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)



The screenshot shows a web browser window with the following content:

Browser tabs: Discover - Kibana, 192.168.136.88:9091/robo, Honeypot-Project/honey, bold in markdown - Google

Address bar: 192.168.136.88:9091/db\_backup.1560534496

Page content (robots.txt):

```
User-agent: *  
Allow: /  
User-agent: Googlebot  
Disallow: /backup/  
Disallow: /cgi-bin/  
Disallow: /admin.bak/  
Disallow: /old/  
Disallow: /db_backup.1560534496/ # Old DB crash data
```

A "Sign in" dialog box is overlaid on the page, displaying:

Sign in  
http://192.168.136.88:9091  
Your connection to this site is not private

Username: Admin

Password: .....

Buttons: Cancel, Sign in

# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)

```
t message      🔍 📄 * {"transaction":{"time":"15/Jun/2019:16:46:14 +0000","transaction_id":"XQUg1rK5cZK41YStHbsupgAAAA
M","remote_address":"192.168.112.210","remote_port":33974,"local_address":"172.17.0.3","local_por
t":80},"request":{"request_line":"GET /db_backup.1560617158/ HTTP/1.1","headers":{"Host":"192.168.
136.88:9091","Connection":"keep-alive","Authorization":"Basic QWRtaW46UGFzc3dvcmQ=","Upgrade-Insec
ure-Requests":"1","User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge
cko) Chrome/71.0.3578.98 Safari/537.36","DNT":"1","Accept":"text/html,application/xhtml+xml,applic
ation/xml;q=0.9,image/webp,image/apng,*/*;q=0.8","Accept-Encoding":"gzip, deflate","Accept-Languag
e":"en-GB,en-US;q=0.9,en;q=0.8"},"response":{"protocol":"HTTP/1.1","status":401,"headers":{"WWW-A
uthenticate":"Basic realm=\"Admin\"","WWW-Authenticate":"Basic realm=\"Admin\"","Keep-Alive":"time
out=5, max=100","Connection":"Keep-Alive","Transfer-Encoding":"chunked","Content-Type":"text/html;
charset=iso-8859-1"},"audit_data":{"messages":["Warning. Pattern match \\\"^/db_backup\\.\\.\\.d{10}\\\"
at REQUEST_FILENAME. [file \"/etc/httpd/modsecurity.d/modsecurity.conf"] [line \"250\"] [id \"99
9006\"] [msg \"HoneyTrap Alert: Disallowed robots.txt Entry Accessed.\"] [data \"/db_backup.156061
7158/\"]","Warning. Pattern match \".*\" at TX:1. [file \"/etc/httpd/modsecurity.d/modsecurity.con
f"] [line \"259\"] [id \"999012\"] [msg \"HoneyTrap Alert: Authentication Attempt to Fake Resourc
e.\"] [data \"Credentials used: Admin:Password\""],"Warning. Pattern match \\\"^[\\"" data-bbox="129 181 837 944"/>
```



# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)

```
#Fake robots.txt file
```

```
SecRule REQUEST_FILENAME "@streq /robots.txt" \  
"id:'999005',phase:4,t:none,nolog,pass,append:'Disallow:  
/db_backup.%(time_epoch)/' "
```

```
#Identifying the malicious client
```

```
SecRule REQUEST_FILENAME "^/db_backup.\d{10}" \  
"id:'999006',phase:1,t:none,log,block,msg:'HoneyTrap  
Alert: Disallowed robots.txt Entry  
Accessed.',logdata:'%(matched_var)',setvar:ip.malicious_  
client=1"
```

```
#Setting the Fake Authentication
```



# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)

```
#Setting the Fake Authentication
SecRule REQUEST_FILENAME "^/db_backup.\d{10}"
" id: '999011', phase: 3, t: none, log, deny, status: 401, msg: 'HoneyTrapAlert: Disallowed robots.txt Entry Accessed.', logdata: '%{matched_var}', setvar: ip.malicious_client=1, setenv: basic_auth=1"
Header always set WWW-Authenticate "Basic realm=\"Admin\"" env= basic_auth
```



# HoneyTrap-2 (Adding Fake Disallow Entry in robots.txt file)

```
#For Decoding the Password given by the Hacker  
#we use following ruleset to extract and decode  
thecredentials.
```

```
SecRule REQUEST_FILENAME "^/db_backup.\d{10}"  
"chain,id:'999012',phase:1,t:none,log,msg:'HoneyTrap  
Alert: Authentication Attempt to Fake  
Resource.',logdata:'Credentials used: %{matched_var}'"
```

```
SecRule REQUEST_HEADERS:Authorization "^Basic (.*)" "  
"chain,capture"
```

```
SecRule TX:1 ".*" "t:base64Decode"
```



