Pacific Northwest
NATIONAL LABORATORY

PNNL-33514

FIC Consequence Profile – Hypothetical Cybercrime Syndicate Adversary Dossier

Provided by PNNL's Shamrock Cyber

September 2022

Jacob Beaman
Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Emma Lancaster
Danielle Nodine
Patrick O'Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Bianca Steele
Angela Steinmetz
Chance Younkin

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-33514

FIC Consequence Profile – Hypothetical Cybercrime Syndicate Adversary Dossier

September 2022

Jacob Beaman
Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Emma Lancaster
Danielle Nodine
Patrick O'Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Bianca Steele
Angela Steinmetz
Chance Younkin

https://shamrockcyber.pnnl.gov

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

The Flagpole Installation Commission's (FIC) web development team has engaged PNNL's Shamrock Cyber team to produce this Consequence Profile. This Consequence Profile is an Adversary Dossier, which provides the foundation for a thorough understanding of unacceptable mission outcomes, and the threats and vulnerabilities that make these outcomes plausible. The dossier helps stakeholders and development teams understand each other's viewpoints. It also provides a means for reducing overall risk by prioritizing threats and vulnerabilities based on unacceptable outcomes. The Consequence Profile can be used as is, or as content to inform other reports tailored to a specific audience. It is intended to enable decision makers at all levels to improve the security posture of the system. The abuse case scenarios were mapped and prioritized for the FIC system and are summarized in the table below.

#	Scenario	Explanation
Most unacceptable outcome		
1	*Denial of Service / Data Destruction*	A HCCS or terrorist targets the FIC website with a SQL injection attack aimed at denying the availability of FIC services to the public by causing a persistent crashing condition that could also result in the destruction of data.
2	*Data Manipulation / Defamation*	A hacktivist or script kiddie may vandalize the public-facing FIC site by using SQL injection attacks to manipulate and modify the database.
3	*Data Exfiltration / credential dumping*	A HCCS wanting to exfiltrate personally identifiable information or other sensitive data from the FIC website may perform different SQL command injections attempting to dump the password database, exfiltrating it to use in a follow-on attack later, to sell on the dark web, or to elevate their current privileges so they can use a legitimate external web service as a means for relaying data to/from a compromised system.
Somewhat unacceptable outcome		
4	*Adversary in the Middle*	The HCCS or terrorist stands up a fake FIC website masquerading as the real FIC site. The attacker acts as a proxy, being able to read, insert, and modify the data in the intercepted communication. It is also possible to capture a session cookie to gain access to a valid account that can be exploited and used for data exfiltration or valid account access
5	*Lack of Integrity Checks / Masquerading*	Anyone can apply for a permit, anyone can take the quiz and become certified, the quiz shows correct answers after the first attempt, and no one checks the location of where the flagpole is being installed and who the company or business is. This could lead to defamation, terrorist groups flying their flag instead of the U.S. flag, etc.
Least unacceptable outcome		
6	*Extortion / Notoriety*	An adversary or hacktivist may upload malware, acting as a payload, backdoor, or as a way to consume system resources and crash the FIC website. This could be done by automating the process of inputting a file, submitting possibly thousands of requests per second/minute, causing a network denial of service. The adversary could demand payment to cease the DoS condition or do it for notoriety among other cybercriminals.
7	*Spoofing*	Contact information is displayed, including a phone number on the main FIC site. The phone number can be spoofed making it look like FIC is making phone calls, or the number can be redirected to call someone who is not part of FIC as a prank, for example an ex-spouse.

Contents

Figures

Tables

Acknowledgements

In this effort, the Shamrock Cyber team engaged with FIC's development and management teams on several occasions. The intent of this engagement strategy was to meet with and gather information from those with the best knowledge of and most insight into both the current state and the future state of the FIC project as well as the IT and security environment in which it will operate. This approach also ensures that the equities of the various stakeholders are communicated to the Shamrock team so that they may be accounted for in the assessment and addressed in reporting or feedback.

Engagements with the FIC team focused on the project itself and provided background information, outlined the problem being solved, project goals, and use cases. Discussions with the FIC development team provided an understanding of the software and network infrastructure in which the FIC service would operate, along with identifying additional concerns and sensitivities of other supported or connected applications. This allowed the adversarial threat environment and context to be adequately assessed with defined and workable parameters.

Acronyms and Abbreviations

CCO	Cybercriminal Organization
CIA	Confidentiality, Integrity, and Availability
CVEs	Common Vulnerabilities and Exposures
DoS	Denial of Service
FAE	Functional Abuse Element
FUE	Functional Use Element
HAC	Hypothetical Abuse Case
HCCS	Hypothetical Cybercrime Syndicate
IDDIL-ATC	Identify Assets, Define the Attack Surface, Decompose the System, Identify Attack Vectors, List the Threat Actors, Analysis & Assessment, Triage, Controls
IAC	Implied Abuse Case
OSA	Open-Source Analysis
PII	Personally Identifiable Information
PNNL	Pacific Northwest National Laboratory
RBAC	Role Based Access Controls
SAST	Static Application Security Testing
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TAE	Technical Abuse Element
TBA	Threat-Based Analysis
TMT	Threat Modeling Tool

1.0 Introduction

The FIC team engaged with Pacific Northwest National Laboratory's ***Shamrock Cyber*** team to perform cybersecurity analyses of the FIC system. Shamrock offers several cybersecurity services as shown in Figure 1. These services are ultimately used together to inform business decision makers and minimize mission risk. This ***Consequence Profile*** is an ***Adversary Dossier*** and is part of Shamrock's Consequence-Based Analysis services. The dossier summarizes abuse case analysis of FIC within the adversarial context of a sophisticated Hypothetical Cybercrime Syndicate (HCCS) or hacktivist.