# HoneyTrap-3 (Adding Fake HTML Comments in the login page)

The screenshot shows a web browser window with the address bar displaying `https://www.ev... 192.168.136.88:9091/login.html`. The browser tabs include `Running Gnuplo`, `Hype Cycle Rese...`, `Give Me 45 Minu...`, `Evaluating Cont...`, and `COL867 Term Pa...`. The page content includes a heading `Add entry`, a sub-heading `Add another Article`, a `Username` input field, a `Password:` input field, and a `Login` button.

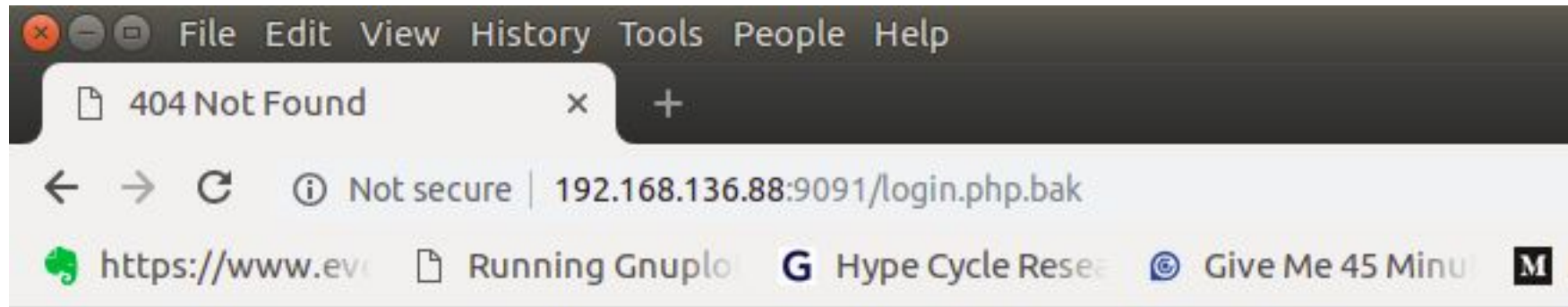
The developer console is open, showing the `Elements` tab. The HTML structure is as follows:

```
<html>
  <head>...</head>
  <body>
    <h3>Add entry</h3>
    <p> Add another Article</p>
    ... <!-- DEBUG - the source code for the old login page is login.php.bak -->
    <form action="login.html" method="post">...</form>
  </body>
</html>
```

The fake comment `<!-- DEBUG - the source code for the old login page is login.php.bak -->` is highlighted in blue in the original image. The console also shows the `html`, `body`, and `<!-->` elements in the breadcrumb at the bottom.



# HoneyTrap-3 (Adding Fake HTML Comments in the login page)



## Not Found

The requested URL /login.php.bak was not found on this server.