Consequence-Based Analysis – analyzes the abuse, misuse, and hazards that determine risks of developing and deploying a system. The result is a Consequence Profile detailing the consequence-based analysis.

Threat-Based Software Analysis – determines and prioritizes threats against the system and recommends mitigations. The result is a Threat Profile that contains a threat model, threat findings, and mitigations.

Vulnerability-Based Analysis – analyzes a system from a vulnerability perspective and includes structural security analysis, operational security analysis, and security testing. The result is a Vulnerability Profile detailing the vulnerability-based analysis.

Figure 1. Shamrock Cyber services.

This context was selected by the FIC development team because of the general prevalence of attacks on government-owned systems. The destructive and disruptive consequences of denial of service, data exfiltration, extortion, vandalism, and masquerading attacks are significant across these sectors and should thus be addressed. This dossier provides abuse case scenarios for 8 plausible attack types. No specific cybercriminal organization is identified in this dossier.

The analysis determined the HCCS or hacktivist to be primarily motivated by industrial espionage, hacking for hire, political messaging, defamation, disinformation, vandalism, and personal curiosity. The means for executing these attacks assessed a combination of technical abuse elements made available through previous source code scans and research into the vulnerabilities associated with the products in use that provide the FIC service.

2.0 Methods

The development of this dossier relies on several factors—key among them are the following:

- Adversarial context – the technical capabilities, motives, and level of motivation of the HCCS or hacktivist. The assessed “technical capabilities” in this analysis includes the use of the MITRE ATT&CK Matrix to provide a standardized and well-documented reference to adversarial tactics and techniques and to assist the design of system defenses and risk mitigations (a link to the matrix is included in Table 1).
- Functional Abuse Elements (FAEs) – the FIC functions that the HCCS can take advantage of and abuse to achieve their goals.
- Technical Abuse Elements (TAEs) – the technical means via vulnerabilities or exploits that enable execution of the FAEs.
- Abuse Cases (Actual) – these scenarios exist when TAEs have been identified that would enable one or more of the FAEs.
- Abuse Case (hypothetical) – these scenarios are listed where it is plausible that a TAE does or could exist that enables one or more of the FAEs but has yet to be fully identified. These hypothetical abuse cases are documented as “watchlist” items to provide enhanced situational awareness for proactive system security.

3.0 Abuse Case Scenarios

The abuse case analysis led to 8 plausible scenarios in which an HCCS or hacktivist could execute a successful attack against FIC. The scenarios are plausible because the FAEs and TAEs align to the adversary context, thus providing clear prioritization of the vulnerabilities (TAEs) that should be addressed to further strengthen FIC against an HCCS or hacktivist attack. The final impact—effect on target—of a chained attack may be prevented by breaking the chain at any point by implementing a control or other defense that eliminates one of the chain's components. However, any effects, accesses, capabilities, or exploits gained before the break in the chain could remain in place and still serve as an attack vector for reattacks or redirected attacks.

3.1 Scenario 1: Denial of Service (Actual)

3.1.1 FAE: Input Forms; SQL Injection

A HCCS or terrorist organization wanting notoriety targets the FIC website with a SQL injection attack aimed at denying the availability of FIC services to the general public by causing a persistent crashing condition that could also result in the destruction of data.

- Tactic: Initial Access; Exploit Public Facing Application ID: T1190
- Tactic: Execution Technique: Exploitation for Client Execution ID: T1203
- Tactic Impact: Endpoint Denial of Service; Application or System Exploitation ID: T1499.004
- Tactic Impact: Data Destruction ID: T1485

3.2 Scenario 2: Data Exfiltration / Credential Dumping (Actual)

3.2.1 FAE: Input Forms; SQL Injection

A HCCS wanting to exfiltrate personally identifiable information (PII) or other sensitive data from the FIC website may perform different SQL command injections attempting to dump the password database, exfiltrating it to use in a follow-on attack later, to sell on the dark web, or to elevate their current privileges so they can use a legitimate external web service as a means for relaying data to/from a compromised system.

- Tactic: Initial Access; Exploit Public Facing Application ID: T1190
- Tactic: Execution Technique; Exploitation for Client Execution ID: T1203
- Tactic: Credential Access; OS Credential Dumping ID: T1003
- Tactic Exfiltration Technique: Exfiltration Over Web Service ID: T1567
- Tactic Privilege Escalation: Valid Accounts; Local Accounts ID: T1078
- Tactic Command and Control: Web Service ID: T1102

3.3 Scenario 3: Vandalism / Defamation (Actual)

3.3.1 FAE: Input Forms; SQL Injection

A hacktivist or script kiddie wanting to mess around for fun may use SQL injection to manipulate and modify the database in a way that would cause defamation or embarrassment to the FIC employees and stakeholders through vandalism.

- Tactic: Initial Access; Exploit Public Facing Application ID: T1190 / SQL injection
- Tactic: Execution Technique; Exploitation for Client Execution ID: T1203
- Tactic: Credential Access; OS Credential Dumping ID: T1003
- Tactic Exfiltration Technique: Exfiltration Over Web Service ID: T1567
- Tactic Privilege Escalation: Valid Accounts; Local Accounts ID: T1078
- Tactic Command and Control: Web Service ID: T1102

3.4 Scenario 4: Impersonation / Adversary in the Middle (Actual)

3.4.1 FAE: Missing HSTS Headers; Exfiltration

The HCCS or terrorist group wants to stand up a fake FIC website masquerading as the real FIC site. Web servers without the Strict-Transport-Security header expose clients to adversary-in-the-middle attacks by forcing an initial connection over HTTP before being redirected to use HTTPS. Once the transmission control protocol connection is intercepted, the attacker acts as a proxy, being able to read, insert, and modify the data in the intercepted communication. It is also possible to capture a session cookie to gain access to a valid account that can be exploited and used for data exfiltration or valid account access.