# HoneyTrap-3 (Adding Fake HTML Comments in the login page)

```
t message      Q Q [ * {"transaction":{"time":"17/Jun/2019:14:46:40 +0000","transaction_id":"XQen0G-vetL1qCS1AhmDmgAAAA
A","remote_address":"192.168.112.210","remote_port":51984,"local_address":"172.17.0.3","local_por
t":80},"request":{"request_line":"GET /login.php.bak HTTP/1.1","headers":{"Host":"192.168.136.88:9
091","Connection":"keep-alive","Upgrade-Insecure-Requests":"1","User-Agent":"Mozilla/5.0 (X11; Lin
ux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36","DNT":"1","Ac
cept":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8","Acc
ept-Encoding":"gzip, deflate","Accept-Language":"en-GB,en-US;q=0.9,en;q=0.8","Cookie":"(null)=Admi
n:0"},"response":{"protocol":"HTTP/1.1","status":404,"headers":{"Set-Cookie":"(null)=Admin:0","Co
ntent-Length":"211","Keep-Alive":"timeout=5, max=100","Connection":"Keep-Alive","Content-Type":"te
xt/html; charset=iso-8859-1"},"body":"<!DOCTYPE HTML PUBLIC \"-//IETF//DTD HTML 2.0//EN\">\n<html>
<head>\n<title>404 Not Found</title>\n</head><body>\n<h1>Not Found</h1>\n<p>The requested URL /log
in.php.bak was not found on this server.</p>\n</body></html>\n"},"audit_data":{"messages":["Warnin
g. String match \"/login.php.bak\" at REQUEST_FILENAME. [file \"/etc/httpd/modsecurity.d/modsecuri
ty.conf"] [line \"274\"] [id \"999008\"] [msg \"HoneyTrap Alert: Fake HTML Comment Data Use
d.\"],\"Warning. Pattern match \"^[\\\\\\\\d.]+\"$\" at REQUEST_HEADERS:Host. [file \"/etc/httpd/modsec
urity.d/owasp-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line \"810\"] [id \"920350\"] [r
ev \"2\"] [msg \"Host header is a numeric IP address\"] [data \"192.168.136.88:9091\"] [severity
\"WARNING\"] [ver \"OWASP_CRS/3.0.0\"] [maturity \"9\"] [accuracy \"9\"] [tag \"application-multi
\"] [tag \"language-multi\"] [tag \"platform-multi\"] [tag \"attack-protocol\"] [tag \"OWASP_CRS/P
ROTOCOL_VIOLATION/IP_HOST\"] [tag \"WASCTC/WASC-21\"] [tag \"OWASP_TOP_10/A7\"] [tag \"PCI/6.5.10
\"],\"error_messages\":[\"[file \"apache2_util.c\"] [line 273] [level 3] [client %s] ModSecurity: %
s%s [uri \"%s\"]%s\", \"[file \"apache2_util.c\"] [line 273] [level 3] [client %s] ModSecurity: %s%s
 [uri \"%s\"]%s\"],\"stopwatch\":{\"p1\":964,\"p2\":1979,\"p3\":61,\"p4\":415,\"p5\":156,\"sr\":104,\"sw\":99,\"l\":
0,\"gc\":0},\"response_body_dechunked\":true,\"producer\":[\"ModSecurity for Apache/2.9.1 (http://www.mod
security.org/)\",\"OWASP_CRS/3.0.2\"],\"server\":\"Apache/2.4.27 (Fedora)\",\"engine_mode\":\"ENABLED\"}]

# offset      Q Q [ * 122,155
t source      Q Q [ * /var/log/modsec_audit.log
t tags        Q Q [ * beats_input_codec_plain_applied
```





## HoneyTrap-3 (Adding Fake HTML Comments in the login page)

```
##We will add some fake HTML comments  
##With this data, an attacker may be able to better plan  
and execute attacks against your web application
```

```
SecRule REQUEST_FILENAME "@streq /login.html"  
"chain,id:'999007',phase:4,t:none,nolog,pass,setvar:'tx.  
form_comment_honeytrap=<form action=\"login.html\"  
method=\"post\">'"
```

```
SecRule STREAM_OUTPUT_BODY "@rsub  
s/{tx.form_comment_honeytrap}/<!-- DEBUG - the source  
code for the old login page is login.php.bak  
-->{tx.form_comment_honeytrap}/d"
```