- Tactic Collection, Credential Access Technique: Adversary in the Middle ID: 1557 / Missing HSTS Header
- Tactic Exfiltration Technique: Exfiltration Over Web Service ID T1567
- Lateral Movement, Defense Evasion; Use Alternate Web Authentication Material: Web Session Cookie; T1550.004
- Persistence; Valid Accounts: Domain Accounts; T1078.002

3.5 Scenario 5: Forced Authentication Leads to Clickable Links (Actual)

3.5.1 FAE: Clickable Links

After doing a SQL injection to dump the database password, the adversary can use the hardcoded password obtained from the source code to gain elevated access to the FIC site. The adversary, having elevated their privileges, could manipulate the website and host malicious links that would capture other user credentials and PII or execute malware for follow-on activity.

- Tactic: Resource Development; Develop Capabilities: Malware ID: T1587.001

- Tactic: Initial Access; Exploit Public Facing Application ID: T1190 / Hardcoded Password
- Tactic: Execution Technique: Exploitation for Client Execution ID: T1203 / SQL Injection
- Tactic: Execution Technique: User Execution: Malicious Links ID:1204.001
- Tactic: Defense Evasion, Privilege Escalation Technique: Access Token Manipulation; Token Impersonation / Theft ID: T1134
- Tactic Impact Technique: Data Manipulation ID: T1565

3.6 Scenario 6: Denial of Service due to Hacktivism / Extortion (Implied)

3.6.1 FAE: Upload File Button; SQL Injection

An adversary or hacktivist may upload malware, acting as a payload, backdoor, or as a way to consume system resources and crash the FIC website. This could be done by automating the process of inputting a file, submitting possibly thousands of requests per second/minute, causing a network denial of service. The adversary could demand payment to cease the DoS condition.

- Tactic: Resource Development; Develop Capabilities: Exploits ID: T1587.004
- Tactic: Initial Access; Exploit Public Facing Application ID: T1190
- Tactic: Impact Technique: Network Denial of Service ID: T1498

3.7 Scenario 7: Data Manipulation / Spoofing (Implied)

3.7.1 FAE: Contact Information

Contact information is displayed, including a phone number. The phone number can be spoofed making it look like FIC is making phone calls, or the number can be redirected to call someone who is not part of FIC as a prank, for example an ex-spouse.

- Tactic: Initial Access Privilege Escalation; Valid Accounts: Domain Accounts ID: T1078.002
- Tactic: Persistence; Lateral Movement; Valid Accounts / Hardcoded Password
- Tactic: Execution; User Execution ID: T1204
- Tactic Impact Technique: Data Manipulation ID: T1565

3.8 Scenario 8. Lack of Integrity Checks Leads to Defamation / Loss of Credibility / Masquerading (Hypothetical)

3.8.1 FAE: Quiz / Fillable Forms

Anyone can apply for a permit, anyone can take the quiz and become certified, the quiz shows correct answers after the first attempt, and no one checks the location of where the flagpole is being installed and who the company or business is. This could lead to defamation, terrorist groups flying their flag instead of the U.S. flag, etc.

- Tactic: Initial Access; Privilege Escalation; Valid Accounts: ID: T1078

4.0 Dossier for Hypothetical Cybercrime Syndicate

Table 1 is the adversary dossier for the Cybercrime Syndicate. However, The left column shows the parameter name and a definition of the parameter. The right column shows the value of that parameter as determined by the abuse case analysis.

Table 1. Adversary Dossier for Hypothetical Cybercrime Syndicate

Parameter	Value
Adversary *Specific existing adversary if known or identified (e.g., Cult of the Dead Cow, Anonymous, REvil, Fancy Bear, Deep Panda, etc.)*	**None Known**
Adversary type *One of the following:* • *State or state-supported actor* • *Cybercrime syndicate* • *Hacktivists/disgruntled employee* • *Illicit cyber profiteer* • *Sophisticated hacker* • *Script kiddie*	Cybercrime Syndicate Hacktivist Script kiddie
Adversary sophistication level *One of the following:* • *VERY HIGH – State of the art, state level* • *HIGH – Imaginative to unique use of known exploits and scripting of new exploits, capable of running complex campaigns* • *MEDIUM – Use of known exploits and established tactics with some level of adaptability* • *LOW – Rudimentary use of well-known and published exploit*	High - Imaginative to unique use of known exploits and scripting of new exploits, capable of running complex campaigns Medium – Use of known exploits and established tactics with some level of adaptability
Adversary motivation(s) *The primary interests/goals of the adversary, which can be any of the following:* • *Intelligence gathering* • *Cyber warfare* • *Industrial espionage* • *Profit* • *Hacking for hire* • *Political messaging* • *Defamation* • *Disinformation* • *Vandalism* • *Notoriety* • *Personal curiosity* • *Chaos* • *etc.*	Industrial espionage Hacking for hire Political messaging Defamation Disinformation Vandalism Personal curiosity Chaos

Desired effects/actions *Description of the actions on target or effects (network, device, or physical) that the adversary intends to employ in support of their motive.*	Data exfiltration and credential dumping (confidentiality) Manipulation of system for profit (integrity) Denial of service (availability)
Assessed capabilities *Description of the types of attacks and complexities of those attacks and campaigns that could be employed by an adversary based on sophistication level, motivations, and desired effects. These are assessed potential capabilities, not observed specific capabilities.*	Knowledge and experience using open-source recon and exploitation tools Computational resources such as botnets Knowledge on exploitation of SQL injection Mirroring or hosting fake sites for impersonation
Observed capabilities *Specific and observed capabilities that are attributed to an adversary (if a specific adversary has been identified).*	TBD - Requires identification of specific adversary group
Assessed tactics *Description of the nature and exploit types and tools that could be employed by an adversary based on sophistication level, motivations, and desired effects. Often presented in terms of industry standards or published lists of vulnerabilities and/or exploits. These are assessed potential tactics, not observed specific tactics.* *Examples:* *MITRE ATT&CK Matrix – https://attack.mitre.org/* *CISA Known Exploited Vulnerabilities – https://www.cisa.gov/known-exploited-vulnerabilities-catalog*	Reconnaissance: None Resource Dev: Stage Capabilities, Develop Capabilities Initial Access: Exploit public facing application, Valid Accounts Execution: Command and scripting interpreter, exploitation of client execution, Native API, User Execution Persistence: Valid Accounts Privilege Escalation: Process injection, Valid Accounts Defense Evasion: Process injection, Use Alternate Authentication Material, Valid Account Credential Access: Adversary In The Middle, OS Credential Dumping, Unsecured Credentials Discovery: None Lateral Movement: Use Alternate Authentication Material Collection: Adversary in the middle Command And Control: Web Service Exfiltration: Exfiltration over web service Impact: Data Manipulation, Data Destruction, Endpoint Denial of Service, Network Denial of Service

5.0 Implied FUE, FAE, and TAE Table

The implied FUE scenarios are listed when applicable common vulnerabilities and exposures (CVEs) exist or are documented within the used technology at large, but the specific implementation to the FIC product is unknown. Further investigation is required to determine if there are actual TAEs in FIC's context.

FUE	FUE EXPLANATION	FAE	TAE
Clickable links	On the webpage to obtain a permit, there are clickable links that forward to external sites for reference material	Manipulation of link / spoofing / hosting a malicious link that takes you outside of FIC	Tactic: Defense Evasion, Privilege Escalation Technique: Process Injection ID: T1055 Tactic: Execution Technique: User Execution: Malicious links ID:1204.001
Docker	Open platform for developing and running applications. Connects to APIs used by the front end	Exploit software vulnerabilities in the code base to elevate privileges or gain initial access	Tactic: Initial Access Technique: Exploit Public Facing Application ID: T1190 Privilege Escalation: Exploitation for Privilege Escalation ID: T1068
Node JS	Uses postgreSQL, serves up the APIs used by the front end	Has CVEs that relate to man in the middle / authentication	Tactic: Credential access Technique: Unsecured Credentials: Container API ID:T1552.007 Tactic: Execution Technique: Command and Scripting Interpreter: JavaScript ID: 1059.007

FUE	FUE EXPLANATION	FAE	TAE
API	Misconfigurations can lead to initial access, adversary in the middle attacks, or endpoint denial of service	Denial of service / adversary in the middle	Tactic: Execution Technique: Exploitation for Client Execution ID: T1203 Execution through API; ID: T0871 Tactic; Execution Technique: Native API ID: T1106 Adversary in the Middle; ID: T1557
React JS	Renders web page on the browser	Attack pathways are DOM-based XSS / data manipulation	Tactic: Execution Technique: Native API ID: T1106 Tactic: Impact; Technique: Data Manipulation ID: 1565
Button to choose a file	Button to upload a flagpole plan	An attacker could upload a malware file if there is no criteria to check the validity of the file. If there are no frame busting checks or anything to counter clickjacking, a victim could be redirected to a malicious site. An attacker could cause a denial of service if uploading a massive file that consumes system resources. Possible abuses would be clickjacking, denial of service, or injecting malware	Tactic: Execution Technique: Command and Scripting Interpreter: JavaScript ID: 1059.007 Tactic: Impact Technique: Network Denial of Service ID: T1498 Tactic: Resource Development Technique: Stage Capabilities: Upload Malware ID:T1608.001
Network access / HTTPS	Communication protocol	Adversary in the middle	Tactic: Execution Technique: User Execution: Malicious links ID:1204.001 Tactic Collection, Credential Access Technique: Adversary in the Middle ID: 1557

FUE	FUE EXPLANATION	FAE	TAE
Certification quiz	To become a flag pole installer, you must first pass the quiz	Answers are shown after the first take. Anyone can become certified. Anyone can pose as legitimate, which could cause chaos	Tactic: Initial Access, Privilege Escalation: Valid Accounts; Local Accounts; ID: T1078
Reporting violations is not anonymous. Contact info must be entered	Whistleblowers, may be exposed or identified	Dumping of databases may include PII of those who have reported violations	Tactic: Credential Access; Technique: OS Credential Dumping ID: T1003
Apply for permit	Fillable forms to apply for a permit to have a flagpole installed	There are no human validity checks on the data input to the database. It could be false data, and the perpetrator can claim repudiation. Terrorists could pose as legitimate organizations and get permissions to fly their flag and defame the FIC organization	Tactic: Impact; Technique: Defacement: External Defacement ID: T1491
Fillable forms	Fillable forms to apply for a permit to have a flagpole installed	If able to automate the input form, it could act as a programmatic denial of service	Tactic: Resource Development Technique: Stage Capabilities: Upload Malware ID:T1608.001 Tactic: Impact Technique: Network Denial of Service ID: T1498

6.0 Actual FUE, FAE, and TAE Table

The actual FUEs are listed when applicable CVEs exist and have been documented in previous static application security testing. The TAE is attributable to the language used in ATT&CK to define the technique that could be employed to achieve a desired impact.