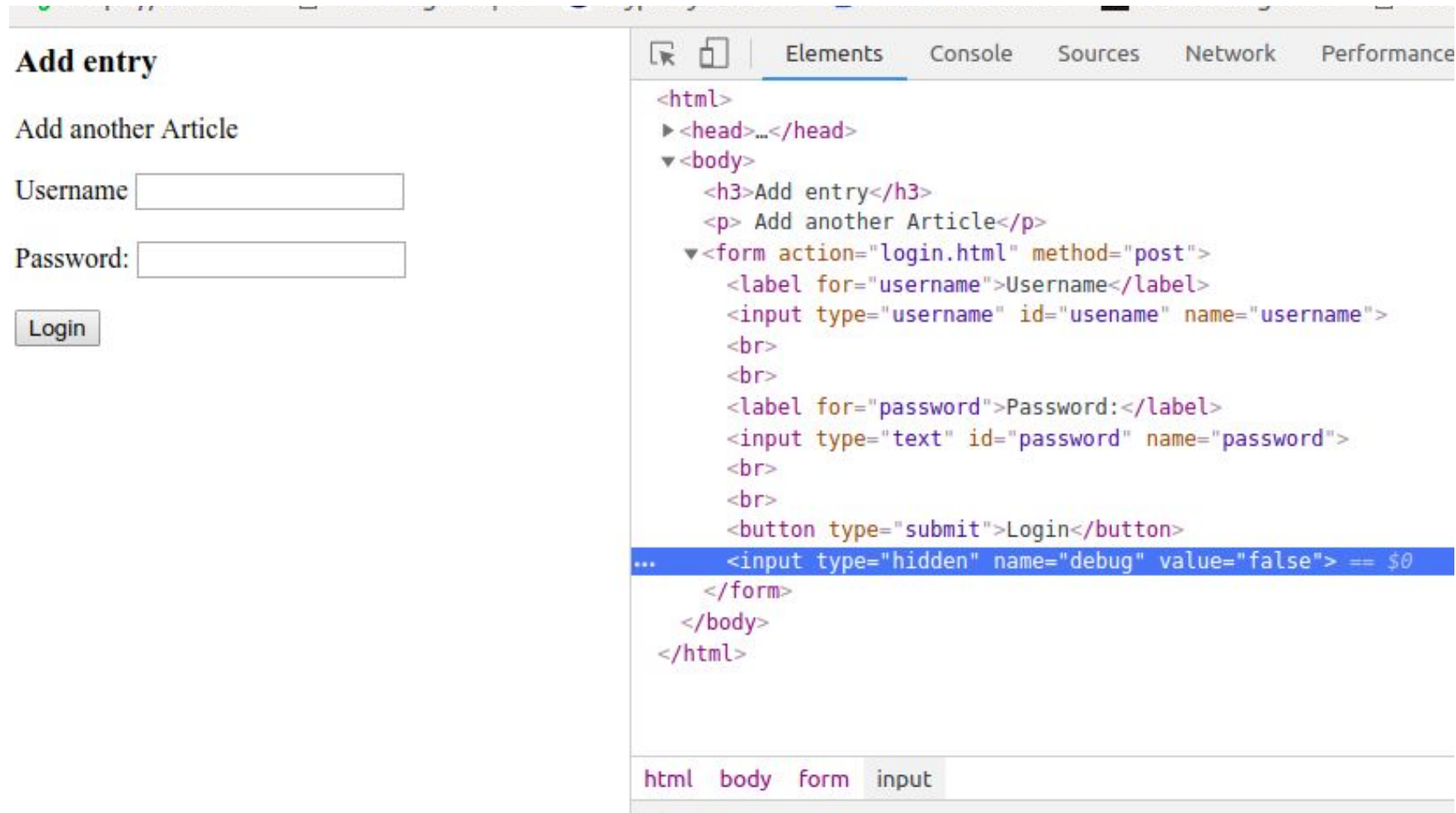


## HoneyTrap-3 (Adding Fake HTML Comments in the login page)

```
SecRule REQUEST_FILENAME "@streq /login.php.bak"  
"id:'999008',phase:1,t:none,log,block,msg:'HoneyTrap  
Alert: Fake HTML Comment Data  
Used.',setvar:ip.malicious_client=1"
```



# HoneyTrap-4 (Adding Fake Hidden Form Fields)



The screenshot displays a web browser window with a login form titled "Add entry". The form contains the following elements:

- A heading "Add entry"
- A paragraph "Add another Article"
- A "Username" label followed by an input field.
- A "Password:" label followed by an input field.
- A "Login" button.

The browser's developer tools are open to the "Elements" tab, showing the HTML structure of the page. The highlighted code is:

```
<input type="hidden" name="debug" value="false"> == $0
```

The breadcrumb at the bottom of the developer tools indicates the path: `html > body > form > input`.

# HoneyTrap-4 (Adding Fake Hidden Form Fields)

```
<html>
  ▶ <head>...</head>
  ▼ <body>
    <h3>Add entry</h3>
    <p> Add another Article</p>
    ▼ <form action="login.html" method="post">
      <label for="username">Username</label>
      <input type="username" id="username" name="username">
      <br>
      <br>
      <label for="password">Password:</label>
      <input type="text" id="password" name="password">
      <br>
      <br>
      <button type="submit">Login</button>
      ... <input type="hidden" name="debug" value="true"> == $0
    </form>
  </body>
</html>
```



# HoneyTrap-4 (Adding Fake Hidden Form Fields)

```
t message      🔍 📄 * {"transaction":{"time":"17/Jun/2019:14:59:46 +0000","transaction_id":"XQeq4jmFefuH2zSfV1NoewAAAA
U","remote_address":"192.168.112.210","remote_port":55028,"local_address":"172.17.0.3","local_por
t":80},"request":{"request_line":"POST /login.html HTTP/1.1","headers":{"Host":"192.168.136.88:909
1","Connection":"keep-alive","Content-Length":"41","Cache-Control":"max-age=0","Origin":"http://19
2.168.136.88:9091","Upgrade-Insecure-Requests":"1","DNT":"1","Content-Type":"application/x-www-for
m-urlencoded","User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36","Accept":"text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,image/apng,*/*;q=0.8","Referer":"http://192.168.136.88:9091/","Accept-Encoding":"gzi
p, deflate","Accept-Language":"en-GB,en-US;q=0.9,en;q=0.8","Cookie":{"(null)=Admin:0"},"body":{"use
rname=admin&password=dsdsds&debug=true"}}, "response":{"protocol":"HTTP/1.1","status":200,"header
s":{"Set-Cookie":{"(null)=Admin:0"},"Last-Modified":"Sun, 16 Jun 2019 09:04:51 GMT","ETag":"\b4-58
b6d2c1bd075","Accept-Ranges":"bytes","Content-Length":"556","Keep-Alive":"timeout=5, max=100","C
onnection":"Keep-Alive","Content-Type":"text/html; charset=UTF-8"},"body":"<html>\n<head>\n  <ti
tle>Login</title>\n</head>\n  <h3>Add entry</h3>\n  <p> Add another Article</p>\n  <form act
ion=\login.html\ method=\post\>\n    <label for=\username\>Username</label> <input type=
\username\ id=username\ name=username\><br /><br />\n    <label for=\password\>Passwo
rd:</label> <input type=\text\ id=password\ name=password\><br /><br />\n    <button t
ype = \submit\>Login</button>\n  </form>\n</html>\n"},"audit_data":{"messages":["Warning. Patt
ern match \^[\\d.]+$\" at REQUEST_HEADERS:Host. [file \"/etc/httpd/modsecurity.d/owasp-crs/rul
es/REQUEST-920-PROTOCOL-ENFORCEMENT.conf\" [line \"810\" [id \"920350\" [rev \"2\" [msg \"Host
header is a numeric IP address\" [data \"192.168.136.88:9091\" [severity \"WARNING\" [ver \"OW
ASP_CRS/3.0.0\" [maturity \"9\" [accuracy \"9\" [tag \"application-multi\" [tag \"language-mul
ti\" [tag \"platform-multi\" [tag \"attack-protocol\" [tag \"OWASP_CRS/PROTOCOL_VIOLATION/IP_HO
ST\" [tag \"WASCTC/WASC-21\" [tag \"OWASP_TOP_10/A7\" [tag \"PCI/6.5.10\"], \"Warning. Match of
\\streq false\" against \\\ARGs:debug\" required. [file \"/etc/httpd/modsecurity.d/modsecurity.con
f\" [line \"300\" [id \"999010\" [msg \"HoneyTrap Alert: Fake HIDDEN Form Data Manipulate
d.\"], \"error_messages\":[[file \"apache2_util.c\" [line 273] [level 3] [client %s] ModSecurity:
%s%s [uri \"%s\"]%s\", [file \"apache2_util.c\" [line 273] [level 3] [client %s] ModSecurity: %s%
s [uri \"%s\"]%s\"], \"stopwatch\":{\"p1\":1136, \"p2\":4450, \"p3\":68, \"p4\":683, \"p5\":180, \"sr\":131, \"sw\":10
9, \"l\":0, \"gc\":0}, \"response_body_dechunked\":true, \"producer\":[\"ModSecurity for Apache/2.9.1 (http://w
ww.modsecurity.org/)\", \"OWASP_CRS/3.0.2\"], \"server\":\"Apache/2.4.27 (Fedora)\", \"engine_mode\":\"ENABLE
n111
```