FUE	FUE EXPLANATION	FAE	TAE
Clickable links	On the webpage to obtain a permit, there are clickable links that forward to external sites for reference material	Manipulation of link / spoofing / hosting a malicious link that takes you outside of FIC	Tactic: Defense Evasion, Privilege Escalation Technique: Process Injection ID: T1055 Tactic: Execution Technique: User Execution: Malicious links ID:1204.001
Use of SQL	A language that communicates with databases	There is a known SQL injection vulnerability in the code base that could be a vector for attack	Initial Access; Exploit Public Facing Application ID: T1190 Tactic: Execution Technique: Exploitation for Client Execution ID: T1203
Missing_HSTS_Header	Strict-Transport-Security ensures the connection will always happen over HTTPS	Web servers without the Strict-Transport-Security header expose clients to man-in-the-middle attacks by forcing an initial connection over HTTP before being redirected to use HTTPS	Tactic: Credential Access / Collection: Technique: Adversary in the Middle ID: T1557
Use_Of_Hardcoded_Password	Authentication	The application uses a hard-coded password, allowing database access to anyone with access to the source code	Credential Access; Credentials from Password Stores: Credentials from Web Browsers ID: T1555.003 Credential Access; Unsecured Credentials T1552

FUE	FUE EXPLANATION	FAE	TAE
Missing_CSP_Header	Restricts how resources in the browser load	Web servers without the Strict-Transport-Security header are vulnerable to attacks such as Cross-Site Scripting	Tactic: Initial Access; Technique: Modify Authentication Process ID: T1556
Potential_Clickjacking_on_Legacy_Browsers	Enables the browser content to be rendered	HTML does not attack against clickjacking attacks, which could result in a user clicking a malicious link unintentionally	Potential clickjacking on legacy browsers Tactic: Execution; Technique; User Execution: Malicious Link; T1204.001
Potentially_Vulnerable_To_Csrf	Website navigation and authorization	HTML does not protect against clickjacking attacks, which could result in a user clicking a malicious link unintentionally	Tactic: Execution; Technique; User Execution: Malicious Link; T1204.001 Tactic: Credential Access; Technique: Steal Web Session Cookie ID: T1539
Client_Hardcoded_Domain	From source code scans	A resource is being loaded from a remote domain, allowing an attacker to replace its contents	Tactic: Credential Access / Collection: Technique: Adversary in the Middle ID: T1557 Tactic: Impact; Technique: Data Manipulation; ID: T1565

7.0 Watchlists

The determined FAEs along with other software uses have led to two applicable watchlists for the FIC product.

7.1 Implied Product Watchlist

Table 2. A summary of implied watchlist items with links to security advisories.

Implied Product Watchlist: Docker	
Summary	Notes/Links
214 total CVEs associated with Docker. Place on watchlist. 69 CVEs since 2021.	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Docker
Implied Product Watchlist: APIs	
Summary	Notes/Link
Depending on the type of API and the protocol being used, there are many different instantiations that could be implemented. There are 3,285 CVEs generally related to APIs. It is recommended to place the specific technologies in use on a consistent patching schedule and watchlist.	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=api
Implied Product Watchlist: Node JS	
Summary	Notes/Link
There are 584 matching CVEs for Node JS. It is recommended to place on a consistent patching schedule and watchlist.	https://nvd.nist.gov/vuln/search/results?isCpeNameSearch=false&query=node+js&results_type=overview&form_type=Basic&search_type=all&startIndex=0
Implied Product Watchlist: React JS	
Summary	Notes/Link
There are 21 CVEs related to React JS, 16 discovered within the last two years.	https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=React+JS&search_type=all&isCpeNameSearch=false
Implied Product Watchlist: HTTPS	
Summary	Notes/Link
There are over 150,000 vulnerabilities relating to HTTPS, with multiple new ones being found every day.	https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=HTTPS&search_type=all&isCpeNameSearch=false

7.2 Actual Product Watchlist

Table 3. A summary of actual watchlist items with links to security advisories.

Actual Product Watchlist: Clickable Links	
Summary	Notes/Links
On the webpage to obtain a permit, there are clickable links that forward to external sites for reference material.	https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html
Actual Product Watchlist: Missing Content Security Policy Header	
Summary	Notes/Link
Restricts how resources in the browser load.	Refer to FIC Vulnerability Profile (VP) for mitigation guidance.
Actual Product Watchlist: Missing HSTS Header	
Summary	Notes/Link
Strict-Transport-Security ensures the connection will always happen over HTTPS.	Refer to FIC VP for code location and mitigation guidance.
Actual Product Watchlist: Potential clickjacking on legacy browser	
Summary	Notes/Link
Enables the browser content to be rendered.	Refer to FIC VP for code locations and mitigation guidance.
Actual Product Watchlist: Potentially Vulnerable to Cross Site Request Forgery	
Summary	Notes/Link
HTML does not protect against clickjacking attacks, which could result in a user clicking a malicious link unintentionally.	Refer to FIC VP for code locations and mitigation guidance.
Actual Product Watchlist: Client Hardcoded Domain	
Summary	Notes/Link
A resource is being loaded form a remote domain. This could allow an attacker to replace its contents.	Refer to FIC VP for code locations and mitigation guidance.
Actual Product Watchlist: SQL	
Summary	Notes/Link
There is a known SQL injection vulnerability in the code base that serves as a vector for attack.	Refer to FIC VP for code locations and mitigation guidance.

8.0 Conclusion

This FIC Consequence Profile offers a consequence-based cybersecurity perspective for mission owners, stakeholders, and development teams. It presents plausible scenarios where adversaries could achieve their objectives, and associates those impacts with the specific system components and technologies in the FIC service. The scenarios are abuse cases derived from our analyses and from MITRE ATT&CK tactics and techniques. They describe adversarial behaviors and facilitate an understanding of how a HCCS or hacktivist would initially access and affect the FIC system components. This Consequence Profile provides the opportunity for decision makers most concerned with optimizing cybersecurity controls, the most plausible attack surfaces the HCCS would try to exploit, so they may begin to investigate and document the corresponding controls they have in place to mitigate these scenarios.

This consequence-based analysis illustrates the due diligence of the FIC team. By seeking an external analysis of their services, FIC increases the security and reliability of their operating environment and their capability. It also provides a foundation for a thorough understanding of possible malicious behaviors and addresses the top concerns that could affect the development team, the testing team, management, stakeholders, and partners of FIC. This enables decision makers at all levels to improve the security posture of the system. This effort leads to more secure software and better-understood security. The FIC team is to be commended for their rigorous approach to employing cybersecurity throughout the development life cycle of their products.

Appendix A MITRE ATT&CK Mapping

Reconnaissance	None			
Resource Development	T1608	T1587		
Initial Access	T1190	T1078		
Execution	T1203	T1204	T1059	T1106
Persistence	T1078			
Privilege Escalation	T1078	T1055		
Defense Evasion	T1550	T1078	T1055	
Credential Access	T1552	T1003	T1557	
Discovery	None			
Lateral Movement	T1550			
Collection	T1557			
Command and Control	T1102			
Exfiltration	T1567			
Impact	T1565	T1485	T1499	T1498

Appendix B Terms of Reference

Term	Definition	Examples
Abuse Case	A product of consequence analysis that focuses on how systems can be abused and the consequences when a potential adversary takes an intentional hostile action against an organization's operations. An abuse case consists of three elements: Functional Use Element (FUE), Technical Abuse Element (TAE), and Functional Abuse Element (FAE) that combine to achieve a malicious outcome of effect that is intended to support an adversary's motives. NOTE: An abuse case is a single pass through the sets of FUEs, FAEs, TAEs	
Adversary	An entity whose intentions are hostile to an organization or its stakeholders	• *Hacktivist* – see relevant entry for definition • *Industrial espionage actor* – see relevant entry for definition • *Nation state actor* – see relevant entry for definition • *Organized crime actor* – see relevant entry for definition • *Script kiddie* – see relevant entry for definition • *Terrorist actor* – see relevant entry for definition • *Traditional hacker* – see relevant entry for definition
Adversary Context	A cybersecurity and risk management analysis perspective that emphasizes consideration of the actions and motives of potential adversaries when vetting and prioritizing potential risks.	
Adversary Dossier	An analytic report that presents risks, threats, or consequences of an adversary's actions and based on that adversary's capabilities, accesses, and motives	

Term	Definition	Examples
Availability	Ensuring timely and reliable access to and use of information – NIST	
Capability	The means by which harm is inflicted by an adversary using an arsenal of exploits, techniques, and tactics. An adversary's capabilities are dependent upon their levels of technical competence, funding, and resolve to act.	
CIA Triad	A common cyber security model that identifies the three essential characteristics of information to be Confidentiality, Integrity, and Availability. This model is used to support the assessment of threats and vulnerabilities and for developing security strategies. The three elements of the CIA Triad are: • *Confidentiality* – see relevant entry for definition • *Integrity* – see relevant entry for definition • *Availability* – see relevant entry for definition	
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information – NIST	
Consequence	Harmful impact to a system, its operations, its mission outcome, or its stakeholders' equities through the realization of risk. Realized risk can be the result of an adversary's actions (Abuse Case risk), unintended misuse of the system (Misuse Case risk), or by a hazard acting on the system (Hazard Case risk).	
Consequence Based Analysis	The cumulative process of generating or identifying specified conditions which produce harm to a system, operations, mission outcomes, or stakeholder equities. The product/outcome of consequence-based analysis are Abuse Cases, Misuse Cases, or Hazard Cases.	

Term	Definition	Examples
Dossier	An analytic report that organizes the results and findings as details about or related to a specific entity or subject	*Adversary dossier* – see relevant entry for definition *Others to come later* – relevant entries to be added
Denial of Service	When the process or data store is unable to service incoming requests	
Elevation of Privilege	When an adversary gains increased capability on a system or network	
Exploit/Weapon	"The means through which a vulnerability can be leveraged for malicious activity by hackers" – Rapid7	
Functional Abuse Element (FAE)	Part of the Abuse Case analysis methodology that specifically details an undesirable physical or logical capability of the system being analyzed. This is the consequence or effect that an adversary desires to accomplish in an Abuse Case.	
Functional Use Element (FUE)	Part of the Abuse Case analysis methodology that specifically details a physical or logical capability of the system being analyzed. FUEs include both the operationally intended functions of the system, and any other capabilities that extend beyond the intended use of the system.	
Hacktivist	A cyber threat adversary who utilizes illicit cyber-based techniques as a form of protest or civil disobedience to promote political or ideological goals.	
Industrial Espionage Actor	A cyber threat adversary whose primary motivation is business or industry related (e.g., theft of intellectual property, trade secrets or other sensitive/secret data; damaging business reputation; etc.)	
Information Disclosure	When the information can be read by an unauthorized party	

Term	Definition	Examples
Integrity	Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity – NIST	
Motive	The reason an adversary desires to enact a specific malicious effect on a system or organization	
Nation State Actor	A cyber threat adversary that is acting on behest of and/or with the financial and technological backing of a nation state.	
Organized Crime Actor (referred to as cybercrime syndicate here)	A cyber threat adversary working as part of or an extension of a criminal group and who's illegal cyber activities provide material support or revenue for that group	
Operational Context	A cybersecurity and risk management analysis perspective that emphasizes system operations, interactions, and the operational environment when vetting or prioritizing potential risks.	
Script Kiddie	A cyber threat adversary that lacks the programing skill to develop their own cyberattack tools and instead relies on previously developed programs, software, and tools. Script kiddie is generally a pejorative term for the lowest-tier level of hackers. However, history has shown that script kiddies have launched devastating attacks.	
Security Based Development	The process of applying security principles, profiles, and dossiers to the design, development, and deployment of a system	