# HoneyTrap-4 (Adding Fake Hidden Form Fields)

```
# Adding Fake Hidden Form Fields

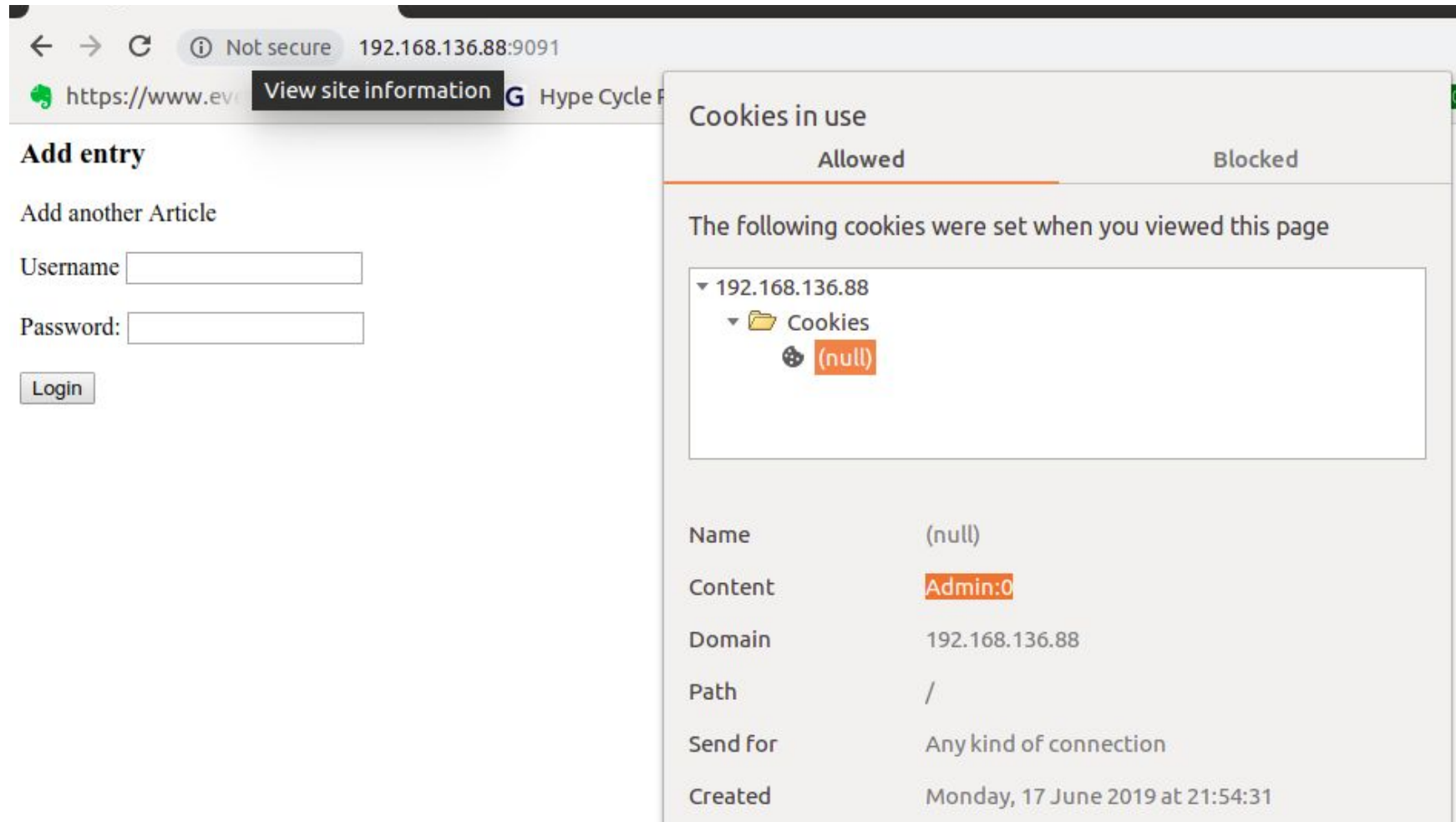
SecRule STREAM_OUTPUT_BODY "@rsub s/<\/form>/<input
type=\"hidden\" name=\"debug\"
value=\"false\"><\/form>/"
"id:'999009',phase:4,t:none,nolog,pass"

#Detecting the client if the rule is triggered

SecRule ARGS:debug "!@streq false"
"id:'999010',phase:2,t:none,log,block,msg:'HoneyTrap
Alert: Fake HIDDEN Form Data
Manipulated.',setvar:ip.malicious_client=1"
```



# HoneyTrap-5 (Adding Fake Cookies)



The screenshot shows a web browser window with the address bar displaying "Not secure 192.168.136.88:9091" and the URL "https://www.ev...". The page content includes a "View site information" button and a "Hype Cycle" link. Below this is a section titled "Add entry" with the sub-heading "Add another Article". It contains two input fields: "Username" and "Password:", followed by a "Login" button.


Overlaid on the right side of the browser is a "Cookies in use" popup window. It has two tabs: "Allowed" (selected) and "Blocked". The popup contains the text "The following cookies were set when you viewed this page" and a tree view showing a folder for "192.168.136.88" containing a "Cookies" folder with a single cookie entry: "(null)".


Name	Value
Name	(null)
Content	Admin:0
Domain	192.168.136.88
Path	/
Send for	Any kind of connection
Created	Monday, 17 June 2019 at 21:54:31


# HoneyTrap-5 (Adding Fake Cookies)

http://192.168.136.88:9091/login.html

▼ 192.168.136.88 | (null)

 Value  
Admin:5






Domain  
192.168.136.88

Path  
/

Expiration  
Wed Jun 17 2020 22:11:35 GMT+0530 (India Standard Time)

SameSite  
No Restriction ▼

HostOnly       Session       Secure       HttpOnly

 [Help](#)



# HoneyTrap-5 (Adding Fake Cookies)

```
t message      🔍 📄 * {"transaction":{"time":"17/Jun/2019:14:59:46 +0000","transaction_id":"XQeq4jmFefuH2zSfV1NoewAAAA
U","remote_address":"192.168.112.210","remote_port":55028,"local_address":"172.17.0.3","local_por
t":80},"request":{"request_line":"POST /login.html HTTP/1.1","headers":{"Host":"192.168.136.88:909
1","Connection":"keep-alive","Content-Length":"41","Cache-Control":"max-age=0","Origin":"http://19
2.168.136.88:9091","Upgrade-Insecure-Requests":"1","DNT":"1","Content-Type":"application/x-www-for
m-urlencoded","User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36","Accept":"text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,image/apng,*/*;q=0.8","Referer":"http://192.168.136.88:9091/","Accept-Encoding":"gzi
p, deflate","Accept-Language":"en-GB,en-US;q=0.9,en;q=0.8","Cookie":"(null)=Admin:0"},"body":{"use
rname=admin&password=dsdsds&debug=true"}}, "response":{"protocol":"HTTP/1.1","status":200,"header
s":{"Set-Cookie":"(null)=Admin:0","Last-Modified":"Sun, 16 Jun 2019 09:04:51 GMT","ETag":"\"1b4-58
b6d2c1bd075\"","Accept-Ranges":"bytes","Content-Length":"556","Keep-Alive":"timeout=5, max=100","C
onnection":"Keep-Alive","Content-Type":"text/html; charset=UTF-8"},"body":"<html>\n<head>\n  <ti
tle>Login</title>\n</head>\n  <h3>Add entry</h3>\n  <p> Add another Article</p>\n  <form act
ion=\"/login.html\" method=\"post\">\n    <label for=\"username\">Username</label> <input type=
\"username\" id=\"username\" name=\"username\"><br /><br />\n    <label for=\"password\">Passwo
rd:</label> <input type=\"text\" id=\"password\" name=\"password\"><br /><br />\n    <button t
ype = \"submit\">Login</button>\n  </form>\n</html>\n"},"audit_data":{"messages":["Warning. Patt
ern match \"^[\\d.]+$\" at REQUEST_HEADERS:Host. [file \"/etc/httpd/modsecurity.d/owasp-crs/rul
es/REQUEST-920-PROTOCOL-ENFORCEMENT.conf\" [line \"810\" [id \"920350\" [rev \"2\" [msg \"Host
header is a numeric IP address\" [data \"192.168.136.88:9091\" [severity \"WARNING\" [ver \"OW
ASP_CRS/3.0.0\" [maturity \"9\" [accuracy \"9\" [tag \"application-multi\" [tag \"language-mul
ti\" [tag \"platform-multi\" [tag \"attack-protocol\" [tag \"OWASP_CRS/PROTOCOL_VIOLATION/IP_HO
ST\" [tag \"WASCTC/WASC-21\" [tag \"OWASP_TOP_10/A7\" [tag \"PCI/6.5.10\"], \"Warning. Match of
\"streq false\" against \"ARGS:debug\" required. [file \"/etc/httpd/modsecurity.d/modsecurity.con
f\" [line \"300\" [id \"999010\" [msg \"HoneyTrap Alert: Fake HIDDEN Form Data Manipulate
d.\"], \"error_messages\":[\"[file \"apache2_util.c\" [line 273] [level 3] [client %s] ModSecurity:
%s%s [uri \"%s\"]%s\", \"[file \"apache2_util.c\" [line 273] [level 3] [client %s] ModSecurity: %s%
s [uri \"%s\"]%s\"], \"stopwatch\":{\"p1\":1136,\"p2\":4450,\"p3\":68,\"p4\":683,\"p5\":180,\"sr\":131,\"sw\":10
9,\"l\":0,\"gc\":0}, \"response_body_dechunked\":true,\"producer\":[\"ModSecurity for Apache/2.9.1 (http://w
ww.modsecurity.org/)\", \"OWASP CRS/3.0.2\"], \"server\":\"Apache/2.4.27 (Fedora)\", \"engine mode\":\"FNARI F
```



# HoneyTrap-5 (Adding Fake Cookies)

```
##Adding Fake Cookies
```

```
SecRule RESPONSE_HEADERS:Set-Cookie "^ (.*) ="  
"id:'999013',phase:3,t:none,nolog,pass,capture,setenv:honeytrap_cookie_name=%{tx.1}-user_role"
```

```
Header always set Set-Cookie  
"%{HONEYTRAP_COOKIE_NAME}e=Admin:0"
```



## HoneyTrap-5 (Adding Fake Cookies)

```
SecRule REQUEST_HEADERS:Cookie "@contains  
%{global.honeytrap_cookie_name}"  
"chain,id:'999014',phase:1,t:none,log,block,msg:'HoneyTr  
ap Alert: Fake Cookie Data Manipulation'"
```

```
SecRule REQUEST_HEADERS:Cookie "!@contains =Admin:0"  
"setvar:ip.malicious_client=1"
```




- [View Event](#)
- [View Correlation Graph](#)
- [View Event History](#)

- [Edit Event](#)
- [Delete Event](#)
- [Add Attribute](#)
- [Add Object](#)
- [Add Attachment](#)
- [Populate from...](#)
- [Enrich Event](#)
- [Merge attributes from...](#)

- [Publish Event](#)
- [Publish \(no email\)](#)
- [Contact Reporter](#)
- [Download as...](#)

- [List Events](#)
- [Add Event](#)

## Attack identified from the "172.17.0.1" at ti...

Event ID	45
UUID	5d36f849-9e80-4276-a46a-0137ac110002
Creator org	<a href="#">ORGNAME</a>
Owner org	<a href="#">ORGNAME</a>
Email	admin@admin.test
Tags	<span>AutoGenerated</span> <span>HoneytrapEvent</span> <span>ModSecurity</span> <span>+</span>
Date	2019-07-23
Threat Level	High
Analysis	Initial
Distribution	Your organisation only <span>🔒</span> <span>↩</span>
Info	Attack identified from the "172.17.0.1" at timestamp "23/Jul/2019:12:06:24 +0000" ["Warning. Pattern match \"\\(8000 8080 8888)\$\" at SERVER_PORT. [file \"/etc/modsecurity.d/modsecurity.conf\" [line \"237\" [id \"999004\"] [msg \"HoneyTrap Alert: Traffic Received on Fake Port.\"]] This information is generated from [\"ModSecurity for Apache/2.9.3 (http://www.modsecurity.org)\", \"OWASP_CRS/3.1.0\"]
Published	No
#Attributes	0 (0 Object)
First recorded change	2019-07-23 12:06:34
Last change	2019-07-23 12:06:34
Modification map	
Sightings	0 (0) - restricted to own organisation only. <span>🔑</span>

[-](#) Pivots [-](#) Galaxy [+](#) Event graph [+](#) Correlation graph [+](#) ATT&CK matrix [-](#) Attributes [-](#) Discussion



# บทสรุป

- แนวทางปฏิบัติในการแบ่งปันข้อมูลมาจากการผู้ใช้งานและตัวอย่าง (เช่น การเรียนรู้โดยการเลียนแบบจากข้อมูลที่แบ่งปัน)
- MISP เป็นเพียงเครื่องมือ สิ่งที่สำคัญคือแนวปฏิบัติในการแบ่งปันขององค์กร เครื่องมือควรมีความโปร่งใสมากที่สุดเพื่อสนับสนุนผู้ใช้งาน
- ให้ผู้ใช้ปรับแต่ง MISP เพื่อให้สอดคล้องกับกรณีการใช้งานของกลุ่ม
- โครงการ MISP เกิดขึ้นจากการรวมกันของ ซอฟต์แวร์โอเพ่นซอร์ส มาตรฐานแบบเปิด แนวทางปฏิบัติที่ดี และกลุ่มคนเพื่อทำให้การแบ่งปันข้อมูล มีการทำงานใกล้เคียงความเป็นจริงที่สุด

Questions?



A tall, white lighthouse stands on a sandy beach at sunset. The sun is low on the horizon, casting a warm glow across the sky and reflecting on the wet sand. The lighthouse is the central focus, with its reflection visible in the shallow water. The sky is a mix of blue, orange, and yellow. In the foreground, a seagull is visible on the left. The text 'THANK YOU' is overlaid in a white box in the center of the image.

THANK YOU