Term	Definition	Examples
Risk	The possibility of a negative, consequence-based event occurring in the context of the: Asset being protected Stakeholder equities Abilities of the adversary Motives or intentions of the adversary Vulnerabilities that can be exploited Harm that can be inflicted	
Spoofing	When a person, process, file, website, network address, etc. is not what it claims to be	
Static Application Security Testing (SAST)	Assessment of source code and binaries for indications of security vulnerabilities conducted from the inside out while the software is in a nonrunning (static) state	
STRIDE Model	A Microsoft methodology of characterizing cybersecurity threats into six categories, with STRIDE being the mnemonic for remembering those categories, which are as follows: ***S****poofing* – see relevant entry for definition ***T****ampering* – see relevant entry for definition ***R****epudiation* – see relevant entry for definition ***I****nformation Disclosure* – see relevant entry for definition ***D****enial of Service* – see relevant entry for definition ***E****levation of Privilege* – see relevant entry for definition	
Technical Abuse Element (TAE)	Part of the Abuse Case analysis methodology that details some manner in which an adversary can have an effect on a system. TAEs include such things as system vulnerabilities, exploits, attack vectors, etc.	

Term	Definition	Examples
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (https://csrc.nist.gov/glossary/term/threat)	
Threat-Based Analysis	The cumulative process of generating Threat Models, Threat Findings, and a Threat Profile for a given system. The product/outcome of a Threat Based Analysis is a Threat Findings document with categorized and prioritized threats (from task overview table in the Shamrock Engagement Playbook).	
Threat Profile	The result of a systematic process including system decomposition, abuse case modeling, asset characterization, STRIDE threat modeling, and risk reduction through mitigation development. The threat profile document itself gives an overview of these activities and guides the system owners on how to proceed in risk reduction.	
Threat Findings	A list of threats found against a system, including a short description, their categorization, and project-based prioritization.	
Threat Model	A set of one or more diagrams representing system components, their connections, and possible attack points within the diagram.	
Use Case	A system analysis product that consists of assembling sequences of events and interactions between (and within) systems and their users in order to achieve particular goals (use)	
Vulnerability	The susceptibility of a system or component to intentional or unintentional sources of harm.	

Term	Definition	Examples
Vulnerability Profile	The result of a systematic process including a static source code scan which highlights vulnerabilities at a line-by-line level, an analysis of the vulnerabilities found, and risk reduction through mitigation development. The vulnerability profile document gives an overview of these activities and guides the system owners on how to proceed in risk reduction.	

Appendix C Brief on Threat-Based Analysis

The Shamrock Cyber team combines three segments of Threat-Based Analysis (TBA), as shown in Figure 2. TBA optimizes portions of Lockheed Martin's IDDIL-ATC methodology, adopts Microsoft's STRIDE model, and maps results to NIST cybersecurity standards. The analysis provides cost-effective, time-efficient results that lead to immediately actionable controls. Shamrock Cyber often requests that the customer project team write ***Usage Narratives*** be written by members of the project team. The narratives provide the Shamrock team with valuable context in simple, non-jargon terms. With this context, ***User Roles*** are established to define who uses the system and for what purpose.

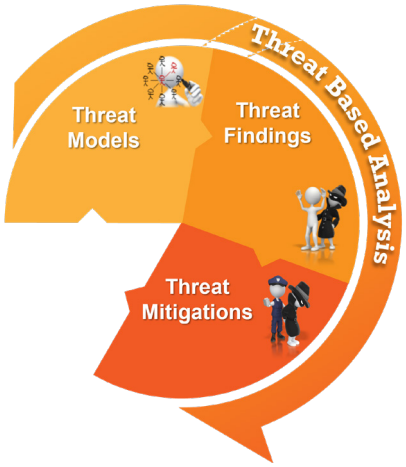

Figure 2. The TBA leaf of Shamrock Cyber.

The next step is to establish initial threat priorities based on ***Confidentiality***, ***Integrity***, and ***Availability (CIA)***. The CIA Triad (see Figure 3) is a commonly used cybersecurity model that Shamrock Cyber uses for this purpose. The idea is simply to rank C, I, and A in priority order, where each is defined as:

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity

Availability – ensuring timely and reliable access to and use of information

Figure 3. The CIA triad.

With CIA priorities established, the Shamrock Cyber team then collaborates with the project team to develop an appropriate set of system and context diagrams. The user roles, CIA priorities, and diagrams comprise the first segment of TBA, known as a ***Shamrock Cyber Threat Model***. The threat model is the foundation for executing the other segments of threat-based analysis.

Analysis begins when the Shamrock Cyber team uses the diagrams as input to Microsoft's Threat Modeling Tool (TMT). The TMT is a free download that comes with standard threat templates. The TMT reads the diagrams and uses the templates to provide initial analysis and assessment as well as STRIDE based triage results. The initial results from the TMT are then analyzed by Shamrock subject matter experts to complete the second segment: the ***Shamrock Cyber Threat Findings*** for review by the project team.

With the Threat Findings in hand, Shamrock goes back to the project team to collaboratively analyze and determine mitigations. Mitigations are then mapped to NIST cybersecurity standards. When this exercise is complete, the Shamrock Cyber team organizes the information into the third segment and final product, the ***Shamrock Cyber Threat Profile***.

Appendix D Brief on Vulnerability-Based Analysis

The Shamrock Cyber team performs Vulnerability-Based Analysis (VBA) in the areas depicted in Figure 4. While this can, should, and will be applied to any domain, Shamrock's current focus is Software Assurance, which means executing vulnerability-based analysis on software applications and systems. The three segments of VBA are:

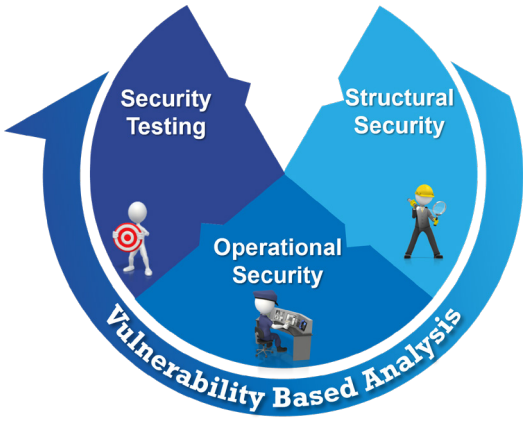

Figure 4. The VBA leaf of Shamrock Cyber.

Structural Security – the security of a system based on its construction. For software assurance, this means Static Application Security Testing (SAST) and Open-Source Analysis (OSA). Shamrock executes SAST scans with Checkmarx, a commercial off the shelf (COTS) tool used extensively at Pacific Northwest National Laboratory (PNNL). Checkmarx also provides OSA tools that Shamrock utilizes. OSA is a software-focused analysis of third-party code.

Operational Security – the security of the system's behavior while in operation. For software assurance, this means Dynamic Application Security Testing (DAST). Shamrock executes DAST scans with AppSpider, a COTS tool used at PNNL.

Security Testing – scenario-based, comprehensive security testing. One example is Penetration Testing. This is an emerging capability for Shamrock, and the team is still developing collaborations and methods.

The objective of VBA is to perform an analysis that eliminates false positives, summarizes the vulnerabilities, and makes recommendations. The result of this analysis is a ***Shamrock Cyber Vulnerability Profile***. The Vulnerability Profile provides customized guidance and allows the project team to prioritize vulnerabilities. For software assurance, this process is described in these steps:

1. ***Receive source code***
   The source code comes from the customer development team in the form of a zip file or a URL to a code repository. The source code will be used as input to the Checkmarx scanner.
2. ***Execute a Checkmarx SAST scan***
   Every file contained in the software (from the repo or the zip file) will be scanned, and the results form the foundation for Shamrock Cyber analysis.
3. ***Execute a Checkmarx OSA scan***
   Dependency libraries will be scanned by Checkmarx, and vulnerable libraries along with out-of-date libraries will be documented, forming the foundation for Shamrock analysis.
4. ***Analyze SAST scan results***
   The results of Shamrock analysis of SAST go into the final report.
5. ***Analyze OSA scan results***

The results of Shamrock analysis of OSA go into the final report.

Appendix E Brief on Consequence Based Analysis

The Shamrock Cyber team performs Consequence-Based Analysis (CBA) to assess mission risk to business operations by . Figure 5 shows the three categories of CBA, each of which is composed of three elements: a system function, a negative outcome, and a technical capability that, through the system function, enables the negative outcome. These elements, when present and combined in a system, have the potential to impart harm to some part of the system, its operation, its mission, or its stakeholders. The negative outcome is a plausible consequence of something going wrong with the system or its operation. The technical element is the link that could transform normal operations into the identified negative outcome. MITRE's ATT&CK matrix is used during analysis to provide a mapping to known adversarial behaviors. The categories of CBA are constructed as follows:

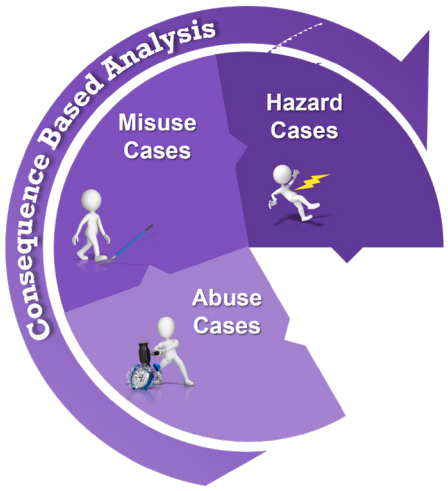

Figure 5. The CBA leaf of Shamrock Cyber.

Abuse Case – damage caused by intentional acts of an adversary

- Adversaries and their Motives (A&M) – who wants to do damage and why
- Functional Use Element (FUE) – what the system does
- Functional Abuse Element (FAE) – the harmful outcome
- Technical Abuse Element (TAE) – how the system can be "hacked" intentionally

Misuse Case – damage caused by unintentional acts and human error

- Mistakes and Misbehavior (M&M) – foreseeable user mistakes or misuse
- Functional Use Element (FUE) – what the system does
- Functional Misuse Element (FME) – the harmful outcome
- Technical Misuse Element (TME) – how the system errors when misused

Hazard Case – damage caused by non-human events in the system's operating environment

- Environmental Events (EE) – something that occurs naturally in the environment
- Functional Use Element (FUE) – what the system does
- Functional Hazard Element (FHE) – harmful outcome
- Technical Hazard Element (THE) – how the system could malfunction due to a hazard

The Shamrock Cyber team engages with customers (developers, operators, owners, and other stakeholders) to understand system operations, use cases, and missions. The team also gathers stakeholders' unacceptable mission outcomes to derive plausible scenarios that could lead to unacceptable consequences. Assessments for threats and vulnerabilities are then either gathered or performed and used to build the various "cases." Each case is directly linked to one or more technical elements that direct system security and defense personnel in the identification, design, and implementation of security controls, vulnerability remediations, and risk mitigations. MITRE's ATT&CK matrix is used

The Shamrock Cyber team engages customers as needed throughout the process. When analysis is complete, ***Shamrock Cyber Consequence Profiles*** such as ***Adversary Dossiers*** are developed to explain in simple, non-technical terms, the business risks and consequences to stakeholder equities. This allows greater stakeholder access and understanding to risk assessment and management processes.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov